# HIGHER EDUCATION EXAMINATIONS COUNCIL

**2025**

# REGULATIONS AND MODULES FOR

# NATIONAL DIPLOMA

# IN

# COMPUTER AND DIGITAL FORENSICS

**Course Code: 682/25/CO/M0**

***Implementation date: August 2025***

*HERITAGE-BASED EDUCATION 5.0*

## PREAMBLE

The programme is designed to develop a Digital Forensics Technician with knowledge, skills and attitudes to satisfy the basic needs of the Information and Communications Technology and Digital Forensics industry. The total duration of the programme is 2 200 hours spread over two (2) and one (1) on OJET. The minimum entry requirements into this programme are English Language and Mathematics passed at Ordinary level with a grade C or better and any other three Ordinary level subjects or relevant National Foundation Certificate (NFC) subjects. The programme is offered on a full-time, part-time, Block release or Open Distance Learning (ODL) basis. Assessment is through continuous assessment and written examinations. The programme will inculcate a Science, Technology and Engineering culture for sustainable industrialization and modernization.

The programme will consider gender mainstreaming, sustainable development, physical challenges, health dispositions, and the intersections between race, class, and culture. It shall embrace innovative heritage-based education and training philosophy to solve national problems and to produce goods and services for industrialization and modernization.

## CONSULTATIONS

| | INSTITUTION | YEAR |
|---|---|---|
| 1. | Econet Wireless | 2025 |
| 2. | Zimbabwe National Chamber of Commerce | 2025 |
| 3. | Scientific and Industrial Research Centre (SIRDC) | 2025 |
| 4. | Zimbabwe Republic Police (ZRP) | 2025 |
| 5. | Harare Institute of Technology | 2025 |
| 6. | Ministry of Information Communication Technology | 2025 |
| 7. | Cassava Technologies | 2025 |
| 8. | Computer Society of Zimbabwe (CSZ) | 2025 |
| 9. | TelOne Zimbabwe | 2025 |
| 10. | Liquid Telecommunications | 2025 |
| 11. | Bankers Association of Zimbabwe | 2025 |
| 12. | Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) | 2025 |

## PART I: PROGRAMME REGULATIONS

## 1.0 TITLE AND LEVEL OF AWARD

National Diploma in Computer and Digital Forensics.

## 2.0 PROGRAMME AIM

The aim of the programme is to develop a Digital Forensics Technician the theoretical knowledge, practical skills, and ethical understanding necessary to effectively investigate cybercrimes, recover digital evidence, and contribute to justice or organizational security.

## 3.0 PROGRAMME LEARNING OUTCOMES

By the end of the programme, the student should be able to:-

3.1 Contribute to an organization's success by communicating effectively and professionally in a business context

3.2 Extract and analyze digital evidence effectively and legally, regardless of the device or context by applying forensic principles to various digital devices and scenarios

3.3 Ensure a secure digital environment by proactively identifying and mitigating security risks

3.4 Minimize damage to digital assets and ensure the continuity of operations by managing and responding to security incidents.

3.5 Ensure that digital evidence is admissible in court and that the rights of all parties are protected by conducting digital forensics investigations in a legally sound and ethical manner.

3.6 Extract, analyze, and report on digital evidence from mobile devices by applying techniques and tools

3.7 Reconstruct network activities and extract digital evidence that supports forensic investigations by capturing, analyzing, and interpreting network traffic.

3.8 Extract, analyze, and interpret digital evidence from various operating systems (Windows, Linux, macOS) in a forensically sound manner.

3.9 Plan, execute, and evaluate digital forensics projects by applying research and project management principles.

3.10 Respond to malware threats across diverse digital environments by applying appropriate forensic techniques, threat intelligence, and mitigation strategies

3.11 Uncover evidence of malicious activity, system intrusions, or other relevant information by acquiring and analyzing volatile data from a computer's Random Access Memory (RAM).

3.12 Acquire, analyze, and interpret digital evidence from cloud environments while adhering to legal and ethical considerations.

3.13 Automate tasks, develop custom tools, and analyze digital evidence more effectively by applying programming tools and frameworks.

3.14 Extract, examine, and interpret digital evidence from databases by applying forensic tools in conducting forensic investigations

3.15 Install, configure, maintain, and troubleshoot computer hardware to ensure the optimal functionality, reliability, and security of computer systems

3.16 Design, implement, and manage computer networks by applying network principles, technologies, and protocols.

3.17 Demonstrate appropriate industrial experience in journalism.

3.18 Demonstrate patriotism to national issues.

3.19 Operate a sustainable business in the field of digital forensics.

## 4.0 PROGRAMME STRUCTURE

| MODULE | CODE | HOURS |
|---|---|---|
| **Year 1 Semester I** | | |
| Business Communication | 682/25M01 | 50 |
| Computer Networking | 682/25/M02 | 100 |
| Computer Organization and Architecture | 682/25/M03 | 100 |
| Legal Aspects in Digital Forensics | 682/25/M04 | 120 |
| National Studies | 401/24/M01 | 50 |
| Skills Proficiency | 682/25/M21 | |
| **Year 1 Semester II** | | |
| Computer Forensics | 682/25/M05 | 120 |
| Programming for Digital Forensics | 682/25/M06 | 150 |
| Fundamentals of Operating Systems | 682/25/M07 | 100 |
| Incident Response | 682/25/M08 | 120 |
| Entrepreneurial Skills Development | 402/25/M01 | 50 |
| Skills Proficiency | 682/25/M21 | |
| **Year 2 Semester I** | | |
| Database Security and Forensics | 682/25/M09 | 160 |
| Network Forensics | 682/25/M10 | 160 |
| Operating System Forensics | 682/25/M11 | 120 |

| | | |
|---|---|---|
| Malware Forensics | 682/25/M12 | 120 |
| Ethical Hacking | 682/25/M13 | 120 |
| Skills Proficiency | 682/25/M21 | |
| **Year 2 Semester II** | | |
| Mobile Device Forensics | 682/25/M14 | 120 |
| Cloud Forensics | 682/25/M15 | 120 |
| Memory Forensics | 682/25/M16 | 120 |
| Research Methods | 682/25/M17 | 100 |
| Emerging Technologies in Digital Forensics | 682/25/M18 | 100 |
| Skills Proficiency | 682/25/M21 | |
| **Year 3 Semester I & II** | | |
| On-the-job Education and Training | 682/25/M20 | 1 Year |
| Research Project | 682/25/M19 | |
| **Total** | | 2 200 + 1 Year |

## 5.0 DURATION

The programme duration is 2 200 hours spread over two (2) years and one (1) on OJET.

## 6.0 ENTRY REQUIREMENTS

6.1 English Language and Mathematics passed at Ordinary Level with grade C or better and any other three (3) Ordinary Level subjects or relevant National Foundation Certificate subjects.

6.2 The single module part qualification pathway is exempted from the 5 Ordinary levels requirement.

6.3 The single modular part qualifications should be taken 1 (one) module at a time by those without 5 Ordinary levels (but requisite modules should have been covered at National Certificate and National Diploma level).

## 7.0 MODE OF STUDY

Full time: 2 200 hours

Part time: 2 200 hours

Block Release: 2 200 hours

ODeL: 2 200 hours

## 8.0 ASSESSMENT SCHEME

| MODULE TITLE AND CODE | WRITTEN EXAMINATION 40% | CONTINUOUS ASSESSMENT 60% | WEIGHTING |
|---|---|---|---|
| Business Communication 682/25/M01 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Computer Networking 682/25/M02 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Computer Organization and Architecture 682/25/M03 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Legal Aspects in Digital Forensics 682/25/M04 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| National Studies 401/24/M01 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Computer Forensics 682/25/M05 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Programming for Digital Forensics 682/25/M06 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |

| | | | |
|---|---|---|---|
| Fundamentals of Operating Systems 682/25/M07 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Incident Response 682/25/M08 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Entrepreneurial Skills Development 402/25/M01 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Database Security and Forensics 682/25/M09 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Network Forensics 682/25/M10 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Operating System Forensics 682/25/M11 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Malware Forensics 682/25/M12 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Ethical Hacking 682/25/M13 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Mobile Device Forensics | 3-hour written examination | A minimum of<br>• 2 Theory Assignments | 100% |

| | | | |
|---|---|---|---|
| 682/25/M14 | | 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | |
| Cloud Forensics 682/25/M15 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Memory Forensics 682/25/M16 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Research Methods 682/25/M17 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Emerging Technologies in Digital Forensics 682/25/M18 | 3-hour written examination | A minimum of<br>• 2 Theory Assignments 20%<br>• 2 Practical assignments 20%<br>• 2 Tests 20% | 100% |
| Skills Proficiency 682/25/M21 | | Submit Marks | 100% |
| Research Project 682/25/M19 | As per Project Guidelines | Submit Project Report | 100% |
| On-the-job Education and Training 682/25/M20 | Submit Log book | As per log Book | 100% |

## 9.0 CONDITIONS OF GRADING

| | | |
|---|---|---|
| 0% to 49% | - | Fail |
| 50% to 59% | - | Pass |
| 60% to 79% | - | Credit |
| 80% and above | - | Distinction |

## 10.0 CONDITIONS OF AWARD

10.1 A candidate should attend at least 100% of learning sessions to qualify for examinations. An approved absent shall be considered as present.

10.2 Approved absenteeism shall not exceed 15% of the learning sessions.

10.3 The final mark should be obtained through aggregation, provided the candidate scores at least 50 % in each of the continuous assessment and examinations.

10.4 The pass mark shall be 50%.

10.5 A candidate should pass all modules to be awarded a National Diploma in Computer and Digital Forensics.

10.6 Non-submission of coursework marks will result in the candidate being deferred.

10.7 Single module candidates will be awarded part certificates in passed single modules.

## 11.0 RE-WRITES

11.1 Re-write(s) should conform to the current programme structure.

11.2 Any candidate who fails to pass at least two-thirds of the semester should rewrite the failed modules before proceeding to the next semester.

11.3 A candidate shall not be allowed to register for a module before passing the prerequisite for that module

11.4 A candidate is given no time limit in which to rewrite the failed module (s).

11.5 There is no aggregation for rewrites.

11.6 All re-writes should pass on performance in the examination.

11.7 If a candidate fails coursework, he/she repeats the module.

## 12.0 EXEMPTIONS

12.1 Exemptions are only granted in modules already attained from a complete accredited qualification, provided an exemption certificate specifying exempted modules is produced.

12.2 Transfer of credits is only granted in modules passed from accredited programmes.

12.3 Exemption or Transfer of credits certificate should be applied for at the enrolment stage and produced before registration of examinations

## 13.0 IRREGULAR PRACTICES

13.1 Cheating in examinations will result in disqualification from the affected modules. The candidate will be suspended for one (1) year from the programme and all HEXCO programmes. After the suspension period, the candidate will rewrite the affected modules only.

13.2 Plagiarism with a similarity index of more than 15% in any of the assessments will result in automatic disqualification from the module.

## 14.0 RESOURCES

### 14.1 Lecturers Qualifications

#### 14.1 Lecturers Qualification

The minimum qualification for a lecturer is a Higher National Diploma in Computer and Digital Forensics or equivalent.

#### 14.2 Laboratory Technicians

Minimum National Diploma in Computer and Digital Forensics or equivalent.

#### 14.3 Infrastructure and Equipment

**Facilities**

1. **Dedicated Digital Forensics Lab(s):**
    - Secure Environment: Physically isolated from general campus networks, with restricted access (keycard, biometric), surveillance, and secure storage for evidence and sensitive equipment.
    - Workstations: Sufficient number of high-performance workstations for each student (or pair), configured for forensic analysis.
    - Network Isolation: Ability to create isolated network segments (VLANs) for network forensics exercises and safe malware analysis environments (sandboxes).
    - Power & Cooling: Robust power infrastructure with uninterruptible power supplies (UPS) and adequate cooling to support high-performance computing and prolonged lab sessions.
    - Lighting & Ergonomics: Good lighting, ergonomic chairs, and spacious desks to support long periods of analytical work.
    - Whiteboards/Smart Boards: For collaborative problem-solving and instruction.
2. **Server Room/Data Center:**
    - Virtualization Servers: Powerful servers to host multiple virtual machines (VMs) for student labs, operating system simulations, malware analysis sandboxes, and cloud environment simulations.
    - Centralized Storage: High-capacity, high-speed storage (NAS/SAN) for storing forensic images, analysis results, and large datasets for student exercises.

- Backup Infrastructure: Secure and reliable backup solutions for all lab data and configurations.

3. **Lecture Theatres/Classrooms:**
    - Equipped with projectors or large interactive displays, sound systems, and instructor workstations for theoretical lectures and demonstrations.
    - Reliable internet connectivity for accessing online resources and cloud platforms.

**Tools (Software)**

1. **Operating Systems:**
    - Host OS for Workstations: Windows 10/11 (Professional/Enterprise), Linux distributions (e.g., Ubuntu, Fedora, or specialized forensic distros like Kali Linux, SIFT Workstation).
    - Virtual Machine OSes: A wide variety of operating systems for forensic targets (e.g., Windows XP, 7, 10, 11, various Windows Server versions, multiple Linux distributions, macOS - where licensing permits, Android OS images, iOS simulators).
2. **Core Digital Forensics Suites (Commercial - essential for industry relevance):**
    - EnCase Forensic: Comprehensive suite for acquisition, analysis, and reporting.
    - AccessData FTK (Forensic Toolkit): Another leading all-in-one solution.
    - Magnet AXIOM: Excellent for computer, cloud, and mobile forensics.
    - X-Ways Forensics: Known for its speed and efficiency.
3. **Open Source / Freeware Forensic Tools (for practical understanding and cost-effectiveness):**
    - Autopsy (The Sleuth Kit GUI): Powerful open-source forensic platform.
    - Volatility Framework: For memory forensics.
    - Wireshark: Network protocol analyzer.
    - tcpdump: Command-line packet analyzer.
    - HashCalc / HashMyFiles: Hashing utilities.
    - ExifTool: Metadata analyzer.
    - Bulk Extractor: For extracting email addresses, credit card numbers, etc.
    - HxD / WinHex (or equivalent): Hex editors.
4. **Specialized Forensic Tools:**
    - Mobile Forensics:
        - Commercial: Cellebrite UFED, Oxygen Forensic Detective.

        - Open-source/CLI: ADB (Android Debug Bridge), iTunes backup analysis tools, various mobile-specific scripts.
    - Network Forensics: Zeek (Bro IDS), NetworkMiner, Snort/Suricata (IDS/IPS).
    - Malware Analysis:
        - Static: IDA Pro (or Ghidra - open source), PE-Studio, strings, objdump.
        - Dynamic: Cuckoo Sandbox, Any.Run (online), Procmon, Regshot.
    - Cloud Forensics: Cloud provider-specific CLI tools (AWS CLI, Azure CLI, gcloud CLI), cloud logging/monitoring dashboards, tools for cloud storage acquisition.
    - Blockchain Analysis: Blockchain explorers (web-based), open-source blockchain analysis tools (e.g., GraphSense, custom Python scripts for API interaction).
    - IoT Forensics: Device-specific forensic utilities, firmware analysis tools.
5. **Virtualization Software:**
    - Hypervisors: VMware ESXi (for servers), VMware Workstation Pro, Oracle VirtualBox, Microsoft Hyper-V (for individual workstations/servers).
6. **Programming & Scripting Environments:**
    - Python: Essential for automation, data analysis, and custom tool development.
    - IDEs: VS Code, PyCharm, Jupyter Notebooks.
    - Scripting Languages: PowerShell (Windows), Bash (Linux).
7. **Reporting & Documentation Tools:**
    - Microsoft Office Suite (Word, Excel, PowerPoint) or LibreOffice.
    - Mind mapping tools (e.g., XMind, FreeMind).
    - Diagramming tools (e.g., draw.io, Visio).

**Equipment (Hardware)**

1. **Forensic Workstations (for students and instructors):**
    - High-Performance: Multi-core CPUs (Intel i7/i9 or AMD Ryzen 7/9 equivalent or higher).
    - Ample RAM: Minimum 32GB (64GB or more recommended) for handling large forensic images and running multiple VMs.
    - Fast Storage: Large SSDs (1TB+ NVMe preferred) for the OS and working space, plus additional HDDs for storing forensic images.
    - Dedicated GPU: NVIDIA CUDA-enabled GPUs are highly beneficial for AI/ML tasks and some forensic tools.
    - Multiple Monitors: At least two monitors per workstation for efficient analysis.
    - USB 3.0/3.1/C Ports: For connecting external drives and forensic devices.

2. **Forensic Hardware Tools:**
    - Hardware Write Blockers: For various interfaces (SATA, IDE, USB, SAS, NVMe) to ensure data integrity during acquisition. Examples: Tableau Forensic Imager (TD3/TD4), Logicube Forensic Falcon.
    - Forensic Duplicators: Standalone devices for fast and forensically sound disk-to-disk or disk-to-file imaging.
    - Drive Bays/Adapters: Universal adapters for connecting various types of hard drives and SSDs (2.5", 3.5", M.2, U.2).
    - Disk Docks/Enclosures: For quick connection of drives.
3. **Network Hardware:**
    - Managed Network Switches: Capable of VLANs, port mirroring (SPAN ports) for network traffic capture.
    - Routers/Firewalls: For setting up isolated lab networks and demonstrating network security concepts.
    - Network Taps: Hardware devices for non-intrusive network traffic interception.
    - Wireless Access Points: For wireless network forensics exercises (including WEP/WPA cracking).
4. **Mobile Device Forensic Hardware:**
    - Mobile Forensic Devices: Commercial tools often come with their own hardware (e.g., Cellebrite UFED Touch/4PC).
    - Variety of Mobile Devices: A collection of older and newer smartphones and tablets (iOS, Android) for hands-on acquisition and analysis practice. These should be "burner" devices not used for sensitive data.
    - Specialized Cables & Adapters: For various mobile device models.
    - JTAG/Chip-off Tools (for advanced modules): Specialized equipment for retrieving data directly from chips, requiring careful handling and expertise.
5. **Storage:**
    - External Hard Drives/SSDs: High-capacity, portable drives for temporary evidence storage and transfer.
    - USB Flash Drives: For bootable forensic tools and small data transfers.
6. **Miscellaneous Lab Equipment:**
    - Toolkits: Screwdrivers, anti-static wrist straps, anti-static mats, pliers, tweezers for disassembling computers and devices.
    - Digital Multimeters: For basic electrical troubleshooting.
    - Labels, Evidence Bags, Tags: For proper evidence handling and chain of custody.

- Camera: For documenting forensic scenes and evidence.

## 14.4 SUGGESTED REFERENCE BOOKS


Adair, J (2003), Effective Communication. London: Pan Macmillan Ltd.

Ajmani, J. C. (2012), Good English: Getting it Right. New Delhi: Rupa Publications.

Amos, Julie-Ann. Handling Tough Job Interviews. Mumbai: Jaico Publishing, (2004).

Bonet, Diana. The Business of Listening: Third Edition. New Delhi: Viva Books, (2004).

Bovee, Courtland L, John V. Thill & Barbara E. Schatzman.(2010). Business Communication Today: Tenth Edition. New Jersey: Prentice Hall.

Collins, Patrick. (2009) Speak with Power and Confidence. New York: Sterling,

Guffey, Mary Ellen. (2000). Essentials of Business Writing. Ohio: South- Western College Pubg.

American Heritage Dictionary of the English Language, Fifth Edition (2011), Houghton Mifflin.

Astrow, A., 1983. Zimbabwe: A Revolution That Lost Its. *Way*, pp.1980-1986.

Banana, C. ed., 1989. *Turmoil and tenacity: Zimbabwe 1890-1990*. College Press.

Batchelor, P., Kingma, K. and Lamb, G. eds., 2004. *Demilitarisation and Peace-building in Southern Africa: Concepts and processes* (Vol. 1). Gower Publishing, Ltd.

Birmingham, D. and Martin, P. eds., 1983. *History of Central Africa* (Vol. 2). Addison-Wesley Longman Limited.

Centre for Peace Initiatives in Africa, 2005. *Zimbabwe: The Next 25 Years*. Benaby Printing and Publishing.

Change African Indigenous Knowledge and Disciplines

Chirimuuta, C., Gudhlanga, E. and Bhukuvhani, C., 2012. Indigenous knowledge systems: a panacea in education for development?

Chitiyo, T.K., 2000. Land violence and compensation: reconceptualising Zimbabwe's land and war veterans' debate. *Track Two: Constructive Approaches to Community and Political Conflict*, *9*(1).

Chitsike, F., 2003, December. A critical analysis of the land reform programme in Zimbabwe. In *2nd FIG Regional Conference* (pp. 2-5).

Collins English Dictionary – Complete and Unabridged, 12th Edition (2014) HarperCollins.

De Villiers, B., 2003. Land reform: issues and challenges: a comparative overview of experiences in Zimbabwe. *Namibia, South Africa and Australia, Johannesburg: Konrad Adenauer Publications*.

Emeagwali and Dei, G, J.S (Eds) (2014), Anti-Colonial Educational Perspectives for Transformative

Government of Zimbabwe, 2013. The Constitution of the Republic of Zimbabwe Amendment (No.20).

Hammar, A., Jensen, S. and Raftopoulos, B. eds., 2003. *Zimbabwe's unfinished business: Rethinking land, state and nation in the context of crisis*. Weaver Press.

Hayes, D., 1980. *Human Rights*, Sussex, Wayland Publishers.

Kriger, N., 1995. The politics of creating national heroes: The search for political legitimacy and national identity. *Soldiers in Zimbabwe's liberation war*, *1*, pp.139-162.

Lalonde, A., 1991. African indigenous knowledge and its relevance to environment and development activities. *Canadian International Development Agency*.

Madhuku, L. 2004. Law, Politics and the Land Reform Process. In Masiyiwa, S. 2004. Post-Independence Land Reform in Zimbabwe: Controversies and Impact on the Economy.

Mkabela, Q., 2005. Using the Afrocentric method in researching indigenous African culture. *The qualitative report*, *10*(1), pp.178-190.

Mlambo, A.S., 2014. *A history of Zimbabwe*. Cambridge University Press.

Moyo, S., 2004. *Overall impacts of the fast track land reform programme*. African Institute for Agrarian Studies.

Moyo, S., 2006. The evolution of Zimbabwe's land acquisition. University of Zimbabwe (UZ) Publications/Michigan State University (MSU).

Ogunbanjo, M.B., Human Rights in Africa in the new Global Order: A Dilemma?

Raftopoulos, B. and Mlambo, A. eds., 2009. *Becoming Zimbabwe. A History from the Pre-colonial Period to 2008: A History from the Pre-colonial Period to 2008*. African Books Collective.

Ranger, T., 1985. Peasant Consciousness and Guerrilla Warfare in Zimbabwe: A Comparative Study. *Harare: McMillan*.

Ranger, T.O. ed., 1968. *Aspects of Central African History*. Northwestern University Press.

Richardson, C., 2004. *The collapse of Zimbabwe in the wake of the 2000-2003 land reforms*.

Schmidt, E.S., 1992. Peasants, traders and wives: Shona women in the history of Zimbabwe, 1870-1939.

Shaw, W.H., 2003. 'They Stole Our Land': debating the expropriation of white farms in Zimbabwe. *The Journal of Modern African Studies*, *41*(1), pp.75-89.

Shamuyarira, N.M., 1966. Crisis in Rhodesia.

Warren, D.M., 1989. Linking scientific and indigenous agricultural systems.

Zikhali, P., 2008. *Fast track land reform, tenure security, and investments in Zimbabwe* (No. dp-08-23-efd).

Holt, T.J., Bossler, A.M., and Seigfried-Spellar, K.C. (2022). *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. New York: Routledge.

Luttgens, J.T., Pepe, M., and Mandia, K. (2020). *Incident Response & Computer Forensics*. 3rd ed. New York: McGraw-Hill Education.

Sammons, J. (2021). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 3rd ed. Waltham, MA: Syngress.

Kävrestad, J. (2020). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. 2nd ed. Cham, Switzerland: Springer.

Reith, M., Carr, C., and Gunsch, G. (2022). *Digital Forensics and Incident Response:*

*A Practical Guide to Investigating and Responding to Cyber Attacks*. Birmingham, UK: Packt Publishing.

Casey, E. (2021). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 4th ed. Waltham, MA: Academic Press.

Maras, M.H. (2022). *Computer Forensics: Cybercriminals, Laws, and Evidence*. 3rd ed. Burlington, MA: Jones & Bartlett Learning.

Quick, D. and Choo, K.K.R. (2021). *Digital Forensic Investigation of Internet of Things (IoT) Devices*. 1st ed. Cham, Switzerland: Springer.

Engebretson, P. (2021). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* 3rd ed. Syngress.

Kim, P. and Solomon, M.G. (2020). *Fundamentals of Information Systems Security*. 4th ed. Jones & Bartlett Learning.

Oriyano, S.P. (2020). *Hacker Techniques, Tools, and Incident Handling.* 3rd ed. Jones & Bartlett Learning.

Gregg, M. (2021). *Certified Ethical Hacker (CEH) Version 11 Cert Guide.* Pearson IT Certification.

Weidman, G. (2020). *Penetration Testing: A Hands-On Introduction to Hacking*. 2nd ed. No Starch Press.

Stallings, W. and Brown, L. (2021). *Computer Security: Principles and Practice*. 4th ed. Pearson.

McClure, S., Scambray, J., and Kurtz, G. (2020). *Hacking Exposed 7: Network Security Secrets and Solutions.* 7th ed. McGraw-Hill Education.

Cole, E. (2021). *Advanced Penetration Testing: Hacking the World's Most Secure Networks.* 2nd ed. Wiley.

Hadnagy, C. (2021*). Social Engineering: The Science of Human Hacking.* 2nd ed. Wiley.

Ozkaya, E. (2020). *Cybersecurity: The Beginner's Guide*. Packt Publishing

Luttgens, J.T., Pepe, M., and Mandia, K. (2020). Incident Response & Computer Forensics. 3rd ed. New York: McGraw-Hill Education.

Sammons, J. (2021). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 3rd ed. Waltham, MA: Syngress.

Kävrestad, J. (2020). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. 2nd ed. Cham, Switzerland: Springer.

Reith, M., Carr, C., and Gunsch, G. (2022). Digital Forensics and Incident Response: A Practical Guide to Investigating and Responding to Cyber Attacks. Birmingham, UK: Packt Publishing.

Carrier, B. (2005) File system forensic analysis. Boston, MA: Addison-Wesley Professional.

Casey, E. (2011) Digital evidence and computer crime: forensic science, computers, and the internet. 3rd edn. Waltham, MA: Academic Press.

Luttgens, J.T., Pepe, M. and Mandia, K. (2014) Incident response & computer forensics. 3rd edn. New York, NY: McGraw-Hill Education.

Sammons, J. (2015) The basics of digital forensics: the primer for getting started in digital forensics. 2nd edn. Waltham, MA: Syngress.

Solomon, M.G., Rudolph, K., Tittel, E., Broom, N. and Barrett, D. (2011) Computer forensics jumpstart. 2nd edn. Indianapolis, IN: Wiley.

Stallings W. (2018), Operating Systems: Internals and Design Principles, 8th Ed, Pearson

Silberschatz A, et al (2021), Operating System Concepts, 10th Ed, Wiley

Tomsho G. (2020), Guide to Operating Systems, 5th Ed., Cengage

Arpaci-Dusseau, R. H. & Arpaci-Dusseau, A. C. (2018), Operating Systems: Three Easy Pieces, Arpaci-Dusseau Books

Anderson, T. & Dahlin, M. (2014), Operating Systems: Principles and Practice, 2nd Ed, Recursive Book

Tanenbaum A. S. (2015), Modern Operating Systems, 4th Ed, Pearson

Andrews J. et al (2019), CompTIA A+ Core 2 Exam: Guide to Operating Systems and Security, 10th Ed., Cengage

McHoes M. A. & Flynn M. I. (2017), Understanding Operating Systems, 8th Ed., Cengage

Corswell R. et al. (2015), Guide to Parallel Operating Systems with Windows and Linux, 3rd Ed., Cengage

Rogers, M.K. and Seigfried-Spellar, K.C. (2023). Mobile Forensics: Advanced Investigative Strategies. 1st ed. Boca Raton, FL: CRC Press.

Maras, M.H. (2022). Computer Forensics: Cybercriminals, Laws, and Evidence. 3rd ed. Burlington, MA: Jones & Bartlett Learning.

Quick, D. and Choo, K.K.R. (2021). Digital Forensic Investigation of Internet of Things (IoT) Devices. 1st ed. Cham, Switzerland: Springer.

Nelson, B., Phillips, A., and Steuart, C. (2020). Guide to Computer Forensics and Investigations. 6th ed. Cengage Learning.

Easttom, C. (2021). Computer Security Fundamentals. 4th ed. Pearson IT Certification.

Kruse, W.G. and Heiser, J.G. (2021). Computer Forensics: Incident Response Essentials. 2nd ed. Addison-Wesley Professional.

Bejtlich, R. (2020). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.

Chapple, M., Seidl, D., and Stewart, J.M. (2021). CISSP Official (ISC)2 Practice Tests. 3rd ed. Sybex.

Gregg, M. (2021). Certified Ethical Hacker (CEH) Version 11 Cert Guide. Pearson IT Certification.

Sikorski, M. and Honig, A. (2020). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2nd ed. No Starch Press.

Kruse, W.G. and Heiser, J.G. (2021). Computer Forensics: Incident Response Essentials. 2nd ed. Addison-Wesley Professional.

Bejtlich, R. (2020). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.
Gregg, M. (2021). Certified Ethical Hacker (CEH) Version 11 Cert Guide. Pearson IT Certification.

Sikorski, M. and Honig, A. (2020). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2nd ed. No Starch Press.

Ligh, M.H., Case, A., Levy, J. and Walters, A., 2021. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. 2nd ed. Indianapolis: Wiley.

Eagle, C., 2020. IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler. 3rd ed. San Francisco: No Starch Press.

Skoudis, E. and Liston, T., 2023. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 3rd ed. Upper Saddle River: Prentice Hall.

Altheide, C. and Carvey, H., 2022. Digital Forensics with Open-Source Tools. 2nd ed. Waltham: Syngress.

Engebretson, P., 2023. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. 4th ed. Waltham: Syngress.

Willems, C., 2021. Malware Analysis Using Cuckoo Sandbox: A Practical Guide to Automated Malware Analysis. 1st ed. Birmingham: Packt Publishing.

Messier, R., 2022. Threat Hunting: A Practical Guide to Detecting and Responding to Cyber Threats. 1st ed. New York: Apress.

Paar, C. and Pelzl, J., 2021. Understanding Cryptography: A Textbook for Students and Practitioners. 2nd ed. Berlin: Springer.

Ligh, M.H., Case, A., Levy, J. and Walters, A. (2014) The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis, IN: Wiley.

Carvey, H. (2014) Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8. 4th edn. Waltham, MA: Syngress.

Altheide, C. and Carvey, H. (2011) Digital Forensics with Open Source Tools. Waltham, MA: Syngress.

Russinovich, M.E., Solomon, D.A. and Ionescu, A. (2012) Windows Internals. 6th edn. Redmond, WA: Microsoft Press.

Carrier, B. (2005) File System Forensic Analysis. Boston, MA: Addison-Wesley Professional

Amazon Web Services (AWS), 2020. *AWS CloudTrail User Guide*. [online] Available at: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/ [Accessed 17 February 2025].

Cloud Security Alliance, 2019. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. [online] Available at: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ [Accessed 17 February 2025].

European Union, 2016. *General Data Protection Regulation (GDPR)*. [online] Available at: https://gdpr.eu/ [Accessed 17 February 2025].

ISO/IEC, 2013. *ISO/IEC 27001:2013 - Information Security Management Systems*. [online] Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 17 February 2025].

National Institute of Standards and Technology (NIST), 2020. *NIST Cybersecurity Framework*. [online] Available at: https://www.nist.gov/cybersecurity-framework [Accessed 17 February 2025].

Zscaler, 2021. *Zero Trust Architecture: A Secure and Modern Approach to Protecting Applications and Data*. [online] Available at: https://www.zscaler.com/zero-trust [Accessed 17 February 2025].

Deitel, P., Deitel, H. and Santry, M., 2016. *C++ how to program*. 10th ed. Upper Saddle River, NJ: Pearson.

Nystrom, R., 2014. *Game programming patterns*. San Francisco, CA: Genever Benning.

Sebesta, R.W., 2019. *Programming languages: principles and practice*. 9th ed. Boston: Pearson.

Lutz, M., 2013. *Learning Python*. 5th ed. Sebastopol, CA: O'Reilly Media.

McKinney, W., 2018. *Python for data analysis*. 2nd ed. Sebastopol, CA: O'Reilly Media.

Sedgewick, R. and Wayne, K., 2011. *Algorithms*. 4th ed. Boston: Addison-Wesley.

Johnson, R., 2017. *Effective Java*. 3rd ed. Boston: Addison-Wesley.

Knuth, D.E., 1997. *The art of computer programming, volume 1: Fundamental algorithms*. 3rd ed. Boston: Addison-Wesley.

Zeldman, J., 2015. *Designing with web standards*. 3rd ed. Berkeley, CA: New Riders.

Elliott, A. and Jackson, M., 2020. *Learning JavaScript: The programming language of the web*. 4th ed. Chicago: Apress.

Manuele, F.A., 2013. *On the practice of safety*. 4th ed. John Wiley & Sons, Inc.

Kennesaw, K., 2019. Database security: A comprehensive guide to securing database systems. 2nd ed. San Francisco: Morgan Kaufmann.

Sharma, A. and Rani, R., 2015. Database Security: Concepts, Approaches, and Challenges. 3rd ed. Boca Raton: CRC Press.

Almeshekah, M. and Alsubhi, K., 2017. Forensic investigation of database systems. Journal of Digital Forensics, Security and Law, 12(3), pp. 32-45.

McClure, S., Scambray, J. and Kurtz, G., 2009. Hacking exposed: network security secrets & solutions. 6th ed. New York: McGraw-Hill.

Garfinkel, S., 2014. Digital forensics for legal professionals: Understanding digital evidence from the crime scene to the courtroom. Waltham, MA: Morgan Kaufmann.

Pfleeger, C.P. and Pfleeger, S.L., 2012. Security in computing. 5th ed. Upper Saddle River, NJ: Pearson.

Bertino, E., Sandhu, R. and Gavrila, S., 2004. Database security: concepts, approaches, and challenges. Boston: Addison-Wesley.

Vacca, J.R., 2013. Computer and information security handbook. 3rd ed. Burlington: Elsevier.

Elmasri, R. and Navathe, S.B., 2016. Fundamentals of database systems. 7th ed. Boston: Addison-Wesley.

Hernandez, M., 2016. Database management systems. 4th ed. New York: McGraw-Hill Education.

Eddins, A., 2016. SQL Server 2016 Security Cookbook. Birmingham: Packt Publishing.

Spafford, E.H., 2014. Database management and security: challenges and solutions. International Journal of Computer Applications, 91(5), pp. 11-21.

Kennesaw, K., 2015. Database Forensics: The Need for Security in Database Systems. Journal of Digital Forensics and Cybersecurity, 8(1), pp. 12-23.

Stallings, W. (2009). Computer Organisation and Architecture: Designing for Performance.

Prentice Hall. Null, L., & Lobur, J. (2006). The Essentials of Computer Organization and Architecture. Jones & Barlett Learning. Godse, A.P., & Godse D.A. (2008). Digital Electronics. Pune: Technical

Publications Online links

Beales R.P (2013), PC Systems Installations and Maintenance, Taylor and Francis

Gilster R, (2002), PC Technician Black Book, Paraglyph Inc Press

Henessy J.L and Patterson D.A, (2011), Computer Architecture, a Quantitative Approach, Oxford University Press

Parhami B, (2005), Computer architecture: From Microprocessors to Supercomputers, Oxford Univesity Press

Stallings, W, (2010), Computer Organisation and Architecture, Prentice Hall

Fielding. M, (2014) Effective Communication in Organizations, Juta and Company, South Africa

Forouzan, BA. (2012). Data Communications and Networking. 5th Ed London: McGraw-Hill

Kurose, JF and Ross, KW. (2017). Computer Networking A Top-Down Approach. 7th Ed. New York: Pearson.

Mir, NF. (2014). Computer and Communication Networks 2nd Ed. Prentice Hall, New York.

Peterson, L. L. and Davie, B. S. (2010). Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking). 5th Ed. Amsterdam: Elsevier.

Sharma, S. (2017). Fundamentals of Data Communication and Networks. Kataria & Sons, New Delhi

Stalling, W. (2013). Data and Computer Communication. 10th Ed. New Jersey: Pearson.

White, C. (2015). Data Communications and Computer Networks: A Business User's Approach. 8th Ed. Boston: Cengage Learning

Patterson, D.A. and Hennessy, J.L. (2018) Computer Organization and Design RISC-V Edition: The Hardware/Software Interface. 2nd edn. Morgan Kaufmann.

Stallings, W. (2020) Computer Organization and Architecture: Designing for Performance. 11th edn. Pearson.

Hamacher, V.C., Vranesic, Z.G. and Zaky, S.G. (2011) Computer Organization. 6th edn. McGraw-Hill Education.

Tanenbaum, A.S. and Austin, T. (2012) Structured Computer Organization. 6th edn. Pearson.

Stallings, W. (2020) Computer Organization and Architecture: Designing for Performance. 11th edn. Pearson.

Online resources such as NPTEL lectures, MIT OpenCourseware, and relevant academic journals.

Carrier, B. (2005). *File System Forensic Analysis*. Boston: Addison-Wesley.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Burlington: Academic Press.

Martini, B. and Choo, K.K.R. (2014). Cloud Storage Forensics. Oxford: Syngress.

Sammons, J. (2020). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 3rd ed. Burlington: Syngress.

Weidman, G. (2020). Penetration Testing: A Hands-On Introduction to Hacking. 2nd ed. San Francisco: No Starch Press.

Ozkaya, E. (2020). Cybersecurity: The Beginner's Guide. Birmingham: Packt Publishing.

Hadnagy, C. (2021). Social Engineering: The Science of Human Hacking. 2nd ed. Hoboken: Wiley.

Cloud Security Alliance. (2013). *Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing*. [online] Available at: https://cloudsecurityalliance.org [Accessed 28 Jul. 2025].

National Institute of Standards and Technology (NIST). (2006). *Guide to Integrating Forensic Techniques into Incident Response*. Special Publication 800-86. Gaithersburg: NIST.

Quick, D., Martini, B. and Choo, K.K.R. (2014). *Cloud Storage Forensics*. Oxford: Elsevier.

Conlan, K., Baggili, I. and Breitinger, F. (2016). *Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation*, 18, pp.66–75.

UNODC. (2013). *Comprehensive Study on Cybercrime*. [online] Available at: https://www.unodc.org [Accessed 28 Jul. 2025].

**PART II: MODULES**

| | |
|---|---|
| **Module code:** | **682/25/M01** |
| **Module title:** | **BUSINESS COMMUNICATION** |
| **ZNQF level:** | **5** |
| **Credits:** | 5 |
| **Duration:** | 50 hours |
| **Relationship with qualification standards:** | Based on Unit Standard **Business Communication** of Unit Standards for a Digital Forensics Technician. |
| **Pre-requisite modules:** | None |
| **Purpose of module:** | This module describes the skills, knowledge and attitudes required by an **individual** to be able to effectively communicate in business. This includes applying language and writing skills in business**,** writing business documents, using appropriate communication skills to satisfy business needs, applying effective communication techniques and preparing different types of business meetings.<br>This module is important as it ensures proper and effective communication skills for business. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of learning outcomes:** | **LO1: Compose clear, professional, and context-appropriate written communications by applying language and writing skills in business**<br>**LO2: Produce business documents that meet organizational standards and effectively convey key business information**<br>**LO3: Satisfy business needs by selecting suitable channels, styles, and strategies for diverse scenarios by utilizing communication skills**<br>**LO4: Enhance collaboration, resolve conflicts, and foster stakeholder engagement by applying effective communication techniques in business**<br>**LO5: Prepare different types of meetings by planning agendas, coordinating logistics, and documenting proceedings in accordance with professional conventions** |

| | |
|---|---|
| **Learning outcome 01** | **Compose clear, professional, and context-appropriate written communications by applying language and writing skills in business** |
| **Assessment criteria:** | **1.1 Select the correct language style**<br>**1.2 Use business jargon in appropriate situations.**<br>**1.3 Organize written material logically**<br>**1.4 Select and use the most effective method of communication in a business context.**<br>**1.5 Use telephone effectively** |

| | |
|---|---|
| **Content:** | **1.1 Select the correct language style**<br>● Describe the 'seven (7) Cs of written communication<br>● Describe use of languages<br>**1.2 Use business jargon in appropriate situations**<br>● Identify and avoid barriers to communication<br>● Discuss the selection of words<br>**1.3 Organize written material logically**<br>● Explain the process of making notes<br>● Describe the presentation of business documents<br>**1.4 Select and use the most effective method of communication in a business context**.<br>● Various methods of communication<br>● Select and use the most effective method<br>● Identify major communication channels<br>**1.5 Use the telephone effectively**<br>● Telephone etiquette<br>● Making calls<br>● Answering calls |
| **Assessment tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to select the correct language style, use business jargon in appropriate situations, organize written material logically, select and use the most effective method of communication in a business context and use telephone effectively as outlined in the assessment criteria.<br>2. Practical assessment on the requirements and principles of basic communication |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below: -<br>- Visitors chairs<br>- Secretary chair and desk<br>- Computer<br>- Printer<br>- Photocopier<br>- Stationary and petty cash vouchers |

| Learning outcome 02 | **Produce business documents that meet organizational standards and effectively convey key business information** |
|---|---|
| **Assessment criteria** | **2.1 Produce business letters**<br>**2.2 Generate reports**<br>**2.3 Write a memorandum using the fully-blocked method**<br>**2.4 Write a notice for the company notice board** |
| **Content** | **2.1 Produce business letters**<br>● Explain the different types of letters<br>● Use the 'pea kiss' letter-writing plan<br>**2.2 Generate reports**<br>● Identify types of business reports<br>● Write reports from their own investigation or observation<br>● Explain the functions of reports in organisations.<br>**2.3 Write a memorandum using the fully-blocked method**<br>● Identify the major components of a memo<br>● Uses of notice and memo.<br>● Differentiate between a notice and a memo.<br>**2.4 Write a notice for the company notice board**<br>● The uses of notice<br>● Differentiate between a notice and a memo.<br>● Identify the major components of a notice |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to produce business letters, generate reports, write a memorandum using the fully-blocked method and write a notice for the company notice board as outlined in the assessment criteria.<br>2. Practical assessment on the requirements and principles of basic communication |
| **Conditions/context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution. |

| | |
|---|---|
| | 3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>- Visitors chairs<br>- Secretary chair and desk<br>- Computer<br>- Printer<br>- Photocopier<br>- Stationary and petty cash vouchers |

| **Learning outcome 03** | **Satisfy business needs by selecting suitable channels, styles, and strategies for diverse scenarios by utilizing communication skills to satisfy business needs** |
|---|---|
| **Assessment criteria** | **3.1 Define oral communication**<br>**3.2 Answer questions during a job interview**<br>**3.3 Communicate information correctly in structured language**<br>**3.4 Use written communication effectively** |
| **Content** | **3.1 Define oral communication**<br>● Listening skills<br>● Speaking skills<br>● Use of par-linguistics<br>**3.2 Answer questions during a job interview**<br>● Audibility in speech<br>● Confidence in speech<br>● Concise responses<br>**3.3 Communicate information correctly in a structured language**<br>● Analyse the use of correct common grammar<br>● Explain the meanings of words and phrases<br>**3.4 Use written communication effectively**<br>● Explain the advantages and disadvantages of written communication |
| **Conditions/context of assessment** | 1. Written and/or oral assessment on the skills and knowledge required to define oral communication, answer questions during a job interview, communicate information correctly in structured language and use written communication effectively as outlined in the assessment criteria.<br>2. Practical assessment on the requirements and principles of basic communication |
| **Assessment Task** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated |

| | |
|---|---|
| | work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>- Visitors chairs<br>- Secretary chair and desk<br>- Computer<br>- Printer<br>- Photocopier<br>- Stationary and petty cash vouchers |

| **Learning outcome 04** | **Enhance collaboration, resolve conflicts, and foster stakeholder engagement by applying effective communication techniques in business** |
|---|---|
| **Assessment criteria** | **4.1 Organise written material logically**<br>**4.2 Use grammar and pronunciation according to type of business**<br>**4.3 Interpret information presented orally**<br>**4.4 Communicate clearly** |
| **Assessment tasks** | **4.1 Organise written material logically**<br>● Present business documents<br>● Write different business letters<br>● Write different reports<br>**4.2 Use grammar and pronunciation according to type of business**<br>● Construct sentences that communicate<br>● Use of objective language in communicating<br>● Describe use of direct and indirect speech<br>**4.3 Interpret information presented orally**<br>● Analyse a written passage<br>● Identify key points from the given passage<br>**4.4 Communicate clearly**<br>● Identify and discuss the concept of the 'seven (7) cs' in communication<br>● Identify the most effective methods of communication<br>● Explain the importance of transmitting accurate information |
| **Conditions/context of assessment** | 1. Written and/or oral assessment on the skills and knowledge required to organise written material logically, use grammar and pronunciation according to type of business, interpret information presented orally and communicate clearly as outlined in the assessment criteria.<br>2. Practical assessment on the requirements and principles of basic communication. |
| **Content** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment |

| | |
|---|---|
| | and materials listed below: -<br>- Visitors chairs<br>- Secretary chair and desk<br>- Computer<br>- Printer<br>- Photocopier<br>- Stationary and petty cash vouchers |

| | |
|---|---|
| **Learning outcome 05** | **Prepare different types of meetings by planning agendas, coordinating logistics, and documenting proceedings in accordance with professional conventions** |
| **Assessment criteria** | **5.1 Define different types of meetings.**<br>**5.2 Identify requirements for meetings.**<br>**5.3 Take notes from meetings.**<br>**5.4 Prepare meeting documents** |
| **Content** | **5.1 Define different types of meetings.**<br>● Public meetings<br>● Private meetings<br>● Office bearers<br>**5.2 Identify requirements for meetings.**<br>● Quorum<br>● Notice<br>● Agenda<br>● Convener<br>● Secretary<br>**5.3 Take notes from meetings.**<br>● Narrative minutes<br>● Resolution minutes<br>● Verbatim minutes<br>**5.4 Prepare meeting documents**<br>● Notice<br>● Agenda<br>● Minutes of meetings. |
| **Conditions/context of assessment** | 1. Written and/or oral assessment on the skills and knowledge required to define different types of meetings, identify requirements for meetings, take notes from meetings and prepare meeting documents a**s** outlined in the assessment criteria.<br>2. Practical assessment on the requirements and principles of basic communication |
| **Content** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - |

| | |
|---|---|
| | - Visitors chairs<br>- Secretary chair and desk<br>- Computer<br>- Printer<br>- Photocopier<br>- Stationary and petty cash vouchers |

**Approach to teaching and learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. RPL assessment.
4. Portfolio of evidence.
5. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of trainers, assessors and moderators**

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualifications and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, tools, equipment and materials**
    - Computer
    - Desk
    - Swivel chair
    - Visitors chairs
    - Filing cabinets
    - Puncher
    - Stapler
    - Pens
    - Dust bin
    - Fax machine
    - Printer
    - Paper tray
    - Document scanner
    - Photocopier
    - Heater
    - Fan/air conditioner
    - Document holders
    - Refrigerator
    - Water dispenser
    - Water glasses
    - Tea set

- Electric jugs
- Trays
- Cash box
- Microwave
- Office ornaments
- Paper scissors
- First aid kit

3. **Learning resources**
   Relevant training manual (learners' guide) and facilitators' guide

4. **Reference materials (recommended textbooks, recommended readings)**


Adair, J (2003), Effective Communication. London: Pan Macmillan Ltd.

Ajmani, J. C. (2012), Good English: Getting it Right. New Delhi: Rupa Publications.

Amos, Julie-Ann. Handling Tough Job Interviews. Mumbai: Jaico

Publishing, 2004.

Bonet, Diana. The Business of Listening: Third Edition. New Delhi: Viva

Books, 2004.

Bovee, Courtland L, John V. Thill & Barbara E. Schatzman. Business

Communication Today: Tenth Edition. New Jersey: Prentice Hall, 2010.

Collins, Patrick. Speak with Power and Confidence. New York: Sterling,

2009.

Guffey, Mary Ellen. Essentials of Business Writing. Ohio: South-

Western College Pubg. 2000.

| | |
|---|---|
| **Module Code:** | **401/24/M01** |
| **Module Title:** | **NATIONAL STUDIES** |
| **ZNQF Level:** | **Generic** |
| **Credits:** | **5** |
| **Duration:** | **50 hours** |
| **Relationship with Qualification Standards:** | **Based on Unit Standard TBA CITIZENSHIP STUDIES UNIT STANDARD FOR PATRIOTIC CITIZEN** |
| **Prerequisite modules:** | **NONE** |
| **Purpose of Module:** | This module aims to produce patriotic and responsible citizens with knowledge, skills and attitudes that contribute to the country's development and identity. The module enables graduates to appreciate Zimbabwean history and culture, produce write ups on colonial effects, examine conflict, conflict resolution strategies and peace initiatives and contribute to problem solving through civic participation. In addition, the graduates should demonstrate an understanding of Zimbabwean indigenous knowledge systems, as well as legal and parliamentary affairs. Such a citizen should be prepared to defend, market and present a positive image of the country. Access to this module is open to all target groups, which include the unemployed, youth, men and women willing to develop their country in line with the Education 5.0 Philosophy. |
| **List of Learning Outcomes:** | **LO1: Appreciate Zimbabwean history and culture**<br>**LO2: Produce write ups on colonial effects**<br>**LO3: Demonstrate critical awareness of post-independence developments in Zimbabwe**<br>**LO4: Examine conflict, conflict resolution strategies and peace initiatives**<br>**LO5: Contribute to problem solving through civic participation**<br>**LO6: Demonstrate understanding of indigenous knowledge systems**<br>**LO7 Conscientise students on legal and parliamentary affairs** |

| Learning Outcome 01 | APPRECIATE ZIMBABWEAN HISTORY AND CULTURE |
|---|---|
| **Assessment Criteria:** | 1.1. Analyse pre- colonial states<br>1.2. Assess the role of Christian missionaries<br>1.3. Preserve Zimbabwean cultural heritage |
| **Content** | **1.1 Analyse pre Colonial states**<br>1.1.1 Definition of pre- colonial<br>1.1.2 Identifying pre-colonial states<br>1.1.3 Pre-colonial socio-economic organisation<br>1.1.4 Pre-colonial political structures<br>1.1.5 Causes of decline of pre-colonial states<br>**1.2 Assess the role of Christian missionaries**<br>1.2.1 Identify Christian missionaries<br>1.2.2 Discuss missionary activities<br>1.2.3 Impact of Christian work<br>**1.3 Preserve Zimbabwean cultural heritage**<br>1.3.1 Definition of cultural heritage<br>1.3.2 Assess the importance of cultural heritage<br>1.3.3 Indigenous methods of preserving and conserving cultural heritage<br>1.3.4 Modern ways of preserving and conserving cultural heritage<br>1.3.5 Role of national, regional and international organisations in protecting cultural heritage<br>1.3.6 Threats to the Zimbabwean cultural heritage |
| **Assessment Tasks:** | 1. Written assessment on the skills and knowledge required to maintain the Zimbabwean history and Culture.<br>2. Practical based assignment on ways of preserving cultural heritage sites within the communities. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment.<br>2. The practical based assignment assessment will be conducted based on observations in the communities. |

| Learning Outcome 02 | **PRODUCE WRITE UPS ON COLONIAL EFFECTS** |
|---|---|
| **Assessment Criteria:** | 2.1 Partition of Africa<br>2.2 Colonisation of Zimbabwe<br>2.3 Reactions to colonisation<br>2.4 Effects of colonisation |
| **Content** | **2.1 Partition of Africa**<br>2.1.1 Causes of partition and colonisation of Africa<br>2.1.2 Reasons for the Berlin Conference<br>2.1.3 Effects of the scramble for Africa<br>2.2 **Colonisation of Zimbabwe**<br>2.2.1 Reasons for the colonisation of Zimbabwe<br>2.2.2 Step towards colonisation of Zimbabwe<br>2.2.3 Occupation of Zimbabwe<br>2.2.4 Impact of the colonisation of Zimbabwe<br>**2.3 Reactions to colonisation**<br>2.3.1 Causes and results of the Anglo-Ndebele war<br>2.3.2 Causes and results of the 1st Chimurenga/Umvukela<br>2.3.3 Causes and results of the 2nd Chimurenga/Umvukela<br>2.3.4 Impact of African reactions on colonization<br>**2.4 Effect of colonisation**<br>2.4.1 Social effects<br>2.4.2 Economic effects<br>2.4.3 Political effects |
| **Assessment Tasks:** | 1. Written or oral assessment on the skills and knowledge required to assess the understanding of Zimbabwean history.<br>2. Practical activities based on observations within and outside the institution that demonstrate understanding of Zimbabwean history. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment or practical activities conducted within or outside the institution.<br>2. The practical based assignment/activities will be conducted based on |

| | |
|---|---|
| | participation/observations in the communities. |
| | |

| | |
|---|---|
| **Learning Outcome 03** | **DEMONSTRATE CRITICAL AWARENESS OF POST-INDEPENDENCE DEVELOPMENTS IN ZIMBABWE.** |
| **Assessment criteria** | 3.1 Social developments<br>3.2 Economic developments<br>3.3 Political developments<br>3.4 Colonial vestiges |
| **Content** | **3.1 Social developments**<br>3.1.1 Identify trends in social developments<br>3.1.2 Policies to promote social developments<br>3.1.3 Effects of social developments on citizens' well-being<br>3.1.4 Challenges of social developments<br>**3.2 Economic developments**<br>3.2.1 Identify trends in economic developments<br>3.2.2 Policies to promote economic developments<br>3.2.3 Effects of economic developments on citizens' well-being<br>3.2.4 Challenges of economic developments<br>**3.3 Political developments**<br>3.3.1 Identify trends in political developments<br>3.3.2 Policies to promote political developments<br>3.3.3 Effects of political developments on citizens' well-being<br>3.3.4 Challenges of political developments<br>**3.4 Colonial vestiges**<br>3.4.1 Define colonial vestiges<br>3.4.2 Identify colonial vestiges at family and national levels<br>3.4.3 Strategies to address colonial vestiges<br>3.4.4 Positive colonial developments |
| **Assessment Tasks:** | 1. Written or oral assessment on the skills and knowledge required to assess the understanding of post-independence developments in Zimbabwe**.** |

| | |
|---|---|
| | 2. Practical activities based on observations within and outside the institution that demonstrate understanding of post-independence developments in Zimbabwe. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment or practical activities conducted within or outside the institution.<br>2. The practical based assignment/activities will be conducted based on participation/observations in the communities |

| **Learning outcome 04** | **EXAMINE CONFLICT, CONFLICT RESOLUTION STRATEGIES AND PEACE INITIATIVES** |
|---|---|
| **Assessment Criteria:** | 4.1 Examine causes of conflict<br>4.2 Evaluate conflict resolution strategies<br>4.3 Analyse strategies for sustainable peace |
| **Content** | **4.1 Examine causes of conflict**<br>4.1.1 Definition of conflict<br>4.1.2 Types of Conflicts<br>4.1.3 Impact of conflict on communities<br>**4.2 Evaluate conflict resolution strategies**<br>4.2.1 Defining conflict resolution<br>4.2.2 Exploring conflict resolution strategies<br>4.2.3 Traditional African conflict resolution strategies<br>4.2.4 Modern conflict resolution strategies<br>**4.3 Analyse strategies for sustainable peace**<br>4.3.1 Definition of peace and sustainable peace<br>4.3.2 Exploring peace initiatives<br>4.3.3 Discussing strategies for sustainable peace<br>4.3.4 Role of NGOs, regional and international organizations in promoting sustainable peace. |
| **Assessment Tasks:** | 1. Written or oral assessment on the skills and knowledge required to assess the understanding of conflict, conflict resolution strategies and peace initiatives |

| | |
|---|---|
| | 2. Practical activities based on observations within and outside the institution that demonstrate understanding of conflict, conflict resolution strategies and peace initiatives. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment or practical activities conducted within or outside the institution.<br>2. The practical based assignment/activities will be conducted based on participation/observations in the communities. |

| | |
|---|---|
| **Learning outcome 05** | **CONTRIBUTE TO PROBLEM SOLVING THROUGH CIVIC PARTICIPATION** |
| **Assessment Criteria:** | 5.1 Undertaking civic responsibilities<br>5.2 Participating in disaster management<br>5.3 Engage in citizen duties |
| **Content** | **5.1 Undertaking civic responsibilities**<br>5.1.1 Definition of civic responsibilities<br>5.1.2 Civic responsibilities<br>5.1.3 Justification for civic responsibilities<br>5.1.4 Engaging in civic duties<br>**5.2 Participating in disaster management**<br>5.2.1 Definition of disaster management<br>5.2.2 Justification for disaster management<br>5.2.3 Sustainable disaster management practices<br>**5.3 Engage in citizen duties**<br>5.3.1 Definition of citizen and citizen duties<br>5.3.2 Socio –economic and political citizen duties and responsibilities |
| **Assessment Tasks:** | 1. Written assessment on the skills and knowledge required to maintain problem solving through civic participation .<br>2. Practical based assignment on civic duties and responsibilities. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment.<br>2. The practical based assignment assessment will be conducted based on activities and observations in the communities |

| | |
|---|---|
| **Learning outcome 06** | **DEMONSTRATE UNDERSTANDING OF INDIGENOUS KNOWLEDGE SYSTEMS (IKS).** |
| **Assessment Criteria:** | 6.1 Overview of indigenous knowledge systems<br>6.2 Characteristics of IKS<br>6.3 Significance of IKS<br>6.4 Threats to IKS and opportunities |
| **Content** | **6.1 Overview of Indigenous Knowledge Systems(IKS)**<br>6.1.1 Defining IKS<br>6.1.2 Types of IKS<br>**6.2 Characteristics of IKS**<br>6.2.1 Ecological<br>6.2.2 Traditional<br>6.2.3 Cultural<br>6.2.4 Experiential<br>**6.3 Significance of IKS**<br>6.3.1 Social<br>6.3.2 Economic<br>6.3.3 Political<br>**6.4 Threats to IKS and Opportunities**<br>6.4.1 Threats to IKS<br>6.4.2 Opportunities of IKS |
| **Assessment Tasks:** | 1. Written assignments to assess understanding of indigenous knowledge systems.<br>2. Project or portfolio or booklet capturing local indigenous knowledge systems in the community. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment.<br>2. The practical based assessment will be conducted based on observations in the communities |

| | |
|---|---|
| **Learning outcome 07** | **CONSCIENTISE STUDENTS ON LEGAL AND PARLIAMENTARY AFFAIRS IN ZIMBABWE** |
| **Assessment Criteria** | 7.1 Explain origins of law<br>7.2 Observe constitutional provisions<br>7.3 Describe arms of the state<br>7.4 Describe the law making process |
| **Content** | **7.1 Explain origins of law**<br>7.1.1 Definition of legal terms<br>7.1.2 Purpose of the law to the community<br>7.1.3 Sources of law in Zimbabwe<br>**7.2 Observe constitutional provisions**<br>7.2.1 Justification of the Zimbabwean constitution<br>7.2.2 Rights as enshrined in the Zimbabwean constitution<br>7.2.3 Benefits of rights to the community<br>7.2.4 Role played by stakeholders in upholding rights (NGO, Civil Societies and victim friendly units)<br>7.2.5 Impediments to exercising human rights<br>**7.3 Describe arms of the state**<br>7.3.1 Identification of the three arms of state<br>7.3.2 Functions of the three arms of the state<br>7.3.3 Importance of separation of powers to Zimbabwe<br>7.4 **Describe the law making process**<br>7.4.1 Steps in the law making process<br>7.4.2 Role of community and civic organisations in law making process |
| **Assessment Tasks:** | 1. Written assessment on the skills and knowledge required to appreciate the Zimbabwean legal and parliamentary affairs.<br>2. Practical based assignment on legal and parliamentary affairs. |
| **Conditions/Context of assessment** | 1. Written assessment can be conducted in a classroom environment.<br>2. The practical based assignment assessment will be conducted based on observations in the communities |

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Project or Portfolio or Booklet as evidence.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**

   All trainers, assessors and moderators should have undergone a Bachelor's Degree in History or equivalent.

2. **Facilities, Tools, Equipment and Materials**

- Computer
- Communication equipment
- Data storage devices
- Television
- DVD Recorder/player

3. **Learning Resources**

- Artefacts
- Resource persons
- Museums and heritage sites
- Videos and audio materials

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| | **WEIGHTING** |
|---|---|
| **Appreciation of Zimbabwean history and culture** | 20% |
| **Colonial effects** | 10 % |
| **Post-independence socio-economic and political developments** | 20% |
| **Peace, conflict and resolution** | 10% |
| **Civic responsibilities** | 20 % |
| **Indigenous Knowledge Systems** | 10% |
| **Legal and parliamentary affairs** | 10 % |
| **TOTAL** | **100%** |

**PAPER STRUCTURE**

Students should answer any 5 from a total of 9 questions. Each question carries 20 marks. Total 100 marks.

| | **NUMBER OF QUESTIONS** | **WEIGHTING** |
|---|---|---|
| **Zimbabwean history and culture**<br>● Precolonial States<br>● Christian Missionaries<br>● Zimbabwe cultural Heritage | 2 | 20 % |
| **Colonial Effects**<br>● Partition of Africa<br>● Colonisation of Zimbabwe<br>● Reactions to colonisation<br>● Effects of colonisation | 1 | 10 % |
| **Post-independence socio-economic and political developments**<br>● Social developments<br>● Economic developments | 2 | 20% |

| | | |
|---|---|---|
| ● Political developments<br>● Colonial vestiges | | |
| **Conflict, Conflict resolution strategies and peace initiatives**<br>● Causes of conflict<br>● Conflict resolution strategies<br>● Strategies for sustainable peace | 1 | 10% |
| **Civic participation**<br>● Civic responsibilities<br>● disaster management<br>● Citizen duties | 2 | 20% |
| **Indigenous Knowledge Systems** (IKS)<br>● Characteristics of IKS<br>● Significance of IKS<br>● Threats and opportunities | 1 | 10% |
| **Legal and parliamentary affairs**<br>● Origins of law<br>● Constitutional provisions<br>●<br>● Law making process | 1 | 10% |
| **TOTAL** | **9** | **100%** |

**4. Reference Materials (recommended textbooks, recommended readings)**

American Heritage Dictionary of the English Language, Fifth Edition (2011), Houghton Mifflin.

Astrow, A., 1983. Zimbabwe: A Revolution That Lost Its. *Way*, pp.1980-1986.

Banana, C. ed., 1989. *Turmoil and tenacity: Zimbabwe 1890-1990*. College Press.

Batchelor, P., Kingma, K. and Lamb, G. eds., 2004. *Demilitarisation and Peace-building in Southern Africa: Concepts and processes* (Vol. 1). Gower Publishing, Ltd.

Birmingham, D. and Martin, P. eds., 1983. *History of Central Africa* (Vol. 2). Addison-Wesley Longman Limited.

Centre for Peace Initiatives in Africa, 2005. *Zimbabwe: The Next 25 Years*. Benaby Printing and Publishing.

Change African Indigenous Knowledge and Disciplines

Chirimuuta, C., Gudhlanga, E. and Bhukuvhani, C., 2012. Indigenous knowledge systems: a panacea in education for development?

Chitiyo, T.K., 2000. Land violence and compensation: reconceptualising Zimbabwe's land and war veterans' debate. *Track Two: Constructive Approaches to Community and Political Conflict*, *9*(1).

Chitsike, F., 2003, December. A critical analysis of the land reform programme in Zimbabwe. In *2nd FIG Regional Conference* (pp. 2-5).

Collins English Dictionary – Complete and Unabridged, 12th Edition (2014) HarperCollins.

De Villiers, B., 2003. Land reform: issues and challenges: a comparative overview of experiences in Zimbabwe. *Namibia, South Africa and Australia, Johannesburg: Konrad Adenauer Publications*.

Emeagwali and Dei, G, J.S (Eds) (2014), Anti-Colonial Educational Perspectives for Transformative

Government of Zimbabwe, 2013. The Constitution of the Republic of Zimbabwe Amendment (No.20).

Hammar, A., Jensen, S. and Raftopoulos, B. eds., 2003. *Zimbabwe's unfinished business: Rethinking land, state and nation in the context of crisis*. Weaver Press.

Hayes, D., 1980. *Human Rights*, Sussex, Wayland Publishers.

Kriger, N., 1995. The politics of creating national heroes: The search for political legitimacy and national identity. *Soldiers in Zimbabwe's liberation war*, *1*, pp.139-162.

Lalonde, A., 1991. African indigenous knowledge and its relevance to environment and development activities. *Canadian International Development Agency*.

Madhuku, L. 2004. Law, Politics and the Land Reform Process. In Masiyiwa, S. 2004. Post-Independence Land Reform in Zimbabwe: Controversies and Impact on the Economy.

Mkabela, Q., 2005. Using the Afrocentric method in researching indigenous African culture. *The qualitative report*, *10*(1), pp.178-190.

Mlambo, A.S., 2014. *A history of Zimbabwe*. Cambridge University Press.

Moyo, S., 2004. *Overall impacts of the fast track land reform programme*. African Institute for Agrarian Studies.

Moyo, S., 2006. The evolution of Zimbabwe's land acquisition. University of Zimbabwe (UZ) Publications/Michigan State University (MSU).

Ogunbanjo, M.B., Human Rights in Africa in the new Global Order: A Dilemma?

Raftopoulos, B. and Mlambo, A. eds., 2009. *Becoming Zimbabwe. A History from the Pre-colonial Period to 2008: A History from the Pre-colonial Period to 2008*. African Books Collective.

Ranger, T., 1985. Peasant Consciousness and Guerrilla Warfare in Zimbabwe: A Comparative Study. *Harare: McMillan*.

Ranger, T.O. ed., 1968. *Aspects of Central African History*. Northwestern University Press.

Richardson, C., 2004. *The collapse of Zimbabwe in the wake of the 2000-2003 land reforms*.

Schmidt, E.S., 1992. Peasants, traders and wives: Shona women in the history of Zimbabwe, 1870-1939.

Shaw, W.H., 2003. 'They Stole Our Land': debating the expropriation of white farms in Zimbabwe. *The Journal of Modern African Studies*, *41*(1), pp.75-89.

Shamuyarira, N.M., 1966. Crisis in Rhodesia.

Warren, D.M., 1989. Linking scientific and indigenous agricultural systems.

Zikhali, P., 2008. *Fast track land reform, tenure security, and investments in Zimbabwe* (No. dp-08-23-efd).

| | |
|---|---|
| **Module Code:** | **402/25/M01** |
| **Module Title:** | **ENTREPRENEURSHIP SKILLS DEVELOPMENT** |
| **ZNQF Level:** | **4** |
| **Credits:** | 5 |
| **Duration:** | 50hrs |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Entrepreneurship Skills Development** Unit Standard of Qualification Standard for an Entrepreneur |
| **Pre-requisite modules:** | N/A |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an entrepreneur to acquire leadership, business and time management, creative thinking and problem-solving in a job role and industries. This module will ensure that the entrepreneur will develop a bankable business plan, formalise a business, manage a business and optimise a business. The advantages of entrepreneurship skills development are that growth and development are constant, beneficial networks are developed and work life autonomy is possible. Access to this module is open to all youth, man and woman who want to own a business. |
| **List of Learning Outcomes:** | **LO1: Develop a bankable business plan**<br>**LO2: Formalise a business**<br>**LO3: Manage a business**<br>**LO4: Optimize a business** |

| Learning outcome 01 | Develop a bankable business plan |
|---|---|
| **Assessment criteria** | **1.1 Define business concept**<br>**1.2 Conduct comprehensive market research**<br>**1.3 Outline marketing strategies clearly**<br>**1.4 Develop operational plan**<br>**1.5 Establish organizational structure**<br>**1.6 Complete financial projections**<br>**1.7 Define risk management strategies**<br>**1.8 Address sustainability and social impact**<br>**1.9 Plan is investment-ready or bankable** |
| **Content** | **1.1 Business concept clearly defined**<br>1.1.1 Definition of entrepreneurship and entrepreneur<br>1.1.2 Characteristics of successful patriotic entrepreneurs<br>1.1.3 Identifying and validating business opportunities<br>1.1.4 Developing a business idea using tools e.g., Lean Canvas, Design Thinking<br>1.1.5 Differentiating between vision, mission, goals, and objectives<br>1.1.6 Value proposition and competitive advantage<br>**1.2 Comprehensive market research conducted**<br>1.2.1 Definition and types of markets<br>1.2.2 Tools and methods of market research<br>1.2.3 Understanding customer needs and preferences<br>1.2.4 Competitor analysis (SWOT, PESTEL)<br>1.2.5 Market segmentation and targeting<br>1.2.6 Trends and forces shaping the industry<br>1.3 Marketing strategies clearly outlined<br>1.3.1 Introduction to marketing<br>1.3.2 Elements of the marketing mix (7 Ps: Product, Price, Place, Promotion, People, Process, Physical Evidence)<br>1.3.3 Branding and customer value<br>1.3.4 Developing a simple actionable marketing plan<br>1.3.5 Use of digital tools and social media marketing<br>1.3.6 Low-cost marketing strategies for start-ups<br>**1.4 Operational plan developed**<br>1.4.1 Basics of business operations<br>1.4.2 Workflow planning and production processes<br>1.4.3 Procurement and supplier management<br>1.4.4 Tools for managing inventory and logistics<br>1.4.5 Location selection and physical setup |

| | |
|---|---|
| | 1.4.6 Operational policies and procedures<br>**1.5 Organizational structure established**<br>1.5.1 Types of business ownership structures (sole proprietorship, cooperative, partnership, company)<br>1.5.2 Functions and roles of organisational structure within a business<br>1.5.3 Designing an organizational chart<br>1.5.4 Human resource needs<br>1.5.5 Leadership and management in small businesses<br>**1.6 Financial projections completed**<br>1.6.1 Purpose and components of a financial plan<br>1.6.2 Start-up costs and working capital estimation<br>1.6.3 Preparing projected income statements, cash flow, and balance sheets<br>1.6.4 Break-even analysis<br>1.6.5 Sources of finance e.g. personal savings, loans, grants, crowdfunding<br>1.6.6 Record-keeping basics<br>**1.7 Risk management strategies defined**<br>1.7.1 Definition and types of risks in business<br>1.7.2 Internal and external risks<br>1.7.3 Risk identification and assessment<br>1.7.4 Strategies for mitigating risks (e.g., insurance, contracts, diversification)<br>1.7.5 Legal compliance and regulatory risks<br>**1.7.6** Crisis and contingency planning<br>**1.8 Sustainability and social impact addressed**<br>1.8.1 Introduction to sustainable entrepreneurship<br>1.8.2 Environmental, Social, and Governance (ESG) practices<br>1.8.3 Integrating sustainability into products and operations<br>1.8.4 Corporate Social Responsibility (CSR)<br>1.8.5 Aligning business with the SDGs (especially SDG 8 & 9)<br>**1.9 Plan is investment-ready or bankable**<br>1.9.1 What makes a business plan bankable<br>1.9.2 Aligning business plan with investor and lender expectations<br>1.9.3 Structuring a business plan for clarity and professionalism<br>1.9.4 Pitching the business plan to funders<br>1.9.5 Common reasons why plans are rejected and how to |

| | |
|---|---|
| | avoid them<br>1.9.6 Portfolio development: business plan as part of final assessment |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to develop a business plan as outlined in the assessment criteria and content above.<br>2. Practical assessment on the development of a bankable business plan |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials as per entrepreneur's occupation. |

| **Learning outcome 02** | **Formalise a business** |
|---|---|
| **Assessment criteria** | **2.1 Select business structure appropriately**<br>**2.2 Obtain a certificate of incorporation or registration**<br>**2.3 Establish basic record-keeping systems**<br>**2.4 Demonstrate awareness of legal and regulatory obligations** |
| **Content** | **2.1 Business structure appropriately selected**<br>2.1.1 Types of business ownership<br>2.1.2 Characteristics of each business structure<br>2.1.3 Factors to consider when choosing a business structure<br>2.1.4 Comparison table of advantages and disadvantages of each business structure<br>**2.2 Certificate of incorporation/registration obtained**<br>2.2.1 Purpose of business registration<br>2.2.2 Overview of the registration process<br>2.2.3 Types of companies that can be registered<br>2.2.4 Required documents for registration<br>2.2.5 Post-registration documents<br>2.2.6 Use of online portals<br>**2.3 Basic record-keeping systems established** |

| | |
|---|---|
| | 2.3.1 Importance of record keeping<br>2.3.2 Types of business records<br>▪ Financial (e.g. cash book, sales ledger, receipts, invoices)<br>▪ Administrative (e.g. employee records, statutory documents)<br>▪ Inventory records<br>2.3.3 Manual and digital record keeping<br>2.3.4 Introduction to basic accounting tools<br>2.3.5 Setting up a simple filing or folder system.<br>**2.4 Awareness of legal and regulatory obligations demonstrated**<br>2.4.1 Legal Compliance Overview:<br>• Tax registration (ZIMRA)<br>• NASSA registration (for employees)<br>• Local authority by-laws and licensing<br>• Sector-specific regulations (e.g. health, transport, agriculture)<br>2.4.2 Business legal rights and responsibilities<br>2.4.3 Statutory returns and filing deadlines<br>2.4.4 Labour law basics e.g. contracts of employment, minimum wage and working conditions<br>2.4.5 Consumer protection laws<br>2.4.6 Penalties for non-compliance<br>**2.5 Benefits of formalisation articulated**<br>2.5.1 Define is business formalisation<br>2.5.2 Benefits of formalisation<br>2.5.3 Risks of informal operation<br>2.5.4 Testimonials and case studies |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to formalise a business as outlined in the assessment criteria and content above.<br>2. Practical assessment on the formalisation of a business. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials as per entrepreneur's occupation |

| **Learning outcome 03** | **Manage a business** |
|---|---|
| **Assessment criteria** | **3.1 Manage a business according to organisational policy**<br>**3.2 Develop business strategies to ensure effectiveness**<br>**3.3 Allocate resources according to line of business**<br>**3.4 Cost products in line with procedures**<br>**3.5 Price products according to company procedures**<br>**3.6 Update and maintain records**<br>**3.7 Control stock in line with organisational requirements**<br>**3.8 Design day-to-day business processes**<br>**3.9 Formulate market plans**<br>**3.10 Manage risks in line with organisational requirements**<br>**3.11 Observe business ethics and social responsibility**<br>**3.12 Apply customer care tips**<br>**3.13 Motivate employees in line with organisational requirements** |
| **Content** | **3.1 Manage a business according to organisational policy**<br>3.1.1 Define business management<br>3.1.2 Explain the functions of management in a business<br>3.1.3 Discuss the importance of computers as a business management tool<br>**3.2 Develop business strategies to ensure effectiveness**<br>3.2.1 Analyse internal capabilities and external market forces<br>3.2.2 Formulate clear strategic goals and action plans<br>3.2.3 Align departmental objectives with overall business vision<br>3.2.4 Allocate resources according to line of business<br>3.2.5 Define resource allocation<br>3.2.6 Explain the importance of properly allocating resources e.g. human, capital, material<br>3.2.7 Prepare budgets<br>**3.3 Cost products in line with procedures**<br>3.4.1 Define various costing terms<br>3.4.2 Explain the importance of costing to a business<br>3.4.3 Describe the costing processes of a business<br>3.4.4 Price products in line with business policy<br>3.4.5 Define various pricing terms<br>3.4.6 Explain the importance of pricing to a business<br>3.4.7 Analyse the pricing processes of a business<br>3.4.8 Calculate prices of products |

| | |
|---|---|
| | 3.4.9 Describe pricing strategies<br>**3.5 Update and maintain records**<br>3.5.1 Define record keeping in business<br>3.5.2 Identify source business document<br>3.5.3 Explain the importance of record keeping<br>3.5.4 Describe the purposes of books of accounts<br>3.5.5 Control stock in line with organisation requirements<br>3.5.6 Define stock control in business<br>3.5.7 Describe the importance of stock control<br>3.5.8 Analyse effective stock control procedures<br>**3.6 Design day-to-day business processes**<br>3.6.1 Map operational workflows for clarity<br>3.6.2 Define roles, responsibilities, and key tasks<br>3.6.3 Integrate technology for automation and efficiency<br>3.6.4 Establish quality control checkpoints and reviews<br>**3.7 Formulate market plans**<br>3.7.1 Analyse target audience and market segmentation<br>3.7.2 Develop integrated sales funnels and marketing campaigns<br>3.7.3 Allocate budget and resources for promotional activities<br>3.7.4 Devise a marketing plan for a business<br>3.7.5 Explain the Ps of marketing<br>3.7.6 Discuss the marketing mix strategies<br>**3.8 Manage risks in line with organisation requirements**<br>3.8.1 Define risk management<br>3.8.2 Discuss the importance of risk covers in entrepreneurship<br>3.8.3 Explain the principles of risk management to a business<br>3.8.4 Analyse the steps involved in risk management process<br>3.8.5 Identify the various risk management strategies in business<br>3.8.6 Prepare a comprehensive risk register<br>**3.9 Adopt growth strategies**<br>3.9.1 Define business growth strategies<br>3.9.2 Explain the four business growth strategies<br>**3.10 Observe business ethics and social responsibility**<br>3.10.1 Define business ethics and social responsibility<br>3.10.2 Explain the importance of business ethics and social responsibility to entrepreneurs |

| | |
|---|---|
| | 3.10.3 Discuss social responsibility principles<br>**3.11 Practise customer care**<br>3.11.1 Define customer care<br>3.11.2 Discuss ten tips of customer care<br>3.11.3 Explain benefits of customer care<br>**3.12 Motivate employees in line with organisational requirements**<br>3.12.1 Define motivation<br>3.12.2 Outline theories of staff motivation in business<br>3.12.3 Discuss the importance of motivation<br>**3.13 Formulate standard operating procedures**<br>3.13.1 Document step-by-step instructions for key tasks<br>3.13.2 Establish clear guidelines for process execution<br>3.13.3 Implement review cycles for continuous improvement<br>3.13.4 Compile rules and procedures for the business<br>3.13.5 Establish a clear code of conduct and ethics<br>3.13.6 Develop operational guidelines for all departments<br>3.13.7 Define compliance protocols for regulatory adherence |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to manage a business as outlined in the assessment criteria and content above.<br>2. Practical assessment on how to manage a business |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials as per entrepreneur's occupation |

| Learning outcome 04 | Optimize a business |
|---|---|
| **Assessment criteria** | **4.1 Analyse business performance to determine growth**<br>**4.2 Identify business processes for improvement**<br>**4.3 Develop strategies for enhanced customer care**<br>**4.4 Evaluate market expansion opportunities**<br>**4.5 Evaluate resource allocation**<br>**4.6 Monitor market trends**<br>**4.7 Track Key Performance Indicators (KPIs)**<br>**4.8 Formulate strategies for sustainable growth and scalability**<br>**4.9 Maintain records**<br>**4.10 Develop business continuity plans** |
| **Content** | **4.1 Analyse business performance to determine growth**<br>4.1.1 Evaluate relevant financial KPIs e.g. revenue growth rate, profit margins, customer acquisition costs<br>4.1.2 Analyze relevant operational KPIs e.g., inventory turnover, customer satisfaction scores<br>4.1.3 Benchmark KPIs with industrial standards<br>4.1.4 Analyse the financial statements for growth insights<br>**4.2 Identify business processes for improvement**<br>4.2.1 Map current business processes to visualize workflows<br>4.2.2 Identify areas that are causing wastage of resources<br>4.2.3 Explain approaches to eliminate wastage of resources<br>4.2.4 Perform Root Cause Analysis (RCA) for processing inefficiencies<br>4.2.5 Benchmark against industry standards<br>**4.3 Develop strategies for enhanced customer care**<br>4.3.1 Analyze customer feedback to identify business pain points<br>4.3.2 Design framework for enhanced customer communication<br>4.3.3 Implement customer complaint resolution systems<br>4.3.4 Design training on proactive customer service skills<br>**4.4 Evaluate market expansion opportunities**<br>4.4.1 Research new geographical markets and demographics<br>4.4.2 Assess market demands and competitive landscape<br>4.4.3 Analyze entry barriers and regulatory environment<br>**4.5 Evaluate resource allocation**<br>4.5.1 Analyze current financial expenditure and Return On Investment (ROI)<br>4.5.2 Assess human capital utilization and skills gaps<br>4.5.3 Optimize technology and infrastructure deployment<br>**4.6 Monitor market trends**<br>4.6.1 Track industry publications and news sources<br>4.6.2 Analyze consumer behaviour and search data<br>4.6.3 Analyze competitor strategies and emerging technologies |

| | |
|---|---|
| | **4.7 Track Key Performance Indicators (KPIs)**<br>4.7.1 Define new key metrics and data collection methods<br>4.7.2 Implement dashboard for real-time performance monitoring<br>**4.8 Formulate strategies for sustainable growth and scalability**<br>4.8.1 Develop adaptable business models for future expansion<br>4.8.2 Plan infrastructure and talent acquisition for scale<br>4.8.3 Integrate sustainability principles into growth strategies<br>**4.9 Maintain records**<br>4.9.1 Establish systematic data entry and storage protocols<br>4.9.2 Implement secure digital and physical record-keeping systems. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to optimise a business as outlined in the assessment criteria and content above.<br>2. Practical assessment on how to optimise a business |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials as per entrepreneur's occupation |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

## 1. Qualifications and experience of trainers, assessors and moderators

All trainers, assessors and moderators should have undergone Zimbabwe National Qualifications Framework (ZNQF) accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

## 2. Facilities, tools, equipment and materials

- Computer
- Communication equipment
- Data storage devices
- Television
- DVD Recorder/player which are relevant to the type of business

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

Weighting 60% Coursework and 40% Examination (as per existing HEXCO rules and regulations)

| | **TOPIC** | **% WEIGHTING** |
|---|---|---|
| 1 | Develop a bankable a business plan | 40 |
| 2 | Formalise a business | 20 |
| 3 | Manage a business | 20 |
| 4 | Optimize a business | 20 |

| | | |
|---|---|---|
| | **TOTAL** | **100%** |

**PAPER STRUCTURE**

Students should answer any 5 from a total of 9 questions. Each question carries 20 marks. Total 100 marks.

| | **NUMBER OF QUESTIONS** | **WEIGHTING** |
|---|---|---|
| **Develop a bankable a business plan**<br>▪ Business concept clearly defined<br>▪ Comprehensive market research conducted<br>▪ Marketing strategies clearly outlined<br>▪ Operational plan developed<br>▪ Organizational structure established<br>▪ Financial projections completed<br>▪ Risk management strategies defined<br>▪ Sustainability and social impact addressed<br>▪ Plan is investment-ready or bankable | 3 | 40% |
| **Formalise a business**<br>▪ Business structure appropriately selected<br>▪ Certificate of incorporation or registration obtained<br>▪ Awareness of legal and regulatory obligations demonstrated | 1 | 20% |
| **Manage a business**<br>▪ Manage a business according to organisational policy<br>▪ Develop business strategies to ensure effectiveness<br>▪ Allocate resources according to line of business<br>▪ Cost products in line with procedures<br>▪ Price products according to company procedures<br>▪ Update and maintain records<br>▪ Control stock in line with organisational requirements<br>▪ Design day-to-day business processes<br>▪ Formulate market plans<br>▪ Manage risks in line with organisational requirements<br>▪ Observe business ethics and social responsibility<br>▪ Apply customer care tips | 3 | 20% |

| | | |
|---|---|---|
| ▪ Motivate employees in line with organisational requirements<br>▪ Formulate standard operating procedures<br>▪ Compile rules and procedures for the business Employee motivation | | |
| **Optimize a business**<br>▪ Analyse business performance to determine growth<br>▪ Identify business processes for improvement<br>▪ Develop strategies for enhanced customer care<br>▪ Evaluate market expansion opportunities<br>▪ Evaluate resource allocation<br>▪ Monitor market trends<br>▪ Track Key Performance Indicators (KPIs)<br>▪ Formulate strategies for sustainable growth and scalability<br>▪ Maintain records<br>▪ Develop business continuity plans | 2 | 20% |
| **TOTAL** | **9** | **100%** |

**Approach to Teaching and Learning:**

Observation of adult learning principles.
Both institution-based and work-based learning to facilitate the integration of theory and practice.
Face-to-face education and learning.
Problem-based learning.
Online/distance education and learning.
Blended/hybrid education and learning.
Use of social media.

**Approach to Assessment:**

Weighting of practical and theory assessment: 60% theory and 40% practical.
Weighting of institution-based and work-based assessment: 50% institution-based assessment and 50%.
Oral assessment to be conducted by a panel of two or more assessors.
Portfolio of evidence.
Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

**1 Qualifications and experience of Trainers, Assessors and Moderators**

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualifications and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

**Facilities, Tools, Equipment and Materials Facilities, Tools, Equipment and Materials**

Computer
Communication equipment
Data storage devices
Television
DVD Recorder/player Generic which are relevant to the type of business

**Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

**Reference Materials (recommended textbooks, recommended readings)**


1. Alderman,P.,J.,(2011) Entrepreneurial Finance,Pearson Education LTD, London
2. Appleby R (1994) Modern Business Administration
3. Barringer,B.,R., &Ireland,D.,R.,(2006) Entrepreneurship:Successfully Launching New Ventures, Pearson Education
4. Bridge, S., O'Neill , K. & Martin, F., (2009) Understanding Entrerprise: Entrepreneurship &Small Business, Third Edition, Palgrave Macmillan, London
5. Burns, P. & Dewhurst, J., (eds)91990)Small Business and Entrepreneurship, Macmillan Education LTD,Hampshire
6. City and Guilds, (2012) Hospitality supervision & Leadership,Heinemann,Essex,
7. Deakins, D., & Freel, M., (2012) Entrepreneurship and Small Firms,McGraw-Hill,Berkshire
8. Hisrich, R. D. & Peters, M. P. (2016) Entrepreneurship, Tatq McGraw Hill New Delphi Entre
9. Holt, D.T., (2017) Entrepreneurship, Prentice Hall, London
10. Jarskoy, H. & Stevenson, D., (2014) International Labour Organisation Start Your Business. ILO, Harare
11. Justin Smith (2000) Business Management Trainer's Guide
12. Kotler Philip & Armstrong G (2001) Principles of Marketing
13. Kuratiko, D., F., (2008) Introduction to Entrepreneurship, Cengage Learning , Hampshire
14. Lee, C.,L., &Melicher,W.,(2012) Entrepreneurial Finance,4th Edition,Cengage Learning, South Western
15. Marcourse, I.(2016) Business Studies @nd Ed Hodder Arnold, London
16. McGuckin Frances (1988) Business for Beginners (A simple step by step Guide to Start Your New Business)
17. Mullins L (1999) Management and Organisational Behaviour 5th edition
18. Need Harm, D, & Dransfield, R.(2000) Advanced Business and Dexel, Oxford
19. Rae, D., (2007) Entrepreneurship,From opportunity to action,Palgrave Macmillan, New York
20. Rwegema , V., U., Entrepreneurship:theory in practice, 2nd edition,Oxford University Press, Cape Town
21. Stokes, D., Wilson, N. & Mador, M.,(2010) Entrepreneurshp,Cengage Learning EMEA, Hampshire
22. Stoner, J., A. F., Freeman, R., E. & Gilbert, D, R., J. R. (2017) Management 6th Edition, Prentice Hall International Englenwood Cliffs, New Jersey.
23. Van Der Wagen & Davies, C.(1998) Supervision and Leadership, Hospitality PressPty LtdElsternwick Victoria
24. Burns, P. (2023). *Entrepreneurship and small business: Start-up, growth and maturity* (6th ed.). London, UK: Red Globe Press.
25. Barringer, B. R., & Ireland, R. D. (2023). *Entrepreneurship: Successfully launching new ventures* (7th ed.). Boston, MA: Pearson.

26. Byers, T., Dorf, R., & Nelson, A. (2023). *Technology ventures: From idea to enterprise* (6th ed.). New York, NY: McGraw-Hill Education.Spinelli, S., & Adams, R. (2022). *New venture creation: Entrepreneurship for the 21st century* (11th ed.). New York, NY: McGraw-Hill Education.
27. Hisrich, R. D., Peters, M. P., & Shepherd, D. A. (2023). *Entrepreneurship* (12th ed.). New York, NY: McGraw-Hill Education.
28. Kuratko, D. F. (2024). *Entrepreneurship: Theory, process, and practice* (12th ed.). Boston, MA: Cengage Learning.
29. Ries, E. (2011). *The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses*. New York, NY: Crown Business.
30. Scarborough, N. M. (2022). *Essentials of entrepreneurship and small business management* (9th ed.). Boston, MA: Pearson.
31. Audretsch, D. B., & Lehmann, E. E. (2023). Entrepreneurial ecosystems and small business growth. *Small Business Economics, 61*(3), 445–463. https://doi.org/10.1007/s11187-022-00638-4
32. Cliff, J. E., Jennings, P. D., & Greenwood, R. (2023). How entrepreneurial identity shapes venture growth. *Entrepreneurship Theory and Practice, 47*(1), 55–78. https://doi.org/10.1177/10422587221096540
33. Newbert, S. L., & Tornikoski, E. T. (2024). Resource orchestration in nascent ventures: A longitudinal perspective. *Journal of Small Business Management, 62*(1), 89–110. https://doi.org/10.1080/00472778.2023.2134567
34. Wennberg, K., Wiklund, J., & Wright, M. (2023). The effectiveness of university entrepreneurship centers: A longitudinal study. *Journal of Business Venturing, 38*(2), 106278. https://doi.org/10.1016/j.jbusvent.2022.106278
35. Zimmerer T.W, Scarborough M Norman – Essentials of Entrepreneurship and Small Business Management – End Edition

| | |
|---|---|
| **Module Code:** | **682/25/M02** |
| **Module Title:** | **COMPUTER NETWORKING** |
| **ZNQF Level:** | **5** |
| **Credits:** | 10 |
| **Duration:** | 100 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard **COMPUTER NETWORKING** of Qualification Standard for a Digital Forensics Technician. |
| **Pre-requisite modules:** | N/A |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by a Digital Forensics Technician to network computers. This includes identifying network requirements, implementing network requirement solutions, maintaining network operations, providing user support and monitoring performance. The advantages of networking computers are that it enhances resource sharing, communication and collaboration. Access to this module is open to all target groups including unemployed youths, women and men wishing to establish or improve SMEs in the networking of computers. |
| **List of Learning Outcomes:** | **LO1: Identify network requirements by analyzing organizational needs and existing infrastructure to accurately assess and document all necessary network specifications.**<br>**LO2: Implement network requirement solutions by configuring and deploying network hardware and software to enable successful integration and functionality of all implemented solutions according to design specifications.**<br>**LO3: Maintain network operations by performing routine checks, troubleshooting issues, and applying necessary updates to enable continuous availability and optimal performance of the network infrastructure.**<br>**LO4: Provide network user support by responding to inquiries, diagnosing problems, and offering effective solutions to allow for user satisfaction and efficient resolution of network-related issues.**<br>**LO5: Monitor network performance by utilizing monitoring tools and analyzing performance metrics to identify and report on network bottlenecks and anomalies proactively.** |

| | |
|---|---|
| **Learning Outcome 01** | **IDENTIFY NETWORK REQUIREMENTS BY ANALYZING ORGANIZATIONAL NEEDS AND EXISTING INFRASTRUCTURE TO ACCURATELY ASSESS AND DOCUMENT ALL NECESSARY NETWORK SPECIFICATIONS.** |
| **Assessment Criteria:** | **1.1 Define computer networks in line with organisational needs**<br>**1.2 Illustrate network types and designs**<br>**1.3 Identify appropriate networking equipment**<br>**1.4 Describe internetworking technologies** |
| **Content:** | **1.1 Explain computer networks in line with organisational needs**<br>● Define data communications and computer networks<br>✓ State the advantages and disadvantages of using computer networks<br>✓ Differentiate analogue and digital signals<br>● Outline applications of computer networks<br><br>**1.2 Illustrated network types and designs**<br>● Discuss network types and topologies<br>✓ Network types<br>⇒ LANs<br>⇒ WLANs<br>⇒ WANs<br>⇒ MANs<br>⇒ CANs<br>⇒ PANs<br>✓ Topologies<br>⇒ Bus<br>⇒ Ring<br>⇒ Star<br>⇒ Mesh<br>⇒ Hybrid<br><br>1.3 Identify appropriate networking equipment<br>● Outline data transmission media, connectivity devices and software<br>✓ Transmission media<br>⇒ Twisted Pair (UTP, STP)<br>⇒ Coaxial<br>⇒ Fibre-optic<br>⇒ Wireless<br>✓ Connectivity devices<br>⇒ Firewall<br>⇒ Router<br>⇒ Switch<br>⇒ Hub<br>⇒ Bridge |

- ⇒ Modem
- ⇒ Wireless Access Point
- ⇒ Media Converter
- ⇒ Wireless Range Extender
- ⇒ VoIP endpoint

✓ Network Operating Systems

● Explain data transmission modes
- ✓ Broadband versus baseband
- ✓ Synchronous versus asynchronous
- ✓ Simplex, half-duplex, full duplex

**1.4 Describe internetworking technologies**

● Describe circuit switching, message switching, packet switching, narrowband and broadband networks

● Discuss networking models
- ✓ OSI Model
- ✓ TCP/IP Model

● Explain network ports and protocols
- ⇒ Connection-oriented versus connectionless protocols
- ⇒ IP
- ⇒ TCP
- ⇒ UDP
- ⇒ FTP
- ⇒ SFTP
- ⇒ TFTP
- ⇒ SMTP
- ⇒ HTTP
- ⇒ HTTPS
- ⇒ POP
- ⇒ IMAP
- ⇒ Telnet
- ⇒ Secure Shell
- ⇒ ICMP
- ⇒ NTP
- ⇒ LDAP
- ⇒ SNMP
- ⇒ SIP
- ⇒ RDP
- ⇒ SMB
- ⇒ ARP and RARP
- ⇒ Port functions

✓ DNS

✓ DHCP

● Discuss Internet Access Technologies
- ✓ DSL
- ✓ Cable broadband

| | |
|---|---|
| | ✓ Dial-up<br>✓ Public Switched Telephone Network<br>✓ Satellite Internet Access<br>✓ Wireless Internet Access |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to identify network requirements outlined as follows: explain computer networks in line with organisational needs, illustrated network types and designs identify appropriate networking equipment and describe internetworking technologies.<br>2. Practical assessment on networking computers inclusive of requirements gathering, network equipment selection and description of internetworking technologies based on the performance criteria of identify network requirements. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>a) Network simulation software<br>b) Networking devices |

| | |
|---|---|
| **Learning Outcome 02** | **IMPLEMENT NETWORK REQUIREMENT SOLUTIONS BY CONFIGURING AND DEPLOYING NETWORK HARDWARE AND SOFTWARE TO ENABLE SUCCESSFUL INTEGRATION AND FUNCTIONALITY OF ALL IMPLEMENTED SOLUTIONS ACCORDING TO DESIGN SPECIFICATIONS.** |
| **Assessment Criteria:** | **2.1 Place networking equipment in strategic positions in line with network design**<br>**2.2 Configure network devices**<br>**2.3 Test network connectivity**<br>**2.4 Generate network documentation** |
| **Content:** | **2.1 Place networking equipment in strategic positions in line with network design**<br>● Interpret network designs<br>● Implement standards:<br>✓ 568A and 568B<br>✓ Straight-through cable termination<br>✓ Crossover cable termination<br>✓ Ethernet deployment standards<br>**2.2 Configure network devices**<br>● Setup computer network devices |

| | |
|---|---|
| | ✓ IP Addressing (IPv4, IPv6)<br>✓ NAT, PAT, SNAT, DNAT<br>✓ Routing<br>⇒ Static<br>⇒ Dynamic<br>**2.3 Test network connectivity**<br>● Describe network connectivity test at the following layers<br>✓ Physical layer<br>✓ Network layer<br>● Interpret results of network connectivity tests<br>**2.4 Generate network documentation**<br>● Develop network documentation<br>✓ Wiring and port locations<br>✓ Physical and logical network diagrams<br>✓ Labelling<br>✓ Configuration documentation |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to implement network requirement solutions outlined as follows: place networking equipment in strategic positions in line with network design, configure network devices, test network connectivity and generate network documentation.<br>2. Practical assessment on networking computers inclusive of interpreting network design, device configuration, performing connectivity tests and network documentation based on the performance criteria of implement network requirement solutions. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>a) Network simulation software<br>b) Networking devices<br>c) Transmission media<br>d) Networking toolkit |

| | |
|---|---|
| **Learning Outcome 03** | **MAINTAIN NETWORK OPERATIONS BY PERFORMING ROUTINE CHECKS, TROUBLESHOOTING ISSUES, AND APPLYING NECESSARY UPDATES TO ENABLE CONTINUOUS AVAILABILITY AND OPTIMAL PERFORMANCE OF THE NETWORK INFRASTRUCTURE.** |
| **Assessment Criteria:** | **1.1 Monitor network performance**<br>**1.2 Update network security measures periodically**<br>**1.3 Perform network troubleshooting**<br>**1.4 Perform necessary network repairs**<br>**1.5 Implement network upgrades**<br>**1.6 Service network hardware** |
| **Content:** | **1.1 Monitor network performance**<br>● Justify importance of network monitoring<br>● Apply network monitoring tools<br>✓ SNMP monitors<br>✓ Packet sniffers<br>✓ Port scanners<br>✓ Vulnerability scanners<br>● Perform network performance testing<br>✓ Load testing<br>✓ Stress testing<br>✓ Throughput testing<br>**1.2 Update network security measures periodically**<br>● Describe physical security measures<br>● Explain authentication and access controls<br>● Discuss wireless network security<br>✓ WPA<br>✓ WPA2<br>**1.3 Perform network troubleshooting**<br>● Explain the troubleshooting process steps<br>● Use hardware and software troubleshooting tools<br>✓ Multimeter<br>✓ Cable tester<br>✓ Tone generator<br>✓ tracert/traceroute<br>✓ ping<br>✓ netstat<br>✓ ifconfig<br>✓ ipconfig<br>✓ nslookup<br>**1.4 Perform necessary network repairs**<br>● Discuss common network problems and their solutions<br>● Document implemented solutions<br>**1.5 Implement network upgrades**<br>● Discuss network upgrade causes<br>● Perform network upgrade |

| | |
|---|---|
| | ✓ Hardware<br>✓ Software<br>**1.6 Service network hardware**<br>● Describe network maintenance approaches<br>✓ Preventive<br>✓ Corrective<br>✓ Adaptive |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to maintain network operations outlined as follows: monitor network performance, update network security measures periodically, perform network troubleshooting, perform necessary network repairs, implement network upgrades and service network hardware.<br>2. Practical assessment on networking computers inclusive of network performance monitoring, network troubleshooting, network repair and network upgrading based on the performance criteria of maintain network operations. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below.<br>a) Network simulation software<br>b) Network monitoring software<br>c) Networking devices<br>d) Transmission media<br>e) Networking toolkit |

| | |
|---|---|
| **Learning Outcome 04** | **PROVIDE NETWORK USER SUPPORT BY RESPONDING TO INQUIRIES, DIAGNOSING PROBLEMS, AND OFFERING EFFECTIVE SOLUTIONS TO ALLOW FOR USER SATISFACTION AND EFFICIENT RESOLUTION OF NETWORK-RELATED ISSUES.** |
| **Assessment Criteria:** | **4.1 Set up help desk system**<br>**4.2 Collect and/log user queries**<br>**4.3 Analyse user queries**<br>**4.4 Attend to user queries accordingly**<br>**4.5 Conduct routine maintenance**<br>**4.6 Carry out adhoc maintenance where necessary** |
| **Content:** | **4.1 Set up the help desk system**<br>● Explain best practices for building a help desk<br>● Describe the characteristics of a successful help desk<br>**4.2 Collect and/log user queries**<br>● Describe the key elements of communication |

| | |
|---|---|
| | ● State and explain barriers to communication<br>● Discuss verbal and non-verbal communication<br>● Discuss listening skills<br>● List types of summaries<br>● Describe the process of note-making<br>**4.3 Analyse user queries**<br>● Categorise user queries in terms of:<br>✓ Level of skill required<br>✓ Type of problem (hardware/software)<br>**4.4 Attend to user queries accordingly**<br>● Describe problem solving process<br>**4.5 Conduct routine maintenance**<br>● Explain the importance of routine maintenance<br>● Describe the routine maintenance workflow<br>**4.6 Carry out ad-hoc maintenance where necessary**<br>● Describe ad-hoc maintenance<br>● Explain the advantages and disadvantages of ad-hoc maintenance |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to provide user support outlined as follows: set up help desk system, collect and/log user queries, analyse user queries, attend to user queries accordingly, conduct routine maintenance and carry out adhoc maintenance where necessary.<br>2. Practical assessment on networking computers inclusive of running a help desk and conducting maintenance based on the performance criteria of provide user support. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>a) Network simulation software<br>b) Network monitoring software<br>c) Networking devices<br>d) Transmission media<br>e) Networking toolkit |

| | |
|---|---|
| **Learning Outcome 05** | **MONITOR NETWORK PERFORMANCE BY UTILIZING MONITORING TOOLS AND ANALYZING PERFORMANCE METRICS TO IDENTIFY AND REPORT ON NETWORK BOTTLENECKS AND ANOMALIES PROACTIVELY.** |
| **Assessment Criteria:** | **3.1 Interpret network monitoring plan**<br>**3.2 Isolate faults in line with problem indicators**<br>**3.3 Implement an appropriate diagnostic methodology**<br>**3.4 Document fault resolution process**<br>**3.5 Maintain operating performance in line with standards** |
| **Content:** | **5.1 Interpret monitoring plan**<br>● Justify the need for network monitoring<br>● Distinguish between agent and agentless monitoring<br>● Describe the following monitoring forms:<br>✓ Active<br>✓ Passive<br>✓ Performance<br>● Document a network monitoring plan<br>**5.2 Isolate faults in line with problem indicators**<br>● Discuss the following:<br>✓ Simple Network Management Protocol<br>✓ Windows Management Instrument<br>✓ Ping<br>● Describe network monitoring maps<br>✔ Horizontal plane<br>✔ Vertical plane<br>✔ View point<br>✔ x-y line<br>**5.3 Implement appropriate diagnostic methodology**<br>● Discuss network problem diagnosis approaches<br>**5.4 Document fault resolution process**<br>● Describe the contents of problem resolution record<br>**5.5 Maintain operating performance in line with standards**<br>● Discuss business continuity and disaster recovery strategies |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to monitor performance outlined as follows: develop monitoring plan, isolate faults in line with problem indicators, implement appropriate diagnostic methodology, document fault resolution process and maintain operating performance in line with standards.<br>2. Practical assessment on networking computers inclusive of documenting monitoring plan, implementing problem solving process and documenting solutions based on the performance criteria of monitor performance. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated |

| | |
|---|---|
| | work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>a) Network simulation software<br>b) Network monitoring software<br>c) Networking devices<br>d) Network cables<br>e) Networking toolkit |

**ASSESSMENT SCHEME**

| | | |
|---|---|---|
| **Theory:**<br>3 hour paper<br>(Weighted 20%) | A minimum of<br>● 2 Assignments 20%<br>● 2 Practical assignments 20%<br>● 2 Tests 20% | 100% |

**ASSESSMENT SPECIFICATION GRID**

| **No.** | **TOPIC** | **WEIGHTING %** |
|---|---|---|
| LO1: | Identify network requirements | 20 |
| LO2: | Implement network requirement solutions | 20 |
| LO3: | Maintain network operations | 20 |
| LO4: | Provide network user support | 20 |
| LO5: | Monitor network performance | 20 |
| **TOTAL** | | **100** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of continuous assessment and examination: 60% and 40% respectively.
2. Weighting of institution-based and work-based assessment: 50% institution-based assessment and 50%.

3. Oral assessment to be conducted by a panel of two or more assessors.
4. RPL assessment.
5. Portfolio of evidence.
6. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualifications and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

   Minimum qualification for Trainer, Assessor and Moderator: National Diploma in Information Technology.

2. **Facilities, Tools, Equipment and Materials**
   Computer repair toolkit
   Software
   Computer hardware
   Protective clothing
   First aid kit
   Storage media
   Internet
   Maps
   Computer network tool kit
   Stationery

3. **Learning Resources**
   Relevant training manual (learners' guide) and facilitators' guide

4. **Reference Materials (recommended textbooks, recommended readings)**


Fielding. M, (2014) **Effective Communication in Organizations**, Juta and Company, South Africa

Forouzan, BA. (2012). **Data Communications and Networking. 5th Ed** London: McGraw-Hill

Kurose, JF and Ross, KW. (2017). **Computer Networking A Top-Down Approach. 7th Ed**. New York: Pearson.

Mir, NF. (2014). **Computer and Communication Networks 2nd Ed**. Prentice Hall, New York.

Peterson, L. L. and Davie, B. S. (2010). **Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking). 5th Ed**. Amsterdam: Elsevier.

Sharma, S. (2017). **Fundamentals of Data Communication and Networks**. Kataria & Sons, New Delhi

Stalling, W. (2013). **Data and Computer Communication. 10th Ed**. New Jersey: Pearson.

White, C. (2015). **Data Communications and Computer Networks: A Business User's Approach. 8th Ed**. Boston: Cengage Learning

| | |
|---|---|
| **Module Code:** | **682/25/M03** |
| **Module Title:** | **COMPUTER ORGANISATION AND ARCHITECTURE** |
| **ZNQF Level:** | **5** |
| **Credits:** | 10 |
| **Duration:** | 100 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard Computer Organisation and Architecture of Qualification Standard for a Digital Forensic Technician. |
| **Pre-requisite modules:** | N/A |
| **Purpose of Module:** | This module describes the skills, knowledge, and attitudes required by an Digital Forensics Technician to understand the fundamental principles governing the internal structure and operation of computer systems. It aims to equip learners with the necessary expertise to analyze data representation, design basic assembly language programs, construct logic circuits, interpret processor diagrams, and diagnose hardware/software issues, providing a crucial foundation for advanced studies in operating systems, compilers, and embedded systems. |
| **List of Learning Outcomes:** | **LO1: Analyse how data is represented, stored, and manipulated within computer systems (binary, hexadecimal, signed and unsigned representations, floating point).**<br>**LO2: Design basic assembly language programs to demonstrate understanding of processor instruction sets and addressing modes.**<br>**LO3: Construct simple logic circuits and combinational logic designs using standard logic gates to implement basic arithmetic and logical operations.**<br>**LO4: Interpret processor organisation diagrams to identify data paths and control signal flows.**<br>**LO5: Diagnose and resolve hardware and software computer-related issues to ensure optimum computer operations.** |

| | |
|---|---|
| **Learning Outcome 01** | **ANALYSE HOW DATA IS REPRESENTED, STORED, AND MANIPULATED WITHIN COMPUTER SYSTEMS (BINARY, HEXADECIMAL, SIGNED AND UNSIGNED REPRESENTATIONS, FLOATING POINT)** |
| **Assessment Criteria:** | 1.1 Convert numbers between binary, decimal, and hexadecimal representations.<br>1.2 Explain signed and unsigned integer representations (e.g., Two's Complement).<br>1.3 Describe floating-point representation (e.g., IEEE 754 standard) and its implications.<br>1.4 Analyze how basic arithmetic operations are performed on binary data. |
| **Content:** | 1.1 Convert numbers between binary, decimal, and hexadecimal representations.<br>• Explain the differences between binary (base-2), decimal (base-10), and hexadecimal (base-16) number systems.<br>1.2 Explain signed and unsigned integer representations (e.g., Two's Complement).<br>• Convert positive and negative numbers to/from Two's Complement representation<br>• Explain the advantages of Two's Complement over other signed representations<br>• Calculate ranges for signed and unsigned integers of various bit widths<br>• Identify overflow conditions in signed arithmetic examples<br>• Compare and contrast all four representation methods with examples<br>1.3 Describe floating-point representation (e.g., IEEE 754 standard) and its implications.<br>• Explain the structure of IEEE 754 floating-point format<br>• Convert decimal numbers to IEEE 754 single precision format showing all steps<br>• Explain the purpose and function of each component (sign, exponent, mantissa)<br>• Identify and explain special values (zero, infinity, NaN) in binary |

| | |
|---|---|
| | representation<br>• Demonstrate understanding of precision limitations with practical examples<br>• Compare floating-point capabilities with fixed-point integer representations<br>1.4 Analyze how basic arithmetic operations are performed on binary data.<br>• Demonstrate binary addition, subtraction, multiplication, and division<br>• Identify overflow conditions and how they're handled in fixed-size registers<br>• Use bitwise operations to optimize arithmetic on low-level systems |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to analyze data representation as outlined in the assessment criteria and content above.<br>2. Practical exercises involving manual and tool-assisted conversions between number systems and demonstrating binary arithmetic. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 02** | **DESIGN BASIC ASSEMBLY LANGUAGE PROGRAMS TO DEMONSTRATE UNDERSTANDING OF PROCESSOR INSTRUCTION SETS AND ADDRESSING MODES.** |
|---|---|
| Assessment Criteria | 2.1 Identify and explain common processor instruction types (e.g., data transfer, arithmetic, logical, control flow).<br>2.2 Describe various addressing modes (e.g., immediate, register, direct, indirect).<br>2.3 Write simple assembly language programs to perform basic computational tasks.<br>2.4 Debug and trace the execution of short assembly language code segments. |

| | |
|---|---|
| Content | 2.1 Identify and explain common processor instruction types (e.g., data transfer, arithmetic, logical, control flow).<br>• **Explain** how data moves between registers, memory, and I/O devices<br>• Compare different data transfer methods (register-to-register vs memory-to-register)<br>• Analyze the efficiency implications of various data transfer operations<br>• **Explain** how arithmetic operations affect processor flags (carry, overflow, zero, sign)<br>• **Distinguish** between signed and unsigned arithmetic operations<br>• Classify given instructions into correct categories with justification<br>• Explain the purpose and effect of at least 3 instructions from each category<br>• Describe real-world scenarios where each instruction type would be used<br>• Compare and contrast the efficiency of different instruction types for specific tasks<br>2.2 Describe various addressing modes (e.g., immediate, register, direct, indirect).<br>• Given assembly instructions, identify the addressing mode used<br>• Explain the memory access pattern for each addressing mode<br>• Calculate effective addresses for different addressing modes<br>• Choose appropriate addressing modes for specific programming scenarios<br>• Trace instruction execution showing how operands are accessed<br>2.3 Write simple assembly language programs to perform basic computational tasks.<br>• Write complete assembly programs that compile and execute correctly<br>• Solve computational problems of increasing complexity |

| | |
|---|---|
| | • Document code with clear comments explaining the algorithm<br>2.4 Debug and trace the execution of short assembly language code segments.<br>• Complete accurate trace tables for given code segments (minimum 10-15 instructions)<br>• Identify and correct at least 3 different types of errors in buggy code<br>• Explain the root cause of each error found<br>• Demonstrate systematic debugging approach with clear documentation<br>• Verify corrected code produces expected results through testing |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to design basic assembly language programs as outlined in the assessment criteria.<br>2. Practical assessment involving writing, assembling, and executing simple assembly language programs using a simulator or development environment, demonstrating correct output and understanding of execution flow. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 03** | **CONSTRUCT LOGIC CIRCUITS AND COMBINATIONAL LOGIC DESIGNS USING STANDARD LOGIC GATES TO IMPLEMENT BASIC ARITHMETIC AND LOGICAL OPERATIONS.** |
|---|---|
| Assessment Criteria | 3.1 Identify and describe the function of basic logic gates (AND, OR, NOT, XOR, NAND, NOR).<br>3.2 Design and draw truth tables for simple combinational logic circuits.<br>3.3 Implement basic arithmetic (e.g., half-adder, full-adder) and logical operations using logic gates.<br>3.4 Utilize Boolean algebra and Karnaugh Maps (K-Maps) for circuit simplification. |
| Content | 3.1 Identify and describe the function of basic logic gates (AND, OR, NOT, XOR, NAND, NOR).<br>• Define basic logic gates and their functions<br>• Construct truth tables for each gate, showing all possible input combinations and their corresponding outputs.<br>• Provide real-world examples or applications where each type of gate might be used in digital circuits.<br>3.2 Design and draw truth tables for simple combinational logic circuits.<br>• Explain what a combinational logic circuit is and how it differs from sequential logic.<br>• Design and draw truth tables for simple circuits, ensuring all possible combinations of inputs are accounted for.<br>• Analyze the truth table to determine the behavior of the circuit under different input conditions.<br>3.3 Implement basic arithmetic (e.g., half-adder, full-adder) and logical operations using logic gates.<br>• Explain the purpose and function of basic arithmetic circuits like half-adders and full-adders.<br>• Draw circuit diagrams for half-adders and full-adders using appropriate logic gates.<br>• Create truth tables for half-adders and full-adders, showing how they compute sums and carries.<br>3.4 Utilize Boolean algebra and Karnaugh Maps (K-Maps) for |

| | |
|---|---|
| | circuit simplification.<br><br>• Define Boolean algebra and its significance in digital logic design<br>• Apply Boolean algebra laws (such as De Morgan's theorem, distributive law, etc.) to simplify logic expressions.<br>• Use K-Maps to find the simplest form of a logic function, minimizing the number of gates required.<br>• Convert simplified Boolean expressions back into logic circuit diagrams, demonstrating an understanding of the relationship between algebraic expressions and physical circuits. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to construct simple logic circuits and combinational logic designs as outlined in the assessment criteria.<br>2. Practical assessment involving designing and simulating logic circuits using digital logic simulation software or constructing physical circuits using breadboards and logic gate ICs (if available). |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 04** | **INTERPRET PROCESSOR ORGANISATION DIAGRAMS TO IDENTIFY DATA PATHS AND CONTROL SIGNAL FLOWS** |
|---|---|
| Assessment Criteria | 4.1 Identify the main components in a typical single-cycle or multi-cycle processor datapath diagram.<br>4.2 Trace the flow of data through the datapath for various instruction types (e.g., R-type, I-type, J-type).<br>4.3 Explain the role of control signals in directing data flow and operation execution.<br>4.4 Analyze how specific instructions are executed by examining the active components and control signals. |
| Content | 4.1 Identify the main components in a typical single-cycle or |

| | |
|---|---|
| | multi-cycle processor datapath diagram.<br>• Identify and label key components of a datapath<br>• Differentiate between single-cycle and multi-cycle datapaths<br>• Interpret diagrams and understand functional layout and interconnections<br>4.2 Trace the flow of data through the datapath for various instruction types (e.g., R-type, I-type, J-type).<br>• Describe the format and function of each instruction type<br>• Outline the path of data for each type from instruction fetch to execution<br>• Draw and annotate the data flow on a diagram or during simulation<br>4.3 Explain the role of control signals in directing data flow and operation execution.<br>• Outline the purpose of control signals (e.g., RegDst, ALUSrc, MemRead, MemWrite, Branch, Jump)<br>• Describe how control signals affect component behavior<br>• Interpret truth tables or control logic that determine signal outputs<br>4.4 Analyze how specific instructions are executed by examining the active components and control signals.<br>• Identify which components are used at each step, and their roles (e.g., ALU for address calculation, Data Memory for read)<br>• Choose specific instructions (e.g., ADD, SUB, LW, SW) and prepare to analyze their execution within the datapath.<br>• Analyze the control signals that are activated during the |

| | |
|---|---|
| | execution of the instruction, detailing how they direct the operation of the datapath.<br>• Discuss how the execution of different instructions may vary in terms of timing, resource usage, and efficiency, considering both single-cycle and multi-cycle datapath designs. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to interpret processor organization diagrams as outlined in the assessment criteria.<br>2. Practical assessment involving analyzing provided processor diagrams and tracing data paths for given instructions, or using a visual CPU simulator to observe data and control flow. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 05** | **DIAGNOSE AND RESOLVE HARDWARE AND SOFTWARE ISSUES RELATED TO COMPUTER ORGANIZATION AND ARCHITECTURE** |
|---|---|
| Assessment Criteria | 5.1 Identify common hardware components and their failure symptoms.<br>5.2 Utilize diagnostic tools to pinpoint hardware faults (e.g., memory, CPU, storage).<br>5.3 Troubleshoot software issues stemming from hardware-software interaction (e.g., drivers, operating system conflicts).<br>5.4 Propose and implement solutions for identified hardware and software problems. |
| Content | 5.1 Identify common hardware components and their failure symptoms.<br>• Outline the function and location of major computer components (CPU, RAM, Motherboard, Storage Devices - HDD/SSD, Power Supply Unit - PSU, Graphics Card - GPU, I/O ports)<br>• Describe common failure symptoms associated with a failing **CPU** (e.g., system freezes, blue screens of death (BSOD), no POST, overheating, random shutdowns).<br>• Describe failure symptoms associated with a failing **GPU** (e.g., no display, distorted video, artifacts on screen, system crashes during graphics-intensive tasks, fan noise).<br>• Explain POST (Power-On Self-Test) codes or beep codes to identify failing components during system startup.<br>5.2 Utilize diagnostic tools to pinpoint hardware faults (e.g., memory, CPU, storage).<br>• Outline operating system-level diagnostic tools for **storage devices** (e.g., Windows Disk Management, chkdsk, sfc /scannow, CrystalDiskInfo for S.M.A.R.T. data, manufacturer-specific diagnostic utilities)<br>• Evaluate system monitoring tools to observe CPU utilization, temperature, and fan speeds to identify overheating or throttling.<br>• Run a memory diagnostic tool and interpret its results to confirm RAM integrity<br>5.3 Troubleshoot software issues stemming from hardware-software interaction (e.g., drivers, operating system conflicts).<br>• Explain how operating system conflicts (e.g., incompatible software, corrupted system files, conflicting services) can manifest as performance issues or crashes. |

| | |
|---|---|
| | • Describe firmware (BIOS/UEFI, SSD firmware, GPU firmware) and its importance in hardware operation<br>• Explain the role of device drivers as the interface between hardware and the operating system.<br>• Perform driver updates, rollbacks, or clean installations<br>5.4 Propose and implement solutions for identified hardware and software problems.<br>• Describe how hardware solutions such as reseating components (RAM, expansion cards), replacing faulty cables, or swapping suspected faulty components (e.g., PSU, GPU, RAM) can be implemented.<br>• Evaluate software solutions such as uninstalling/reinstalling drivers, running system file checkers, performing operating system repairs/reinstallations, or configuring system settings<br>• Explain the process of escalation of a problem to a higher level of support or recommend professional repair/replacement if beyond their capability.<br>• Describe how to document the problem, diagnostic steps, solution implemented, and verification results clearly and concisely. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to diagnose and resolve hardware and software issues as outlined in the assessment criteria.<br>2. Practical assessment involving diagnosing simulated or real hardware/software faults on a test computer system and proposing/implementing appropriate solutions. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

**ASSESSMENT SCHEME**

| | MODE OF ASSESSMENT | | WEIGHTING 100% |
|---|---|---|---|
| | **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | |
| 1 | 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Analyse how data is represented, stored, and manipulated within computer systems (binary, hexadecimal, signed and unsigned representations, floating point). | 20 |
| Design basic assembly language programs to demonstrate understanding of processor instruction sets and addressing modes. | 25 |
| Construct simple logic circuits and combinational logic designs using standard logic gates to implement basic arithmetic and logical operations. | 20 |
| Interpret processor organisation diagrams to identify data paths and control signal flows. | 15 |
| Diagnose and resolve hardware and software issues related to computer organization and architecture. | 20 |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

   **Facilities:**

   - Computer Lab: Equipped with modern computers capable of running simulation software and IDEs.
   - Network Environment: Standard classroom network connectivity.
   - Physical Security: Secure environment for equipment.
   - Adequate Power & Cooling: To support computing equipment.
   - Lecture/Training Rooms: Equipped with projectors/large displays, whiteboards, and network connectivity.

   **Tools (Software):**

   - Operating Systems: Windows 10/11, Linux distributions (e.g., Ubuntu).
   - CPU Simulators: MARS (MIPS Assembler and Runtime Simulator), Logisim (for digital logic circuits and basic CPU design), SPIM (MIPS simulator), or similar tools.
   - Assembly Language IDEs/Assemblers: NASM, MASM (for x86 assembly), or integrated development environments that support assembly language.
   - Digital Logic Simulation Software: Logisim, CircuitVerse, or similar.
   - System Performance Monitoring Tools: Task Manager (Windows), `top`/`htop`/`perf` (Linux) for observing CPU, memory, and I/O usage.
   - Programming Editors/IDEs: VS Code, Sublime Text, Notepad++.
   - Reporting Tools: Microsoft Office Suite, LibreOffice.

   **Equipment (Hardware):**

   - Standard Desktop/Laptop Computers: Sufficient for all students.
   - Demonstration Hardware: Disassembled computer components (motherboards, CPUs, RAM modules, expansion cards) for visual and hands-on identification.
   - Basic Digital Logic Kits (Optional but Recommended): Breadboards, various logic gate ICs (e.g., 74LS series), LEDs, resistors for practical circuit construction.
   - Diagnostic Hardware: Multimeters, POST card testers (optional).
   - External Storage Devices: USB drives for file transfer and backup.

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 4. Reference Materials (recommended textbooks, recommended readings)

Patterson, D.A. and Hennessy, J.L. (2018) **Computer Organization and Design RISC-V Edition: The Hardware/Software Interface.** 2nd edn. Morgan Kaufmann.

Stallings, W. (2020) **Computer Organization and Architecture: Designing for Performance.** 11th edn. Pearson.

Hamacher, V.C., Vranesic, Z.G. and Zaky, S.G. (2011) **Computer Organization**. 6th edn. McGraw-Hill Education.

Tanenbaum, A.S. and Austin, T. (2012) **Structured Computer Organization**. 6th edn. Pearson.

Stallings, W. (2020) **Computer Organization and Architecture: Designing for Performance.** 11th edn. Pearson.

Online resources such as NPTEL lectures, MIT OpenCourseware, and relevant academic journals.

| | |
|---|---|
| **Module code:** | **682/25/M04** |
| **Module title:** | **Legal Aspects in Digital Forensics** |
| **ZNQF level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 |
| **Relationship with qualification standards:** | Based on Unit Standard Legal Aspects in Digital Forensics of Unit Standards for a Digital Forensics Technician |
| **Pre-requisite modules:** | No prerequisites |
| **Purpose of module:** | This module describes the skills, knowledge and attitudes required by an individual to be able to apply data privacy laws, maintain chain of custody, produce admissible evidence handling, apply cybersecurity regulations, notify incident response and breach**.**<br>This module is important as it ensures that evidence is collected, handled, analysed, and presented in a way that is admissible in court. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of learning outcomes:** | **LO1: Demonstrate adherence to data privacy laws by implementing appropriate measures in data handling practices.**<br>**LO2: Maintain the chain of custody for evidence by accurately documenting and securing materials throughout the investigative process.**<br>**LO3: Produce admissible evidence by following established protocols for evidence handling and documentation.**<br>**LO4: Conduct risk assessments and implement necessary security measures by applying cybersecurity regulations effectively.**<br>**LO5: Notify incident response teams and report breaches promptly by following organizational protocols for incident management.** |

| Learning outcome 01 | Demonstrate adherence to data privacy laws by implementing appropriate measures in data handling practices |
|---|---|
| **Assessment criteria:** | **1.1 Obtain consent for data collection and processing.**<br>**1.2 Implement data minimization and purpose limitation.**<br>**1.3 Ensure data subject rights.**<br>**1.4 Report data breaches within mandated timeframes.**<br>**1.5 Conduct Data Protection Impact Assessments (DPIAs).** |
| **Content:** | **1.1 Obtain consent for data collection and processing.**<br>● Define the need for explicit consent under Zimbabwean and international data privacy laws.<br>● Explain the informed consent process, ensuring transparency (e.g., GDPR, Zimbabwe's Data Protection Act).<br>● Outline steps to document and secure consent.<br>● Describe consequences of non-compliance with consent requirements.<br>**1.2 Implement data minimization and purpose limitation.**<br>● Define data minimization and purpose limitation under Zimbabwean and international laws.<br>● Explain collecting only necessary data for specified purposes.<br>● Outline using data solely for its intended purpose.<br>● Describe legal consequences of non-compliance.<br>**1.3 Ensure data subject rights.**<br>● Define data subject rights under Zimbabwean and international data privacy laws (e.g., right to access, rectification, and deletion).<br>● Explain how individuals can exercise their rights to control their personal data.<br>● Outline procedures to ensure data subjects' rights are respected and upheld.<br>● Describe legal obligations for organizations to facilitate these rights.<br>**1.4 Report data breaches within mandated timeframes.**<br>● Define the requirement to report data breaches within mandated timeframes under Zimbabwean and international laws (e.g., GDPR).<br>● Explain the process of identifying, assessing, and reporting a data breach promptly.<br>● Outline the legal timeframes for breach notifications and the information that must be included.<br>● Describe the consequences of failing to report breaches within the required timelines.<br>**1.5 Conduct Data Protection Impact Assessments (DPIAs).** |

| | |
|---|---|
| | ● Define Data Protection Impact Assessments (DPIAs) as a process to assess risks to data privacy under Zimbabwean and international laws (e.g., GDPR).<br>● Explain when and why DPIAs are required, particularly for high-risk data processing activities.<br>● Outline the steps to conduct a DPIA, including identifying risks and implementing mitigation measures.<br>● Describe the legal implications of failing to conduct DPIAs in compliance with data privacy regulations. |
| | **1.** Written and/or oral assessment on the skills and knowledge required to obtain consent for data collection and processing, implement data minimization and purpose limitation, ensure data subject rights, report data breaches within mandated timeframes and conduct Data Protection Impact Assessments (DPIAs) as outlined in the assessment criteria.<br>**2.** Practical assessment on implementing data minimization and purpose limitation, reporting data breaches, and conducting Data Protection Impact Assessments (DPIAs) based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below: -<br>- |

| **Learning outcome 02** | **Maintain the chain of custody for evidence by accurately documenting and securing materials throughout the investigative process** |
|---|---|
| **Assessment criteria** | **2.1 Record events**<br>**2.2 Secure data storage devices**<br>**2.3 Use cryptographic hashing**<br>**2.4 Maintain access logs**<br>**2.5 Use tamper-evident seals**<br>**2.6 Ensure secure transportation of evidence.**<br>**2.7 Conduct regular verification of evidence integrity.**<br>**2.8 Maintain Audit Trails.**<br>**2.9 Adhere to Legal standards for admissibility.**<br>**2.10 Prepare expert testimony** |

| | |
|---|---|
| **Content** | **2.1 Record events**<br>● Define event recording as documenting actions during evidence handling to maintain chain of custody.<br>● Explain its importance for evidence integrity and legal admissibility.<br>● Outline key details to record, such as timestamps and actions taken.<br>● Describe the consequences of improper event recording on evidence credibility.<br>**2.2 Secure data storage devices**<br>● Define secure data storage as the practice of protecting data storage devices from unauthorized access or tampering.<br>● Explain the methods for securing storage devices, including encryption and physical safeguards, in compliance with Zimbabwean and international laws.<br>● Outline the importance of secure storage in maintaining a chain of custody and ensuring evidence integrity.<br>● Describe the legal consequences of failing to secure data storage devices properly.<br>**2.3 Use cryptographic hashing**<br>● Define cryptographic hashing as a method for verifying data integrity.<br>● Explain its role in maintaining the chain of custody by detecting alterations.<br>● Outline common hashing algorithms (e.g., MD5, SHA-256).<br>● Describe its forensic and legal importance in digital evidence authentication.<br>**2.4 Maintain access logs**<br>● Define access logs as records documenting all interactions with digital evidence.<br>● Explain their role in tracking who accessed data, when, and for what purpose.<br>● Outline best practices for maintaining accurate and tamper-proof logs.<br>● Describe the legal importance of access logs in ensuring evidence integrity and admissibility.<br>**2.5 Use tamper-evident seals**<br>● Define tamper-evident seals as security measures that indicate unauthorized access to evidence.<br>● Explain their role in protecting digital evidence integrity within the chain of custody.<br>● Outline best practices for applying and documenting tamper-evident seals.<br>● Describe legal implications of compromised seals under Zimbabwean and international laws.<br>**2.6 Ensure secure transportation of evidence.**<br>● Define secure transportation as the process of safely transferring |

| | |
|---|---|
| | evidence while preventing tampering or loss.<br>● Explain methods for ensuring security, including sealed containers, tracking, and authorized handlers.<br>● Outline best practices for documenting evidence movement to maintain chain of custody.<br>● Describe legal requirements for evidence transportation under Zimbabwean and international laws.<br>**2.7 Conduct regular verification of evidence integrity.**<br>● Define evidence integrity verification as periodic checks to ensure data remains unaltered.<br>● Explain methods like cryptographic hashing and audit trails for verifying integrity.<br>● Outline best practices for conducting regular verification and documentation.<br>● Describe legal implications of compromised evidence under Zimbabwean and international laws.<br>**2.8 Maintain audit trails.**<br>● Define audit trails as chronological records tracking all actions on digital evidence.<br>● Explain their role in ensuring accountability and transparency in the chain of custody.<br>● Outline best practices for maintaining accurate, tamper-proof audit logs.<br>● Describe legal requirements for audit trails under Zimbabwean and international laws.<br>**2.9 Adhere to Legal standards for admissibility.**<br>● Define legal admissibility as the criteria the evidence must meet to be accepted in court.<br>● Explain key standards, including authenticity, reliability, and integrity, under Zimbabwean and international laws.<br>● Outline best practices for handling and documenting evidence to ensure admissibility.<br>● Describe the consequences of failing to meet legal standards, such as evidence being ruled inadmissible.<br>**2.10 Prepare expert testimony**<br>● Define expert testimony as a specialist's presentation of technical findings in legal proceedings.<br>● Explain the role of digital forensic experts in validating evidence integrity.<br>● Outline key elements of preparing testimony, including clarity, accuracy, and adherence to legal standards.<br>● Describe best practices for presenting forensic evidence in court under Zimbabwean and international laws. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to record events, secure data storage devices, use cryptographic hashing, maintain access logs, use tamper-evident seals, ensure secure |

| | |
|---|---|
| | transportation of evidence, conduct regular verification of evidence integrity, maintain audit trails, adhere to legal standards for admissibility, and prepare expert testimony as outlined in the assessment criteria.<br>2. Practical assessment on recording events, securing storage devices, using cryptographic hashing, maintaining access logs, conducting regular verification of evidence, maintaining audit trails and preparing expert testimonies based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: |

| **Learning outcome 03** | **Produce admissible evidence by following established protocols for evidence handling and documentation** |
|---|---|
| **Assessment criteria** | **3.1 Create forensic images**<br>**3.2 Use write-blocking**<br>**3.3 Preserve metadata**<br>**3.4 Obtain legal authority**<br>**3.5 Validate findings using multiple tools or methods.**<br>**3.6 Present evidence.**<br>**3.7 Apply standards compliance**<br>**3.8 Prepare court presentation** |
| **Content** | **3.1 Create forensic images**<br>● Define forensic imaging as the process of creating an exact, bit-by-bit copy of digital storage media.<br>● Explain the importance of forensic images in preserving data integrity and ensuring admissibility in court.<br>● Describe tools like EnCase, FTK Imager, and dd for forensic imaging.<br>● Outline best practices, including write-blocking, hash verification, and chain of custody documentation.<br>● Analyse legal requirements in Zimbabwe and international frameworks (e.g., GDPR, ISO 27037) for forensic imaging.<br>**3.2 Use write-blocking**<br>● Define write-blocking as a method to prevent data modification |

during forensic imaging.

- Explain its importance in maintaining evidence integrity and admissibility.
- Describe hardware and software write-blockers (e.g., Tableau, WiebeTech, Windows Diskpart).
- Outline best practices for using write-blockers in forensic investigations.
- Analyze legal and regulatory requirements for write-blocking under Zimbabwean laws and international standards (e.g., ISO 27037, GDPR).

**3.3 Preserve metadata**

- Define metadata as critical information about digital files (e.g., timestamps, file origins).
- Explain its role in maintaining data authenticity and forensic integrity.
- Describe methods for preserving metadata, such as forensic imaging and hashing.
- Outline best practices to prevent unintentional metadata alteration.
- Analyze compliance with Zimbabwean and international forensic standards (e.g., ISO 27037, GDPR).
- Analyze legal and forensic requirements for preserving metadata under Zimbabwean laws and international standards (e.g., ISO 27037, GDPR).

**3.4 Obtain Legal Authority**

- Define legal authority requirements for evidence collection under Zimbabwean and international laws.
- Explain the importance of warrants, court orders, or consent in digital forensic investigations.
- Outline procedures for obtaining legal authorization to ensure evidence admissibility.
- Outline the process for obtaining legal authority, including obtaining warrants or court orders, to ensure the evidence is legally admissible.

**3.5 Validate findings using multiple tools or methods.**

- Define validation as the process of confirming findings using multiple forensic tools or methods.
- Explain the importance of cross-validating results to ensure evidence reliability and admissibility.
- Describe common tools and methods for validation, such as EnCase, FTK, and hash verification.
- Outline the benefits of using multiple tools to comply with legal standards for admissible evidence.

| | |
|---|---|
| | **3.6 Present evidence.**<br>● Define presenting evidence as the process of clearly and accurately communicating forensic findings in legal proceedings.<br>● Explain the importance of adhering to legal standards and maintaining the integrity of evidence during presentation.<br>● Describe methods for presenting evidence, such as clear documentation, visual aids, and expert testimony.<br>● Outline the steps to ensure evidence presentation complies with Zimbabwean and international legal standards (e.g., ISO 27037, GDPR).<br>**3.7 Apply standards compliance**<br>● Define standards compliance as adherence to legal and procedural guidelines for handling digital evidence.<br>● Explain the importance of following established standards to ensure evidence admissibility in court.<br>● Describe key standards such as ISO 27037, GDPR, and Zimbabwean data protection laws.<br>● Outline steps to ensure compliance with relevant standards during evidence collection and handling.<br>**3.8 Prepare Court Presentation**<br>● Define key elements of a forensic court presentation.<br>● Explain the importance of clear and factual reporting.<br>● Describe best practices for structuring forensic findings.<br>● Outline steps for expert witness testimony.<br>● Analyse past case presentations for improvements. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to create forensic images, use write-blocking, preserve metadata, obtain legal authority, validate findings using multiple tools or methods, present evidence, apply standards compliance, and prepare court presentations as outlined in the assessment criteria.<br>2. Practical assessment on creating forensic images, write-blocking, preserving metadata, presenting evidence, preparing court presentations and validating findings based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>- |

| Learning outcome 04 | **Conduct risk assessments and implement necessary security measures by applying cybersecurity regulations effectively** |
|---|---|
| **Assessment criteria** | **4.1 Conduct Regular risk assessments.**<br>**4.2 Implement Access controls and encryption.**<br>**4.3 Monitor and log Network activity.**<br>**4.4 Develop Test incident response plans.**<br>**4.5 Train Employees on cybersecurity best practices.** |
| **Content** | **4.1 Conduct Regular risk assessments.**<br>● Define regular risk assessments as the ongoing process of identifying, evaluating, and mitigating cybersecurity threats to ensure compliance with legal requirements.<br>● Explain the importance of assessing risks regularly to stay compliant with cybersecurity regulations such as Zimbabwe's Cyber and Data Protection Act of 2021 and international laws like GDPR.<br>● Describe methods for conducting risk assessments, including threat analysis, vulnerability scanning, and risk prioritization.<br>● Outline key steps to apply in risk assessments to ensure that cybersecurity practices align with both Zimbabwean and global cybersecurity regulations.<br>**4.2 Implement Access controls and encryption.**<br>● Define access controls as methods to restrict unauthorized access, ensuring regulatory compliance.<br>● Explain encryption's role in protecting sensitive data, as required by Zimbabwe's Cyber and Data Protection Act and international laws like GDPR.<br>● Describe access control types (role-based, multi-factor) and encryption methods (AES, SSL/TLS).<br>● Outline steps to implement these measures for data protection and compliance.<br>● Outline the process of implementing access controls and encryption, ensuring data protection through proper configuration, monitoring, and regular updates to comply with both Zimbabwean and international regulations.<br>**4.3 Monitor and log Network activity.**<br>● Define the role of network monitoring in detecting cyber threats and ensuring compliance with Zimbabwean and international laws.<br>● Explain tools used for analyzing network traffic and logs to identify security risks.<br>● Describe best practices for maintaining logs to comply with legal requirements and ensure data integrity.<br>**4.4 Develop Test incident response plans.**<br>● Define the key components of an incident response plan, including |

| | |
|---|---|
| | roles, responsibilities, and procedures for responding to cybersecurity incidents.<br>● Outline the steps to develop and test an incident response plan, ensuring compliance with Zimbabwean and international regulations.<br>● Describe methods for simulating incidents to assess the effectiveness of the response plan and improve readiness.<br>**4.5 Train Employees on cybersecurity best practices.**<br>● Define key cybersecurity best practices, such as strong password management, safe browsing habits, and recognizing phishing attempts.<br>● Explain the importance of employee training in preventing cyber threats and complying with Zimbabwean and international cybersecurity regulations.<br>● Outline a training program that covers relevant topics like data protection, access control, and incident reporting procedures. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to conduct regular risk assessments, implement access controls and encryption, monitor and log network activity, develop test incident response plans, and train employees on cybersecurity best practices as outlined in the assessment criteria.<br>2. Practical assessment on conducting risk assessments, implementing access controls, monitoring and logging network activity, and training employees on cybersecurity best practices based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>- |

| Learning outcome 05 | **Notify incident response teams and report breaches promptly by following organizational protocols for incident management** |
|---|---|
| **Assessment criteria** | **5.1 Develop an incident response plan.**<br>**5.2 Identify and contain breaches.**<br>**5.3 Notify affected individuals and regulators.**<br>**5.4 Conduct post-incident reviews.**<br>**5.5 Update policies and procedures based on lessons learned.** |
| **Content** | **5.1 Develop an incident response plan.**<br>● Define the purpose and scope of an incident response plan, ensuring compliance with Zimbabwe's Cyber and Data Protection Act and global standards like GDPR.<br>● Explain key components such as detection, containment, and recovery.<br>**5.2 Identify and contain breaches.**<br>● Define breach identification criteria, referencing global standards like GDPR and Zimbabwe's Cyber and Data Protection Act.<br>● Analyse evidence to confirm a breach and evaluate its scope.<br>● Explain containment strategies, ensuring they align with legal requirements to prevent further exposure.<br>**5.3 Notify affected individuals and regulators.**<br>● Define the criteria for notifying affected individuals and regulators, ensuring compliance with the Cyber and Data Protection Act of Zimbabwe and GDPR.<br>● Analyze the breach's impact on individuals and assess the urgency of the notification process.<br>● Explain the legal timelines and requirements for notifying affected individuals (e.g., within 72 hours under GDPR).<br>● Outline the information to be provided in the notification, ensuring transparency and clarity on the breach and its potential consequences.<br>**5.1 Conduct post-incident reviews.**<br>● Define the process for conducting post-incident reviews, focusing on lessons learned and improvements.<br>● Analyze the effectiveness of the incident response, identifying gaps and areas of improvement.<br>● Explain the importance of reviewing response protocols for future breach prevention.<br>● Outline necessary documentation and reporting, ensuring compliance with local and international laws (e.g., Zimbabwe's Cyber and Data Protection Act, GDPR).<br>**5.2 Update policies and procedures based on lessons learned.**<br>● Define the process for updating cybersecurity policies and |

| | |
|---|---|
| | procedures based on insights gained from incident reviews.<br>● Analyze identified weaknesses or gaps from past breaches and incorporate improvements into policies.<br>● Explain the need for continuous policy evolution to address emerging threats and ensure legal compliance (e.g., Zimbabwe's Cyber and Data Protection Act, GDPR).<br>● Outline the steps to revise procedures, including stakeholder input, testing, and final approval for implementation. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to develop an incident response plan, identify and contain breaches, notify affected individuals and regulators, conduct post-incident reviews, and update policies and procedures based on lessons learned as outlined in the assessment criteria.<br>2. Practical assessment on developing an incident response plan, conducting post-incident reviews and updating policies and procedures based on lessons learnt based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>- |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| **Demonstrate adherence to data privacy laws by implementing appropriate measures in data handling practices** | **20%** |
| **Maintain the chain of custody for evidence by accurately documenting and securing materials throughout the investigative process** | **20%** |
| **Produce admissible evidence by following established protocols for evidence handling and documentation** | **20%** |
| **Conduct risk assessments and implement necessary security measures by applying cybersecurity regulations effectively** | **20%** |
| **Notify incident response teams and report breaches promptly by following organizational protocols for incident management** | **20%** |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

## 2. Facilities, Tools, Equipment and Materials

### Facilities

1. **Standard Classroom/Lecture Theatre:**
    - **Layout:** Flexible seating arrangements to facilitate lectures, group discussions, and role-playing exercises (e.g., mock court scenarios).
    - **Audiovisual Equipment:** Projector/large display, sound system, and whiteboard/smart board for presentations and collaborative brainstorming.
    - **Internet Connectivity:** Reliable internet access for research, accessing legal databases, and online resources.
2. **Moot Courtroom (Optional but Highly Recommended):**
    - A dedicated space designed to simulate a courtroom environment. This is invaluable for practicing expert witness testimony, cross-examination, and understanding courtroom procedures.
3. **Computer Lab (General Purpose):**
    - Access to a general computer lab for individual research, report writing, and accessing legal databases. High-end forensic workstations are not typically required for this specific module, but standard office productivity machines are.

### Tools (Software)

1. Productivity Software:
    - Word Processing: Microsoft Word, LibreOffice Writer for drafting reports, affidavits, and legal documents.
    - Spreadsheet Software: Microsoft Excel, LibreOffice Calc for organizing case data, timelines, and evidence logs.
    - Presentation Software: Microsoft PowerPoint, LibreOffice Impress for preparing expert witness presentations and training materials.
    - PDF Editors: For reviewing and annotating legal documents and reports.
2. Communication & Collaboration Tools:
    - Video Conferencing Software: Zoom, Microsoft Teams, Google Meet for remote guest lectures, mock depositions, or collaborative discussions.
    - Learning Management System (LMS): Moodle, Canvas, Google Classroom for distributing course materials, submitting assignments, and facilitating online discussions.
3. Legal Research & Case Management Software (Optional/Demonstration):
    - Access to legal research databases (e.g., LexisNexis, Westlaw - if available and relevant to jurisdiction).
    - Demonstration versions of digital forensics case management software (e.g., Case IQ, Axon Investigate) to show how evidence is tracked legally.

4. Specialized Documentation Tools:
    - Software for creating and managing evidence logs, chain of custody forms, and forensic reports templates.

## Equipment (Hardware)

1. Instructor Workstation:
    - Standard desktop/laptop with internet connectivity, capable of running all required software and connecting to classroom AV equipment.
2. Student Workstations:
    - Standard desktop/laptop computers for each student (or pair) with internet access and productivity software.
3. Printers/Scanners:
    - For printing legal documents, reports, and scanning physical evidence or documentation.
4. Projector/Large Display:
    - For lectures, presentations, and displaying legal documents or case studies.
5. Audio Recording Equipment (Optional):
    - For recording mock court sessions or expert witness testimony practice for review and feedback.
6. Basic Office Supplies:
    - Whiteboards, markers, flip charts for brainstorming and outlining legal concepts.

## Materials

1. Legal & Regulatory Documents:
    - Relevant National Cybercrime Laws: Specific acts, statutes, and amendments related to digital evidence, computer misuse, data protection, and privacy in the relevant jurisdiction.
    - International Laws & Treaties: (e.g., Budapest Convention on Cybercrime) where applicable.
    - Rules of Evidence: Specific rules governing the admissibility of digital evidence in court.
    - Data Protection Regulations: (e.g., GDPR, HIPAA, local equivalents) relevant to handling sensitive data.
    - Industry Standards & Guidelines: (e.g., NIST publications on digital evidence, ISO standards for information security management) that have legal implications.
2. Case Studies & Precedents:
    - Real-world Digital Forensics Cases: Anonymized or publicly available case summaries that highlight legal challenges, successful prosecutions, or landmark rulings involving digital evidence.
    - Mock Case Files: Hypothetical scenarios designed for students to practice applying legal principles.
3. Templates & Forms:
    - Chain of Custody Forms: Blank and completed examples.
    - Evidence Log Sheets:
    - Forensic Report Templates: Structured templates that meet legal requirements.
    - Affidavit/Declaration Templates:
    - Search Warrant Examples: (if relevant to the curriculum).

4. Expert Witness Testimony Resources:
    - Sample expert witness reports.
    - Videos of actual or mock expert witness testimony (for analysis).
    - Checklists for preparing for deposition and trial testimony.
5. Ethical Guidelines:
    - Professional codes of conduct for digital forensics practitioners.
    - Discussions on ethical dilemmas specific to digital forensics (e.g., privacy vs. investigation, scope creep).

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 4. Reference Materials (recommended textbooks, recommended readings)

Ryan, D.J. and Shpantzer, G., 2008. *Legal Aspects of Digital Forensics*. Carnegie Mellon University.
Aleke, N.T. and Trigui, M., 2025. *Legal and Ethical Challenges in Digital Forensics Investigations*. Illinois Institute of Technology. In: IGI Global
Maratsi, M.I., Popov, O., Alexopoulos, C. and Charalabidis, Y., 2022. *Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition*. In: ICEGOV 2022, Guimarães, Portugal. ACM.
Ofori, A.Y. and Akoto, D., 2020. *Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence*. *Journal of Forensic Legal & Investigative Sciences*, [online]
Sammons, J., 2014. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2nd ed. Syngress.

Casey, E., 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd ed. Academic Press.

| | |
|---|---|
| **Module Code:** | **682/25/M05** |
| **Module Title:** | **COMPUTER FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 hours |
| **Relationship with Unit Standard** | Based on Unit Standard **Computer Forensics** of Unit Standards for a Digital Forensic Technician. |
| **Pre-requisite modules:** | NONE |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an **individual** to be able to effectively communicate in business. This includes demonstrating knowledge of computer forensics concepts and principles, acquiring memory, analyzing memory, detecting and analyze malware present in memory, applying advanced techniques to uncover sophisticated threats, utilizing automated tools in memory forensics and providing Incident Response for memory forensics<br>.<br>This module is important as it helps detecting, analysing, and mitigating cyber threats by uncovering volatile evidence, such as malware, encryption keys, and unauthorized activities, that traditional forensic methods may miss. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of Learning Outcomes:** | **LO1: Demonstrate knowledge of computer hardware, software, and file systems by accurately identifying components, functions, and interrelationships, demonstrating a comprehensive understanding of foundational computing principles.**<br>**LO2: Ensure integrity and compliance in all aspects of digital evidence handling and reporting by adhering to legal and ethical standards in computer forensics.**<br>**LO3: Preserve evidence integrity and admissibility in legal proceedings by employing forensically sound methods and tools for digital evidence acquisition.**<br>**LO4: Recover and analyze digital evidence from storage media by utilizing specialized software and techniques for extracting, reconstructing, and interpreting data from fragmented or hidden digital artifacts.** |

| | |
|---|---|
| | **LO5: Dissect and observe malware functionalities in identifying attack vectors, propagation mechanisms, and potential damages caused by malicious code by analyzing malicious software through reverse engineering techniques and sandbox environments.**<br>**LO6: Reconstruct attack timelines and identify compromised systems within a network environment by using network forensic tools and methodologies in detecting, containing, and eradicating threats.**<br>**LO7: Communicate complex technical information by preparing clear and concise forensic reports by documenting findings, methodologies, and conclusions in a structured and objective manner.**<br>**LO8: Respond to incidents involving computer systems by applying legal frameworks and forensic protocols to identify, preserve, analyze, and report digital evidence in accordance with admissibility standards and regulatory requirements** |

| | |
|---|---|
| **Learning Outcome 01** | **Demonstrate knowledge of computer hardware, software, and file systems by accurately identifying components, functions, and interrelationships, demonstrating a comprehensive understanding of foundational computing principles** |
| **Assessment Criteria:** | **1.1 Identify computer system components**<br>**1.2 Explain structure and functioning of common file systems**<br>**1.3 Describe how data is stored, accessed, and deleted on storage media** |
| **Content:** | **1.1 Identify computer system components**<br>● Define the key components of a computer system<br>● Classify hardware components based on their functions<br>● Examine the role of each component in the overall functioning of a computer system.<br>● Compare the performance and functionality of different types of hardware components (e.g., HDD vs. SSD).<br>● Investigate how hardware advancements have influenced system design and capabilities.<br>● Illustrate the differences between volatile and non-volatile memory with examples.<br><br>**1.2 Explain the structure and functioning of common file systems**<br>● Describe the concept of a file system and its purpose in managing data on storage media.<br>● Analyse the structure and organization of common file systems such as NTFS, FAT32, ext4, and APFS.<br>● Explain how file systems handle data storage, retrieval, and management.<br>● Evaluate the advantages and limitations of different file systems in various use cases.<br>● Discuss the role of metadata in file systems and its importance for data integrity.<br>● Outline the process of file allocation and directory management in a file system.<br><br>**1.3 Describe how data is stored, accessed, and deleted on storage media**<br>● Identify the processes involved in data storage.<br>● Explore the mechanisms used by storage media (e.g., HDDs, SSDs) to read and write data.<br>● Assess the differences between logical and physical storage and their relevance in data management.<br>● Clarify how data is accessed by the operating system and applications, including the role of file pointers and directories.<br>● Review the implications of data deletion and overwriting for data recovery.<br>● Summarize the lifecycle of data on storage media, from creation |

| | |
|---|---|
| | to deletion. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to identify computer system components, explain structure and functioning of common file systems, describe how data is stored and accessed, and deleted on storage media as outlined in the assessment criteria.<br>2. Practical assessment on identifying computer system components, explaining structure and functioning of common file systems and describing how data is stored, accessed, and deleted on storage media based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:-<br><br>CPU-Z, HWiNFO, Speccy, CrystalDiskInfo, GParted, MiniTool Partition Wizard, File Explorer (Windows), Finder (macOS), Linux File Managers (e.g., Nautilus), Hex Editors (e.g., HxD), Disk Management Tools (e.g., Windows Disk Management), Registry Editor (Windows), Terminal/Command Line Tools (e.g., Linux Terminal, Windows Command Prompt), Virtual Machines (e.g., VMware, VirtualBox), BIOS/UEFI Interfaces<br><br>**2.1.1 Materials:**<br><br>Computer hardware components (e.g., CPUs, RAM, motherboards, storage devices), operating system installation media (e.g., Windows, Linux, macOS), file system documentation (e.g., NTFS, FAT32, ext4, APFS), training manuals and guides, hardware diagnostic tools, system monitoring software, case studies, collaboration platforms (e.g., Slack, Teams), report templates, legal and compliance guidelines, virtual machine images, forensic workstations |

| | |
|---|---|
| **Learning Outcome 02** | **Ensure integrity and compliance in all aspects of digital evidence handling and reporting by adhering to legal and ethical standards in computer forensics** |
| **Assessment Criteria** | **2.1 Follow chain of custody procedures to ensure evidence admissibility in court.**<br>**2.2 Ensure compliance with relevant laws and regulations.**<br>**2.3 Obtain authorization before accessing and analysing digital evidence.** |
| **Content** | **3.5 Follow chain of custody procedures to ensure evidence admissibility in court**<br>● Define the concept of chain of custody and its significance in computer forensics.<br>● Analyse the role of chain of custody in maintaining the integrity and admissibility of digital evidence in legal proceedings.<br>● Describe the steps involved in establishing and documenting a chain of custody.<br>● Explain how breaches in the chain of custody can compromise the validity of evidence and impact forensic investigations.<br>● Outline best practices for maintaining a secure and unbroken chain of custody throughout an investigation.<br>**3.6 Ensure compliance with relevant laws and regulations**<br>● Define the legal frameworks and regulations (e.g., GDPR, HIPPA) that govern computer forensics.<br>● Analyse the importance of compliance with laws and regulations in ensuring the legality and ethicality of forensic practices.<br>● Describe the potential consequences of non-compliance.<br>● Explain how forensic investigators can stay updated on evolving laws and regulations to ensure ongoing compliance.<br>● Outline the key legal considerations when handling sensitive or personally identifiable information (PII) during investigations.<br>**3.7 Obtain authorization before accessing and analysing digital** |

| | |
|---|---|
| | **evidence**<br>● Define the concept of authorization and its role in ethical and legal forensic investigations.<br>● Analyse the ethical implications of accessing and analysing digital evidence without proper authorization.<br>● Describe the process of obtaining legal permissions.<br>● Explain how unauthorized access to digital systems can lead to legal challenges and reputational damage.<br>● Outline the documentation required to prove authorization and ensure accountability during forensic investigations. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to follow the chain of custody procedures to ensure evidence admissibility in court, ensure compliance with relevant laws and regulations and obtain authorization before accessing and analyzing digital evidence as outlined in the assessment criteria and content above.<br>2. Practical assessment on following the chain of custody procedures to ensure evidence admissibility in court, ensuring compliance with relevant laws and regulations and obtaining authorization before accessing and analyzing digital evidence based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below: -<br>Legal Tools and Materials (eg. Data Protection Act, NIST) and Ethical Tools and Materials (e.g., ACM Code of Ethics, IEEE Code of Ethics) |

| Learning Outcome 03 | **Preserve evidence integrity and admissibility in legal proceedings by employing forensically sound methods and tools for digital evidence acquisition** |
|---|---|
| **Assessment Criteria** | **3.1 Employ write-blocking tools to prevent data alteration during acquisition.**<br>**3.2 Create forensic images of storage devices.**<br>**3.3 Document evidence acquisition process documented**<br>**3.4 Verify the integrity of acquired evidence using hashing algorithms** |
| **Content** | **3.1 Employ write-blocking tools to prevent data alteration during acquisition**<br>● Clarify the purpose of write-blocking tools in digital forensics and their role in preserving evidence integrity.<br>● Compare hardware-based and software-based write-blockers, highlighting their respective strengths and weaknesses.<br>● Illustrate how write-blocking tools interact with storage devices to ensure no data modification occurs during acquisition.<br>● Identify scenarios where write-blocking tools are indispensable, such as acquiring evidence from SSDs or USB devices.<br>● Highlight the risks associated with not using write-blocking tools, including data corruption and compromised evidence.<br>**3.2 Create forensic images of storage devices**<br>● Characterize forensic imaging as the process of creating an exact, bit-by-bit copy of a storage device.<br>● Evaluate the effectiveness of tools like FTK Imager, dd, and Guymager for imaging different types of storage media.<br>● Demonstrate the steps involved in creating a forensic image, from device connection to image storage.<br>● Recognize the challenges of imaging large or encrypted devices and propose solutions to address them.<br>● Emphasize the importance of maintaining a chain of custody during the imaging process to uphold evidence integrity. |

| | |
|---|---|
| | **3.3 Document evidence acquisition process**<br>● Articulate the significance of documentation in ensuring transparency and accountability during evidence acquisition.<br>● Examine the essential components of documentation, such as timestamps, tools used, and personnel involved.<br>● Reinforce how thorough documentation supports the admissibility of digital evidence in legal contexts.<br>● Acknowledge the difficulties of maintaining accurate documentation in complex or high-pressure investigations.<br>● Stress the potential legal and procedural consequences of inadequate documentation.<br>**3.4 Verify the integrity of acquired evidence using hashing algorithms**<br>● Define hashing algorithms (e.g., MD5, SHA-1, SHA-256) and their role in ensuring evidence integrity.<br>● Investigate the process of generating and comparing hash values before and after evidence acquisition.<br>● Validate how hashing confirms that evidence remains unaltered during the acquisition process.<br>● Address the limitations of hashing algorithms and suggest strategies to mitigate these limitations.<br>● Underscore the legal and practical implications of failing to verify evidence integrity using hashing algorithms. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to acquire digital evidence as outlined in the assessment criteria and content above.<br>2. Practical assessment on employing write-blocking tools to prevent data alteration during acquisition, creating forensic images of storage devices, documenting the evidence acquisition process and verifying the integrity of acquired evidence using hashing algorithms based on the performance criteria of the qualification standard Digital Forensics Technician. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>FTK Imager, EnCase, dd, WinHex, X-Ways Forensics, Magnet AXIOM, Autopsy, Belkasoft Evidence Center, Cellebrite, Write Blockers, Tableau Forensic Imager, Guymager, Paladin, OSForensics, FTK (Forensic Toolkit), R-Studio, Disk Drill, Photorec, TestDisk<br>**2.1.2 Materials:**<br>Storage media (HDDs, SSDs, USB drives, memory cards), forensic workstations, write blockers, forensic imaging tools, chain-of-custody forms, documentation and cheat sheets, legal and compliance guidelines, report templates, training datasets, virtual machines (VMs), encryption tools (e.g., VeraCrypt), collaboration platforms (e.g., Slack, Teams), evidence bags, labels, and tags |

| | |
|---|---|
| **Learning Outcome 04** | **Recover and analyze digital evidence from storage media by utilizing specialized software and techniques for extracting, reconstructing, and interpreting data from fragmented or hidden digital artifacts** |
| **Assessment Criteria** | **4.1 Recover deleted files, partitions, and unallocated space.**<br>**4.2 File metadata analysed to reconstruct events.**<br>**4.3 Utilise forensic tools to examine file systems and extract data.**<br>**4.4 Identify and analyse artifacts.** |
| **Content** | **4.10 Recover deleted files, partitions, and unallocated space**<br>● Define the concepts of deleted files, partitions, and unallocated space in the context of digital forensics.<br>● Explain the technical process of recovering deleted files.<br>● Analyse methods for recovering lost or corrupted partitions. |

| | |
|---|---|
| | ● Describe techniques for accessing and analysing unallocated space.<br>**4.11 File Metadata Analysed to Reconstruct Events**<br>● Define file metadata and its components.<br>● Explain how metadata is used to reconstruct events.<br>● Analyse examples of metadata analysis in forensic investigations.<br>● Describe the limitations of relying on metadata.<br>**4.12 Utilise forensic tools to examine file systems and extract data**<br>● Define the role of forensic tools in digital evidence recovery.<br>● Explain how forensic tools examine file systems.<br>● Analyse the process of data extraction using forensic tools.<br>● Describe best practices for using forensic tools.<br>**4.13 Identify and analyse artifacts**<br>● Define digital artifacts and their significance in forensic investigations.<br>● Explain how artifacts are identified during forensic analysis.<br>● Analyse the types of artifacts and their forensic value. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to recover and analyze digital evidence from storage media as outlined in the assessment criteria and content above.<br>2. Practical assessment on recovering deleted files, partitions, and unallocated space, analyzing file metadata to reconstruct events, utilizing forensic tools to examine file systems, extracting data , and identifying and analyzing artifacts based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment |

| | |
|---|---|
| | and materials listed below: -<br>FTK Imager, Autopsy, EnCase, PhotoRec, Recuva, TestDisk, dd, Sleuth Kit, Disk Drill, R-Studio, HxD, WinHex, Magnet AXIOM, Belkasoft Evidence Center, Scalpel, Foremost, Bulk Extractor, RegRipper, Volatility, Write Blockers, HashCalc, FTK (Forensic Toolkit), X-Ways Forensics<br>**2.1.3 Materials:**<br>Storage media (HDDs, SSDs, USB drives), forensic workstations, write blockers, forensic imaging tools, training datasets, documentation and cheat sheets, case studies, legal and compliance guidelines, report templates, virtual machines (VMs), malware samples, operating system artifacts, encryption tools (e.g., VeraCrypt), collaboration platforms (e.g., Slack, Teams), chain-of-custody forms |

| | |
|---|---|
| **Learning Outcome 05** | **Dissect and observe malware functionalities in identifying attack vectors, propagation mechanisms, and potential damages caused by malicious code by analyzing malicious software through reverse engineering techniques and sandbox environments.** |
| **Assessment Criteria** | **5.1 Perform static and dynamic analysis of malware samples.**<br>**5.2 Identify purpose and functionality of malware.**<br>**5.3 Craft actionable recommendations.** |
| **Content** | **5.1 Perform static and dynamic analysis of malware samples**<br>● Define the concepts of static and dynamic analysis in malware investigation.<br>● Discuss the tools and methodologies used in static analysis.<br>● Evaluate the process of dynamic analysis in a controlled environment.<br>● Compare the strengths and limitations of static and dynamic analysis.<br>**5.2 Identify purpose and functionality of malware**<br>● Identify the common purposes of malware. |

| | |
|---|---|
| | ● Analyse how malware functionality is determined through code and behavioural analysis.<br>● Discuss examples of malware functionality and their impact.<br>● Evaluate the broader impact of malware on systems and users.<br>**5.3 Craft actionable recommendations**<br>● Define actionable recommendations in the context of malware analysis.<br>● Explain how findings from malware analysis inform recommendations.<br>● Discuss examples of actionable recommendations based on malware analysis.<br>● Outline the key components of a malware analysis report. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyse malicious software to understand its behaviour and impact outlined in the assessment criteria and content above.<br>2. Practical assessment on performing static and dynamic analysis of malware samples, identifying purpose and functionality of malware and crafting actionable recommendations based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>IDA Pro, Ghidra, OllyDbg, x64dbg, Cuckoo Sandbox, Joe Sandbox, Process Monitor, Process Explorer, Wireshark, Regshot, Volatility, PEiD, Strings, Dependency Walker, Sysinternals Suite, YARA, VirusTotal, Hybrid Analysis, REMnux, Python, PowerShell, Sandboxie, ThreatGrid, CAPE Sandbox |

| | |
|---|---|
| | **Materials:**<br>Malware samples, virtual machines (VMs), forensic workstations, threat intelligence feeds (IoCs), documentation and cheat sheets, training datasets, write blockers, forensic imaging tools, operating system artifacts, report templates, legal and ethical guidelines, case studies, collaboration platforms (e.g., Slack, Teams), encryption tools (e.g., VeraCrypt) |

| | |
|---|---|
| **Learning Outcome 06** | **Reconstruct attack timelines and identify compromised systems within a network environment by using network forensic tools and methodologies in detecting, containing, and eradicating threats** |
| **Assessment Criteria** | **6.1 Capture and analyse network traffic.**<br>**6.2 Identify suspicious network activity.**<br>**6.3 Trace source of network-based attacks** |
| **Content** | **6.1 Capture and analyse network traffic**<br>● Define network traffic<br>● explain the role of network traffic in incident investigation.<br>● Discuss the tools and techniques used to capture network traffic<br>● Analyse the process of interpreting network traffic data<br>**6.2 Identify suspicious network activity**<br>● Define suspicious network activity<br>● outline the common characteristics of suspicious network activity.<br>● Explain how network traffic analysis helps identify suspicious behaviour.<br>● Analyse examples of suspicious network activity<br>● evaluate the potential impact of suspicious network activity on systems and users.<br>● Describe the role of threat intelligence in identifying suspicious activity<br>● Assess the effectiveness of threat intelligence.<br>**6.3 Trace Source of Network-Based Attacks**<br>● Define the concept of tracing network-based attacks<br>● Discuss the techniques used to trace attack sources<br>● Analyse the challenges of tracing network-based attacks.<br>● Assess the importance of collaboration in tracing attacks<br>● Describe how it improves outcomes. |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to investigate network-based incidents and analyze network traffic as outlined in the assessment criteria and content above.<br>2. Practical assessment on capturing and analyzing network traffic, identifying suspicious network activity and trace source of network-based attacks based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - Wireshark, tcpdump, TShark, NetworkMiner, Zeek (formerly Bro), Suricata, Carta, Moloch, Cuckoo Sandbox, Joe Sandbox, Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), AlienVault OTX, MISP (Malware Information Sharing Platform), Nmap, Nessus, Scapy, hping, SSL/TLS Decryption Tools (e.g., ssldump), Microsoft Teams, Slack, JIRA, ServiceNow, Network traffic data (PCAP files), logs from firewalls, routers, and IDS, threat intelligence feeds (IoCs), network diagrams, incident documentation (notes, timelines), training and reference materials, network taps, port mirroring setups, high-performance workstations, legal and compliance guidelines, communication protocols (templates, guidelines) |

| | |
|---|---|
| **Learning Outcome 07** | **Communicate complex technical information by preparing clear and concise forensic reports by documenting findings, methodologies, and conclusions in a structured and objective manner** |
| **Assessment Criteria** | **7.1 Document structured according to international standards.**<br>**7.2 Technical details simplified for non-technical stakeholders.**<br>**7.3 Recommendations for preventing future incidents provided** |
| **Content** | **7.1 Document structured according to international standards**<br>● Define the purpose of forensic reports<br>● explain the role of forensic reports in incident response and legal proceedings.<br>● Analyse the structure of forensic reports based on international standards (e.g., ISO/IEC 27037)<br>● Discuss the benefits of adhering to international standards<br>● Describe the challenges of structuring reports according to standards<br>**7.2 Technical details simplified for non-technical stakeholders**<br>● Identify the challenges of communicating technical details to non-technical audiences<br>● Analyse examples of effective communication in forensic reports<br>● Assess the importance of tailoring reports to the audience<br>**7.3 Recommendations for preventing future incidents provided**<br>● Define the role of recommendations in forensic reports<br>● Explain how recommendations contribute to risk mitigation.<br>● Analyse how recommendations are derived from forensic findings.<br>● Discuss examples of effective recommendations<br>● Evaluate the importance of clear, actionable recommendations |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to p**repare clear and concise forensic reports** as outlined in the assessment criteria and content above.<br>2. Practical assessment on structuring documents according to international standards, simplifying technical details non-technical stakeholders, and giving recommendations for preventing future incidents provided based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment |

| | |
|---|---|
| | and materials listed below**:** Autopsy, FTK (Forensic Toolkit), EnCase, Microsoft Excel, Tableau, Lucidchart , Microsoft Teams, Slack, Google Workspace, international standards (e.g., ISO/IEC 27037), Grammarly or Hemingway Editor |

| | |
|---|---|
| **Learning Outcome 08** | **Respond to incidents involving computer systems** by applying legal frameworks and forensic protocols to identify, preserve, analyze, and report digital evidence in accordance with admissibility standards and regulatory requirements |
| **Assessment Criteria** | **8.1 Identify and contain computer-related security incidents.**<br>**8.2 Triage/assess scope and impact of the incident**<br>**8.3 Analyse root cause of the incident**<br>**8.4 Notify relevant stakeholders promptly** |
| **Content** | **8.1 Identify and contain computer-related security incidents**<br>● Define computer-related security incidents<br>● Explain the potential impact of computer-related security incidents on systems and organizations.<br>● Analyse the process of identifying security incidents through monitoring and detection tools.<br>● Describe containment strategies to prevent the spread of incidents<br>**8.2 Triage/assess scope and impact of the incident**<br>● Define incident triage<br>● Explain the role of incident triage in prioritizing response efforts.<br>● Analyse the factors considered during incident assessment<br>● Illustrate examples of incident scoping<br>● Assess the challenges of accurately assessing incident scope and impact outline best practices for improvement.<br>**8.3 Analyse root cause of the incident**<br>● Define Root Cause Analysis (RCA)<br>● Explain the importance of root cause analysis in incident response.<br>● Analyse the techniques used to determine the root cause<br>● Discuss examples of root cause analysis<br>● Assess the challenges of conducting root cause analysis<br>● describe strategies to address challenges of conducting root cause analysis.<br>**8.4 Notify relevant stakeholders promptly**<br>● Define the role of stakeholder notification in incident response<br>● Explain the importance of notifying stakeholders in incident response. |

| | |
|---|---|
| | ● Analyse the process of identifying relevant stakeholders.<br>● Describe best practices for communicating incidents to stakeholders<br>● Assess the challenges of timely stakeholder notification<br>● Outline strategies to improve communication. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to respond to incidents involving computer systems as outlined in the assessment criteria and content above.<br>2. Practical assessment on identifying and containing computer-related security incidents, triaging/assessing the scope and impact of the incident, analysing root cause of the incident and notifying relevant stakeholders promptly based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - Splunk, IBM QRadar, ArcSight, Snort, Suricata, Cisco Firepower, CrowdStrike, Microsoft Defender, Carbon Black, ELK Stack, Graylog , Firewalls like Palo Alto, Fortinet, Microsoft Defender, Symantec Endpoint Protection, access Control Tools (e.g., Active Directory, Okta, Volatility, Rekall, Redline, FTK Imager, EnCase, Autopsy, Bulk Extractor, Hex editors, Splunk, ELK Stack, Cuckoo Sandbox, VirusTotal, IDA Pro, ServiceNow, Jira, PagerDuty, Slack, Microsoft Teams, Zoom , **Documentation and Templates,** Incident Response Plan (IRP),Communication Templates, Forensic report templates, Forensic workstation, write blockers, External Storage Devices, **c**hain of custody forms, Regulatory Guidelines (e.g., GDPR, HIPAA, PCI-DSS) |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Demonstrate knowledge of computer hardware, software, and file systems by accurately identifying components, functions, and interrelationships, demonstrating a comprehensive understanding of foundational computing principles | 20% |
| Ensure integrity and compliance in all aspects of digital evidence handling and reporting by adhering to legal and ethical standards in computer forensics | 10 % |
| Preserve evidence integrity and admissibility in legal proceedings by employing forensically sound methods and tools for digital evidence acquisition | 10% |
| Recover and analyze digital evidence from storage media by utilizing specialized software and techniques for extracting, reconstructing, and interpreting data from fragmented or hidden digital artifacts | 10% |
| Dissect and observe malware functionalities in identifying attack vectors, propagation mechanisms, and potential damages caused by malicious code by analyzing malicious software through reverse engineering techniques and sandbox environments | 20 % |
| Reconstruct attack timelines and identify compromised systems within a network environment by using network forensic tools and methodologies in detecting, containing, and eradicating threats | 10% |
| Communicate complex technical information by preparing clear and concise forensic reports by documenting findings, methodologies, and conclusions in a structured and objective manner | 10 % |
| Respond to incidents involving computer systems by applying legal frameworks and forensic protocols to identify, preserve, analyze, and | 10% |

| | |
|---|---|
| report digital evidence in accordance with admissibility standards and regulatory requirements | |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**

   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

   Splunk, IBM QRadar, ArcSight, Snort, Suricata, Cisco Firepower, CrowdStrike, Microsoft Defender, Carbon Black, ELK Stack, Graylog , Firewalls like Palo Alto, Fortinet, Microsoft Defender, Symantec Endpoint Protection, access Control Tools (e.g., Active Directory, Okta, Volatility, Rekall, Redline, FTK Imager, EnCase,Belkasoft, UFED Cellebrite, Magnet Axiom, Autopsy, Bulk Extractor, Hex editors, Splunk, ELK Stack, Cuckoo Sandbox, VirusTotal, IDA Pro, ServiceNow, Jira, PagerDuty, Slack, Microsoft Teams, Zoom , **Documentation and Templates,** Incident Response Plan (IRP),Communication Templates, Forensic report templates, Forensic

workstation, write blockers, External Storage Devices, **c**hain of custody forms, Regulatory Guidelines (e.g., GDPR, HIPAA, PCI-DSS)

CPU-Z, HWiNFO, Speccy, CrystalDiskInfo, GParted, MiniTool Partition Wizard, File Explorer (Windows), Finder (macOS), Linux File Managers (e.g., Nautilus), Hex Editors (e.g., HxD), Disk Management Tools (e.g., Windows Disk Management), Registry Editor (Windows), Terminal/Command Line Tools (e.g., Linux Terminal, Windows Command Prompt), Virtual Machines (e.g., VMware, VirtualBox), BIOS/UEFI Interfaces

### 2.1.4 Materials:

Computer hardware components (e.g., CPUs, RAM, motherboards, storage devices), operating system installation media (e.g., Windows, Linux, macOS), file system documentation (e.g., NTFS, FAT32, ext4, APFS), training manuals and guides, hardware diagnostic tools, system monitoring software, case studies, collaboration platforms (e.g., Slack, Teams), report templates, legal and compliance guidelines, forensic workstations

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 4. Reference Materials (recommended textbooks, recommended readings)


**Holt, T.J., Bossler, A.M., and Seigfried-Spellar, K.C.** (2022). *Cybercrime and Digital Forensics: An Introduction*. 3rd ed. New York: Routledge.

**Luttgens, J.T., Pepe, M., and Mandia, K.** (2020). *Incident Response & Computer Forensics*. 3rd ed. New York: McGraw-Hill Education.

**Sammons, J.** (2021). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 3rd ed. Waltham, MA: Syngress.

**Kävrestad, J.** (2020). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. 2nd ed. Cham, Switzerland: Springer.

**Reith, M., Carr, C., and Gunsch, G.** (2022). *Digital Forensics and Incident Response: A Practical Guide to Investigating and Responding to Cyber Attacks*. Birmingham, UK: Packt Publishing.

**Casey, E.** (2021). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 4th ed. Waltham, MA: Academic Press.

**Maras, M.H.** (2022). *Computer Forensics: Cybercriminals, Laws, and Evidence*. 3rd ed. Burlington, MA: Jones & Bartlett Learning.

**Quick, D. and Choo, K.K.R.** (2021). *Digital Forensic Investigation of Internet of Things (IoT) Devices*. 1st ed. Cham, Switzerland: Springer.

| | |
|---|---|
| **Module Code:** | **682/25/M06** |
| **Module Title:** | **Programming for Digital Forensics** |
| **ZNQF Level:** | **5** |
| **Credits:** | 15 |
| **Duration:** | 150 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Programming for Digital Forensics** of Unit Standards for a Digital Forensics Technician |
| **Pre-requisite modules:** | None |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an individual to be able to effectively communicate in business. This includes selecting suitable programming languages for forensic tasks, implementing decision-making statements, managing forensic data using lists, arrays, and dictionaries and handling different file formats, automating forensic tasks using scripting languages and applying regular expressions in forensic analysis, verifying hashing and data integrity and search in forensic evidence using string and pattern, capturing and analyzing network traffic, and parse and interpret log files, automating malware detection and de obfuscate and analyzing malicious scripts, extracting forensic data from databases and analyzing database logs for forensic investigation, writing scripts for memory and disk analysis and automating forensic imaging and extraction, applying programming skills to forensic case studies and Generating forensic reports using automated tools. |
| **List of Learning Outcomes:** | **LO1: Select suitable programming languages for forensic tasks by evaluating language features, libraries, and community support against specific forensic requirements.**<br>**LO2: Create robust and optimized code for forensic analysis and automation tasks by constructing programmatic solutions that control flow and process data effectively.**<br>**LO3: Organize and manipulate complex digital evidence for forensic analysis using lists, arrays, and dictionaries in handling different file formats.**<br>**LO4: Enhance efficiency and precision in digital investigations by automating forensic tasks using scripting languages and applying regular expressions in forensic analysis.**<br>**LO5: Maintain the chain of custody by pinpointing relevant data within large forensic images, verifying hashing and searching in forensic evidence using strings and patterns.**<br>**LO6: Reconstruct network events and derive actionable intelligence from diverse network data sources by capturing and analyzing network traffic, and parsing and interpreting log files.** |

| | |
|---|---|
| | **LO7: Write scripts for memory and disk analysis and automate forensic imaging and extraction by developing custom tools that interact with operating system internals and storage devices.** |

| Learning Outcome 01 | **Select suitable programming languages for forensic tasks by evaluating language features, libraries, and community support against specific forensic requirements** |
|---|---|
| **Assessment Criteria:** | **1.1 Explain the role of programming in digital forensics and its applications.**<br>**1.2 Identify and Compare Programming languages commonly used in forensic investigations.**<br>**1.3 Set up a basic programming environment for forensic scripting.** |
| **Content:** | **1.1 Explain the role of programming in digital forensics and its applications.**<br>● Define programming concepts relevant to digital forensics<br>● Explain how scripting automates forensic investigations<br>● Identify common programming languages used in digital forensics (e.g., Python, C, Bash)<br>● Describe common programming languages used in digital forensics (e.g., Python, C, Bash).<br>● Demonstrate the use of programming in forensic data extraction and analysis.<br><br>**1.2 Identify and compare programming languages commonly used in forensic investigations.**<br>● Explain use cases of different languages in forensic analysis (e.g., Python for automation, C++ for deep system analysis)<br>● Define key programming languages used in digital forensics, such as Python, C++, Java, and Bash.<br>● Analyze the strengths and weaknesses of each language in forensic investigations.<br>● Explain the use cases of different languages in forensic analysis, such as Python for automation and C++ for deep system analysis.<br><br>**1.3 Set up a basic programming environment for forensic scripting.**<br>● Demonstrate the process of setting up a forensic scripting environment, including the installation of essential programming tools and libraries.<br>● Explain the steps for installing and configuring forensic programming environments for languages such as Python, C++, and Bash.<br>● Outline the configuration of key forensic libraries and tools, including Scapy, Volatility, and PyTSK.<br>● Define the functions of IDEs and text editors, such as PyCharm and VS Code, in facilitating forensic scripting.<br>● Analyze compatibility factors to ensure optimal performance with |

| | |
|---|---|
| | forensic tools and operating systems. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to identify and compare programming languages commonly used in forensic investigations as outlined in the assessment criteria and content above.<br>2. Practical assessment on selecting a suitable programming language for a given forensic investigation scenario, justifying the choice, setting up a programming environment for forensic scripting, and demonstrating its application in forensic tasks.<br>3. Hands-on task on setting up a basic programming environment and writing a simple forensic script for data extraction, log analysis, or evidence parsing. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The assessment context should include the necessary facilities, tools, equipment, and materials, such as computer systems, forensic and cybersecurity software, ethical hacking toolkits, and documentation resources. |

| **Learning Outcome 02** | **Create robust and optimized code for forensic analysis and automation tasks by constructing programmatic solutions that control flow and process data effectively** |
|---|---|
| **Assessment Criteria** | **2.1 Write scripts using conditional statements to automate forensic decision-making.**<br>**2.2 Implement loops to iterate over forensic data for bulk analysis.**<br>**2.3 Develop logical expressions to filter relevant forensic artifacts.** |
| **Content** | **2.1 Write scripts using conditional statements to automate forensic decision-making**<br><br>● Define key forensic decision points that require automation in digital investigations.<br>● Develop scripts using languages like Python or Bash to streamline forensic processes.<br>● Explain the use of conditional statements (if/else, switch) for processing evidence data.<br>● Describe automation techniques for tasks such as file classification and alert triggering. |

| | |
|---|---|
| | ● Outline the process of testing and documenting scripts for clarity and maintainability.<br><br>**2.2 Implement loops to iterate over forensic data for bulk analysis.**<br><br>● Explain the implementation of loops (for, while) to iterate over forensic data for bulk analysis, ensuring efficient processing of large datasets.<br>● Describe how loops can be used to automate file hashing (MD5, SHA-256) for integrity verification in forensic investigations.<br>● Outline the process of iterating over log files, registry entries, and network packets to systematically extract digital evidence.<br>● Analyze error handling techniques to manage corrupted or missing data, ensuring reliability in forensic scripting.<br>● Define optimization strategies to enhance loop performance, minimizing resource consumption while processing large forensic datasets.<br><br>**2.3 Develop logical expressions to filter relevant forensic artifacts.**<br><br>● Explain logical operators (AND, OR, NOT) for filtering forensic data.<br>● Describe comparison operators (>, <, =) for refining searches.<br>● Outline regex use for pattern matching (emails, IPs).<br>● Analyze optimization techniques for efficient data filtering. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to implement decision-making statements, write efficient loops, and develop logical expressions as outlined in the assessment criteria.<br>2. Practical assessment on writing decision-making statements (if, else, elif) to process and analyze forensic data, ensuring correct flow of program execution based on specific conditions. **Assess** on developing efficient loops to process large datasets, optimizing for performance and memory management when iterating over forensic data for bulk analysis. Also **assess** on creating and applying logical expressions to filter relevant forensic artifacts, such as identifying unauthorized access attempts or specific file types in a dataset. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, |

| | |
|---|---|
| | equipment and materials listed below. |

| **Learning Outcome 03** | **Organize and manipulate complex digital evidence for forensic analysis using lists, arrays, and dictionaries in handling different file formats** |
|---|---|
| **Assessment Criteria** | **3.1 Write scripts to extract, store, and manipulate forensic data.**<br>**3.2 Implement file handling techniques to parse forensic artifacts.**<br>**3.3 Implement data structures to organize and store digital evidence efficiently.**<br>**3.4 Write scripts to read, parse, and manipulate structured forensic data files.**<br>**3.5 Extract and process Forensic artifacts from various file formats.** |
| **Content** | **3.1 Write scripts to extract, store, and manipulate forensic data.**<br>● Define the role of data structures such as lists, arrays, and dictionaries in managing forensic data efficiently.<br>● Explain how scripts can be used to extract, store, and manipulate forensic data for analysis.<br>● Describe methods for handling different file formats (e.g., CSV, JSON, XML) to ensure compatibility with forensic tools.<br>● Outline techniques for organizing and structuring forensic data to improve retrieval and analysis.<br>● Analyze the efficiency of different data management approaches in forensic investigations.<br>**3.2 Implement file handling techniques to parse forensic artifacts.**<br>● Define file handling techniques used to read, write, and parse forensic artifacts from different file formats.<br>● Describe methods for extracting forensic artifacts from log files, memory dumps, and databases.<br>● Outline best practices for handling large forensic datasets while maintaining data integrity.<br>● Analyze the effectiveness of various parsing techniques in identifying and preserving digital evidence.<br>**3.3 Implement data structures to organize and store digital evidence efficiently.**<br>● Define the use of lists, dictionaries, and databases (SQL/NoSQL) for efficiently organizing and storing digital evidence.<br>● Explain how structured data storage, including hash tables, |

| | |
|---|---|
| | improves retrieval speed in forensic analysis.<br>● Describe methods for categorizing extracted forensic artifacts using lists and dictionaries.<br>● Outline the implementation of databases for secure and accessible management of digital evidence.<br>● Analyze the effectiveness of different data structures in optimizing storage and handling large forensic datasets.<br><br>**3.4 Write scripts to manipulate structured forensic data files.**<br>● Write a parser to analyze and manipulate log files, registry files, or event logs.<br>● Implement automation to filter, sort, and summarize forensic data for reporting.<br>● Use scripting to convert forensic data between different formats for compatibility.<br><br>**3.5 Extract and process Forensic artifacts from various file formats.**<br><br>● Identify and extract artifacts from different file formats, including logs, emails, databases, and system files.<br>● Use forensic tools and scripts to recover and analyze data from structured (CSV, JSON, XML) and unstructured (TXT, DOC, PDF) files.<br>● Process deleted or hidden files from storage media using forensic recovery techniques.<br>● Analyze metadata and timestamps from files to determine authenticity and integrity.<br>● Convert and normalize extracted data for further analysis and reporting in forensic investigations. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to manage forensic data using lists, arrays, and dictionaries, as well as handling different file formats, as outlined in the assessment criteria.<br>2. Practical assessment on utilizing lists, arrays, and dictionaries to store, categorize, and retrieve forensic artifacts efficiently. The learner must demonstrate knowledge in developing scripts to read, parse, and manipulate forensic data from various file formats (e.g., JSON, CSV, XML, log files). Practical assessment on automating forensic data extraction, filtering, and structuring using appropriate data structures for analysis and reporting must be assessed. Additionally, assessment on processing and converting forensic data between different formats to ensure compatibility and integrity in forensic investigations, based on the performance criteria of the qualification standard **Digital Forensics Technician**. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 04** | **Enhance efficiency and precision in digital investigations by automating forensic tasks using scripting languages and applying regular expressions in forensic analysis** |
| **Assessment Criteria:** | **4.1 Develop scripts to extract and analyze log data.**<br>**4.2 Use regex for searching patterns in forensic evidence.**<br>**4.3 Develop Scripts to automate forensic evidence collection and processing.**<br>**4.4 Create regular expressions to extract relevant information from forensic logs.**<br>**4.5 Write Scripts to generate forensic reports based on extracted data.** |
| **Content:** | **4.1 Develop scripts to extract and analyze log data.**<br>● Write scripts to automate the extraction of log data from system logs, network logs, and security event logs.<br>● Parse and filter log files to identify key forensic artifacts such as login attempts, file modifications, and unauthorized access.<br>● Utilize regular expressions to search for specific patterns in log files (e.g., IP addresses, timestamps, error codes).<br>● Analyze extracted log data to detect anomalies, security breaches, and suspicious activities.<br>● Generate structured reports summarizing findings from log analysis for forensic investigations.<br>● Ensure data integrity by hashing and securely storing extracted logs for future reference.<br><br>**4.2 Use regex for searching patterns in forensic evidence.**<br>● Develop regular expressions (regex) to identify critical forensic artifacts such as email addresses, IP addresses, URLs, and file paths in digital evidence.<br>● Use regex patterns to extract timestamps, MAC addresses, and system event logs from raw forensic data.<br>● Implement regex filtering to detect specific keywords, error codes, and user activities in log files. |

| | |
|---|---|
| | ● Automate data extraction by integrating regex in forensic scripts for searching large datasets efficiently.<br>● Validate and refine regex patterns to minimize false positives and ensure accuracy in forensic investigations.<br><br>**4.3 Develop Scripts to automate forensic evidence collection and processing.**<br>● Write scripts to automate the acquisition of forensic artifacts from storage devices, memory dumps, and log files.<br>● Implement automated parsing of extracted data, including timestamps, metadata, and system logs.<br>● Integrate hashing techniques (e.g., MD5, SHA-256) to verify the integrity of collected evidence.<br>● Use scripting tools (e.g., Python, PowerShell, Bash) to extract and process forensic evidence efficiently.<br>● Automate reporting by generating structured summaries of collected evidence for legal and investigative use.<br>● Schedule and execute forensic tasks for continuous monitoring and evidence collection in cybersecurity investigations.<br><br>**4.4 Create regular expressions to extract relevant information from forensic logs.**<br>● Develop regex patterns to identify and extract key forensic artifacts such as IP addresses, MAC addresses, email addresses, and URLs from log files.<br>● Use regex to parse timestamps and event logs to reconstruct a timeline of system activities.<br>● Filter and extract login attempts, error messages, and unauthorized access events from security logs.<br>● Detect file paths, registry changes, and command execution logs using structured regex queries.<br>● Validate regex accuracy to minimize false positives and improve forensic data extraction efficiency.<br>● Implement regex-based automation in forensic scripts to quickly analyze large log datasets.<br><br>**4.5 Write Scripts to generate forensic reports based on extracted data.**<br>● Develop scripts to process and format extracted forensic data into structured reports.<br>● Automate report generation with key details such as timestamps, user activities, system logs, and security events.<br>● Use scripting languages (e.g., Python, PowerShell) to create interactive or static reports in formats like PDF, CSV, and JSON. |

| | |
|---|---|
| | ● Integrate data visualization tools (e.g., Matplotlib, Seaborn) to generate charts and graphs for forensic analysis.<br>● Ensure report integrity by including hash values and digital signatures for authenticity verification.<br>● Customize report templates to align with legal and investigative standards for forensic documentation. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to automate forensic tasks using scripting languages and apply regular expressions in forensic investigations, as outlined in the assessment criteria.<br>2. Practical assessment on developing scripts to automate forensic evidence collection, log analysis, and data parsing using scripting languages such as Python, PowerShell, or Bash.<br>3. Hands-on task on creating and applying regular expressions to extract key forensic artifacts (e.g., IP addresses, timestamps, file paths) from system logs and digital evidence.<br>4. Scenario-based assessment on designing and implementing an automated forensic workflow using scripts and regex to filter, analyze, and generate forensic reports from extracted data.<br>5. Validation task on testing and refining regex patterns for accuracy and efficiency in forensic investigations, ensuring minimal false positives and false negatives. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The assessment context should include the necessary facilities, tools, equipment, and materials, such as computer systems, forensic and cybersecurity software, ethical hacking toolkits, and documentation resources. |
| **Learning Outcome 05** | **Maintain the chain of custody by pinpointing relevant data within large forensic images, verifying hashing and searching in forensic evidence using strings and patterns** |
| **Assessment Criteria:** | **5.1 Implement hashing algorithms (md5, sha-256) to verify digital evidence integrity.**<br>**5.2 Develop scripts to automate keyword searches in forensic data.**<br>**5.3 Apply data processing techniques to analyze forensic logs and artifacts.** |

| | |
|---|---|
| **Content:** | **5.1 Implement hashing algorithms (md5, sha-256) to verify digital evidence integrity.**<br>● Develop scripts in Python, PowerShell, or Bash to compute and compare hash values of digital evidence.<br>● Use Python's hashlib library to generate MD5 and SHA-256 hashes for files and forensic artifacts.<br>● Automate integrity verification by comparing precomputed and recalculated hash values to detect tampering.<br>● Implement hashing in forensic workflows to validate collected evidence before and after analysis.<br>● Log and report hash values in forensic reports for legal and investigative documentation.<br><br>**5.2 Develop scripts to automate keyword searches in forensic data.**<br>● Create scripts to scan and search forensic data (e.g., logs, emails, chat history, and documents) for specific keywords.<br>● Implement case-insensitive and pattern-based searches using regular expressions for accurate detection.<br>● Use scripting languages such as Python, PowerShell, or Bash to automate keyword searches in bulk forensic data.<br>● Optimize search performance by integrating indexing techniques or searching only relevant file types.<br>● Generate reports with highlighted keyword matches, timestamps, and file paths for forensic documentation.<br><br>**5.3 Apply data processing techniques to analyze forensic logs and artifacts.**<br>● Preprocess forensic logs by removing irrelevant data, normalizing timestamps, and structuring information for analysis.<br>● Parse and extract key fields such as IP addresses, timestamps, usernames, and event types from log files.<br>● Use scripting languages (Python, Bash, PowerShell) to automate log analysis and identify anomalies.<br>● Identify regular expressions to detect patterns related to security incidents (e.g., brute-force attempts, unauthorized access).<br>● Outline data visualization tools like Pandas, Matplotlib, or ELK Stack to generate graphical insights from forensic logs.<br>● Correlate multiple log sources (e.g., system logs, network traffic, event logs) to reconstruct timelines and track malicious activity.<br>● Generate forensic reports summarizing findings, key artifacts, and potential security threats. |

| | |
|---|---|
| **Assessment Tasks:** | 1. Written and/or oral assessment on the concepts of hashing algorithms (e.g., MD5, SHA-256) and their role in verifying digital evidence integrity, as well as the use of string and pattern matching techniques in forensic investigations.<br>2. Practical assessment on generating and comparing hash values to detect data integrity violations, ensuring evidence has not been tampered with.<br>3. Hands-on task on developing scripts to perform keyword searches and apply regular expressions for pattern detection in forensic logs, emails, and other digital artifacts.<br>4. Scenario-based assessment where candidates analyze a dataset, verify its integrity using hashing techniques, and extract relevant forensic evidence using pattern matching. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The assessment context should include the necessary facilities, tools, equipment, and materials, such as computer systems, forensic and cybersecurity software, ethical hacking toolkits, and documentation resources. |

| **Learning Outcome 06** | **Reconstruct network events and derive actionable intelligence from diverse network data sources by capturing and analyzing network traffic, and parsing and interpreting log files** |
|---|---|
| **Assessment Criteria** | **6.1 Write scripts to extract and analyze network packets.**<br>**6.2 Develop log analysis scripts for forensic investigations.**<br>**6.3 Develop scripts to process and detect anomalies in system logs.**<br>**6.4 Generate reports on network-based forensic investigations**. |
| **Content** | **6.1 Write scripts to extract and analyze network packets.**<br>● Capture network traffic using tools like tcpdump, Wireshark, or scapy in Python.<br>● Extract relevant packet details such as source and destination IP addresses, ports, protocols, timestamps, and payload data.<br>● Filter network packets based on specific criteria (e.g., suspicious IPs, abnormal traffic patterns, protocol types).<br>● Reassemble fragmented packets to analyze full communication streams in forensic investigations. |

| | |
|---|---|
| | ● Automate analysis using scripts to identify anomalies, detect unauthorized access, or extract indicators of compromise (IoCs).<br>● Generate forensic reports summarizing key findings from packet analysis, highlighting suspicious activity.<br><br>**6.2 Develop log analysis scripts for forensic investigations.**<br>● Collect and parse logs from various sources such as system logs, web server logs, authentication logs, and firewall logs.<br>● Filter relevant forensic data using timestamps, user activity, IP addresses, and error messages.<br>● Outline pattern matching and regular expressions for identifying suspicious behavior, unauthorized access, or malware activity.<br>● Describe the automation of log correlation to detect anomalies across multiple log sources and reconstruct event timelines.<br>● Generate structured reports summarizing key findings, highlighting security incidents, and providing forensic insights.<br><br>**6.3 Develop scripts to process and detect anomalies in system logs.**<br>● Parse and filter system logs to extract relevant security events, including failed logins, privilege escalations, and unauthorized access attempts.<br>● Implement pattern matching with regular expressions to detect suspicious activities, such as repeated failed logins or unusual command executions.<br>● Use statistical analysis and threshold-based detection to identify anomalies in system logs, such as sudden spikes in network activity or unusual login times.<br>● Automate log correlation across multiple sources (e.g., system logs, firewall logs, and application logs) to identify coordinated attacks.<br>● Generate alerts and reports summarizing detected anomalies for forensic investigations and incident response.<br><br>**6.4 Generate reports on network-based forensic investigations.**<br><br>● Collect and analyze network traffic from sources such as packet captures (PCAP), firewall logs, and intrusion detection system (IDS) logs.<br>● Extract key forensic artifacts, including IP addresses, MAC addresses, timestamps, and packet payloads.<br>● Identify suspicious network activities such as unauthorized access, data exfiltration, and malware communication.<br>● Correlate network events across multiple log sources to reconstruct |

| | |
|---|---|
| | attack timelines.<br>● Generate structured forensic reports summarizing findings, including detailed logs, graphical analysis, and recommendations for mitigation. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to capture live network traffic, analyze packet data, and interpret log files as outlined in the assessment criteria.<br>2. Practical assessment on using network forensic tools (e.g., Wireshark, tcpdump) to capture and analyze network traffic, identify anomalies, and extracting key forensic artifacts.<br>3. Hands-on task on parsing and interpreting log files (e.g., firewall logs, IDS/IPS logs, system logs) using scripting languages such as Python, Bash, or PowerShell.<br>4. Scenario-based assessment where candidates investigate a simulated cybersecurity incident, analyze network traffic and logs, and produce a forensic report detailing findings and recommendations. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 07** | **Write scripts for memory and disk analysis and automate forensic imaging and extraction by developing custom tools that interact with operating system internals and storage devices** |
|---|---|
| **Assessment Criteria:** | **7.1 Develop scripts to detect, identify and extract malware indicators.**<br>**7.2 Create scripting to analyze and reverse-engineer malware code.**<br>**7.3 Use Scripting to analyze the behavior of suspicious files and scripts.**<br>**7.4 Implement deobfuscation techniques to decode malware and identify threats.** |
| **Content:** | **7.1 Develop scripts to detect, identify and extract malware indicators.**<br>● Choose a suitable scripting language (e.g., Python) for malware analysis.<br>● Define known malware indicators such as file hashes, strings, and behavioral patterns.<br>● Develop detection logic using conditional statements and pattern matching to identify malware. |

| | |
|---|---|
| | ● Automate the extraction of key malware indicators from forensic data.<br>● Test the script using sample malware datasets to validate its accuracy.<br>● Document the script's functionality and assumptions for future maintenance.<br>**7.2 Use scripting to analyze and reverse-engineer malware code.**<br>● Select a scripting language (e.g., Python) with libraries suited for binary analysis and reverse engineering.<br>● Develop scripts to extract and parse code segments from malware binaries.<br>● Utilize disassembly and decompilation techniques within the script to reveal malware structure.<br>● Automate the detection of obfuscation methods and decoding routines in malware code.<br>● Integrate debugging and logging functionalities to monitor malware behavior during analysis.<br>● Document the reverse-engineered code findings for further forensic review.<br>**7.3 Use Scripting to analyze the behavior of suspicious files and scripts.**<br>● Choose a scripting language, such as Python, to develop automation scripts for behavior analysis.<br>● Develop scripts to execute suspicious files in a controlled, sandboxed environment.<br>● Monitor and log system calls, file modifications, and network activity during execution.<br>● Analyze collected logs to detect anomalous or malicious behavior patterns.<br>● Automate report generation to summarize the behavioral analysis of suspicious files and scripts.<br>**7.4 Implement deobfuscation techniques to decode malware and identify threats.**<br>● Select a scripting language and tools that support deobfuscation techniques.<br>● Develop scripts to automatically detect and reverse common obfuscation methods.<br>● Analyze encoded malware code to reveal hidden threat indicators.<br>● Use pattern matching and decoding algorithms to identify encryption schemes.<br>● Validate decoded outputs by comparing them with known threat |

| | |
|---|---|
| | signatures.<br>● Document the deobfuscation process and findings for further analysis. |
| **Assessment Tasks:** | 1. Written and/or Oral Assessment: Assess knowledge of malware detection techniques and obfuscation methods. Evaluate understanding of scripting languages used for malware analysis (e.g., Python, PowerShell).<br>2. Practical Assessment: Develop a script to automatically scan logs and files for malware indicators. Implement a regex-based script to detect encoded or obfuscated malware.<br>3. Hands-on Task: Write a script to de-obfuscate a given malicious script and extract key indicators. Analyze and generate a report on malware behavior using extracted forensic artifacts. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The assessment context should include the necessary facilities, tools, equipment, and materials, such as computer systems, forensic and cybersecurity software, ethical hacking toolkits, and documentation resources. |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Select suitable programming languages for forensic tasks by evaluating language features, libraries, and community support against specific forensic requirements | 15% |

| | |
|---|---|
| Create robust and optimized code for forensic analysis and automation tasks by constructing programmatic solutions that control flow and process data effectively | 15% |
| Organize and manipulate complex digital evidence for forensic analysis using lists, arrays, and dictionaries in handling different file formats | 15% |
| Enhance efficiency and precision in digital investigations by automating forensic tasks using scripting languages and applying regular expressions in forensic analysis | 15% |
| Maintain the chain of custody by pinpointing relevant data within large forensic images, verifying hashing and searching in forensic evidence using strings and patterns | 15% |
| Reconstruct network events and derive actionable intelligence from diverse network data sources by capturing and analyzing network traffic, and parsing and interpreting log files | 10% |
| Write scripts for memory and disk analysis and automate forensic imaging and extraction by developing custom tools that interact with operating system internals and storage devices | 15% |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**

   All trainers, assessors, and moderators should have a Bachelor's Degree in Computer Science, Information Technology, Cybersecurity, or Digital Forensics, or Information Security or an equivalent qualification.

## 2. Facilities, Tools, Equipment and Materials

- Computers with programming environments (e.g., Python, C++, PowerShell)
- Secure coding platforms
- Virtual machines and sandbox environments
- Debugging and reverse engineering tools
- Network simulation and penetration testing tools
- Digital forensic analysis software
- Secure data storage devices
- Internet access and networking equipment

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

Programming manuals and textbooks

Digital forensic case studies

Open-source forensic tools and frameworks

Online cybersecurity and digital forensics platforms

Video tutorials and interactive coding platforms

Research papers and industry reports on forensic programming

## 4. Reference Materials (recommended textbooks, recommended readings)

Deitel, P., Deitel, H. and Santry, M., 2016. *C++ how to program*. 10th ed. Upper Saddle River, NJ: Pearson.

Nystrom, R., 2014. *Game programming patterns*. San Francisco, CA: Genever Benning.

Sebesta, R.W., 2019. *Programming languages: principles and practice*. 9th ed. Boston: Pearson.

Lutz, M., 2013. *Learning Python*. 5th ed. Sebastopol, CA: O'Reilly Media.

McKinney, W., 2018. *Python for data analysis*. 2nd ed. Sebastopol, CA: O'Reilly Media.

Sedgewick, R. and Wayne, K., 2011. *Algorithms*. 4th ed. Boston: Addison-Wesley.

Johnson, R., 2017. *Effective Java*. 3rd ed. Boston: Addison-Wesley.

Knuth, D.E., 1997. *The art of computer programming, volume 1: Fundamental algorithms*. 3rd ed. Boston: Addison-Wesley.

Zeldman, J., 2015. *Designing with web standards*. 3rd ed. Berkeley, CA: New Riders.

Elliott, A. and Jackson, M., 2020. *Learning JavaScript: The programming language of the web*. 4th ed. Chicago: Apress.

Manuele, F.A., 2013. *On the practice of safety*. 4th ed. John Wiley & Sons, Inc.

| | |
|---|---|
| Module Code: | **682/25/M07** |
| Module Title: | **FUNDAMENTALS OF OPERATING SYSTEMS** |
| ZNQF Level: | **5** |
| Credits: | 15 |
| Duration: | 150 |
| Relationship with Qualification Standards: | Based on Unit Standard "Emerging Technologies in Digital Forensics" or similar advanced unit standards in Digital Forensics, Cybersecurity, or ICT Forensics Technician qualifications. |
| Pre-requisite modules: | N/A |
| Purpose of Module: | This module describes the skills, knowledge, and attitudes required by an ICT specialist to understand the fundamental concepts, principles, and mechanisms of operating systems. It focuses on equipping learners with the necessary expertise to analyze process and memory management, implement synchronization techniques, manage file systems and I/O operations, and assess operating system performance and security. This module aims to provide a solid theoretical and practical foundation for advanced studies in system administration, cybersecurity, and software development. |

| | |
|---|---|
| **List of Learning Outcomes:** | **LO1: Analyze and apply core techniques in process management and CPU scheduling within diverse operating system environments.**<br>**LO2: Implement and manage inter-process communication (IPC) and synchronization methods to ensure effective coordination of concurrent system processes.**<br>**LO3: Evaluate and apply memory management strategies, including paging and virtual memory, to optimize resource utilization in operating systems.**<br>**LO4: Manage file systems and input/output (I/O) operations using command-line and GUI tools across multiple OS platforms.**<br>**LO5: Assess operating system performance through monitoring tools, benchmarking metrics, and performance tuning techniques.**<br>**LO6: Apply essential operating system security measures and protection mechanisms to safeguard system integrity and user data.** |

| **Learning Outcome 01** | **Analyze and apply core techniques in process management and CPU scheduling within diverse operating system environments** |
|---|---|
| Assessment Criteria: | 1.1 Describe the concept of a process and its states within an operating system.<br>1.2 Differentiate between various CPU scheduling algorithms and their characteristics.<br>1.3 Analyze the performance implications of different scheduling algorithms on system metrics. |
| Content: | **1.1 Describe the concept of a process and its states within an operating system:**<br>1.1.1 Define a process vs. a program.<br>1.1.2 Explain the Process Control Block (PCB) and its contents.<br>1.1.3 Illustrate the process state model (New, Ready, Running, Waiting, Terminated) and transitions between states.<br>1.1.4 Differentiate between processes and threads, explaining the benefits of multithreading.<br>**1.2 Differentiate between various CPU scheduling algorithms and their characteristics:**<br>1.2.1 Explain the goals of CPU scheduling (e.g., maximize CPU utilization, maximize throughput, minimize turnaround time, minimize waiting time, minimize response time).<br>1.2.2 Describe common non-preemptive algorithms: First-Come, First-Served (FCFS), Shortest-Job-First (SJF).<br>1.2.3 Describe common preemptive algorithms: Round Robin (RR), Preemptive SJF, Priority Scheduling.<br>1.2.4 Discuss Multilevel Queue and Multilevel Feedback Queue scheduling.<br>**1.3 Analyze the performance implications of different scheduling algorithms on system metrics:**<br>1.3.1 Calculate turnaround time, waiting time, and average waiting time for given processes under different scheduling |

| | |
|---|---|
| | algorithms.<br>1.3.2 Compare the advantages and disadvantages of each algorithm in various scenarios (e.g., batch systems, interactive systems).<br>1.3.3 Discuss the concept of context switching and its overhead. |
| Assessment Tasks: | 1. Written and/or oral assessment on the skills and knowledge required to analyze process management and scheduling techniques as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using a CPU scheduling simulator to run different algorithms on a set of processes and analyze the resulting performance metrics. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a simulated lab environment with access to operating system simulators or tools that demonstrate process scheduling.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 02** | **Implement and manage inter-process communication (IPC) and synchronization methods to ensure effective coordination of concurrent system processes** |
|---|---|
| Assessment Criteria | 2.1 Describe the challenges of concurrent process execution (e.g., race conditions, deadlocks).<br>2.2 Explain and apply various inter-process communication (IPC) mechanisms.<br>2.3 Implement synchronization techniques to prevent race conditions and manage critical sections.<br>2.4 Analyze common deadlock conditions and strategies for handling them |
| Content | **2.1 Describe the challenges of concurrent process execution (e.g., race conditions, deadlocks):**<br>2.1.1 Define concurrency and parallelism.<br>2.1.2 Explain the concept of a critical section.<br>2.1.3 Illustrate race conditions with examples and their potential |

| | |
|---|---|
| | impact.<br>2.1.4 Describe deadlock, starvation, and livelock.<br>**2.2 Explain and apply various inter-process communication (IPC) mechanisms:**<br>2.2.1 Describe shared memory (e.g., pipes, message queues) and message passing (e.g., sockets).<br>2.2.2 Discuss the advantages and disadvantages of different IPC methods.<br>2.2.3 Implement simple IPC mechanisms in a programming environment (e.g., using pipes or shared memory in a simulated environment).<br>**2.3 Implement synchronization techniques to prevent race conditions and manage critical sections:**<br>2.3.1 Explain the requirements for a valid critical section solution (mutual exclusion, progress, bounded waiting).<br>2.3.2 Describe and apply software-based solutions (e.g., Peterson's Solution - conceptual).<br>2.3.3 Describe and apply hardware-based solutions (e.g., TestAndSet, CompareAndSwap - conceptual).<br>2.3.4 Implement and use semaphores and mutexes for process synchronization in a programming context.<br>2.3.5 Solve classic synchronization problems (e.g., Producer-Consumer, Dining Philosophers - conceptually and with basic implementation).<br>**2.4 Analyze common deadlock conditions and strategies for handling them:**<br>2.4.1 Explain the four necessary conditions for deadlock (Mutual Exclusion, Hold and Wait, No Preemption, Circular Wait).<br>2.4.2 Describe strategies for deadlock prevention (e.g., breaking one of the four conditions).<br>2.4.3 Discuss deadlock avoidance (e.g., Banker's Algorithm - conceptual).<br>2.4.4 Explain deadlock detection and recovery methods. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to implement IPC and synchronization mechanisms as outlined in the assessment criteria and content above.<br>2. Practical assessment involving writing code (e.g., in C/C++/Python) to demonstrate inter-process communication and implementing synchronization primitives (e.g., mutexes, semaphores) to solve a simple concurrency problem. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a simulated lab |

| | |
|---|---|
| | environment with access to a programming language IDE and a multi-threaded/multi-process environment.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 03** | **Evaluate and apply memory management strategies, including paging and virtual memory, to optimize resource utilization in operating systems** |
|---|---|
| Assessment Criteria | 3.1 Describe the fundamental concepts of memory management and address binding.<br>3.2 Differentiate between various contiguous and non-contiguous memory allocation techniques.<br>3.3 Explain the principles of virtual memory, paging, and segmentation.<br>3.4 Analyze page replacement algorithms and their impact on system performance |
| Content | 3.1 **Describe the fundamental concepts of memory management and address binding:**<br>3.1.1 Explain the need for memory management.<br>3.1.2 Differentiate between logical and physical addresses.<br>3.1.3 Discuss compile-time, load-time, and execution-time address binding.<br>3.1.4 Explain the Memory Management Unit (MMU).<br>3.2 **Differentiate between various contiguous and non-contiguous memory allocation techniques:**<br>3.2.1 Outline contiguous allocation: Fixed partitioning, Variable partitioning (First-Fit, Best-Fit, Worst-Fit).<br>3.2.2 Explain fragmentation (internal and external) and compaction.<br>3.2.3 Non-contiguous allocation: Paging and Segmentation (as separate concepts before virtual memory).<br>3.3 **Explain the principles of virtual memory, paging, and segmentation:**<br>3.3.1 Define virtual memory and its benefits (e.g., larger address space, less I/O).<br>3.3.2 Explain paging: page table, page faults, Translation Lookaside Buffer (TLB).<br>3.3.3 Explain segmentation: segment table, advantages over paging for user view.<br>3.3.4 Discuss demand paging and copy-on-write.<br>3.4 **Analyze page replacement algorithms and their impact on system performance:**<br>3.4.1 Explain the concept of thrashing.<br>3.4.2 Describe and apply common page replacement algorithms: FIFO (First-In, First-Out), LRU (Least Recently Used), |

| | |
|---|---|
| | Optimal (OPT - for comparison).<br>3.4.3 Calculate page fault rates for given page reference strings under different algorithms.<br>3.4.4 Compare the performance characteristics of these algorithms. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to evaluate memory management strategies as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using a memory management simulator to observe the effects of different allocation techniques or page replacement algorithms on page faults. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a simulated lab environment with access to operating system simulators or tools that demonstrate memory management.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 04** | **Manage file systems and input/output (I/O) operations using command-line and GUI tools across multiple OS platforms** |
|---|---|
| Assessment Criteria | 4.1 Describe the structure and organization of various file systems.<br>4.2 Explain different file access methods and directory structures.<br>4.3 Differentiate between various I/O hardware and software components.<br>4.4 Analyze disk scheduling algorithms and their impact on I/O performance |
| Content | 4.1 **Describe the structure and organization of various file systems:**<br>4.1.1 Outline the attributes of a file.<br>4.1.2 Explain file operations (create, read, write, delete, seek).<br>4.1.3 Discuss common file system structures (e.g., FAT, NTFS, Ext4, HFS+).<br>4.1.4 Describe file allocation methods (contiguous, linked, indexed).<br>4.2 **Explain different file access methods and directory structures:**<br>4.2.1 Explain file access methods: Sequential access, Direct access, |

| | |
|---|---|
| | Indexed sequential access.<br>4.2.2 Describe directory structures: Single-level, Two-level, Tree-structured, Acyclic-graph, General graph.<br>4.2.3 Discuss file system mounting and unmounting.<br>4.3 **Differentiate between various I/O hardware and software components:**<br>4.3.1 I/O hardware: Devices (block, character), controllers, ports.<br>4.3.2 I/O software: Device drivers, interrupt handlers, I/O scheduling.<br>4.3.3 Explain Direct Memory Access (DMA) and its role in I/O.<br>4.4 **Analyze disk scheduling algorithms and their impact on I/O performance:**<br>4.4.1 Explain the goals of disk scheduling (e.g., minimize seek time, maximize throughput).<br>4.4.2 Describe and apply common disk scheduling algorithms: FCFS (First-Come, First-Served), SSTF (Shortest-Seek-Time-First), SCAN (Elevator), C-SCAN, LOOK, C-LOOK.<br>4.4.3 Calculate total head movement for given disk request queues under different algorithms.<br>4.4.4 Compare the performance characteristics of these algorithms. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to manage file systems and I/O operations as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using command-line tools (e.g., ls, cd, mkdir, rm, df, mount in Linux; dir, cd, md, rd, fsutil in Windows) to manage files and directories, and using a disk scheduling simulator. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a simulated lab environment with access to various operating systems and disk scheduling simulators.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 05** | **Assess operating system performance through monitoring tools, benchmarking metrics, and performance tuning techniques** |
|---|---|
| Assessment Criteria | **5.1 Identify key metrics for evaluating operating system performance.**<br>**5.2 Utilize operating system monitoring tools to gather performance data.**<br>**5.3 Analyze collected performance data to identify bottlenecks and trends.**<br>**5.4 Propose strategies to optimize operating system performance.** |
| Content | **5.1 Identify key metrics for evaluating operating system performance:**<br>5.1.1 Explain the following:<br>• CPU utilization, context switch rate, process/thread count.<br>• Describe memory usage (physical, virtual, swap), page fault rate, cache hit/miss ratio.<br>• Disk I/O (read/write speed, queue length, utilization).<br>• Network I/O (bandwidth, latency, packet loss).<br>• System uptime, response time, throughput.<br>**5.2 Utilize operating system monitoring tools to gather performance data:**<br>• Describe the following operating system tools:<br>⇒ Windows: Task Manager, Resource Monitor, Performance Monitor (Perfmon).<br>⇒ Linux: `top`, `htop`, `vmstat`, `iostat`, `netstat`, `free`, `sar`, `perf`.<br>• Interpret basic output from these tools.<br>**5.3 Analyze collected performance data to identify bottlenecks and trends:**<br>5.3.1 Correlate high CPU usage with specific processes.<br>5.3.2 Identify excessive paging/swapping indicating memory pressure. |

| | |
|---|---|
| | 5.3.3 Analyze disk queue lengths for I/O bottlenecks.<br>5.3.4 Recognize network saturation or latency issues.<br>5.3.5 Identify performance trends over time (e.g., gradual degradation).<br>**5.4 Propose strategies to optimize operating system performance:**<br>5.4.1 Explain the following:<br>• CPU optimization: process priority, scheduling adjustments.<br>• Memory optimization: increasing RAM, optimizing application memory usage.<br>• Disk optimization: defragmentation, upgrading storage, RAID configurations.<br>• Network optimization: bandwidth management, QoS.<br>• General OS tuning: disabling unnecessary services, driver updates, kernel parameter tuning (conceptual). |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to assess operating system performance as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using OS monitoring tools on a running system (physical or virtual) to collect performance data, analyze it, and identify potential performance issues. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a lab environment with access to various operating systems and their built-in performance monitoring tools.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 06** | **Apply essential operating system security measures and protection mechanisms to safeguard system integrity and user data** |
|---|---|
| Assessment Criteria | **6.1 Describe the principles of operating system security and protection.**<br>**6.2 Apply access control mechanisms to secure system resources.**<br>**6.3 Explain common security threats and vulnerabilities in operating systems.**<br>**6.4 Implement basic security hardening techniques for operating systems.** |
| Content | **6.1 Describe the principles of operating system security and protection:**<br>6.1.1 Define security goals: Confidentiality, Integrity, Availability (CIA triad).<br>6.1.2 Explain protection mechanisms: separation of domains, least privilege, access matrix.<br>6.1.3 Discuss trusted computing base (TCB).<br>**6.2 Apply access control mechanisms to secure system resources:**<br>6.2.1 Explain discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC).<br>6.2.2 Implement file and directory permissions (e.g., Linux chmod, Windows NTFS permissions).<br>6.2.3 Discuss user authentication (passwords, multi-factor authentication) and authorization.<br>• Malware (viruses, worms, Trojans, ransomware, rootkits).<br>• Buffer overflows, privilege escalation attacks.<br>• Denial of Service (DoS) attacks.<br>• Social engineering and phishing (as they relate to OS compromise).<br>• Vulnerabilities due to misconfiguration, unpatched software, weak passwords.<br>6.2.4 Implement basic security hardening techniques for operating |

| | |
|---|---|
| | systems:<br>• Regular patching and updates.<br>• Disabling unnecessary services and ports.<br>• Configuring firewalls (host-based).<br>• Implementing strong password policies.<br>• User account management (creating, deleting, managing privileges).<br>• Basic auditing and logging (enabling security logs).<br>• Antivirus/Anti-malware software installation and configuration. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to apply OS security and protection mechanisms as outlined in the assessment criteria and content above.<br>2. Practical assessment involving configuring user permissions, enabling basic firewall rules, and analyzing security logs on a test operating system (e.g., Linux or Windows). |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in a lab environment with access to various operating systems for security configuration.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

**ASSESSMENT SCHEME**

| MODE OF ASSESSMENT | | WEIGHTING 100% |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Analyze and apply core techniques in process management and CPU scheduling within diverse operating system environments | 15 |
| Implement and manage inter-process communication (IPC) and synchronization methods to ensure effective coordination of concurrent system processes | 20 |
| Evaluate and apply memory management strategies, including paging and virtual memory, to optimize resource utilization in operating systems | 20 |
| Manage file systems and input/output (I/O) operations using command-line and GUI tools across multiple OS platforms | 15 |
| Assess operating system performance through monitoring tools, benchmarking metrics, and performance tuning techniques | 15 |
| Apply essential operating system security measures and protection mechanisms to safeguard system integrity and user data | 15 |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media for collaborative learning and resource sharing.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.

2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

5. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

6. **Facilities, Tools, Equipment and Materials**

   **Facilities:**

   - Computer Laboratory: Equipped with modern desktops/laptops to run operating systems, simulators, and programming environments.
   - Virtualization Lab: A controlled environment for creating and managing multiple virtual machines to simulate different OS environments and concurrency scenarios.
   - Smart Classroom/Multimedia Room: For delivering interactive lessons, showcasing simulations, and playing relevant videos.
   - Server Room (optional): To host virtual machines for larger-scale simulations or centralized lab environments.
   - Secure Storage Room (optional): For storing sensitive lab configurations or physical media.

   **Tools (Software):**

   - Operating Systems:
     - Host OS: Windows 10/11, Linux distributions (e.g., Ubuntu, Fedora).
     - Virtual Machine OSes: Various versions of Windows (e.g., 7, 10, Server), Linux distributions (e.g., Debian, CentOS), and potentially macOS (licensing permitting).
   - Virtualization Software: VMware Workstation/Player, Oracle VirtualBox, Microsoft Hyper-V.
   - OS Simulators:
     - CPU Scheduling Simulators (e.g., online tools, custom-built Python/Java simulators).
     - Memory Management Simulators (e.g., for paging, segmentation, page replacement algorithms).
     - Disk Scheduling Simulators.
   - Programming Languages & IDEs: C/C++, Python (for scripting and demonstrating concurrency), VS Code, PyCharm, Jupyter Notebooks.
   - System Monitoring Tools:
     - Windows: Task Manager, Resource Monitor, Performance Monitor (Perfmon).
     - Linux: `top`, `htop`, `vmstat`, `iostat`, `netstat`, `free`, `sar`, `perf`.
   - Basic Security Tools (OS-level): Built-in firewalls, user/group management interfaces, security log viewers (e.g., Windows Event Viewer, `journalctl` in Linux).
   - Productivity Software: Microsoft Office Suite or LibreOffice for documentation and presentations.

**Equipment (Hardware):**

- Workstations: High-performance desktops/laptops for each student (or pair) with sufficient CPU, RAM (16GB+ recommended), and SSD storage to run multiple VMs smoothly.
- Network Switches & Routers: For setting up basic lab networks and demonstrating network I/O.
- Projector and Smart Boards: For delivering visual content in class.
- External Hard Drives/USBs: For storing and transferring VM images and lab files.

## 7. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 8. Reference Materials (recommended textbooks, recommended readings)

Silberschatz, A., Galvin, P.B. and Gagne, G. (2018) *Operating System Concepts*. 10th edn. John Wiley & Sons.
Tanenbaum, A.S. and Bos, H. (2015) *Modern Operating Systems*. 4th edn. Pearson.
Stallings, W. (2018) *Operating Systems: Internals and Design Principles*. 9th edn. Pearson.
Arpaci-Dusseau, R.H. and Arpaci-Dusseau, A.C. (2018) *Operating Systems: Three Easy Pieces*. OSP. (Online resource).
Online resources such as NPTEL lectures, MIT OpenCourseware, and relevant academic journals.

Silberschatz, A., Galvin, P.B. and Gagne, G., 2018. *Operating System Concepts*. 10th ed. Hoboken: Wiley.

Tanenbaum, A.S. and Bos, H., 2015. *Modern Operating Systems*. 4th ed. Harlow: Pearson Education.

McHoes, A. and Flynn, I.M., 2018. *Understanding Operating Systems*. 8th ed. Boston: Cengage Learning.

Stallings, W., 2018. *Operating Systems: Internals and Design Principles*. 9th ed. Harlow: Pearson.

Bovet, D.P. and Cesati, M., 2005. *Understanding the Linux Kernel*. 3rd ed. Sebastopol: O'Reilly Media.

Love, R., 2010. *Linux Kernel Development*. 3rd ed. Upper Saddle River: Addison-Wesley.

Robbins, K.A. and Robbins, S., 2003. *Practical UNIX Programming: A Guide to Concurrency, Communication, and Multithreading*. Upper Saddle River: Prentice Hall.

Arpaci-Dusseau, R.H. and Arpaci-Dusseau, A.C., 2018. *Operating Systems: Three Easy Pieces*. [online]

| | |
|---|---|
| **Module Code:** | **682/25/M08** |
| **Module Title:** | **Incident Response** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 Hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Incident Response** of Unit Standards for a Digital Forensic Technician. |
| **Pre-requisite modules:** | No Pre-requisites |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an **individual** to be able to effectively communicate in business. This includes producing an incident response plan, identifying and detecting incidents, containing incidents, eradicating incident, recovering from incidents and documenting lessons learned.<br>This module is important as it helps mitigate malicious activity in computer systems and networks. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of Learning Outcomes:** | **LO1: Minimize impact and ensure business continuity by developing comprehensive strategies and procedures for handling cybersecurity incidents.**<br><br>**LO2: Detect incidents by monitoring systems, analyzing alerts, and recognizing indicators of compromise (IOCs).**<br><br>**LO3: Limit the scope and impact of security breaches by isolating affected systems, implementing temporary countermeasures, and preventing further damage or spread.**<br><br>**LO4: Cleanse affected systems and prevent recurrence by removing the root cause of the compromise, eliminating malicious artifacts, and patching vulnerabilities.**<br><br>**LO5: Recover from incident by restoring systems to normal operation, validating functionality, and implementing enhanced security measures.**<br><br>**LO6: Document lessons learned by conducting post-incident reviews, identifying areas for improvement, and updating incident response procedures.** |

| | |
|---|---|
| **Learning Outcome 01** | **Minimize impact and ensure business continuity by developing comprehensive strategies and procedures for handling cybersecurity incidents.** |
| **Assessment Criteria:** | **1.1 Develop Incident Response Plan (IRP)**<br>**1.2 Establish Incident Response Team (IRT) with defined roles and responsibilities**<br>**1.3 Conduct regular training and simulations (e.g., tabletop exercises).**<br>**1.4 Maintain an up-to-date inventory of assets and systems** |
| **Content:** | **1.1 Develop Incident Response Plan (IRP)**<br>● Define incident<br>● Describe types of incident<br>● Classify incidents<br>● Explain the structure of Incident Response Plan (IRP)<br><br>**1.2 Establish Incident Response Team (IRT) with defined roles and responsibilities**<br>● Define an incident in digital forensics (e.g., data breaches, malware infections, unauthorized access).<br>● Illustrate why a dedicated team is necessary for handling incidents.<br>● Articulate the Incident Lifecycle<br>● Describe the team structure and responsibilities for each team member.<br>● Describe Mobile Device Forensics in Incident Response<br>● Extrapolate Incident Response Plan (IRP) for digital forensics<br>● Explain Legal and Compliance Considerations in incident response.<br>● Explain communication channels/links in the IRT<br><br>**1.3 Conduct regular training and simulations (e.g., tabletop exercises).**<br>● Describe the phases taken by the Incidents Response Team in real world.<br><br>**1.4 Maintain an up-to-date inventory of assets and systems**<br>● Identify different types of assets (e.g., hardware, software, data, network devices).<br>● Classify assets based on their criticality, sensitivity, and value to the organization.<br>● Describe asset inventory management tools (Nessus, Nmap).<br>● Explain data collection and documentation methods.<br>● Describe risk assessment and prioritization of assets.<br>● Outline compliance and legal requirements. |

| | |
|---|---|
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to produce an incident response plan as outlined in the assessment criteria.<br>2. Practical assessment on developing an Incident Response Plan (IRP), establishing an Incident Response Team (IRT) with defined roles and responsibilities, Conducting Regular training and simulations (e.g., tabletop exercises), identifying Tools and technologies for monitoring, detection, and analysis, and maintaining an up-to-date inventory of assets and systems based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:-<br>● Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics |

| **Learning Outcome 02** | **Detect incidents by monitoring systems, analyzing alerts, and recognizing indicators of compromise (IOCs).** |
|---|---|
| **Assessment Criteria** | **2.1 Monitor systems and networks for unusual activity.**<br>**2.2 Utilize tools like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM).**<br>**2.3 Analyse Logs, traffic, and user behavior for signs of compromise.**<br>**2.4 Validate the incident and classify its severity.** |
| **Content** | **2.1 Monitor systems and networks for unusual activity.**<br>● Define system and network monitoring and its role in cybersecurity.<br>● Explain the importance of continuous monitoring in identifying potential threats.<br>● Describe common indicators of compromise (IoCs), including unusual network traffic, unauthorized access attempts, and system anomalies.<br>● Outline different monitoring techniques, such as signature-based, anomaly-based, and heuristic detection**.**<br>**2.2 Utilize tools like Intrusion Detection Systems (IDS) and Security** |

| | |
|---|---|
| | **Information and Event Management (SIEM).**<br>● Define Intrusion Detection Systems (IDS) and differentiate between host-based (HIDS) and network-based (NIDS) IDS.<br>● Explain the functionality of Security Information and Event Management (SIEM) in centralizing log collection, correlation, and analysis.<br>● Describe the benefits of IDS and SIEM integration in improving threat detection capabilities.<br>● Outline challenges in configuring and managing IDS/SIEM.<br>**2.3 Analyse Logs, traffic, and user behaviour for signs of compromise.**<br>● Define log analysis and its importance in identifying security incidents.<br>● Explain different types of logs (system, application, network, firewall) and their relevance in incident detection.<br>● Describe traffic analysis techniques, including packet inspection and flow monitoring, to detect anomalies.<br>● Analyse user behaviour to identify suspicious activities, such as unauthorized logins, privilege escalation, or data exfiltration. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to identify and detect incidents as outlined in the assessment criteria and content above.<br>2. Practical assessment on monitor systems and networks for unusual activity, utilize tools like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM), analyse logs, traffic, and user behaviour for signs of compromise, validate incident and classify its severity based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>Legal Tools and Materials (eg. Data Protection Act, NIST) and Ethical Tools and Materials (e.g., ACM Code of Ethics, IEEE Code of Ethics), Splunk, QRadar, ArcSight, Snort, Suricata, CrowdStrike, SentinelOne, ELK Stack, Graylog |

| Learning Outcome 03 | **Limit the scope and impact of security breaches by isolating affected systems, implementing temporary countermeasures, and preventing further damage or spread** |
|---|---|
| **Assessment Criteria** | **3.1 Isolate affected systems or networks to prevent further damage**<br>**3.2 Apply temporary fixes to allow systems to operate safely while investigation continues.**<br>**3.3 Preserve evidence (for forensic analysis).** |
| **Content** | **3.1 Isolate affected systems or networks to prevent further damage**<br>● Define incident containment and its importance in preventing an attack from spreading.<br>● Explain different isolation techniques, including network segmentation, host quarantine, and disabling compromised accounts.<br>● Describe the impact of improper isolation, such as persistence of threats or disruption of critical services.<br>● Outline best practices for containing malware infections, insider threats, and denial-of-service (DoS) attacks.<br>**3.2 Apply temporary fixes to allow safe system operation during investigation**<br>● Define temporary fixes and their role in maintaining business continuity during an incident.<br>● Explain the difference between short-term containment (e.g., blocking malicious IPs) and long-term remediation (e.g., patching vulnerabilities).<br>● Describe techniques for limiting damage while maintaining system functionality, such as enabling firewall rules, disabling specific services, or implementing security patches.<br>● Outline challenges in applying temporary fixes, including the risk of incomplete containment or unintended disruptions.<br>**3.3 Preserve evidence for forensic analysis**<br>● Define evidence preservation and its significance in cybersecurity investigations.<br>● Explain the principles of chain of custody to maintain the integrity of forensic evidence.<br>● Describe different methods of evidence collection, including capturing volatile memory, securing log files, and creating forensic disk images.<br>● Outline best practices for handling digital evidence, such as using write-blocking tools, hashing techniques for verification, and secure storage procedures |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to contain incidents as outlined in the assessment criteria and content above.<br>2. Practical assessment on using appropriate tools to isolate affected systems or networks to prevent further damage, applying temporary fixes to allow systems to operate safely while investigation continues and preserving evidence (for forensic analysis) based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - Firewalls (Palo Alto, Cisco ASA, Fortinet), VLAN Segmentation Tools, TheHive, Cortex XSOAR, Antivirus, Autopsy, FTK Imager |

| | |
|---|---|
| **Learning Outcome 04** | **Cleanse affected systems and prevent recurrence by removing the root cause of the compromise, eliminating malicious artifacts, and patching vulnerabilities** |
| **Assessment Criteria** | **4.1 Remove Malware and unauthorized access.**<br>**4.2 Patch vulnerabilities and update software.**<br>**4.3 Clean and restore affected systems.** |
| **Content** | **4.1 Remove malware and unauthorized access**<br>● Define malware removal and explain its role in restoring system integrity.<br>● Describe different malware removal techniques, including antivirus scans, endpoint detection and response (EDR) tools, and manual removal using forensic analysis.<br>● Explain the importance of removing backdoors and persistence mechanisms to prevent re-infection.<br>● Outline methods for revoking unauthorized access, such as resetting compromised credentials, disabling malicious accounts, and reconfiguring network access controls.<br>**4.2 Patch vulnerabilities and update software**<br>● Define vulnerability patching and explain its role in closing security gaps.<br>● Describe common types of vulnerabilities, including unpatched |

| | |
|---|---|
| | software, misconfigurations, and outdated security controls.<br>● Explain the importance of prioritizing patches based on risk severity, exploitability, and impact.<br>● Outline best practices for safe patching, including testing patches in a controlled environment before deployment.<br><br>**4.3 Clean and restore affected systems**<br>● Define system restoration and explain the steps involved in returning a system to a secure state.<br>● Describe methods for verifying system integrity, including scanning for residual threats, checking system logs, and validating data integrity.<br>● Explain the use of backup and recovery strategies to restore clean versions of affected systems.<br>● Outline post-eradication measures, such as monitoring for reinfection, conducting forensic reviews, and reassessing security controls. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to eradicate incident as outlined in the assessment criteria and content above.<br>2. Practical assessment on removing malware and unauthorized access, patching vulnerabilities and updating software and cleaning and restoring affected systems based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:- Malwarebytes,Windows Defender, ClamAV, Nessus, OpenVAS, Qualys, Volatility, Rekall |

| | |
|---|---|
| **Learning Outcome 05** | **Recover from incident by restoring systems to normal operation, validating functionality, and implementing enhanced security measures** |
| **Assessment Criteria** | **5.1 Rebuild and reconfigure systems.**<br>**5.2 Test systems.**<br>**5.3 Reintegrate systems into the production environment** |
| **Content** | **5.3 Rebuild and reconfigure systems**<br>● Define system rebuilding and its importance in ensuring a clean, uncompromised environment.<br>● Describe different approaches to system rebuilding, such as reimaging systems, reinstalling operating systems, and restoring from trusted backups.<br>● Explain best practices for secure configuration, including applying security baselines, implementing least privilege access, and hardening system settings.<br>● Outline challenges in system reconfiguration, such as compatibility issues, ensuring all security patches are applied, and minimizing downtime.<br><br>**5.4 Test systems**<br>● Define post-recovery testing and its role in verifying system security and functionality.<br>● Describe different testing methods, including penetration testing, vulnerability scans, and functionality testing.<br>● Explain how to validate system integrity, such as checking for residual threats, ensuring logs are functioning, and monitoring network traffic.<br>● Outline best practices for system verification, including conducting controlled user access tests, auditing system logs, and ensuring compliance with security policies.<br><br>**5.5 Reintegrate systems into the production environment**<br>● Define system reintegration and explain its significance in restoring normal operations.<br>● Describe the steps for reintegrating systems, including phased deployment, continuous monitoring, and controlled rollouts.<br>● Explain risk mitigation strategies, such as using a staged approach, isolating newly restored systems for observation, and implementing enhanced monitoring post-reintegration.<br>● Outline best practices for ensuring business continuity, including validating data integrity, ensuring user access control, and documenting lessons learned. |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to recover from incident outlined in the assessment criteria and content above.<br>2. Practical assessment on rebuild and reconfigure systems, test systems and reintegrate systems into the production environment based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - Veeam Backup & Replication, Acronis Cyber Protect, Commvault, Tripwire, OSSEC, Ansible, Puppet, Chef |

| | |
|---|---|
| **Learning Outcome 06** | **Document lessons learned by conducting post-incident reviews, identifying areas for improvement, and updating incident response procedures** |
| **Assessment Criteria** | **6.1 Perform Post-incident review**<br>**6.2 Update incident response plan based on lessons learned.**<br>**6.3 Share findings with stakeholders**<br>**6.4 Produce Incident document** |
| **Content** | **6.1 Conduct post-incident review**<br>● Define post-incident review (PIR) and explain its role in improving future incident response.<br>● Describe the key elements of a PIR, including incident timeline, root cause analysis, response effectiveness, and areas for improvement.<br>● Explain different methods for conducting a PIR, such as debriefing meetings, incident response reports, and forensic analysis.<br>● Outline best practices for ensuring a comprehensive review, including gathering feedback from all involved teams, analyzing system logs, and identifying patterns in recurring incidents.<br>**6.2 Update incident response plan based on lessons learned**<br>● Define the importance of updating the Incident Response Plan (IRP) after an incident.<br>● Describe key areas for IRP updates, such as refining detection mechanisms, improving response coordination, and addressing procedural gaps. |

| | |
|---|---|
| | ● Explain methods for integrating lessons learned, including adjusting escalation protocols, enhancing security controls, and updating employee training.<br>● Outline strategies for ensuring continuous improvement, such as conducting regular IRP reviews and adapting to emerging threats.<br><br>**6.3 Share findings with stakeholders**<br>● Define the importance of stakeholder communication in cybersecurity incident management.<br>● Describe key stakeholders involved in incident response, including executives, IT teams, legal departments, compliance officers, and external regulators.<br>● Explain best practices for sharing findings, such as creating executive summaries, using clear and non-technical language for non-technical stakeholders, and providing actionable recommendations.<br>● Outline confidentiality considerations when sharing sensitive information, ensuring compliance with data protection regulations.<br><br>**6.4 Produce incident report document**<br>● Define an incident report and its purpose in documenting the incident response process.<br>● Describe essential components of an incident report.<br>● Explain the importance of maintaining a standardized report format to ensure consistency and compliance.<br>● Outline best practices for storing and managing incident reports, including secure storage, access control, and regulatory retention requirements. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to document lessons learnt from the incident as outlined in the assessment criteria and content above.<br>2. Practical assessment on performing post-incident review, updating incident response plan based on lessons learned, sharing findings with stakeholders and producing incident report based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - JIRA, ServiceNow, |

| | |
|---|---|
| | Confluence, Case Management Systems |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING 100%** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Minimize impact and ensure business continuity by developing comprehensive strategies and procedures for handling cybersecurity incidents | 20% |
| Detect incidents by monitoring systems, analyzing alerts, and recognizing indicators of compromise (IOCs) | 20 % |
| Limit the scope and impact of security breaches by isolating affected systems, implementing temporary countermeasures, and preventing further damage or spread | 10% |
| Cleanse affected systems and prevent recurrence by removing the root cause of the compromise, eliminating malicious artifacts, and patching vulnerabilities | 20% |
| Recover from incident by restoring systems to normal operation, validating functionality, and implementing enhanced security measures | 20 % |
| Document lessons learned by conducting post-incident reviews, identifying areas for improvement, and updating incident response procedures | 10% |

| | |
|---|---|
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**
   Forensic Lab Setup, Virtual Machines, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics, Legal Tools and Materials (eg. Data Protection Act, NIST) and Ethical Tools and Materials (e.g., ACM Code of Ethics, IEEE Code of Ethics), Splunk, QRadar, ArcSight, Snort, Suricata, CrowdStrike, SentinelOne, ELK Stack, Graylog

3. **Learning Resources**

   Relevant training manual (learners' guide) and facilitators' guide

4. **Reference Materials (recommended textbooks, recommended readings)**

   Holt, T.J., Bossler, A.M., and Seigfried-Spellar, K.C. (2022). Cybercrime and Digital Forensics: An Introduction. 3rd ed. New York: Routledge.

Luttgens, J.T., Pepe, M., and Mandia, K. (2020). Incident Response & Computer Forensics. 3rd ed. New York: McGraw-Hill Education.

Sammons, J. (2021). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 3rd ed. Waltham, MA: Syngress.

Kävrestad, J. (2020). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. 2nd ed. Cham, Switzerland: Springer.

Reith, M., Carr, C., and Gunsch, G. (2022). Digital Forensics and Incident Response: A Practical Guide to Investigating and Responding to Cyber Attacks. Birmingham, UK: Packt Publishing.

Carrier, B. (2005) File system forensic analysis. Boston, MA: Addison-Wesley Professional.

Casey, E. (2011) Digital evidence and computer crime: forensic science, computers, and the internet. 3rd edn. Waltham, MA: Academic Press.

Luttgens, J.T., Pepe, M. and Mandia, K. (2014) Incident response & computer forensics. 3rd edn. New York, NY: McGraw-Hill Education.

Sammons, J. (2015) The basics of digital forensics: the primer for getting started in digital forensics. 2nd edn. Waltham, MA: Syngress.

Solomon, M.G., Rudolph, K., Tittel, E., Broom, N. and Barrett, D. (2011) Computer forensics jumpstart. 2nd edn. Indianapolis, IN: Wiley.

| | |
|---|---|
| **Module Code:** | **682/25/M09** |
| **Module Title:** | **DATABASE SECURITY AND FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 16 |
| **Duration:** | 160 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Database Security And Forensics** of Qualification Standard for Digital Forensic Technician. |
| **Pre-requisite modules:** | N/A |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by a Digital Forensic Technician to understand and apply database management, security, and forensic techniques, including data recovery, analysis, securing database environments, ensuring evidence integrity, and complying with legal and regulatory standards during database-related investigations.<br>This includes analyzing database models and architectures, Identifying Data Storage & Retrieval Mechanisms, Implementing Authentication & Access Management, Applying Database Encryption & Data Protection, Identifying & Mitigate Database Attacks, Configuring Log Monitoring & Anomaly Detection, Acquire and preserve forensic data, Recover Deleted & Modified Data, Respond to Database Breaches, Conduct Root Cause Analysis & Reporting, Implement Cloud Database Security & Compliance, Identify Cloud Forensic Tools & Data Acquisition methods, Check Real-World Database Forensic Investigations, Provide Advanced Forensic Techniques & Expert Testimony. |
| **List of Learning Outcomes:** | **LO1: Determine the appropriateness of database models and architectures for specific applications and organisational contexts.**<br>**LO2: Identify data storage and retrieval mechanisms to understand how data is persistently stored and efficiently accessed within various database systems.**<br>**LO3: Control database access by configuring user roles, permissions, and authentication protocols.**<br>**LO4: Configure backup and recovery strategies to safeguard sensitive information against unauthorized disclosure and data loss by implementing encryption techniques for data at rest and in transit.**<br>**LO5: Protect database systems from various threats by identifying and mitigating database attacks through recognizing common attack vectors, vulnerabilities, and implementing appropriate security controls and countermeasures.** |

| | |
|---|---|
| | **LO6: Configure log monitoring and anomaly detection by setting up logging mechanisms, analyzing log data, and implementing rules for identifying unusual activities to detect and respond to suspicious behavior and potential security incidents within database environments.**<br>**LO7: Acquire and preserve forensic data by employing forensically sound methods and tools to collect data from various sources**<br>**LO8: Reconstruct and restore deleted or altered data from database systems by utilizing specialized tools and techniques.**<br>**LO9: Minimize the impact of security incidents and restore database integrity and confidentiality by executing incident response plans, containing the breach, and coordinating with relevant stakeholders.**<br>**LO10: Conduct root cause analysis and reporting by investigating the underlying factors contributing to database incidents and documenting findings in comprehensive reports.**<br>**LO11: Secure data and maintain compliance in dynamic cloud environments by configuring cloud-native security features, adhering to industry best practices, and ensuring regulatory compliance for cloud-based databases.** |

| Learning Outcome 01 | **Determine the appropriateness of database models and architectures for specific applications and organisational contexts** |
|---|---|
| **Assessment Criteria:** | **1.1 Describe Different types of database models (relational, NoSQL, object-oriented, etc.).**<br>**1.2 Compare centralized, distributed, and cloud-based database architectures.**<br>**1.3 Demonstrate the ability to structure and query a relational database.**<br>**1.4 Evaluate the strengths and weaknesses of various database models in forensic investigations.** |
| **Content:** | **1.1 Describe Different types of database models (relational, NoSQL, object-oriented, etc.).**<br>● Define Relational Database Model<br>● Describe NoSQL Database Model<br>● Explain Object-Oriented Database Model<br>● Outline Hierarchical Database Model<br>● Analyse Network Database Model<br>● Compare Different Database Models<br><br>**1.2 Compare centralized, distributed, and cloud-based database architectures.**<br>● Define Centralized Database Architecture<br>● Describe Distributed Database Architecture<br>● Explain Cloud-Based Database Architecture<br>● Compare Performance & Scalability<br>● Analyse Security & Reliability<br>● Outline Use Cases<br><br>**1.3 Demonstrate the ability to structure and query a relational database.**<br>● Outline the process of structuring data to eliminate redundancy and improve efficiency (e.g., 1NF, 2NF, 3NF).<br>● Demonstrate the use of SELECT, INSERT, UPDATE, DELETE statements to manipulate data in a relational database.<br>● Use JOINs, GROUP BY, HAVING, and subqueries to retrieve and analyze data efficiently.<br>● Analyse how indexes and constraints (e.g., UNIQUE, NOT NULL, CHECK) optimize performance and enforce data integrity.<br>● Outline best practices for improving query performance, such as indexing, avoiding unnecessary computations, and optimizing SQL |

| | |
|---|---|
| | execution plans.<br><br>**1.4 Evaluate the strengths and weaknesses of various database models in forensic investigations.**<br>● Define the Role of Databases in Forensics.<br>● Analyse Relational Databases – Describe their strength in maintaining data integrity, structured querying (SQL), and ACID compliance but highlight challenges with scalability and unstructured data. Example: MySQL, PostgreSQL.<br>● Explain their advantage in handling large volumes of unstructured forensic data (e.g., logs, social media) but note issues with consistency and complex querying. Example: MongoDB, Cassandra.<br>● Assess Object-Oriented Databases – Outline their ability to store forensic objects (e.g., multimedia evidence) efficiently but highlight challenges in adoption and query standardization. Example: ObjectDB.<br>● Compare Centralized vs. Distributed Models. |
| **Assessment Tasks:** | 1. Written and/or Oral Assessment on the skills and knowledge required to identify, describe, and compare different database models (Relational, NoSQL, Object-Oriented) as outlined in the content above. This includes discussing the advantages and limitations of each model in various forensic applications.<br><br>2. Practical Assessment on Database Architecture Selection given a forensic investigation scenario, select and justify the most suitable database architecture (centralized, distributed, or cloud-based) based on the specific needs of the case. Demonstrate how the selected architecture meets performance, scalability, and security requirements.<br><br>3. Hands-on Tasks on Structuring and Querying a Relational Database, Design and implementation of a relational database for a forensic investigation, demonstrating the creation of tables, relationships, and normalization techniques and performing SQL queries (SELECT, INSERT, UPDATE, DELETE, JOINs) to extract, modify, and analyze forensic data. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 02** | **Identify data storage and retrieval mechanisms to understand how data is persistently stored and efficiently accessed within various database systems** |
| **Assessment Criteria** | **2.1 Identify different types of data storage mechanisms (SQL, NoSQL, data warehouses).**<br>**2.2 Use SQL queries to retrieve and manipulate data efficiently.**<br>**2.3 Explain the impact of indexing, partitioning, and caching on data retrieval.**<br>**2.4 Apply forensic techniques to retrieve deleted or hidden records.** |
| **Content** | **1.1 Identify different types of data storage mechanisms (SQL, NoSQL, data warehouses).**<br>● Define SQL Storage Mechanisms.<br>● Describe NoSQL Storage Mechanisms.<br>● Explain Data Warehouses.<br>● Highlight the strengths and weaknesses of SQL, NoSQL, and data warehouses in terms of scalability, performance, and use cases.<br>**1.2 Use SQL queries to retrieve and manipulate data efficiently.**<br>● Explain how SELECT, INSERT, UPDATE, and DELETE are used for data retrieval and manipulation.<br>● Use SELECT with filters (WHERE), sorting (ORDER BY), and limiting results (LIMIT).<br>● Use INSERT to add, UPDATE to modify, and DELETE to remove data.<br>● Demonstrate JOINs, GROUP BY, and HAVING for complex data operations.<br>● Outline Optimization by discussing indexes and query structure improvements for better performance.<br>**1.3 Explain the impact of indexing, partitioning, and caching on data retrieval.**<br>● Explain how indexes speed up data retrieval by allowing faster searches and sorting.<br>● Outline how partitioning splits data into smaller sections to improve query performance and parallel processing.<br>● Analyze how caching stores frequently accessed data in memory to reduce retrieval time.<br>● Compare how indexing, partitioning, and caching enhance query efficiency and reduce system load.<br>**1.4 Apply forensic techniques to retrieve deleted or hidden records.**<br>● Explain how forensic techniques can recover deleted or hidden records.<br>● Outline how file carving reconstructs deleted files from raw data.<br>● Analyze how deleted records in slack space can be retrieved. |

| | |
|---|---|
| | ● Describe methods like steganography and hidden partitions used to conceal data.<br>● Demonstrate the use of forensic tools (e.g., EnCase, FTK) to recover and analyze deleted/hidden records. |
| **Assessment Tasks** | 1. Written and/or Oral Assessment on the skills and knowledge required to identify and compare different data storage mechanisms (SQL, NoSQL, data warehouses). This includes describing their advantages, limitations, and typical use cases in forensic investigations.<br>2. Practical Assessment on data storage mechanism selection, given a forensic investigation scenario, select and justify the most suitable data storage mechanism (SQL, NoSQL, or data warehouse) based on data volume, retrieval speed, and query complexity. Demonstrate how the selected mechanism supports forensic tasks such as evidence retrieval and analysis.<br>3. Hands-on Task on Data Retrieval Techniques to perform a practical task to retrieve and manipulate data from a selected database (e.g., SQL or NoSQL). Use techniques like indexing, partitioning, and caching to optimize data retrieval and demonstrate the retrieval of both active and deleted/hidden records.<br>4. Case Study on Forensic Data Recovery:<br>● Analyze a case study where deleted or hidden records need to be retrieved from a forensic investigation. Demonstrate the use of forensic techniques like file carving, slack space recovery, and steganography to recover relevant evidence. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 03** | **Control database access by configuring user roles, permissions, and authentication protocols** |
|---|---|
| **Assessment Criteria** | **1.1 Configure and implement user authentication mechanisms (passwords, MFA, tokens).**<br>**1.2 Identify and mitigate role-based access control (RBAC) for database users.**<br>**1.3 Identify and mitigate risks associated with privilege escalation.**<br>**1.4 Apply best practices for database access control in forensic** |

| | |
|---|---|
| | **scenarios.** |
| **Content** | **3.1 Configure and implement user authentication mechanisms (passwords, MFA, tokens).**<br>● Explain how user authentication secures access by verifying authorized users.<br>● Outline password policies, creating strong passwords, and secure storage methods (e.g., hashing).<br>● Analyze how MFA requires multiple verification factors to enhance security.<br>● Explain how token-based authentication works with JWTs or OAuth tokens for user sessions.<br>● Demonstrate configuration and implementation of password policies, MFA, and token-based authentication.<br><br>**3.2 Identify and mitigate role-based access control (RBAC) for database users.**<br>● Explain RBAC as a model where access is granted based on user roles with specific permissions.<br>● Describe RBAC Implementation – Outline how to assign roles (e.g., admin, user) and permissions (e.g., read, write) to database users.<br>● Analyze how RBAC reduces unauthorized access and minimizes security risks.<br>● Explain common RBAC issues, such as overly permissive roles or lack of separation of duties.<br>● Describe practices like role audits and the principle of least privilege to secure access.<br><br>**3.3 Identify and mitigate risks associated with privilege escalation.**<br><br>● Explain privilege escalation as gaining unauthorized higher access rights.<br>● Outline vertical (higher privileges) and horizontal (same-level access) privilege escalation.<br>● Analyze common vulnerabilities like weak controls or misconfigurations that enable privilege escalation.<br>● Describe practices like the principle of least privilege and regular privilege reviews to prevent escalation.<br>● Explain using tools like audit logs and intrusion detection systems to block escalation attempts. |

| | |
|---|---|
| | **3.4 Apply best practices for database access control in forensic scenarios.**<br><br>● Explain managing user permissions to protect sensitive forensic data.<br>● Based Access Control limits privileges to essential forensic tasks.<br>● Analyze how restricting access to only necessary tasks reduces risks.<br>● Describe the importance of access audits and monitoring to detect suspicious activity.<br>● Explain how encrypting data ensures confidentiality and integrity in forensic scenarios. |
| **Assessment Tasks** | 1. Written/Oral Assessment on the skills and knowledge of authentication mechanisms, access control models, and best practices in database management as outlined in the learning content above, covering topics such as password policies, MFA, RBAC, and privilege escalation.<br>2. Practical Assessment – Evaluate the ability to configure and implement user authentication mechanisms (passwords, MFA, tokens) in a forensic environment. The student must demonstrate how to apply these mechanisms to secure a forensic system.<br>3. Hands-On Task – Implement Role-Based Access Control (RBAC) for a sample forensic database. The student will configure roles, assign permissions, and apply the least privilege principle to ensure data security.<br>4. Case Study Analysis – Provide a forensic scenario where privilege escalation has occurred. The student will identify vulnerabilities and apply mitigation strategies such as auditing, least privilege, and RBAC to prevent future incidents.<br>5. Practical Assessment – Set up a secure database environment, apply encryption, and demonstrate effective database access control in a forensic investigation. The student will also monitor access and create audit logs to track user actions. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| Learning Outcome 04 | **Configure backup and recovery strategies to safeguard sensitive information against unauthorized disclosure and data loss by implementing encryption techniques for data at rest and in transit** |
|---|---|
| **Assessment Criteria** | **4.1 Explain different encryption methods used in database security (TDE, AES, hashing).**<br>**4.2 Implement encryption mechanisms for securing sensitive database records.**<br>**4.3 Assess the impact of encryption on database performance.**<br>**4.4 Apply decryption techniques for forensic analysis of secured data.** |
| **Content** | **4.1 Explain different encryption methods used in database security (TDE, AES, hashing).**<br>● Define Encryption – Explain encryption as the process of converting data into an unreadable format to protect it from unauthorized access.<br>● Outline how TDE encrypts entire databases at rest, securing data without requiring application-level modifications.<br>● Analyze how AES, a symmetric encryption method, provides strong data security using key lengths of 128, 192, or 256 bits.<br>● Explain how hashing transforms data into a fixed-length value, ensuring integrity and authentication without allowing data reversal.<br>● Outline the differences between TDE, AES, and hashing, and explain when each method is best applied in database security.<br>**4.2 Implement encryption mechanisms for securing sensitive database records.**<br>● Explain the need for encryption in protecting sensitive database records from unauthorized access.<br>● Outline TDE Implementation – Describe how to enable Transparent Data Encryption (TDE) for encrypting databases at rest.<br>● Analyze how AES encryption secures data in transit and at rest using strong cryptographic keys.<br>● Apply hashing techniques to protect passwords and ensure data integrity.<br>● Implement Access Controls – Outline best practices for managing encryption keys and restricting access to encrypted data.<br>**4.3 Assess the impact of encryption on database performance.**<br>● Explain how encryption adds processing load, affecting query execution and storage.<br>● Describe how encryption impacts CPU usage, memory, and disk I/O.<br>● Outline how encryption can limit indexing and slow down search |

| | |
|---|---|
| | performance.<br>● Assess the performance differences between TDE, AES, and hashing.<br>● Describe strategies like selective encryption and hardware acceleration to reduce impact.<br>**4.4 Apply decryption techniques for forensic analysis of secured data.**<br>● Explain the process of converting encrypted data back into its readable form.<br>● Outline the role of encryption keys and their secure retrieval for decryption.<br>● Analyze techniques like AES decryption, private key usage, and password-based recovery.<br>● Describe how tools like EnCase and FTK assist in decrypting secured database records.<br>● Outline the ethical and legal constraints of decrypting protected data in forensic investigations. |
| **Assessment Tasks** | 1. Written and/or oral assessment applying database encryption & data protection based on the assessment criteria.<br>2. Practical assessment on implementing encryption (e.g., TDE, AES) to secure sensitive database records and analyze its performance impact.<br>3. Hands-on task on applying decryption techniques to recover encrypted forensic data using forensic tools and analyzing retrieved records. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 05** | **Protect database systems from various threats by identifying and mitigating database attacks through recognizing common attack vectors, vulnerabilities, and implementing appropriate security controls and countermeasures** |
| **Assessment Criteria** | **5.1 Detect and analyze SQL injection vulnerabilities in databases detected and analyzed.**<br>**5.2 Mitigated the risks of unauthorized database access through proper configurations mitigated.**<br>**5.3 Enforce threats posed by insider attacks identified and security measures enforced.**<br>**5.4 Develop countermeasures against common database attacks (e.g.,** |

| | |
|---|---|
| | **privilege escalation, buffer overflow).** |
| **Content** | **5.1 Detect and analyze SQL injection vulnerabilities in databases detected and analyzed.**<br>● Explain how attackers exploit input fields to execute malicious SQL queries.<br>● Outline methods such as input validation, error-based analysis, and log monitoring.<br>● Explain common SQL injection types, including Union-based, blind, and Time-based attacks.<br>● Assess the consequences, such as data breaches, privilege escalation, and unauthorized access.<br>● Describe secure coding practices, parameterized queries, and the use of Web Application Firewalls (WAFs).<br><br>**5.2 Mitigated the risks of unauthorized database access through proper configurations mitigated.**<br>● Explain threats like weak authentication, misconfigured permissions, and exposed databases.<br>● Outline steps such as enforcing least privilege, disabling unused services, and securing default accounts.<br>● Explain how RBAC limits user permissions and minimizes security risks.<br>● Describe how encrypting sensitive data prevents unauthorized access even if breached.<br>● Emphasize the importance of logging, anomaly detection, and security patches.<br><br>**5.3 Enforce threats posed by insider attacks identified and security measures enforced.**<br><br>● Explain risks posed by employees, contractors, or partners misusing database access.<br>● Describe privilege abuse, data theft, and unauthorized modifications.<br>● Outline RBAC, least privilege, and need-to-know principles to limit exposure.<br>● Highlight encryption, multi-factor authentication (MFA), and periodic access reviews.<br><br>**5.4 Develop countermeasures against common database attacks (e.g., privilege escalation, buffer overflow).** |

| | |
|---|---|
| | ● Explain privilege escalation, buffer overflow, and SQL injection threats.<br>● Outline input validation and secure coding techniques.<br>● Highlight access controls, parameterized queries, and regular patching.<br>● Outline Defensive Monitoring – Emphasize the role of intrusion detection systems (IDS) and database activity monitoring (DAM). |
| **Assessment Tasks** | 1. Written and/or oral assessment on identifying and analyzing common database attacks such as SQL injection, privilege escalation, and insider threats, as outlined in the assessment criteria.<br>2. Practical assessment on detecting SQL injection vulnerabilities in a database, demonstrating exploitation techniques and applying mitigation measures such as parameterized queries and input validation.<br>3. Hands-on task on securing a database by configuring access controls, implementing least privilege principles, and monitoring unauthorized access attempts.<br>4. Scenario-based task where students develop countermeasures against a simulated database attack, explaining their security choices and demonstrating risk mitigation techniques. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 06** | **Configure log monitoring and anomaly detection by setting up logging mechanisms, analyzing log data, and implementing rules for identifying unusual activities to detect and respond to suspicious behavior and potential security incidents within database environments** |
| **Assessment Criteria** | **6.1 Configure database logging mechanisms to capture critical events.**<br>**6.2 Analyze database logs to identify suspicious activities and anomalies.**<br>**6.3 Correlated database logs with system and network logs for forensic analysis.**<br>**6.4 Implement automated alerting mechanisms for security breaches**. |
| **Content** | **6.1 Configure database logging mechanisms to capture critical events.**<br>● Define database logging and its role in security and forensic investigations. |

| | |
|---|---|
| | ● Explain different types of database logs (e.g., transaction logs, error logs, audit logs) and their importance.<br>● Describe how to enable and configure logging features in various database systems (e.g., MySQL, SQL Server, PostgreSQL).<br>● Outline best practices for log retention, storage, and protection against tampering.<br>● Analyze how logging helps in detecting anomalies, unauthorized access, and suspicious activities.<br>**6.2 Analyze database logs to identify suspicious activities and anomalies.**<br>● Define database log analysis and its role in detecting security threats.<br>● Explain common indicators of suspicious activities, such as failed login attempts, unauthorized queries, and unusual data modifications.<br>● Describe techniques for parsing and filtering logs using SQL queries or log analysis tools.<br>● Analyze patterns in database logs to detect anomalies, insider threats, or external attacks.<br>● Outline best practices for real-time monitoring and alerting based on log data.<br>**6.3 Correlated database logs with system and network logs for forensic analysis.**<br>● Define log correlation and its importance in forensic investigations.<br>● Explain how database, system, and network logs provide a comprehensive view of security incidents.<br>● Describe techniques for linking database events with system and network activity to detect threats.<br>● Analyze case studies where log correlation helped in identifying cyberattacks or policy violations.<br>● Outline tools and methods used for automated log correlation in forensic analysis.<br>6.4 **Implement automated alerting mechanisms for security breaches**<br>● Define automated alerting and its role in security monitoring.<br>● Explain how real-time alerts help in detecting and responding to breaches.<br>● Describe key components of an effective alerting system (e.g., thresholds, triggers, notifications).<br>● Analyze different alerting techniques, such as SIEM-based alerts and anomaly detection.<br>● Outline best practices for configuring alerts to minimize false |

| | |
|---|---|
| | positives and ensure timely responses. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to explain the importance of log monitoring in detecting security breaches, including different log sources (database, system, network) and the role of log correlation in forensic investigations.<br>2. Practical assessment on configuring database logging mechanisms for critical events, demonstrating the correct setup and explaining how these logs can be used in future forensic analysis.<br>3. Hands-on task on analyzing database logs to identify suspicious activities and anomalies, followed by explaining the significance of the identified anomalies in the context of security.<br>4. Scenario-based assessment on correlating database logs with system and network logs to identify and investigate a potential security breach, demonstrating an understanding of the relationship between different log types. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 07** | **Acquire and preserve forensic data by employing forensically sound methods and tools to collect data from various sources** |
|---|---|
| **Assessment Criteria** | **7.1 Identify and acquire relevant database artifacts for forensic investigations.**<br>**7.2 Apply and maintain industry-standard forensic acquisition tools (FTK, encase) to collect database evidence.**<br>**7.3 Maintain integrity preserved and chain of custody for collected database artifacts.**<br>**7.4 Ensure compliance with forensic and legal guidelines during evidence acquisition.** |
| **Content** | **7.1 Identify and acquire relevant database artifacts for forensic investigations.**<br>● Define database artifacts (e.g., records, logs, metadata) in forensic investigations.<br>● Explain the process of identifying relevant artifacts to support the investigation.<br>● Describe the techniques for acquiring artifacts while maintaining |

| | |
|---|---|
| | data integrity.<br>● Outline tools for artifact acquisition (e.g., SQL queries, data extraction software).<br>● Analyze data preservation methods to ensure authenticity and prevent tampering.<br>**7.2 Apply and maintain industry-standard forensic acquisition tools (FTK, encase) to collect database evidence.**<br>● Define industry-standard forensic acquisition tools such as FTK and EnCase.<br>● Explain the process of using these tools to collect database evidence, ensuring proper chain of custody.<br>● Describe the steps involved in using FTK and EnCase to capture and preserve database artifacts.<br>● Outline the best practices for ensuring data integrity and authenticity during evidence collection.<br>● Analyze the effectiveness of FTK and EnCase in capturing different types of database evidence in forensic investigations.<br>**7.3 Maintain integrity preserved and chain of custody for collected database artifacts.**<br>● Define the concept of chain of custody and its importance in maintaining the integrity of database artifacts during forensic investigations.<br>● Explain the procedures for documenting the collection, handling, and storage of database artifacts to ensure integrity.<br>● Describe best practices for preserving the integrity of evidence, including the use of write blockers and ensuring proper encryption.<br>● Outline the process for creating a chain of custody log that details every individual who handles the evidence, along with timestamps and signatures.<br>● Analyze how failures in maintaining chain of custody can impact the admissibility of database evidence in court.<br>**7.4 Ensure compliance with forensic and legal guidelines during evidence acquisition.**<br>● Define relevant forensic and legal guidelines, such as FRE and ISO/IEC 27037.<br>● Explain the importance of legal compliance to ensure evidence admissibility in court.<br>● Describe steps for compliant evidence acquisition, including proper authorization and protocol adherence.<br>● Outline the role of forensic professionals in maintaining evidence integrity within legal frameworks. |

| | |
|---|---|
| | ● Analyze the risks of non-compliance, including the potential for evidence to be deemed inadmissible. |
| **Assessment Tasks** | 1. Written assessment on the knowledge and skills required to identify relevant database artifacts for forensic investigations, including legal and ethical considerations in evidence collection.<br>2. Practical assessment on using industry-standard forensic acquisition tools (e.g., FTK, EnCase) to collect database evidence, ensuring proper procedures and protocols are followed.<br>3. Case study analysis where students must demonstrate how to maintain the integrity and chain of custody for collected evidence, explaining the impact of mishandling.<br>4. Scenario-based task to ensure compliance with forensic and legal guidelines during evidence acquisition, where students must identify potential legal pitfalls and mitigate them |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 08** | **Reconstruct and restore deleted or altered data from database systems by utilizing specialized tools and techniques** |
|---|---|
| **Assessment Criteria** | **8.1 Use forensic tools to recover deleted database records.**<br>**8.2 Identify unauthorized modifications by analyzing database transaction logs.**<br>**8.3 Reconstruct the timeline of changes made to the database.**<br>**8.4 Validate recovered data to ensure accuracy and integrity.** |
| **Content** | **8.1 Use forensic tools to recover deleted database records.**<br>● Explain how forensic tools identify deleted database records through unallocated space and transaction logs.<br>● Describe how tools like FTK Imager and EnCase recover deleted data by scanning raw storage areas.<br>● Outline techniques for recovering deleted data using transaction logs, journal entries, and shadow copies.<br>● Define logical and physical deletion and how tools differentiate between them for recovery. |

| | |
|---|---|
| | ● Analyze challenges in data recovery, such as overwriting, fragmentation, and database maintenance.<br>**8.2 Identify unauthorized modifications by analyzing database transaction logs.**<br>● Explain how transaction logs track changes to the database, including updates and deletions.<br>● Describe how to analyze logs for unauthorized modifications by reviewing timestamps, user IDs, and changes.<br>● Outline methods to compare logs with baseline data to spot discrepancies.<br>● Define techniques like log hashing to verify log integrity.<br>● Analyze indicators of unauthorized activity, such as unusual access patterns or excessive changes.<br>**8.3 Reconstruct the timeline of changes made to the database.**<br>● Define the concept of a timeline in the context of database changes, focusing on key events such as insertions, updates, and deletions.<br>● Explain how to gather relevant data from transaction logs, system logs, and backup files to piece together the sequence of changes.<br>● Describe methods for correlating timestamps and identifying patterns of changes to reconstruct an accurate timeline.<br>● Outline the process of using forensic tools (e.g., FTK, EnCase) to automate the reconstruction of changes and generate detailed reports.<br>● Analyze the impact of each change in the timeline to determine the context of the database modification and any potential security breaches.<br>**8.4 Validate recovered data to ensure accuracy and integrity.**<br>● Define the validation process, ensuring recovered data's accuracy and integrity.<br>● Explain techniques like hash comparisons and checksum verification to confirm data correctness.<br>● Describe methods to cross-check recovered data with backups or transaction logs.<br>● Outline steps for assessing data integrity, checking for corruption or tampering.<br>● Analyze the impact of errors in validation on the forensic value of the data. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to recover deleted and modified database records, identify unauthorized modifications through transaction logs, reconstruct timelines of changes, |

| | |
|---|---|
| | and validate recovered data for accuracy and integrity, as outlined in the assessment criteria and content above.<br>2. Practical assessment on using forensic tools to recover deleted database records, analyzing transaction logs for unauthorized modifications, reconstructing a timeline of database changes, and validating the recovered data to ensure its integrity and accuracy. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 09** | **Minimize the impact of security incidents and restore database integrity and confidentiality by executing incident response plans, containing the breach, and coordinating with relevant stakeholders** |
|---|---|
| **Assessment Criteria** | **9.1 Develop an incident response plan specific to database security breaches developed.**<br>**9.2 Identify database breaches investigated and compromised data.**<br>**9.3 Contain and mitigate ongoing database threat.**<br>**9.4 Document findings and report incidents to relevant stakeholders.** |
| **Content** | **9.1 Develop an incident response plan specific to database security breaches developed.**<br>● Define key components of an incident response plan (IRP) for database breaches, including objectives, roles, and communication strategies.<br>● Analyze database security risks and identify vulnerabilities that should be addressed in the plan.<br>● Explain methods for detecting, classifying, and assessing the severity of database security breaches.<br>● Describe steps to contain a breach, including data isolation, access restriction, and team coordination.<br>● Outline procedures for recovery and restoring systems, emphasizing backup data and business continuity.<br>● Develop post-incident reporting practices, ensuring proper documentation and regulatory compliance.<br>**9.2 Identify database breaches investigated and compromised data.**<br>● Define common database breaches (e.g., SQL injection, unauthorized access). |

| | |
|---|---|
| | ● Analyze indicators of compromise like suspicious queries and login attempts.<br>● Explain the investigation process, including evidence collection and log analysis.<br>● Describe methods for detecting data leakage and compromised records.<br>● Outline procedures for correlating database and system logs to assess the breach.<br>● Identify compromised data by detecting unauthorized changes or access patterns.<br>**9.3 Contain and mitigate ongoing database threat.**<br>● Define actions to contain a database threat, such as isolating systems or disabling compromised accounts.<br>● Analyze the breach's scope and identify affected systems.<br>● Explain applying patches to close exploited vulnerabilities.<br>● Describe limiting access through firewalls, ACLs, or VPNs.<br>● Outline restoring secure database configurations and backups.<br>● Identify ongoing threats and implement monitoring to detect further issues.<br>**9.4 Document findings and report incidents to relevant stakeholders.**<br>● Define the key findings of the database breach, including attack methods, affected data, and compromised systems.<br>● Analyze the breach's impact on business operations, compliance, and data integrity.<br>● Explain the steps taken to contain and mitigate the breach, along with any corrective measures.<br>● Describe how evidence is documented, ensuring it aligns with legal and regulatory requirements.<br>● Outline the process of preparing a formal incident report for stakeholders, including management, legal teams, and external partners.<br>● Identify the stakeholders who require incident reporting and ensure the information is communicated promptly and clearly. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to respond to database breaches as outlined in the assessment criteria and content above.<br>2. Practical assessment on developing an incident response plan specific to database security breaches developed, containing and mitigating ongoing database threats and documenting findings and reporting incidents to relevant stakeholders**.** |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 10** | **Conduct root cause analysis and reporting by investigating the underlying factors contributing to database incidents and documenting findings in comprehensive reports** |
| **Assessment Criteria** | **10.1 Conduct forensic analysis to determine the root cause of database security incidents.**<br>**10.2 Generate forensic reports detailing the impact and timeline of the breach.**<br>**10.3 Provide recommendations for mitigating future security risks provided.**<br>**10.4 Ensure proper legal documentation for potential court proceedings ensured.** |
| **Content** | **10.1 Conduct forensic analysis to determine the root cause of database security incidents.**<br>● Define forensic analysis for database security, focusing on gathering and interpreting evidence to find the breach origin.<br>● Describe techniques for investigating incidents, including reviewing logs and transaction records to detect malicious activity.<br>● Explain the process of correlating database, network, and system logs to pinpoint the breach cause.<br>● Analyze common causes like SQL injection, privilege escalation, and misconfigurations.<br>● Outline tools such as EnCase, FTK, and log management software used for forensic analysis.<br>● Identify security gaps and vulnerabilities that may have contributed to the breach.<br>**10.2 Generate forensic reports detailing the impact and timeline of the breach.**<br>● Define forensic reporting as documenting findings from a security incident with accuracy and legal compliance.<br>● Describe the report structure, including breach summary, impact, and a detailed event timeline.<br>● Explain the importance of documenting the timeline, from breach to |

| | |
|---|---|
| | recovery, for clarity.<br>● Outline methods for identifying compromised data, affected systems, and calculating breach scope.<br>● Analyze collected data to include key evidence, system vulnerabilities, and operational impact.<br>● Generate a report with findings, root cause analysis, and preventive recommendations.<br>● Highlight legal requirements for reporting, ensuring compliance with data breach regulations.<br>**10.3 Provide recommendations for mitigating future security risks provided.**<br>● Explain the importance of addressing root causes to prevent recurrence.<br>● Analyze past incidents to identify vulnerabilities and gaps in security.<br>● Describe best practices like access control, encryption, and audit logging.<br>● Outline strategies for continuous monitoring and regular security assessments.<br>● Provide recommendations for staff training and stronger authentication.<br>● Recommend technology upgrades like firewalls and intrusion detection systems.<br>● Emphasize improving incident response plans for better future responses.<br>**10.4 Ensure proper legal documentation for potential court proceedings ensured.**<br>● Define legal documentation as accurate records of forensic analysis and incident response for court use.<br>● Explain the importance of proper documentation to meet legal and regulatory standards.<br>● Describe key elements of legal documentation, such as chain of custody and incident logs.<br>● Outline procedures for secure evidence handling and detailed record-keeping.<br>● Analyze the role of clear, verifiable documentation in supporting investigation integrity.<br>● Ensure compliance with laws and regulations regarding digital evidence and data privacy in court proceedings. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to understand the legal and regulatory requirements for documentation of |

| | |
|---|---|
| | digital forensic evidence, as outlined in the assessment criteria and content above.<br>2. Practical assessment on ensuring proper legal documentation for potential court proceedings by applying correct procedures in a simulated forensic investigation, including the proper handling and recording of evidence. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 11** | **Secure data and maintain compliance in dynamic cloud environments by configuring cloud-native security features, adhering to industry best practices, and ensuring regulatory compliance for cloud-based databases** |
|---|---|
| **Assessment Criteria** | **11.1 Explain cloud database architectures and their security challenges.**<br>**11.2 Implement access controls for securing cloud-based databases.**<br>**11.3 Identify legal and compliance requirements for cloud database forensics.**<br>**11.4 Investigate cloud database security breaches using forensic tools.** |
| **Content** | **11.1 Explain cloud database architectures and their security challenges.**<br>● Explain the structure of cloud databases, including storage models and data distribution.<br>● Analyze risks such as data breaches, unauthorized access, and shared responsibility between users and cloud providers.<br>● Outline encryption, access control, and data integrity measures for cloud databases.<br>● Explain the importance of compliance with data protection laws (e.g., GDPR, HIPAA) in cloud environments.<br>**11.2 Implement access controls for securing cloud-based databases.**<br>● Define access control mechanisms: Outline RBAC, ABAC, and DAC for restricting database access.<br>● Describe multi-factor authentication (MFA) and single sign-on (SSO) for secure access.<br>● Configure user roles to grant appropriate access and minimize security risks.<br>● Implement logging and continuous monitoring to detect |

| | |
|---|---|
| | unauthorized access.<br>● Describe compliance: Ensure access controls meet industry regulations like GDPR and ISO 27001.<br>**11.3 Identify legal and compliance requirements for cloud database forensics.**<br>● Explain GDPR, HIPAA, and CCPA, focusing on cloud database forensics.<br>● Discuss how data storage locations affect compliance.<br>● Explain data retention, deletion, and documentation requirements.<br>● Outline logging and reporting for compliance.<br>● Define timelines and protocols for breach notifications.<br>**11.4 Investigate cloud database security breaches using forensic tools.**<br>● Explain tools like EnCase and FTK for cloud database investigations.<br>● Identify attack vectors and how forensic tools detect them.<br>● Describe recovery methods for cloud platforms like AWS and Azure.<br>● Outline log analysis techniques for detecting suspicious activities.<br>● Explain the use of cloud platforms such as AWS CloudTrail or Azure Security Center for breach investigations. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to implement cloud database security & compliance as outlined in the assessment criteria and content above.<br>2. Practical assessment on using forensic tools to investigate cloud database security breaches, including log analysis, recovery, and breach detection techniques. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

**ASSESSMENT SCHEME**

| MODE OF ASSESSMENT | | WEIGHTING 100% |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | |
| 3-hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Determine the appropriateness of database models and architectures for specific applications and organisational contexts | 10 |
| Identify data storage and retrieval mechanisms to understand how data is persistently stored and efficiently accessed within various database systems | 10 |
| Control database access by configuring user roles, permissions, and authentication protocols | 10 |
| Configure backup and recovery strategies to safeguard sensitive information against unauthorized disclosure and data loss by implementing encryption techniques for data at rest and in transit | 8 |
| Protect database systems from various threats by identifying and mitigating database attacks through recognizing common attack vectors, vulnerabilities, and implementing appropriate security controls and countermeasures | 10 |
| Configure log monitoring and anomaly detection by setting up logging mechanisms, analyzing log data, and implementing rules for identifying unusual activities to detect and respond to suspicious behavior and potential security incidents within database environments | 8 |
| Acquire and preserve forensic data by employing forensically sound methods and tools to collect data from various sources | 8 |
| Reconstruct and restore deleted or altered data from database systems by utilizing specialized tools and techniques | 8 |
| Minimize the impact of security incidents and restore database integrity and confidentiality by executing incident response plans, containing the breach, and coordinating with relevant stakeholders | 8 |
| Conduct root cause analysis and reporting by investigating the underlying factors contributing to database incidents and documenting findings in comprehensive reports | 10 |
| Secure data and maintain compliance in dynamic cloud environments by configuring cloud-native security features, adhering to industry | 10 |

| | |
|---|---|
| best practices, and ensuring regulatory compliance for cloud-based databases | |
| **TOTAL** | **100** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF-accredited training programs and should have qualifications and experience recognized by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**
   **Tools and equipment**
   - Database management software (e.g., MySQL, SQL Server, Oracle)
   - Forensic analysis tools (e.g., FTK, EnCase, X1 Social Discovery)
   - Data recovery tools (e.g., R-Studio, Recuva)
   - Backup and restoration tools
   - Encryption and decryption tools
   - Disk imaging software
   - Secure storage devices (e.g., external hard drives, USB drives)

   **Materials**
   - Stationery

- Data storage media (e.g., USB drives, external hard drives)
- Documentation templates and forms
- Reference books and manuals on database management and security
- Encryption keys or security tokens
- Backup tapes and disks
- Evidence bags for secure data handling

**3. Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

**4. Reference Materials (recommended textbooks, recommended readings)**

Kennesaw, K., 2019. Database security: A comprehensive guide to securing database systems. 2nd ed. San Francisco: Morgan Kaufmann.

Sharma, A. and Rani, R., 2015. Database Security: Concepts, Approaches, and Challenges. 3rd ed. Boca Raton: CRC Press.

Almeshekah, M. and Alsubhi, K., 2017. Forensic investigation of database systems. Journal of Digital Forensics, Security and Law, 12(3), pp. 32-45.

McClure, S., Scambray, J. and Kurtz, G., 2009. Hacking exposed: network security secrets & solutions. 6th ed. New York: McGraw-Hill.

Garfinkel, S., 2014. Digital forensics for legal professionals: Understanding digital evidence from the crime scene to the courtroom. Waltham, MA: Morgan Kaufmann.

Pfleeger, C.P. and Pfleeger, S.L., 2012. Security in computing. 5th ed. Upper Saddle River, NJ: Pearson.

Bertino, E., Sandhu, R. and Gavrila, S., 2004. Database security: concepts, approaches, and challenges. Boston: Addison-Wesley.

Vacca, J.R., 2013. Computer and information security handbook. 3rd ed. Burlington: Elsevier.

Elmasri, R. and Navathe, S.B., 2016. Fundamentals of database systems. 7th ed. Boston: Addison-Wesley.

Hernandez, M., 2016. Database management systems. 4th ed. New York: McGraw-Hill Education.

Eddins, A., 2016. SQL Server 2016 Security Cookbook. Birmingham: Packt Publishing.

Spafford, E.H., 2014. Database management and security: challenges and solutions. International Journal of Computer Applications, 91(5), pp. 11-21.

Kennesaw, K., 2015. Database Forensics: The Need for Security in Database Systems. Journal of Digital Forensics and Cybersecurity, 8(1), pp. 12-23.

| | |
|---|---|
| **Module code:** | **682/25/M10** |
| **Module title:** | **NETWORK FORENSICS** |
| **ZNQF level:** | **5** |
| **Credits:** | 16 |
| **Duration:** | 160 hours |
| **Relationship with qualification standards:** | Based on Unit Standard **Network Forensics** of Unit Standards for a Digital Forensics Technician |
| **Pre-requisite modules:** | None |
| **Purpose of module:** | This module describes the skills, knowledge and attitudes required by an individual to be able to apply data privacy laws, maintain chain of custody, produce admissible evidence handling, apply cybersecurity regulations, notify incident response and breach**.**<br>This module is important as it ensures that evidence is collected, handled, analysed, and presented in a way that is admissible in court. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of learning outcomes:** | **LO1: Capture network traffic by utilizing network sniffing tools and configuring appropriate filters to collect relevant data packets to accurately acquire raw network communication for subsequent analysis.**<br>**LO2: Interpret low-level network communication for troubleshooting, security analysis, and forensic investigations by examining network packets using packet analysis software to identify protocols, services, and anomalies.**<br>**LO3: Derive actionable insights and detect suspicious patterns from large volumes of log data by collecting, parsing, and correlating log entries from various network devices and applications.**<br>**LO4: Perform intrusion detection and prevention by deploying and configuring intrusion detection/prevention systems (IDS/IPS), analyzing alerts, and implementing appropriate response actions to thwart network attacks.**<br>**LO5: Detect and categorize malware-related activities by identifying malware traffic for effective incident response and threat intelligence.**<br>**LO6: Monitor network flow by utilizing flow analysis tools to track network conversations, identify top talkers, and detect unusual traffic patterns to gain insights into network utilization, performance, and potential security anomalies at a high level.**<br>**LO7: Resolve security incidents within a network environment by responding to network incidents.**<br>**LO8: Ensure network operations and data handling adhere to legal and** |

| | |
|---|---|
| | **ethical requirements by enforcing relevant laws, regulations, and industry standards in network security practices and incident response activities.**<br>**LO9: Trace network activities during forensic examinations and after incidents by reconstructing the network.**<br>**LO10: Integrate threat intelligence by incorporating external threat feeds, indicators of compromise (IOCs), and attack patterns into network security tools and processes.** |

| **Learning outcome 01** | **Capture network traffic by utilizing network sniffing tools and configuring appropriate filters to collect relevant data packets to accurately acquire raw network communication for subsequent analysis** |
|---|---|
| **Assessment criteria:** | **1.1 Capture traffic packets using network tools**<br>**1.2 Filter and store relevant traffic for further analysis**<br>**1.3 Select appropriate tools for capturing network traffic** |
| **Content:** | **1.1 Capture traffic packets using network tools**<br>● Explain the basics of network traffic capture<br>● Outline Types of Network Packets (TCP, UDP, ICMP, etc.)<br>● Illustrate packet Capture Techniques (Passive vs. Active Capture)<br>● Discuss common network sniffing tools<br>● Demonstrate network interface modes (Promiscuous Mode & Monitor Mode)<br>● Explain legal & ethical considerations in packet capture<br>**1.2 Filter and store relevant traffic for further analysis**<br>● Categorise packet filtering techniques<br>● Identify Suspicious or Relevant Traffic<br>● Perform traffic segmentation based on protocols (HTTP, FTP, DNS, etc.)<br>● Illustrate packet export and storage formats<br>● Demonstrate automating packet filtering & storage<br>**1.3 Select appropriate tools for capturing network traffic**<br>● Compare packet-capturing tools<br>● Differentiate hardware vs. software-based packet capturing<br>● Propose best practices for choosing a packet capture tool<br>● Deploy network capture solutions in various environments |
| **Assessment tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to capture traffic packets using network tools, filter and store relevant traffic for further analysis and select appropriate tools for capturing network traffic as outlined in the assessment criteria. |

| | |
|---|---|
| | 2. Practical assessment on capturing network traffic packets using network tools, filtering and storing traffic for further analysis and selecting appropriate tools for capturing network traffic based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below: -<br><br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| **Learning outcome 02** | **Interpret low-level network communication for troubleshooting, security analysis, and forensic investigations by examining network packets using packet analysis software to identify protocols, services, and anomalies** |
|---|---|
| **Assessment criteria** | **2.1** Analyse packet headers and payloads<br>**2.2** Identify suspicious IP addresses, ports, or protocols<br>**2.3** Detect patterns of malicious behavior |
| **Content** | **2.1 Analyse packet headers and payloads**<br><br>● Illustrate structure of network packets (Ethernet, IP, TCP, UDP)<br>● Categorise Packet Header Fields (Source/Destination IP, Ports, Flags, Sequence Numbers)<br>● Explain payload analysis (extracting and inspecting packet content) |

| | |
|---|---|
| | ● Perform Deep Packet Inspection (DPI) (Examining full packet data)<br>● Compare Tools (Wireshark, TCPDump, Zeek)<br><br>**2.2 Identify Suspicious IP Addresses, Ports, or Protocols**<br><br>● Examine IP Address (Geolocation, WHOIS lookup, Blacklist checking)<br>● Identify common and uncommon Ports (Recognizing unusual port activity)<br>● Interpret Malicious Protocols & Anomalies (DNS tunneling, ICMP misuse, encrypted C2 traffic)<br>● Traffic flow analysis (Detecting port scanning, DoS/DDoS activity)<br>● Employ threat intelligence integration (Using OSINT and security feeds)<br><br>**2.3 Detect patterns of malicious behavior**<br><br>● Perform behavioral analysis of traffic (Recognizing reconnaissance, lateral movement)<br>● Compare Signature vs. Anomaly-based Detection (IDS/IPS rule matching vs. behavioral deviations)<br>● Identify Indicators of Compromise (IoCs) (Known IPs, domains, hashes)<br>● Correlate events across logs (SIEM analysis, correlation of multiple alerts)<br>● Employ AI and Machine Learning in Detection |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyze packet headers and payloads, identify suspicious IP addresses, ports, or protocols, and detect patterns of malicious behavior as outlined in the assessment criteria.<br>2. Practical assessment on analyzing packet headers and payloads, identifying suspicious IP addresses, ports or protocols and detecting patterns of malicious behaviour based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, |

| | |
|---|---|
| | AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| **Learning outcome 03** | **Derive actionable insights and detect suspicious patterns from large volumes of log data by collecting, parsing, and correlating log entries from various network devices and applications** |
|---|---|
| **Assessment criteria** | **3.1 Identify anomalies in logs from multiple sources.**<br>**3.2 Detect unauthorized access or policy violations.**<br>**3.3 Record timelines of events during an incident.** |
| **Content** | **3.1 Identify anomalies in logs from multiple sources**<br>● Identify types of logs: system logs, application logs, firewall logs, intrusion detection system (IDS) logs, etc.<br>● Explain log analysis techniques: pattern recognition, correlation of events, anomaly detection.<br>● Outline common indicators of anomalies: Unusual login attempts, failed authentication spikes, high outbound traffic, unknown processes.<br>● Employ tools for log analysis: SIEM (Splunk, ELK Stack, Graylog), OSSEC, Windows Event Viewer, Linux syslog.<br>**3.2 Detect unauthorized access or policy violations**<br>● Outline types of unauthorized access: brute-force attacks, privilege escalation, insider threats.<br>● Categorise access control policies: role-based access control (RBAC), least privilege, multi-factor authentication (MFA).<br>● Identify indicators of policy violations: Unusual file access, changes in system settings, unauthorized privilege escalation.<br>● Employ detection tools: IDS/IPS (Snort, Suricata), SIEM, endpoint detection and response (EDR) solutions. |

| | |
|---|---|
| | **3.3 Record timelines of events during an incident**<br>● Demonstrate creation, modification, access (MAC) times, event log correlation.<br>● Explain detection, containment, eradication, recovery, lessons learned.<br>● Compare tools for timeline analysis: Plaso/Log2Timeline, Autopsy, Volatility, Sleuth Kit.<br>● Outline best practices to ensure log integrity, using standardized time formats (UTC), documenting all findings. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to identify anomalies in logs from multiple sources, detect unauthorized access or policy violations, and record timelines of events during an incident as outlined in the assessment criteria.<br>2. Practical assessment on identifying anomalies in logs from multiple sources, detecting unauthorized access or policy violations, and recording timelines of events during incidents based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| | |
|---|---|
| **Learning outcome 04** | **Perform intrusion detection and prevention by deploying and configuring intrusion detection/prevention systems (IDS/IPS), analyzing alerts, and implementing appropriate response actions to thwart network attacks** |
| **Assessment criteria** | **4.1 Detect attack signatures**<br>**4.2 Generate and analyze Intrusion detection systems (IDS) alerts**<br>**4.3 Detect False positives and validate true threats** |
| **Content** | **4.1 Detect attack signatures**<br>● Demonstrate understanding of attack signatures and patterns<br>● Discuss common attack vectors (e.g., DoS, DDoS, SQL injection, malware)<br>● Compare signature-based vs. anomaly-based detection<br>● Perform packet analysis using tools like Wireshark and Snort<br>● Identify malicious traffic in logs<br>**4.2 Generate and analyze Intrusion Detection Systems (IDS) Alerts**<br>● Outline Types of IDS (Network-based IDS - NIDS, Host-based IDS - HIDS)<br>● Employ IDS tools (Snort, Suricata, Zeek)<br>● Configure IDS rules and policies<br>● Interpret IDS alerts and logs<br>● Correlate IDS alerts with real-time network traffic<br>**4.3 Detect false positives and validate true threats**<br>● Explain false positives vs. false negatives<br>● Outline Techniques for reducing false positives<br>● Analyze IDS alerts and cross-checking with threat intelligence<br>● Perform Log correlation and event prioritization<br>● Explain incident validation and escalation procedures |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to detect attack signatures, generate and analyze Intrusion Detection Systems (IDS) alerts, and detect false positives and validate true threats as outlined in the assessment criteria.<br>2. Practical assessment on detecting attack signatures, generating and analyzing IDS attacks as well as detecting false positives and validating |

| | |
|---|---|
| | true threats based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| **Learning outcome 05** | **Detect and categorize malware-related activities by identifying malware traffic for effective incident response and threat intelligence** |
|---|---|
| **Assessment criteria** | **5.1 Detect Command-and-control (C2) communications**<br>**5.2 Analyze DNS queries and HTTP requests for malicious domains**<br>**5.3 Detect data exfiltration attempts** |
| **Content** | **5.1 Identify Command-and-Control (C2) Communications**<br>● Categorise C2 channels and their role in cyber attacks<br>● Outline common C2 protocols: HTTP(S), DNS, ICMP, FTP, SSH, etc.<br>● Discuss techniques for identifying beaconing patterns in network traffic<br>● Identify indicators of C2 traffic: unusual domain requests, periodic connections<br>● Employ tools for detecting C2 activity: Wireshark, Zeek, Suricata, Snort |

| | |
|---|---|
| | ● Analyze logs from firewalls, IDS/IPS, and SIEM solutions<br>● Evaluate threat intelligence sources for identifying known C2 domains and IPs<br><br>**5.2 Analyze DNS Queries and HTTP Requests for malicious domains**<br><br>● Outline DNS resolution process and common attack methods<br>● Identify suspicious domain patterns: fast flux, domain generation algorithms (DGA)<br>● Analyze DNS query logs for unusual requests or high-frequency lookups<br>● Perform HTTP request analysis: checking headers, payloads, and URIs for malicious indicators<br>● Evaluate detection techniques: passive DNS monitoring, DNS sinkholing, and blacklists<br>● Employ tools like Zeek, Splunk, and MISP for domain reputation analysis<br><br>● Correlate DNS data with threat intelligence feeds<br>**5.3 Detect data exfiltration attempts**<br><br>● Discuss Common exfiltration techniques: DNS tunneling, encrypted traffic, cloud storage abuse<br>● Identify abnormal outbound traffic patterns<br>● Detect large data transfers to external destinations<br>● Perform behavioral analytics for spotting insider threats and unauthorized access<br>● Evaluate tools for monitoring exfiltration: Zeek, Suricata, NetFlow analyzers<br>● Outline mitigation strategies: DLP (Data Loss Prevention) solutions, firewall rules, SIEM correlation<br>● Select case studies of real-world data exfiltration incidents |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to detect Command-and-control (C2) communications, analyze DNS queries and HTTP requests for malicious domains, and detect data exfiltration attempts based on lessons learned as outlined in the assessment criteria.<br>2. Practical assessment on detecting Command-and-control (C2) communications, analyzing DNS queries and HTTP requests for malicious domains, and detecting data exfiltration attempts based on the performance criteria of the qualification standard Digital Forensics Technician. |

| | |
|---|---|
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| | |
|---|---|
| **Learning outcome 06** | **Monitor network flow by utilizing flow analysis tools to track network conversations, identify top talkers, and detect unusual traffic patterns to gain insights into network utilization, performance, and potential security anomalies at a high level** |
| **Assessment criteria** | **6.1 Collect flow data**<br>**6.2 Detect unusual traffic patterns**<br>**6.3 Detect potential botnet activity or data breaches** |
| **Content** | **6.1 Collect flow data**<br>● Explain network flow data (NetFlow, IPFIX, sFlow)<br>● Compare Tools for collecting flow data (Wireshark, Zeek, Cisco NetFlow)<br>● Demonstrate Capturing and storing network flow logs<br>● Carry out Filtering and analyzing flow data<br>● Identify source and destination IPs, ports, and protocols<br>**6.2 Detect unusual traffic patterns** |

| | |
|---|---|
| | ● Differentiate normal vs. anomalous traffic behavior<br>● Identify sudden spikes in network traffic<br>● Perform port scanning, DDoS attempts, and excessive connections<br>● Employ Intrusion Detection Systems (IDS) like Snort, Suricata<br>● Analyze network latency, jitter, and throughput anomalies<br><br>**6.3 Detect Potential Botnet Activity or Data Breaches**<br><br>● Recognize botnet Command & Control (C2) traffic<br>● Identify malicious IP addresses and domains<br>● Correlate log sources (firewall, DNS, SIEM) to detect breaches<br>● Determine exfiltration attempts (large outbound data transfers)<br>● Employ behavioral analysis and threat intelligence tools |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to collect flow data, detect unusual traffic patterns, and detect potential botnet activity or data breaches based on lessons learned as outlined in the assessment criteria.<br>2. Practical assessment on collecting flow data, detecting unusual traffic patterns and detecting potential botnet activity or data breaches based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br><br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| Learning outcome 07 | **Resolve security incidents within a network environment by responding to network incidents** |
|---|---|
| **Assessment criteria** | **7.1 Isolate affected systems to prevent further damage**<br>**7.2 Preserve evidence for forensic analysis**<br>**7.3 Restore normal operations and implement preventive measures** |
| **Content** | **7.1 Isolate affected systems to prevent further damage**<br>● Outline incident containment strategies (e.g., network segmentation, disabling compromised accounts)<br>● Demonstrate isolation techniques (disconnecting from the network, using firewalls, blocking malicious IPs)<br>● Identify malicious processes and connections (using tools like Wireshark, Process Explorer)<br>● Design Incident Response Team (IRT) Actions (roles and responsibilities in containment)<br>**7.2 Preserve Evidence for Forensic Analysis**<br>● Explain chain of custody and documentation (proper handling of digital evidence)<br>● Perform disk and memory imaging (using tools like FTK Imager, Autopsy, and Volatility)<br>● Carry out log collection and analysis (retrieving system, network, and application logs)<br>● Differentiate capturing volatile and non-volatile data (order of volatility principles)<br>● Implement legal and compliance considerations (adhering to forensic best practices and laws)<br>**7.3 Restore normal operations and implement preventive measures**<br>● Explain system recovery and restoration (restoring backups, reinstalling clean OS images)<br>● Perform patch management and vulnerability remediation (fixing security weaknesses)<br>● Differentiate post-incident analysis and reporting (lessons learned, documentation)<br>● Evaluate security hardening measures (firewall rules, intrusion detection systems, least privilege access)<br>● Carry out Awareness and Training (educating staff to prevent future incidents) |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to isolate affected systems to prevent further damage, preserve evidence for forensic analysis, and restore normal operations and implement preventive measures as outlined in the assessment criteria.<br>2. Practical assessment on isolating affected systems to prevent further |

| | |
|---|---|
| | damage, preserving evidence for forensic analysis and restoring normal operations based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| **Learning outcome 08** | **Ensure network operations and data handling adhere to legal and ethical requirements by enforcing relevant laws, regulations, and industry standards in network security practices and incident response activities** |
|---|---|
| **Assessment criteria** | **8.1 Apply chain-of-custody procedures for evidence.**<br>**8.2 Ensure Data privacy and compliance with laws.**<br>**8.3 Produce Forensic reports for use in legal proceedings.** |
| **Content** | **8.1 Apply chain-of-custody procedures for evidence**<br>● Explain the importance of chain-of-custody<br>● Outline steps in maintaining chain-of-custody<br>● Evaluate evidence collection and preservation techniques<br>● Document and label digital evidence<br>● Employ secure storage and handling of evidence<br>● Carry out transfer and tracking of evidence in Investigations<br>● Demonstrate best practices to ensure admissibility in court<br>**8.2 Ensure data privacy and compliance with laws** |

| | |
|---|---|
| | ● Explain data privacy principles (Confidentiality, Integrity, and Availability)<br>● Categorise Legal and Regulatory Frameworks (GDPR, HIPAA, CCPA, etc.)<br>● Outline the ethical and legal responsibilities of forensic investigators<br>● Differentiate Personally Identifiable Information (PII) and Sensitive Data<br>● Data protection measures and secure storage<br>● Consequences of non-compliance with privacy laws<br>**8.3 Produce forensic reports for use in legal proceedings**<br>● Outline the structure and components of a forensic report<br>● Produce clear and concise forensic reports<br>● Document findings and evidence in a legal context<br>● Employ technical and non-technical language for different audiences<br>● Outline role of expert witnesses and testimonies |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to apply chain-of-custody procedures for evidence, ensure data privacy and compliance with laws, and produce forensic reports for use in legal proceedings as outlined in the assessment criteria.<br>2. Practical assessment on applying chain of custody procedures for evidence, producing forensic reports for use in legal proceedings based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● GDPR<br>● HIPAA<br>● CCPA<br>● NIST |

| Learning outcome 09 | Trace network activities during forensic examinations and after incidents by reconstructing the network |
|---|---|
| Assessment criteria | **9.1 Recreate network sessions and transactions.**<br>**9.2 Identify the attack vector and methods used by the attacker.**<br>**9.3 Determine the scope and impact of the incident.** |
| Content | **9.1 Recreate network sessions and transactions**<br>● Capture and analyze network traffic using tools like Wireshark or tcpdump.<br>● Reconstruct a network session from captured packets and identify key communication protocols.<br>● Examine logs from firewalls, IDS/IPS, and SIEM systems to trace network activity.<br>● Perform deep packet inspection (DPI) to detect anomalies in network traffic.<br>● Identify and extract relevant HTTP, FTP, DNS, or SMTP transactions from a packet capture file.<br>**9.2 Identify the attack vector and methods used by the attacker**<br>● Identify the initial attack vector used in a given incident scenario.<br>● Analyze network traffic and logs to determine how an attacker gained access.<br>● Detect malicious payloads or scripts within network packets.<br>● Identify common cyberattack techniques (e.g., MITM, DDoS, Phishing, SQL Injection).<br>● Examine Indicators of Compromise (IoCs) to assess the presence of malware or intrusion.<br>**9.3 Determine the scope and impact of the incident**<br>● Conduct an impact assessment by identifying affected systems and data.<br>● Analyze system and network logs to determine how far an attack has spread.<br>● Identify lateral movement techniques used by the attacker.<br>● Document forensic evidence and timeline of the incident.<br>● Prepare a detailed incident report, including mitigation recommendations. |
| Assessment tasks | 1. Written and/or oral assessment on the skills and knowledge required to recreate network sessions and transactions, identify the attack vector and methods used by the attacker, and determine scope and impact of the incident as outlined in the assessment criteria.<br>2. Practical assessment on recreating network sessions and transactions, identifying attack vectors and methods used by the attacker and determining the scope and impact of the incident based on the |

| | |
|---|---|
| | performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.3<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar)<br>● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

| **Learning outcome 10** | **Integrate threat intelligence by incorporating external threat feeds, indicators of compromise (IOCs), and attack patterns into network security tools and processes** |
|---|---|
| **Assessment criteria** | **10.1 Incorporate threat feeds to identify known malicious IPs, domains, or hashes.**<br>**10.2 Analyze network traffic for indicators of compromise (IoCs).**<br>**10.3 Update emerging threats and attack techniques.** |
| **Content** | **10.1 Incorporate threat feeds to identify known malicious IPs, domains, or hashes.**<br>● Define threat intelligence feeds and explain their role in cybersecurity.<br>● List and describe at least three sources of threat intelligence feeds.<br>● Explain how to integrate threat feeds into SIEM or other security monitoring tools?<br>● Identify and categorize different types of malicious indicators (IPs, domains, hashes).<br>● Demonstrate how to use VirusTotal, AlienVault OTX, or AbuseIPDB to check for malicious indicators. |

| | |
|---|---|
| | ● Provide python script or use an API to automate threat feed ingestion.<br><br>**10.2 Analyze network traffic for indicators of compromise (IoCs).**<br>● Explain the key components of network traffic analysis.<br>● Outline common indicators of compromise (IoCs) found in network traffic?<br>● Identify any suspicious traffic on a sample PCAP file using Wireshark.<br>● Describe how Zeek (Bro) or Suricata can be used to detect anomalies in network traffic.<br>● Analyze a given network log and identify any unusual connections or malicious activity.<br>● Cross-reference network traffic logs with threat feeds to detect potential threats.<br><br>**10.3 Update emerging threats and attack techniques.**<br>● Explain why tracking emerging threats is essential in cybersecurity.<br>● Identify at least three sources for monitoring new attack techniques.<br>● Summarize a recent zero-day vulnerability or ransomware attack.<br>● Empoy MITRE ATT&CK framework to map a real-world attack scenario.<br>● Explain how organizations can proactively mitigate emerging threats.<br>● Provide recommendations for updating security policies and SIEM rules based on new threats. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to incorporate threat feeds to identify known malicious IPs, domains, or hashes, analyze network traffic for indicators of compromise (IoCs), and update emerging threats and attack techniques as outlined in the assessment criteria.<br>2. Practical assessment on incorporating threat feeds to identify known malicious IPs, domains or hashes, analyzing network traffic for indicators of compromise, and updating emerging threats and attack techniques based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● Cybersecurity Laboratory with network simulation and analysis tools<br>● Threat Intelligence Platforms (AlienVault OTX, IBM X-Force, AbuseIPDB)<br>● SIEM Tools (Splunk, ELK Stack, QRadar) |

| | |
|---|---|
| | ● Network Traffic Analyzers (Wireshark, Zeek, Suricata)<br>● Forensic Tools (Autopsy, FTK Imager, EnCase, Volatility)<br>● Malware Analysis Sandboxes (Cuckoo Sandbox, Any.Run)<br>● Hashing & Integrity Checkers (MD5sum, SHA256sum, HashCalc)<br>● External Storage Devices (HDD, SSD, USB drives) for data collection<br>● Cybersecurity Frameworks & Guidelines (MITRE ATT&CK, NIST, ISO 27001) |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3-hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Capture network traffic by utilizing network sniffing tools and configuring appropriate filters to collect relevant data packets to accurately acquire raw network communication for subsequent analysis | 10% |
| Interpret low-level network communication for troubleshooting, security analysis, and forensic investigations by examining network packets using packet analysis software to identify protocols, services, and anomalies | 10% |
| Derive actionable insights and detect suspicious patterns from large volumes of log data by collecting, parsing, and correlating log entries from various network devices and applications | 10% |
| Perform intrusion detection and prevention by deploying and configuring intrusion detection/prevention systems (IDS/IPS), analyzing alerts, and implementing | 10% |

| | |
|---|---|
| appropriate response actions to thwart network attacks | |
| Detect and categorize malware-related activities by identifying malware traffic for effective incident response and threat intelligence | 10% |
| Monitor network flow by utilizing flow analysis tools to track network conversations, identify top talkers, and detect unusual traffic patterns to gain insights into network utilization, performance, and potential security anomalies at a high level | 10% |
| Resolve security incidents within a network environment by responding to network incidents | 10% |
| Ensure network operations and data handling adhere to legal and ethical requirements by enforcing relevant laws, regulations, and industry standards in network security practices and incident response activities | 10% |
| Trace network activities during forensic examinations and after incidents by reconstructing the network | 10% |
| Integrate threat intelligence by incorporating external threat feeds, indicators of compromise (IOCs), and attack patterns into network security tools and processes | 10% |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).
2. **Facilities, Tools, Equipment and Materials**

- Facilities
  - Dedicated Forensic Lab – A secure environment for conducting investigations.
  - Secure Storage Area – For storing forensic images and evidence.
  - Network Monitoring Room – Equipped with large displays for real-time network analysis.
  - Power Backup (UPS) – Ensures continuous operation during analysis.
  - Access-Controlled Workspaces – Restricted access to maintain evidence integrity.

- Tools (Software)
  - Packet Capture and Analysis:
    - Wireshark – Captures and analyzes network traffic.
    - tcpdump – Command-line tool for packet capturing.
    - TShark – CLI version of Wireshark.
  - Network Forensics & Intrusion Detection:
    - Snort – Open-source intrusion detection/prevention system.
    - Suricata – Advanced network monitoring tool.
    - Zeek (Bro IDS) – Network monitoring and logging tool.
  - Log Analysis:
    - Splunk – Log analysis and security event monitoring.
    - ELK Stack (Elasticsearch, Logstash, Kibana) – Log management and visualization.
    - Graylog – Open-source log monitoring.
  - Memory and Disk Forensics:
    - Autopsy/The Sleuth Kit – For forensic investigation of disk images.
    - Volatility – Memory analysis tool.
    - Magnet AXIOM – Commercial tool for disk and memory analysis.
  - Malware Analysis Tools:
    - VirusTotal – Online malware scanning.
    - Hybrid Analysis – Sandbox for malware testing.
    - YARA – Pattern matching tool for malware research.
  - Traffic Analysis & Visualization:
    - Maltego – Network forensics visualization.
    - NetworkMiner – Passive network sniffer.
    - PcapXray – Graphical representation of PCAP files.
- Equipment (Hardware)
  - Forensic Workstations – High-performance computers with specialized forensic software.

- Network Tap Devices – Hardware for passive network monitoring.
- Dedicated Storage Devices – High-capacity external hard drives for evidence storage.
- Write Blockers – Prevents modification of forensic images.
- Hardware Packet Capture Devices – Tools like Endace DAG cards for real-time packet capture.
- Server Racks and Routers – For creating network forensic test environments.

- Materials
  - Forensic Evidence Bags – Secure storage for collected data.
  - Chain of Custody Forms – Documentation for tracking forensic evidence.
  - Write-Protected USB Drives – Prevents tampering with forensic tools.
  - Log Books and Notebooks – For recording findings and observations.
  - Encrypted Storage Devices – Protects sensitive forensic data.

**3. Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

**4. Reference Materials (recommended textbooks, recommended readings)**

**Casey, E.** (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. Academic Press.

**Sammons, J.** (2021). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 2nd ed. Syngress.

**Maras, M.H.** (2020). Cybercriminology and Digital Investigation. 1st ed. Oxford University Press.

**Nelson, B., Phillips, A., and Steuart, C.** (2020). Guide to Computer Forensics and Investigations. 6th ed. Cengage Learning.

**Easttom, C.** (2021). Computer Security Fundamentals. 4th ed. Pearson IT Certification.

**Kruse, W.G. and Heiser, J.G.** (2021). Computer Forensics: Incident Response Essentials. 2nd ed. Addison-Wesley Professional.

**Bejtlich, R.** (2020). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.

**Chapple, M., Seidl, D., and Stewart, J.M.** (2021). CISSP Official (ISC)2 Practice Tests. 3rd ed. Sybex.

**Gregg, M. (**2021). Certified Ethical Hacker (CEH) Version 11 Cert Guide. Pearson IT Certification.

**Sikorski, M. and Honig, A.** (2020). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2nd ed. No Starch Press.

| | |
|---|---|
| **Module code:** | **682/25/M11** |
| **Module title:** | **OPERATING SYSTEM FORENSICS** |
| **ZNQF level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 Hours |
| **Relationship with qualification standards:** | Based on Unit Standard **Operating System Forensics** of Unit Standards for a Digital Forensics Technician |
| **Pre-requisite modules:** | No prerequisites |
| **Purpose of module:** | This module describes the skills, knowledge and attitudes required by an individual to be able to apply data privacy laws, maintain chain of custody, produce admissible evidence handling, apply cybersecurity regulations, notify incident response and breach**.**<br>This module is important as it ensures that evidence is collected, handled, analysed, and presented in a way that is admissible in court. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of learning outcomes:** | **LO1: Reconstruct events by identifying types of digital remnants and their origins within system images.**<br>**LO2: Perform memory forensics using specialized tools and techniques to analyze volatile memory dumps to identify running processes, network connections, and hidden malicious artifacts that are not persistent on disk.**<br>**LO3: Evaluate system application logs to identify potential security breaches, system malfunctions, and unauthorized activities through log analysis.**<br>**LO4: Trace potential security incidents and reconstruct user actions and pinpoint compromised accounts or insider threats by analyzing user activity.**<br>**LO5: Examine system registry changes to identify persistent malware, unauthorized software installations, and system tampering.**<br>**LO6: Evaluate malware behavior on different operating systems by executing malware samples in controlled environments and observing their interactions with various OS components and security mechanisms to understand platform-specific attack techniques and the adaptability of malicious code across diverse computing environments.**<br>**LO7: Correlate timelines to illustrate events leading to an incident by synthesizing data from multiple sources, including logs, network captures, and system artifacts, to create a chronological sequence of events.** |

| **Learning outcome 01** | **Reconstruct events by identifying types of digital remnants and their origins within system images** |
|---|---|
| **Assessment criteria:** | 1.1 Extract and interpret embedded attributes such as creation date, authorship, and modification history by analyzing file metadata<br>1.2 Recover deleted files using logical and physical recovery techniques applicable to forensic investigations<br>1.3 To retrieve fragmented or metadata-less files from unallocated disk space through file carving.<br>1.4 Detect hidden files obscured through OS-level attributes, alternate data streams, or slack space concealment<br>1.5 Check file integrity using hash comparisons and digital signatures to verify authenticity and identify tampering<br>1.6 Analyse file system artifacts including Master File Table entries, journaling data, and registry hives to reconstruct user activity<br>1.7 Identify encrypted files through file entropy analysis, encryption flag detection, and forensic scanning tools<br>1.8 Review file permissions and access control structures to assess security posture and user privileges<br>1.9 Trace file operations, system events, and timeline activities across multiple artifacts by analyzing file system logs<br>1.10 Determine structural characteristics that affect forensic techniques and data recovery strategies by analyzing file system type |
| **Content:** | **1.1** Extract and interpret embedded attributes such as creation date, authorship, and modification history by analyzing file metadata<br>• Define file metadata and its importance in digital forensics.<br>• Explain the different types of metadata stored in a file.<br>• Demonstrate how to extract metadata from a given file using a forensic tool (e.g., Autopsy or FTK Imager).<br>• Interpret the metadata to determine file history (creation, modification, access).<br>**1.2** Recover deleted files using logical and physical recovery techniques applicable to forensic investigations<br>• Explain what happens when a file is deleted from a system.<br>• List different file recovery techniques and tools.<br>• Demonstrate the recovery of a deleted file using tools like Recuva or TestDisk.<br>• Analyze the recovered file and explain its significance in a forensic investigation.<br>**1.3** To retrieve fragmented or metadata-less files from unallocated disk space through file carving<br>• Define file carving and its role in digital forensics.<br>• Describe different file carving techniques.<br>• Perform file carving on a storage device using a forensic tool |

| | |
|---|---|
| | (e.g., Foremost or Scalpel).<br>• Interpret the recovered data and its forensic relevance.<br>**1.4** Detect hidden files obscured through OS-level attributes, alternate data streams, or slack space concealment<br>• Explain how files can be hidden in an operating system.<br>• List different methods of detecting hidden files.<br>• Use forensic tools (e.g., WinHex, X-Ways Forensics) to identify hidden files.<br>• Analyze the extracted hidden files and explain their significance.<br>**1.5** Check file integrity using hash comparisons and digital signatures to verify authenticity and identify tampering<br>• Define file integrity and its importance in forensics.<br>• Explain hashing algorithms used for verifying file integrity.<br>• Demonstrate how to generate and compare file hashes using tools (e.g., HashMyFiles or FTK Imager).<br>• Analyze the hash results and determine if file tampering has occurred.<br>**1.6** Analyse file system artifacts including Master File Table entries, journaling data, and registry hives to reconstruct user activity<br>• Describe what file system artifacts are and their importance in forensics.<br>• Identify different file system artifacts used in investigations.<br>• Use forensic tools (e.g., Autopsy, EnCase) to analyze artifacts from a disk image.<br>• Interpret the artifact findings and their relevance to forensic timelines.<br>**1.7** Identify encrypted files through file entropy analysis, encryption flag detection, and forensic scanning tools<br>• Define encryption and why files may be encrypted.<br>• Explain the challenges of identifying encrypted files.<br>• Use forensic tools (e.g., Cryptool, Passware) to detect encrypted files.<br>• Analyze encryption metadata and determine possible decryption methods.<br>**1.8** Review file permissions and access control structures to assess security posture and user privileges<br>• Explain the role of file permissions in security.<br>• Describe different file permission structures (Windows, Linux).<br>• Use system commands (e.g., ls -l in Linux, NTFS permissions viewer in Windows) to review file permissions.<br>• Analyze permissions to determine unauthorized access or privilege escalation.<br>**1.9** Trace file operations, system events, and timeline activities across multiple artifacts by analyzing file system logs<br>• Define file system logs and their importance in forensic investigations. |

| | |
|---|---|
| | • Identify different types of logs used in Windows and Linux.<br>• Use log analysis tools (e.g., Windows Event Viewer, Splunk) to extract log data.<br>• Interpret log entries and correlate them with forensic events.<br>**1.10** Determine structural characteristics that affect forensic techniques and data recovery strategies by analyzing file system type<br>• Describe different file system types and their structures.<br>• Explain how file systems impact forensic investigations.<br>• Use forensic tools (e.g., FTK Imager, gparted) to determine the file system type of a storage device.<br>• Analyze file system characteristics to identify anomalies or inconsistencies. |
| **Assessment tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to analyze file metadata, recover deleted file, perform file carving, detect hidden files, check file integrity, analyse file system artefacts, identify encrypted files, review file permissions, analyse file system logs, and analyse file system type as outlined in the assessment criteria.<br>2. Practical assessment on analysing file metadata, recovering deleted files, file carving, detecting hidden files, checking file integrity, analysing file system artefacts, identifying encrypted files, analysing file system logs, and analysing files system types based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>✓ FTK Imager<br>✓ Gparted<br>✓ Windows Event Viewer<br>✓ Splunk<br>✓ ls -l in Linux<br>✓ NTFS |

| | |
|---|---|
| **Learning outcome 02** | **Perform memory forensics using specialized tools and techniques to analyze volatile memory dumps to identify running processes, network connections, and hidden malicious artifacts that are not persistent on disk** |
| **Assessment criteria** | **2.1 Capture a snapshot of the system's memory.**<br>**2.2 Identify process**<br>**2.3 Detect dll injection**<br>**2.4 Identify network connections**<br>**2.5 Detect rootkit**<br>**2.6 Extract artifact**<br>**2.7 Analyse timeline**<br>**2.8 Analyse registry** |
| **Content** | **2.1 Capture a Snapshot of the System's Memory**<br>• Demonstrate capturing of snapshot on live system memory.<br>• Explain importance of capturing volatile memory in forensic investigations.<br>**2.2 Identify Processes**<br>• List all active processes running on a system.<br>• Identify any suspicious or malicious processes.<br>**2.3 Detect DLL Injection**<br>• Analyze a system for signs of DLL injection.<br>• Identify any unauthorized DLLs loaded into processes.<br>• Describe how DLL injection is used by malware<br>**2.4 Identify Network Connections**<br>• Monitor and list active network connections on the system.<br>• Identify connections to suspicious IP addresses or ports.<br>• List active network connections on a system?<br>• Differentiate TCP and UDP connections?<br>**2.5 Detect Rootkits**<br>• Scan the system for rootkit activity.<br>• Identify any hidden processes or kernel modifications.<br>• Describe how rootkit operate<br>• Outline tools used to detect rootkits<br>• Discuss challenges in detecting advanced rootkits<br>**2.6 Extract Artifacts**<br>• Locate and extract digital artifacts such as logs, browsing history, and system records.<br>• Analyze artifacts for forensic evidence.<br>**2.7 Analyze Timeline**<br>• Generate a timeline of system activities.<br>• Correlate timestamps of user actions, file modifications, and security events.<br>**2.8 Analyze Registry**<br>• Extract and analyze the Windows Registry for forensic evidence.<br>• Identify persistence mechanisms used by malware. |

| | |
|---|---|
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to capture a snapshot of the system's memory, identify process, detect dll injection, identify network connections, detect rootkit, extract artefact, analyse timeline, analyse registry as outlined in the assessment criteria.<br>2. Practical assessment on capturing snapshots of memory, detecting dll injects, identifying network connections, detecting rootkits, extracting artfacts, analysing timelines, analysing system registry based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br><br>✓ Magnet RAM Capture<br>✓ FTK Imager<br>✓ Windows Event Viewer<br>✓ Procmon<br>✓ ls -l in Linux<br>✓ Sysinternals |

| Learning outcome 03 | **Evaluate system application logs to identify potential security breaches, system malfunctions, and unauthorized activities through log analysis** |
|---|---|
| **Assessment criteria** | **3.1 Analyze event logs**<br>**3.2 Identify login attempts**<br>**3.3 Detect account changes**<br>**3.4 Review service activity**<br>**3.5 Track file access logs**<br>**3.6 Analyze firewall logs**<br>**3.7 Review antivirus logs**<br>**3.8 Examine application logs.**<br>**3.9 Detect log tampering.**<br>**3.10 Perform correlation analysis.** |
| **Content** | **2.1 Analyze Event Logs**<br>• Define what an event log is and its purpose in security monitoring.<br>• Explain the different types of event logs (System, Security, Application) in Windows and Linux.<br>• Evaluate the effectiveness of event logging in detecting cyber threats.<br>• Differentiate between informational, warning, and error log entries.<br>• Outline the steps to analyze event logs using Windows Event Viewer.<br>• Perform an analysis of a given log file to identify suspicious activity.<br>• List five common event log IDs associated with security incidents.<br>**2.2 Identify Login Attempts**<br>• Define authentication logs and their role in security monitoring.<br>• Explain how to identify failed and successful login attempts in system logs.<br>• Evaluate the impact of brute-force attacks on login security.<br>• Differentiate between local and remote login attempts in logs.<br>• Outline the steps to investigate unauthorized login attempts.<br>• Perform an audit of login attempts using SIEM tools.<br>• List three signs of suspicious login activity.<br>**2.3 Detect Account Changes**<br>• Define account modification logs and why they are important.<br>• Explain how account creation, deletion, and privilege |

| | |
|---|---|
| | changes appear in logs.<br>• Evaluate the risks associated with unauthorized account changes.<br>• Differentiate between normal and suspicious account modifications.<br>• Outline best practices for monitoring account activity.<br>• Perform an analysis of logs to detect unauthorized user account changes.<br>• List five critical account-related events to monitor.<br>**2.4 Review Service Activity**<br>• Define what a system service is and its role in an operating system.<br>• Explain how logs can help detect unauthorized service modifications.<br>• Evaluate the importance of monitoring services for system security.<br>• Differentiate between normal and malicious service activities in logs.<br>• Outline the steps to identify unauthorized service installations.<br>• Perform an analysis of service logs to detect anomalies.<br>• List four common service-related log entries that indicate a security issue.<br>**2.5 Track File Access Logs**<br>• Define file access logs and their significance in forensic investigations.<br>• Explain how file access logs can help detect insider threats.<br>• Evaluate the effectiveness of file auditing in preventing data breaches.<br>• Differentiate between read, write, modify, and delete operations in logs.<br>• Outline the steps to configure file auditing in Windows/Linux.<br>• Perform an analysis of logs to track unauthorized file access.<br>• List three log events that indicate unauthorized file access.<br>**2.6 Analyze Firewall Logs**<br>• Define what firewall logs are and their role in network security.<br>• Explain how to interpret firewall logs to identify threats.<br>• Evaluate the effectiveness of firewall logging in preventing cyber attacks. |

| | |
|---|---|
| | • Differentiate between inbound and outbound traffic in firewall logs.<br>• Outline how to detect a port scan using firewall logs.<br>• Perform an analysis of firewall logs to identify suspicious activity.<br>• List five common firewall log events that indicate a security threat.<br>**2.7 Review Antivirus Logs**<br>• Define antivirus logs and their role in malware detection.<br>• Explain how antivirus logs can help in identifying security threats.<br>• Evaluate the limitations of antivirus logs in advanced threat detection.<br>• Differentiate between quarantined, blocked, and ignored threats.<br>• Outline the process of analyzing antivirus logs for suspicious activity.<br>• Perform an audit of antivirus logs to identify malware infections.<br>• List three common antivirus log entries indicating a threat.<br>**2.8 Examine Application Logs**<br>• Define application logs and their significance in cybersecurity.<br>• Explain how application logs help in troubleshooting and security monitoring.<br>• Evaluate the impact of application log monitoring on system security.<br>• Differentiate between security logs and application error logs.<br>• Outline the process of extracting security-related data from application logs.<br>• Perform an analysis of application logs to detect anomalies.<br>• List four applications that generate critical security logs.<br>**2.9 Detect Log Tampering**<br>• Define log tampering and its impact on forensic investigations.<br>• Explain how attackers manipulate logs to cover their tracks.<br>• Evaluate the effectiveness of log integrity mechanisms in preventing tampering.<br>• Differentiate between normal log modifications and malicious tampering. |

| | |
|---|---|
| | • Outline methods for detecting log alterations using forensic tools.<br>• Perform an analysis to identify evidence of log tampering.<br>• List the signs that indicate possible log tampering.<br>**2.10 Perform Correlation Analysis**<br>• Define log correlation and its role in security event analysis.<br>• Explain how SIEM tools perform log correlation to detect threats.<br>• Evaluate the advantages of log correlation in detecting advanced persistent threats (APTs).<br>• Differentiate between correlation analysis and standard log review.<br>• Outline the process of correlating logs from multiple sources.<br>• Perform a correlation analysis using a security information and event management (SIEM) tool.<br>• List three security events that require log correlation for proper analysis. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyze event logs, identify login attempts, detect account changes, review service activity, track file access logs, analyze firewall logs, review antivirus logs, examine application logs, detect log tampering, and perform correlation analysis as outlined in the assessment criteria.<br>2. Practical assessment on analysing event logs, identifying login attempts, detecting account changes, reviewing service activity, tracking file access logs, analysing firewall logs, reviewing antivirus logs, detecting log tampering and performing correlation analysis based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>✓ Windows Event Viewer<br>✓ Log Parser<br>✓ ELK Stack |

| | |
|---|---|
| | ✓ Splunk<br>✓ Graylog |

| **Learning outcome 04** | **Trace potential security incidents and reconstruct user actions and pinpoint compromised accounts or insider threats by analyzing user activity** |
|---|---|
| **Assessment criteria** | **4.1 Track login history**<br>**4.2 Identify file access**<br>**4.3 Review command history.**<br>**4.4 Analyze browser history.**<br>**4.5 Track USB device usage**<br>**4.6 Monitor printer activity**<br>**4.7 Extract clipboard data**<br>**4.8 Review scheduled tasks**<br>**4.9 Detect remote desktop activity**<br>**4.10 Identify application usage** |
| **Content** | **4.1 Analyze event logs**<br>• Identify relevant system, security, and application logs.<br>• Describe how event logs capture system activities.<br>• Interpret log entries to detect anomalies and security threats.<br>**4.2 Track login history**<br>• Retrieve login records from system logs.<br>• Analyze failed and successful login attempts.<br>• Compare login timestamps to identify suspicious activity.<br>**4.3 Identify file access**<br>• Outline the methods used to track file access.<br>• Demonstrate how to audit file modifications and deletions.<br>• Classify file access based on user permissions and security policies.<br>**4.4 Review command history**<br>• List command history retrieval methods in Windows and Linux.<br>• Examine past commands to detect unauthorized activity.<br>• Differentiate between normal and suspicious command execution.<br>**4.5 Analyze browser history**<br>• Extract browser history, cookies, and cache files. |

| | |
|---|---|
| | • Illustrate how browsing habits can indicate security risks.<br>• Compare different browser history analysis tools.<br>**4.6 Track USB device usage**<br>• Show how to identify connected USB devices from system logs.<br>• Explain how registry keys store USB device information.<br>• Categorize different types of USB forensic evidence.<br>**4.7 Monitor printer activity**<br>• Identify print logs that record document printing activities.<br>• Analyze printer spooler data to detect unauthorized printing.<br>• Infer potential security breaches from print history analysis.<br>**4.8 Extract clipboard data**<br>• Demonstrate how clipboard forensics can reveal copied text.<br>• Retrieve clipboard history to uncover sensitive data leaks.<br>• Interpret clipboard data in relation to user activity.<br>**4.9 Review scheduled tasks**<br>• List system utilities used to examine scheduled tasks.<br>• Break down scheduled task entries to find hidden malware.<br>• Distinguish between normal and suspicious scheduled jobs.<br>**4.10 Detect remote desktop activity**<br>• Report remote access logs and connection attempts.<br>• Detect unauthorized RDP usage using system logs.<br>• Summarize best practices for securing remote access.<br><br>**4.11 Identify application usage**<br>• Analyze installed and executed applications over time.<br>• Compare authorized and unauthorized software usage.<br>• Develop an incident response plan for unauthorized application detection. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to track login history, identify file access, review command history, analyze browser history, track USB device usage, monitor printer activity, extract clipboard data, review scheduled tasks, detect remote desktop activity, identify |

| | |
|---|---|
| | application usage as outlined in the assessment criteria.<br>2. Practical assessment on tracking login history, identifying file access, reviewing command history, analysing browser history, tracking USB device storage, monitoring printer activity, extracting clipboard data, reviewing scheduled tasks, detecting remote desktop activity, and identifying application usage based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br><br>✓ Windows Event Viewer<br>✓ last, wtmp, btmp, auth.log<br>✓ PowerShell Get-EventLog<br>✓ Splunk<br>✓ Graylog<br>✓ Syslog & Logwatch (Linux)<br>✓ Splunk (SIEM tool for log analysis)<br>✓ ELK Stack (Elasticsearch, Logstash, Kibana) (Log monitoring) |

| **Learning outcome 05** | **Examine system registry changes to identify persistent malware, unauthorized software installations, and system tampering** |
|---|---|
| **Assessment criteria** | **5.1 Analyse registry hive**<br>**5.2 Identify startup programs**<br>**5.3 Track user activity**<br>**5.4 Detect malware persistence**<br>**5.5 Analyse shellbags**<br>**5.6 Identify uninstalled programs**<br>**5.7 Detect time stomping**<br>**5.8 Extract browser artifacts**<br>**5.9 Review network settings**<br>**5.10 Analyse registry backup** |
| **Content** | **5.1 Analyze registry hive**<br>• Identify the structure of Windows registry hives.<br>• Analyze registry keys to locate artifacts that could be |

| | |
|---|---|
| | of forensic value (e.g., recently opened files).<br>• Examine registry entries related to system activity, installed software, and user behavior.<br>• Explain the relevance of registry data in digital forensics.<br>• State how registry analysis can reveal malicious activity or system compromises.<br>**5.2 Identify startup programs**<br>• Name common registry keys that control startup programs (e.g., Run, RunOnce).<br>• Label startup programs found in system configurations and their impact on system performance.<br>• Analyze system configuration files for suspicious or unauthorized startup programs.<br>• Explain how malware or unauthorized programs can establish persistence through startup entries.<br>• State the tools used to identify startup programs (e.g., Autoruns).<br>**5.3 Track user activity**<br>• Observe user activity through system logs, browser history, and file access records.<br>• List methods for monitoring user actions on the system.<br>• Analyze patterns of user behavior to identify potential malicious activity or policy violations.<br>• State how user activity can be used as evidence in forensic investigations.<br>• Explain the role of user activity tracking in incident response.<br>**5.4 Detect malware persistence**<br>• Identify techniques used by malware for persistence (e.g., registry keys, scheduled tasks, services).<br>• Analyze system configurations and processes to detect malicious persistence mechanisms.<br>• State methods to detect malware persistence, such as examining startup folders or system services.<br>• Explain how persistence can be used by attackers to maintain control over a system.<br>• Outline how forensic analysis can help identify and remove malware persistence.<br>**5.5 Analyze Shellbags**<br>• Describe shellbag artifacts and their relevance to forensic investigations.<br>• Identify shellbag entries in the Windows registry and their role in tracking user activity. |

| | |
|---|---|
| | • Examine shellbag data to reconstruct a user's file navigation history.<br>• Explain how shellbags can reveal evidence of deleted or hidden files.<br>• State the role of shellbag analysis in uncovering user behavior.<br>**5.6 Identify uninstalled programs**<br>• List artifacts that indicate previously installed software, even after uninstallation.<br>• Identify registry remnants of uninstalled programs.<br>• Analyze the system for traces of removed software and its impact on system security.<br>• Explain why it's important to detect uninstalled programs during forensic investigations.<br>• Retrieve and examine logs that document program installations and uninstalls.<br>**5.7 Detect time stomping**<br>• Explain the concept of time stomping and its use in manipulating file timestamps.<br>• Analyze files and metadata to detect inconsistencies in creation, modification, or access times.<br>• Identify indicators of time stomping, such as anomalous timestamp patterns.<br>• State how time stomping can be used to deceive investigators.<br>• List tools for detecting time stomping (e.g., Timestomp, File History).<br>**5.8 Extract browser artifacts**<br>• Extract browser data, such as history, cookies, and cached files, for forensic analysis.<br>• Identify browser artifacts and their relevance in tracking user activity.<br>• Explain how browser artifacts can reveal a user's online behavior and interactions.<br>• State the importance of browser artifact analysis in tracking internet usage during investigations.<br>• Analyze artifacts to detect possible signs of malicious or unauthorized activity.<br>**5.9 Review network settings**<br>• Examine network configuration files and settings to understand system communication.<br>• Identify important network settings, including IP addresses, DNS configurations, and network interfaces.<br>• Detect unauthorized network connections, devices, or proxies. |

| | |
|---|---|
| | • State how network settings contribute to security investigations and network-based attacks.<br>• Analyze network traffic logs to identify suspicious network behavior.<br>**5.10 Analyze registry backup**<br>• Explain the importance of registry backups in forensic analysis.<br>• Identify registry backup files and their relevance to system restoration or analysis.<br>• Analyze differences between current registry states and previous backups to detect tampering.<br>• Describe how registry backups can provide insight into system changes over time.<br>• State how registry backups can assist in investigating malware or unauthorized system modifications. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyse registry hive, identify startup programs, track user activity, detect malware persistence, analyse shellbags, identify uninstalled programs, detect time stomping, extract browser artifacts, review network settings, analyse registry backup as outlined in the assessment criteria.<br>2. Practical assessment on analysing registry hives, tracking user activity, analysing shellbags, detecting time stomping, extracting browser artifacts, and analysing registry backup based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>2. The context of assessment should include the facilities, tools, equipment and materials listed below:<br>✓ Windows Event Viewer<br>✓ Netwrix Auditor<br>✓ AuditPol<br>✓ LogonTracer<br>✓ RegRipper<br>✓ FTK Imager<br>✓ EnCase<br>✓ Registry Explorer |

| | |
|---|---|
| **Learning outcome 06** | **Evaluate malware behavior on different operating systems by executing malware samples in controlled environments and observing their interactions with various OS components and security mechanisms to understand platform-specific attack techniques and the adaptability of malicious code across diverse computing environments** |
| **Assessment criteria** | **6.1 Detect malware on system**<br>**6.2 Perform behavioural analysis in a controlled environment**<br>**6.3 Detect persistence mechanisms**<br>**6.4 Monitor malware's communication with c2 servers**<br>**6.5 Track file system changes**<br>**6.6 Detect privilege escalation**<br>**6.7 Identify anti-forensic techniques.**<br>**6.8 Extract payload**<br>**6.9 Detect rootkits**<br>**6.10 Evaluate the impact of malware** |
| **Content** | **6.1 Detect malware on system**<br>• Identify suspicious processes and files on a system.<br>• List indicators of malware such as abnormal resource usage.<br>• State the methods for detecting known malware using anti-malware tools.<br>• Report on system anomalies such as unauthorized changes or access patterns.<br>• Explain how system memory and registry can indicate the presence of malware.<br>**6.2 Perform behavioural analysis in a controlled environment**<br>• Set up a controlled sandbox environment for malware analysis.<br>• Observe and record malware behavior in a safe, isolated environment.<br>• Analyze the interaction between malware and system resources, including file changes, network traffic, and registry modifications.<br>• Illustrate the use of tools for observing malware in a controlled environment (e.g., Wireshark, Process Explorer).<br>**6.3 Detect persistence mechanisms**<br>• Identify common persistence techniques (e.g., registry keys, scheduled tasks).<br>• Explain how malware maintains persistence across |

| | |
|---|---|
| | reboots.<br>• Analyze system logs and files to detect persistence mechanisms.<br>• Classify methods malware uses to re-establish itself after rebooting.<br>**6.4 Monitor Malware's communication with command and control (c2) servers**<br>• Detect network communication patterns indicative of C2 interaction.<br>• Monitor traffic for signs of remote command execution, data exfiltration, or malicious instructions.<br>• Capture and analyze network traffic using tools like Wireshark or NetFlow.<br>• State how malware communicates with remote C2 servers and the role of various protocols.<br>**6.5 Track file system changes**<br>• Explain suspicious system file activity (e.g., creation, deletion, modification).<br>• Analyze system events and logs for any signs of file tampering.<br>• Use file integrity checking tools to detect unauthorized changes.<br>• Document the changes made to critical system files and associated directories.<br>**6.6 Detect privilege escalation**<br>• Identify indicators of privilege escalation such as unauthorized user account changes.<br>• Explain methods attackers use to escalate privileges (e.g., exploiting vulnerabilities or misconfigurations).<br>• Monitor logs for suspicious privilege escalation attempts.<br>• Illustrate how privilege escalation can be detected through access control auditing and logging.<br>**6.7 Identify anti-forensic techniques**<br>• Detect techniques used by malware to evade forensic investigation (e.g., file wiping, timestamp tampering).<br>• Explain the impact of anti-forensic techniques on the investigation process.<br>• Classify various types of anti-forensic methods, including rootkits, encryption, and log manipulation.<br>• Report on potential anti-forensic activities and their implications for evidence integrity.<br>**6.8 Extract payload**<br>• Extract malware payloads from infected systems.<br>• Analyze the payload using tools like IDA Pro or Ghidra to understand its functionality. |

| | |
|---|---|
| | • Illustrate the process of reverse-engineering the payload for further analysis.<br>• Explain the methods used to isolate and extract malware from infected files.<br>**6.9 Detect rootkit**<br>• Identify the presence of rootkits through system behavior analysis (e.g., hidden processes or files).<br>• Analyze system resources and memory dumps for signs of rootkits.<br>• Use specialized tools for rootkit detection, such as rkhunter or chkrootkit.<br>• Classify different types of rootkits (e.g., user-mode vs. kernel-mode rootkits).<br>**6.10 Evaluate the impact of malware**<br>• Assess the damage caused by malware, including data corruption or loss.<br>• Estimate the operational impact, including downtime or financial loss.<br>• Discuss the potential long-term effects of malware on business operations, reputation, and legal ramifications.<br>• Report on the overall impact of malware from both a technical and business perspective. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to detect malware on a system, perform behavioral analysis in a controlled environment, detect persistence mechanisms, monitor malware's communication with C2 servers, track file system changes, detect privilege escalation, identify anti-forensic techniques, extract the payload, detect a rootkit, and evaluate the impact of malware as outlined in the assessment criteria.<br>2. Practical assessment on detecting malware on systems, performing behavioural analysis in a controlled environment, detecting persistence mechanisms, monitoring malware's communication with C2 servers, tracking file system changes, detecting privilege escalation, identifying anit-forensic techniques, and extracting payloads based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace |

| | |
|---|---|
| | or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br><br>✓ Wireshark<br>✓ NetFlow Analyzer<br>✓ Suricata<br>✓ Snort<br>✓ Bro/Zeek<br>✓ Fiddler<br>✓ Sysmon<br>✓ Tripwire<br>✓ Auditd<br>✓ OSSEC<br>✓ Veracrypt<br>✓ FTK Imager |

| **Learning outcome 07** | **Correlate timelines to illustrate events leading to an incident by synthesizing data from multiple sources, including logs, network captures, and system artifacts, to create a chronological sequence of events** |
|---|---|
| **Assessment criteria** | **7.1 Perform event correlation**<br>**7.2 Record the timeline of events leading up to and during the incident.**<br>**7.3 Detect anomaly**<br>**7.4 Identify the initial entry point and attack vector.**<br>**7.5 Assess the scope and impact of the incident.**<br>**7.6 Compare timelines from multiple systems.**<br>**7.7 Detect time stomping**<br>**7.8 Perform historical analysis**<br>**7.9 Generate timelines used in reports** |
| **Content** | **7.1 Perform event correlation**<br>• Identify key events from logs.<br>• Analyze relationships between logs from various systems.<br>• Compare logs to find matching events.<br>• Match event patterns across systems.<br>• Explain how event correlation uncovers attack indicators.<br>• State the importance of event correlation in identifying attacks.<br>**7.2 Record the timeline of events leading up to and during the incident**<br>• List key events in chronological order.<br>• Describe the sequence of actions leading to the incident.<br>• Summarize the events and timeline of the attack.<br>• Outline the steps in the attack sequence.<br>• State the events that occurred during the attack.<br>• Show the timeline using graphical representations. |

| | |
|---|---|
| | **7.3 Detect anomaly**<br>• Identify unusual behavior or outliers.<br>• Analyze data to detect anomalies.<br>• Compare baseline data with current system activity.<br>• Classify anomalies into categories (e.g., suspicious, benign).<br>• Explain how anomalies suggest malicious activity.<br>• Detect unexpected or abnormal patterns in logs.<br>**7.4 Identify the initial entry point and attack vector**<br>• Identify how the attack initially entered the system.<br>• Describe the attack vector used (e.g., phishing, RDP exploit).<br>• Explain the process by which the attacker gained access.<br>• Trace the attacker's steps from entry to exploitation.<br>• Detect the method used to bypass system defenses.<br>**7.5 Assess the scope and impact of the incident**<br>• Assess the overall impact of the attack on the system.<br>• Examine the affected areas (e.g., files, systems, data).<br>• Estimate the extent of the damage or data exfiltration.<br>• Analyze how the attack spread through the network.<br>• Compare the impact on different systems.<br>• Classify the severity of the incident.<br>**7.6 Compare timelines from multiple systems**<br>• Compare event timelines from different systems.<br>• Analyze the relationship between timelines from various sources.<br>• Correlate data to form a comprehensive timeline of events.<br>• Identify common events between systems.<br>• Describe the events occurring across multiple systems in parallel.<br>• Match timestamps to synchronize logs.<br>**7.7 Detect Time Stomping**<br>• Identify signs of time stomping in system logs or files.<br>• Examine file metadata for timestamp anomalies.<br>• Detect altered timestamps.<br>• Explain how time stomping hides malicious activity.<br>• Analyze discrepancies in the file system to detect tampering.<br>**7.8 Perform Historical Analysis**<br>• Analyze historical data to detect early signs of compromise.<br>• Review past logs for unusual patterns or unexplained events.<br>• Identify previous incidents or lingering artifacts that suggest long-term access.<br>• Examine older files or logs to find dormant threats.<br>• Trace back through historical events to uncover hidden evidence.<br>**7.9 Generate Timelines Used in Reports**<br>• Create a clear timeline summarizing key events.<br>• Summarize the timeline for reporting purposes.<br>• Illustrate the timeline using charts or tables.<br>• Report the sequence of events accurately in a structured format. |

| | |
|---|---|
| | • State critical milestones in the attack.<br>• Generate timelines using tools for clear presentation. |
| **Assessment tasks** | 1. Written and/or oral assessment on the skills and knowledge required to perform event correlation, record timeline of events leading up to and during the incident, detect anomalies, identify initial entry point and attack vector, assess scope and impact of the incident, compare timelines from multiple systems, detect time stomping, perform historical analysis, generate timelines used in reports as outlined in the assessment criteria.<br>2. Practical assessment on performing event correlation, detecting anomalies, identifying initial entry points and attack vectors, assessing the scope and impact of incident, performing historical analysis, and generating timelines used in reports based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>✓ Splunk<br>✓ ELK Stack<br>✓ Osquery<br>✓ LogRhythm<br>✓ Autopsy<br>✓ X-Ways Forensics<br>✓ TimeMap:<br>✓ SleuthKit |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Reconstruct events by identifying types of digital remnants and their origins within system images | 10 |
| Perform memory forensics using specialized tools and techniques to analyze volatile memory dumps to identify running processes, network connections, and hidden malicious artifacts that are not persistent on disk | 15 |
| Evaluate system application logs to identify potential security breaches, system malfunctions, and unauthorized activities through log analysis | 15 |
| Trace potential security incidents and reconstruct user actions and pinpoint compromised accounts or insider threats by analyzing user activity | 15 |
| Examine system registry changes to identify persistent malware, unauthorized software installations, and system tampering | 15 |
| Evaluate malware behavior on different operating systems by executing malware samples in controlled environments and observing their interactions with various OS components and security mechanisms to understand platform-specific attack techniques and the adaptability of malicious code across diverse computing environments | 15 |
| Correlate timelines to illustrate events leading to an incident by synthesizing data from multiple sources, including logs, network captures, and system artifacts, to create a chronological sequence of events | 15 |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.

2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

**9. Qualifications and experience of Trainers, Assessors and Moderators**

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

**10. Facilities, Tools, Equipment and Materials**

- Facilities
  - Cyber Forensics Laboratory – Secure and controlled environment for forensic investigations.
  - Dedicated Forensics Workstation – High-performance computers for analysis.
  - Secure Storage Facility – For storing evidence securely (e.g., locked cabinets, safe rooms).
  - Network Isolation Environment – Prevents malware from spreading during analysis.
  - Incident Response Center – For managing forensic investigations and team collaboration.

- Tools

  Operating System Forensics Tools:
  - Autopsy – Open-source digital forensics platform.
  - Sleuth Kit (TSK) – Command-line forensics tool for analyzing file systems.
  - FTK Imager – Disk imaging and evidence acquisition tool.
  - EnCase Forensic – Commercial forensic suite for OS and file system analysis.
  - X-Ways Forensics – Advanced forensic analysis tool.
  - Volatility – Memory forensics tool for analyzing volatile memory dumps.

  Disk and File System Analysis Tools:
  - TestDisk – Recover lost partitions and make disks bootable again.
  - Recuva – Recover deleted files from Windows OS.
  - Scalpel – File carving tool for recovering fragmented files.
  - Foremost – Another file carving tool for deleted file recovery.

  Live Forensics Tools:
  - Process Explorer – Windows tool for analyzing running processes.
  - Sysinternals Suite – Collection of Windows tools for monitoring OS activity.
  - LiME (Linux Memory Extractor) – Captures Linux memory for forensic analysis.

  Log Analysis Tools:
  - Event Log Explorer – Analyzes Windows event logs.
  - Log2Timeline (Plaso) – Extracts and analyzes log files from various OS.
  - Syslog (Linux/Unix) – Collects and stores logs from system activity.

Hashing & Integrity Checking Tools:

- MD5sum / SHA256sum – Command-line tools for verifying file integrity.
- HashCalc – GUI tool for calculating file hashes.
- HashMyFiles (NirSoft) – Lightweight tool for generating file hashes.

Registry Analysis Tools:

- Registry Explorer – Windows registry analysis tool.
- RegRipper – Extracts and analyzes Windows registry artifacts.

- Equipment
  - Forensics Workstations – High-performance computers with large storage.
  - Write Blockers (Hardware & Software) – Prevents altering evidence during acquisition.
  - External Hard Drives – For storing forensic images and evidence.
  - High-Capacity Storage Devices – RAID arrays, NAS for evidence storage.
  - Imaging Devices – Hardware-based forensic duplicators (e.g., Tableau, Logicube).
  - USB Write-Blockers – Prevents USB device tampering.
  - Forensic Dongles & Licenses – For tools like EnCase, X-Ways.

- Materials
  - Forensic Evidence Bags – Tamper-proof packaging for digital evidence.
  - Chain of Custody Forms – Documents evidence handling and transfer.
  - Incident Response Checklists – Standard procedures for OS forensics.
  - Secure Flash Drives – Encrypted USB drives for data transfer.
  - Write-Protected DVDs/CDs – For securely storing forensic images.
  - Reference OS Images – Clean OS installations for comparison.
  - Printed OS Forensics Guidelines – Manuals, best practices, and case handling procedures.

## 11. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 12. Reference Materials (recommended textbooks, recommended readings)

Carvey, H.A. (2021). Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10. 5th ed. Syngress.

Casey, E. (2020). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. Academic Press.

Sammons, J. (2021). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 2nd ed. Syngress.

Maras, M.H. (2020). Cybercriminology and Digital Investigation. 1st ed. Oxford University Press.

Nelson, B., Phillips, A., and Steuart, C. (2020). Guide to Computer Forensics and Investigations. 6th ed. Cengage Learning.

Easttom, C. (2021). Computer Security Fundamentals. 4th ed. Pearson IT Certification.

Kruse, W.G. and Heiser, J.G. (2021). Computer Forensics: Incident Response Essentials. 2nd ed. Addison-Wesley Professional.

Bejtlich, R. (2020). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.

Gregg, M. (2021). Certified Ethical Hacker (CEH) Version 11 Cert Guide. Pearson IT Certification.

Sikorski, M. and Honig, A. (2020). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2nd ed. No Starch Press.

| | |
|---|---|
| **Module Code:** | **682/25/M12** |
| **Module Title:** | **MALWARE FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Malware Forensics** of Unit Standards for a Digital Forensic Technician. |
| **Pre-requisite modules:** | None |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an individual to be able to analyse and investigate malicious software to understand its behavior, purpose and impact on the systems and networks for the purpose of mitigating and preventing further effects. This includes performing static analysis, conducting dynamic analysis, analyzing code, conducting behavioral analysis, performing memory forensics, integrating threat intelligence, producing documentation and reports.<br>This module is important as it helps mitigate malicious activity in computer systems and networks. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of Learning Outcomes:** | **LO1:** Demonstrate foundational and advanced knowledge of malware characteristics, classifications, propagation methods, and evasion techniques<br>**LO2:** Perform static analysis on malware samples using disassembly, string examination, and binary inspection to identify embedded code and indicators of compromise**.**<br>**LO3:** Conduct dynamic analysis in controlled environments to observe malware behavior, system interactions, and network activity in real time**.**<br>**LO4:** Detect malicious functionality and vulnerabilities by analysing source or compiled code according to secure coding and forensic standards<br>**LO5:** Map malware execution flow, persistence mechanisms, and potential impacts on host systems by conducting behavioral analysis**.**<br>**LO6:** Extract volatile artifacts, detect in-memory malware, and analyze process-level anomalies using forensic tools**.**<br>**LO7:** Integrate threat intelligence from multiple sources to contextualize malware campaigns, correlate indicators, and enhance investigative insights.<br>**LO8:** Produce comprehensive technical documentation and forensic reports summarizing analysis methodologies, findings, and remediation recommendations**.** |

| | |
|---|---|
| **Learning Outcome 01** | Demonstrate foundational and advanced knowledge of malware characteristics, classifications, propagation methods, and evasion techniques |
| **Assessment Criteria:** | **1.1 Define Malware**<br>**1.2 List types of malware**<br>**1.3 Explain malware infection vectors**<br>**1.4 Discuss common malware behavior and effects**<br>**1.5 Outline malware detection methods**<br>**1.6 Explain malware analysis techniques**<br>**1.7 Discuss the impact of malware on organizations and individuals**<br>**1.8 Explain preventative measures against malware** |
| **Content:** | **1.1 Define Malware**<br>● Define malware<br>● Outline the types of malicious software<br>● Explain the history and evolution of malware<br>● Differentiate malware and other cyber threats<br>**1.2 List types of malware**<br>● Describe various types of malware:<br>⇒ Viruses,<br>⇒ Worms,<br>⇒ Trojans,<br>⇒ Ransomware,<br>⇒ Spyware and Adware,<br>⇒ Rootkits and Bootkits,<br>⇒ Fileless Malware<br>**1.3 Explain malware infection vectors**<br>● Explain common vectors<br>⇒ Phishing Emails and Social Engineering<br>⇒ Malicious Attachments and Links<br>⇒ Drive-by Downloads<br>⇒ Software Vulnerabilities<br>⇒ USB and Removable Media Attacks<br>**1.4 Discuss common malware behaviors and effects**<br>● Describe common malware behaviour and effects<br>⇒ Data Theft and Ex-filtration<br>⇒ Disruption and Destruction<br>⇒ Access and Back doors<br>⇒ Credential Stealing (Keyloggers, Infostealers)<br>⇒ Persistence Mechanisms<br>**1.5 Discuss malware detection methods**<br>● Evaluate common methods |

| | |
|---|---|
| | ✔ Signature-Based Detection<br>✔ Heuristic and Behavioral Analysis<br>✔ Sandboxing and Dynamic Analysis<br>✔ Artificial Intelligence and Machine Learning in Detection<br>**1.6 Explain malware analysis techniques**<br>● Distinguish between static analysis from dynamic analysis<br>● Explain reverse engineering malware<br>● Discuss tools for malware analysis<br>**1.7 Discuss the impact of malware on organizations and individuals**<br>● Explain financial losses and ransom demands<br>● Describe reputational damage<br>● Identify Data Breaches and Privacy Violations<br>● Describe the process of computing operational downtime<br>**1.8 Draw preventative measures against malware**<br>● Outline security best practices (Regular Updates, Patching)<br>● Describe endpoint protection solutions (Antivirus, EDR)<br>● Give an account on network security controls (Firewalls, IDS/IPS)<br>● Describe how awareness and training can be conducted. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to demonstrate understanding of malware as outlined in the assessment criteria and content above.<br>2. Practical assessment on identifying types of malware, explaining malware infection vectors, analyzing malware behavior, detecting indicators of compromise (IOCs), applying malware analysis techniques, assessing the impact on organizations and individuals, proposing preventative measures |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● VirtualBox / VMware<br>● IDA Pro<br>● Wireshark<br>● YARA<br>● Kali Linux<br>● ProcMon |
| **Learning Outcome 02** | **Perform static analysis on malware samples using disassembly, string** |

| | |
|---|---|
| | **examination, and binary inspection to identify embedded code and indicators of compromise** |
| **Assessment Criteria:** | **2.1 Examine file headers, metadata, and structure.**<br>**2.2 Convert binary code into assembly language for review.**<br>**2.3 Detect human-readable strings (e.g., URLs, IPs, commands).**<br>**2.4 Generate hash values (e.g., MD5, SHA-256) for malware identification.**<br>**2.5 Compare malware against known signatures in antivirus databases.**<br>**2.6 Identify weather malware packed or obfuscated.**<br>**2.7 Review DLLs and APIs used by the malware.**<br>**2.8 Inspect raw binary data for anomalies.** |
| **Content:** | **2.1 Examine file headers, metadata, and structure**<br>● Define file headers and their role in malware analysis<br>● Define metadata<br>● Define structure<br>● Explain common file formats (PE, ELF, PDF, DOC) and Their Structures<br>● Describe the extraction and analysis of metadata (timestamps, authors, version info)<br>● List and explain tools for file inspection<br>**2.2 Convert binary code into assembly language for review**<br>● Explain the basics of binary and assembly language<br>● Illustrate reverse engineering fundamentals<br>● Define disassemblers and debuggers<br>● Identify and explain malicious code patterns<br>**2.3 Detect human-readable strings (e.g., URLs, IPs, Commands)**<br>● Define strings<br>● Define executables<br>● Describe how to extract strings from executables<br>● Identify suspicious keywords, domains, and commands<br>● Define techniques for detecting embedded or encrypted strings<br>● List tools for string analysis<br>**2.4 Generate hash values for malware identification**<br>● Explain the importance of cryptographic hashing in malware analysis<br>● Discuss hashing algorithms (MD5, SHA-1, SHA-256)<br>● Compare hashes with threat intelligence databases<br>● Describe how to automate hash generation with Python or bash scripts<br>**2.5 Compare malware against known signatures in antivirus databases**<br>● Differentiate signature-based detection versus heuristic |

| | |
|---|---|
| | ● Analyse common antivirus and threat intelligence databases<br>● Describe how to update and maintain malware signature databases<br>● Describe custom YARA rules for detection<br>**2.6 Identify whether malware is packed or obfuscated**<br>● Explain packing and obfuscation techniques<br>● Discuss common packers (UPX, Themida, VMProtect) and detection methods<br>● Differentiate static versus dynamic unpacking strategies<br>● Outline tools for unpacking malware<br>**2.7 Review DLLs and APIs Used by the Malware**<br>● Define dynamic-link libraries (DLLs) and API calls<br>● Explain common malicious API calls<br>● Identify and explain malware's persistence mechanisms via API calls<br>● Describe tools for API monitoring<br>**2.8 Inspect raw binary data for anomalies**<br>● Define raw binary data structures<br>● Identify code injection, encryption, or padding in binaries<br>● Analyze malware's execution flow in raw data<br>● Discuss hex editors and binary analysis tools |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to perform static analysis as outlined in the assessment criteria and content above.<br>2. Practical assessment on file structure and metadata analysis, reverse engineering & code analysis, string analysis & IOC identification, malware hashing & signature matching, packing & obfuscation detection, dynamic analysis of dependencies, binary data inspection & anomaly detection |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br>**Tools and Equipment**<br>Static analysis tools<br>Code review tools<br>Linters<br>Code formatters<br>Computers<br>High-performance computing clusters |

| | |
|---|---|
| | Cloud-based infrastructure<br><br>**Materials**<br>Source code<br>Documentation<br>Coding standards<br>Vulnerability databases |

| **Learning Outcome 03** | Conduct dynamic analysis in controlled environments to observe malware behavior, system interactions, and network activity in real time |
|---|---|
| **Assessment Criteria** | **3.1 Perform malware isolation test/ run.**<br>**3.2 Track processes created by the malware.**<br>**3.3 Identify connections to command-and-control C2 servers or ex-filtration attempts.**<br>**3.4 Identify and monitor created, modified, or deleted Files.**<br>**3.5 Monitor and identify changes to the Windows registry.**<br>**3.6 Log and intercept API calls made by the malware.**<br>**3.7 Capture screenshots of malware activity.**<br>**3.8 Extract and analyze memory for malicious artifacts.**<br>**3.9 Identify persistence mechanisms.**<br>**3.10 Identify techniques used by malware to evade analysis.** |
| **Content** | **3.1 Perform malware isolation test/run**<br>● Procedure for setting up a safe malware analysis environment (sandboxing, VMs)<br>● Differentiate Static versus dynamic analysis approaches<br>● Explain precautions to prevent accidental infections<br>● Explain tools for controlled malware execution<br>**3.2 Track processes created by the malware**<br>● Explain monitoring child and parent processes<br>● Identify unusual process behavior (e.g., spawning system processes)<br>● Explain Tools for process tracking (Process Explorer, ProcMon, Sysmon)<br>● Detect process injection techniques<br>**3.3 Identify Connections to Command-and-Control (C2) servers or exfiltration attempts**<br>● Describe C2 communication patterns (HTTP/S, DNS tunneling, Tor)<br>● Identify and explain network traffic using Wireshark, Suricata, and Zeek<br>● Identify data exfiltration techniques (encrypted payloads, DNS |

| | |
|---|---|
| | requests)<br>● Describe the processes of blocking C2 domains using threat intelligence feeds<br>**3.4 Identify and monitor created, modified, or deleted files**<br>● Identify and explain file system changes caused by malware execution<br>● Describe how to track file creation/modification using ProcMon, Sysmon<br>● Identify and explain ransomware file encryption patterns<br>● Check for suspicious hidden or temporary files<br>**3.5 Monitor and identify changes to the windows registry**<br>● Identify and explain registry keys commonly modified by malware (Run keys, Startup entries)<br>● Describe the process of detecting persistence mechanisms (registry run keys, DLL hijacking)<br>● Discuss tools for registry monitoring (Regshot, Autoruns, ProcMon)<br>**3.6 Log and intercept API calls made by the malware**<br>● Explain API calls used for malicious activity<br>● Identify API hooking and function redirection techniques<br>● Discuss Tools for API monitoring (API Monitor, Sysmon, OllyDbg, IDA Pro)<br>● Describe the procedure for detecting anti-analysis techniques via API calls<br>**3.7 Capture screenshots of malware activity**<br>● Describe a step by step guide on how to document visual evidence of malware behavior<br>● Explain all the contents/ fields of the template for documenting the visual evidence<br>● Describe the use of screen recording and monitoring tools (CAM Studio, Procmon logs)<br>● Describe a step by step guideon how to capture GUI-based malware activities<br>● Scure screenshot storage for forensic purposes<br>**3.8 Extract and analyze memory for malicious artifacts**<br>● Discuss memory forensics techniques (live vs. post-mortem analysis)<br>● Describe step by step guide on capture memory for analysis (Volatility, Rekall)<br>● Identify and explain in-memory injections (reflective DLL loading, packed malware)<br>● Describe how to extract decrypted payloads from memory<br>**3.9 Identify persistence mechanisms** |

| | |
|---|---|
| | ● Discuss common persistence techniques (scheduled tasks, startup folders, registry keys)<br>● Describe how malware that re-installs after reboot is detected<br>● Discuss Tools for persistence analysis (Autoruns, Sysmon, GMER)<br>**3.10 Identify techniques used by malware to evade analysis**<br>● Discuss anti-debugging and anti-virtualization techniques<br>● Explain code obfuscation and encryption methods<br>● Explain sandboxing detection and evasion tactics<br>● Discuss tools for bypassing evasion techniques (x64dbg, ScyllaHide) |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to Conduct Dynamic analysis. as outlined in the assessment criteria and content above.<br>2. Practical assessment on examining file headers, metadata, and structure converting binary code into assembly language for review, detecting human-readable strings (e.g., urls, ips, commands), generating hash values (e.g., md5, sha-256) for malware identification, comparing malware against known signatures in antivirus databases, identifying whether malware is packed or obfuscated, reviewing dlls and apis used by the malware, inspecting raw binary data for anomalies. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:<br>● FTK Imager<br>● Autopsy (Sleuth Kit)<br>● ExifTool<br>● IDA Pro<br>● Strings (Linux/Windows command)<br>● PEiD (Portable Executable Identifier)<br>● Process Explorer (Sysinternals)<br>● Procmon (Process Monitor - Sysinternals)<br>● Dependency Walker |

| Learning Outcome 04 | **ANALYZE SOURCE OR COMPILED CODE ACCORDING TO SECURE CODING AND FORENSIC STANDARDS TO DETECT MALICIOUS FUNCTIONALITY AND VULNERABILITIES.** |
|---|---|
| **Assessment Criteria** | **4.1 Converted binary code into high-level language**<br>**4.2 Debug execution flow.**<br>**4.3 Identify Key functions**<br>**4.4 Decode Obfuscated or encrypted code.**<br>**4.5 Extract embedded payloads or secondary stages.**<br>**4.6 Explain loops and conditional statements.**<br>**4.7 Identify vulnerabilities and how the malware exploits the system.**<br>**4.8 Analyse code for rootkit capabilities.**<br>**4.9 Identify code that changes to evade detection.**<br>**4.10 Identify code with known malware families.** |
| **Content** | **4.1 Convert binary code into high-level language**<br>● Explain binary code and assembly language<br>● Discuss reverse engineering techniques<br>● Discuss decompilers and disassemblers (e.g., IDA Pro, Ghidra, Radare2)<br>● Describe how assembly code to high-level language (C, Python) is translated<br>● Identify key instructions and function calls<br>**4.2 Debug execution flow**<br>● Explain the importance of execution flow analysis<br>● Discuss debugging tools (e.g., x64dbg, OllyDbg, WinDbg)<br>● Describe how to set breakpoints and step through code<br>● Describe monitor register and memory changes<br>● Identify malicious behavior during execution<br>**4.3 Identify key functions**<br>● Identify and explain common malicious API Calls (e.g., Create Process, Virtual Alloc, Write Process Memory)<br>● Describe how to locate key functionalities (e.g., network communication, privilege escalation)<br>● Describe function hooking and redirection<br>● Identify indicators of malicious intent in function calls<br>**4.4 Decode obfuscated or encrypted code**<br>● Discuss types of code obfuscation (e.g., packing, polymorphism, encryption)<br>● Explain static versus dynamic de-obfuscation techniques<br>● Discuss tools for decrypting Malware (e.g., CyberChef, XORSearch, UnpacMe)<br>● Identify and explain reversing string encoding techniques (Base64, XOR, AES) |

| | |
|---|---|
| | **4.5 Extract embedded payloads or secondary stages**<br>● Explain multi-stage malware<br>● Discuss techniques for extracting payloads (e.g., memory forensics, static analysis)<br>● Identify droppers, loaders, and stagers<br>● Analyze payload execution flow<br>**4.6 Explain loops and conditional statements**<br>● Explain control flow in malware<br>● Discuss common loop and conditional structures in Assembly<br>● Identify and explain infinite loops and execution triggers<br>● Explain how malware use conditions for anti-analysis techniques<br>**4.7 Identify vulnerabilities and how the malware exploits the system**<br>● Explain buffer overflows, code injection, and privilege escalation<br>● Exploit development lifecycle<br>● Identify common exploitation techniques (ROP, Heap Spraying, DLL Hijacking)<br>● Describe the procedure of mapping vulnerabilities to CVEs (Common Vulnerabilities and Exposures)<br>**4.8 Analyze code for rootkit capabilities**<br>● Explain rootkits and their persistence mechanisms<br>● Identify and explain kernel-level and user-mode rootkits<br>● Discuss techniques for detecting rootkit behavior (e.g., API hooking, hidden processes)<br>● Discuss tools for rootkit detection (e.g., GMER, RootkitRevealer)<br>**4.9 Identify code that changes to evade detection**<br>● Explain polymorphic and metamorphic malware techniques<br>● Analyze self-modifying code<br>● Detect anti-debugging and anti-sandboxing mechanisms<br>● Outline techniques for code unpacking and decryption<br>**4.10 Identify code with known malware families**<br>● Discuss code patterns of popular malware Families (e.g., Emotet, TrickBot, Zeus)<br>● Describe how YARA rules for malware family classification are used<br>● Discuss static and dynamic indicators of known malware<br>● Analyze malware signature databases and threat intelligence feeds |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to Analyze Code. as outlined in the assessment criteria and content above.<br>2. Practical assessment on Converting binary code into high-level language, debugging execution flow, Identifying key functions, decoding obfuscated or encrypted code, Extracting embedded payloads or secondary stages, identifying vulnerabilities and how the malware |

| | |
|---|---|
| | exploits the system, Analyzing code for rootkit capabilities, Identifying code that changes to evade detection, Identifying code with known malware families |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below:<br>● IDA Pro<br>● OllyDbg<br>● WinDbg<br>● PE Studio<br>● PE Explorer<br>● Exeinfo PE<br>● Hopper Disassembler<br>● Metasploit<br>● Rootkit Hunter<br>● Process Monitor<br>● VirusTotal |

| **Learning Outcome 05** | **CONDUCT BEHAVIORAL ANALYSIS TO MAP MALWARE EXECUTION FLOW, PERSISTENCE MECHANISMS, AND POTENTIAL IMPACTS ON HOST SYSTEMS** |
|---|---|
| **Assessment Criteria** | **5.1 Identify how malware maintains access (e.g., registry keys, services).**<br>**5.2 Detect attempts to gain higher privileges.**<br>**5.3 Observe attempts to spread across the network.**<br>**5.4 Identify and monitor tempts to steal data.**<br>**5.5 Observe communication with attacker-controlled servers**<br>**5.6 Detect attempts to hide or delete evidence.**<br>**5.7 Observe malware's responds to user actions.**<br>**5.8 Observe additional malware is downloaded or executed.**<br>**5.9 Evaluate Damage caused by the malware.** |
| **Content** | **5.1 Identify how malware maintains access**<br>● Discuss Persistence mechanisms (e.g., registry modifications, startup keys, scheduled tasks)<br>● Explain Service creation and manipulation |

| | |
|---|---|
| | **5.2 Detect attempts to gain higher privileges**<br>● Discuss Privilege escalation techniques and exploitation<br>● Describe how to monitor changes in user rights and token manipulation<br>**5.3 Observe attempts to spread across the network**<br>● Discuss Lateral movement strategies and propagation methods<br>● Demonstrate Network scanning and exploitation of vulnerabilities.<br>**5.4 Identify and monitor attempts to steal data**<br>● Identify and explain data ex-filtration techniques (e.g., file access and unauthorized transfers)<br>● Describe how to monitor for signs of sensitive information being targeted<br>**5.5 Observe communication with attacker-controlled servers**<br>● Identify and explain command and control (C2) communication patterns<br>● Describe the process of detecting outbound connections to suspicious or known malicious IPs/domains<br>**5.6 Detect attempts to hide or delete evidence**<br>● Identify and explain anti-forensic techniques (e.g., log tampering, file deletion, timestamp manipulation)<br>● Describe how to monitor system changes that indicate cleanup activities<br>**5.7 Observe malware response to user actions**<br>● Identify and explain triggered behaviors based on user interaction<br>● Analyse how and when the malware payload activates in response to specific actions<br>**5.8 Observe additional malware is downloaded or executed**<br>● Identify and explain secondary payload deployment and dropper functionalities<br>● Describe how chain infections and further malicious downloads are detected<br>**5.9 Evaluate damage caused by the malware**<br>● Describe how to assess data loss, system corruption, and operational impact<br>● Describe how to analyse performance degradation and overall system compromise |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to Conduct Behavioral Analysis as outlined in the assessment criteria and content above.<br>2. Practical assessment on identifying persistence mechanisms, privilege escalation detection, observing network propagation analysis, identifying data theft monitoring, observing Command and Control |

| | |
|---|---|
| | (C2) communication, detecting anti-forensics and evidence tampering, observing user interaction response, observing payload execution, impact and damage evaluation |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Autoruns<br>● Regshot<br>● Sysinternals Suite<br>● Process Monitor<br>● Windows Event Viewer<br>● Wireshark<br>● Snort<br>● Any.Run<br>● FTK Imager<br>● EnCase<br>● Procmon<br>● Process Explorer<br>● VirusTotal |

| | |
|---|---|
| | ● Splunk |

| **Learning Outcome 06** | **PERFORM MEMORY FORENSICS TO EXTRACT VOLATILE ARTIFACTS, DETECT IN-MEMORY MALWARE, AND ANALYZE PROCESS-LEVEL ANOMALIES USING FORENSIC TOOLS.** |
|---|---|
| **Assessment Criteria** | **6.1 Capture a snapshot of the system's memory**<br>**6.2 Identify malicious processes running in memory.**<br>**6.3 Detect Injected DLLs or code**<br>**6.4 Identify active connections in memory.**<br>**6.5 Uncover hidden processes or drivers**<br>**6.6 Extract Strings, URLs, or encryption keys from memory.**<br>**6.7 Reconstruct events from memory artifacts.**<br>**6.8 Unpack malware that decrypts itself in memory.**<br>**6.9 Extract registry data from memory.** |
| **Content** | **6.1 Capture Snapshot of the System's Memory**<br>● Discuss techniques for capturing a complete memory dump.<br>● Identify and explain tools and commands used in memory acquisition.<br>● Explain practices for ensuring integrity during capture.<br>**6.2 Identify malicious processes running in memory**<br>● Discuss methods for listing all active processes.<br>● Identify and explain anomalies and processes that are not part of the legitimate system.<br>● Describe the use of forensic and process analysis tools.<br>**6.3 Detect injected DLLs or code**<br>● Discuss techniques used to identify code injection and DLL hijacking.<br>● Identify and explain tools for inspecting loaded modules within processes.<br>● Analyze memory for suspicious code patterns.<br>**6.4 Identify active connections in memory**<br>● Discuss methods for capturing network connections from memory. |

| | |
|---|---|
| | ● Analyze open sockets and active ports.<br>● Describe how to correlate network activity with process data.<br>**6.5 Uncover Hidden Processes or Drivers**<br>● Discuss techniques for detecting processes or drivers concealed from standard utilities.<br>● Describe advanced forensic methods to reveal hidden artifacts<br>● Explain how to use advanced forensic methods to reveal hidden artifacts.<br>● Discuss tools that specialize in uncovering stealth techniques.<br>**6.6 Extract strings, URLs, or encryption keys from memory**<br>● Discuss approaches for extracting readable text from memory dumps.<br>● Identify and explain embedded URLs, file paths, or potential encryption keys.<br>● Describe how to use string extraction tools to uncover useful forensic evidence.<br>**6.7 Reconstruct Events from Memory Artifacts**<br>● Discuss methods to piece together timelines and system activities.<br>● Describe how to correlate artifacts to reconstruct user or system behavior.<br>● Analyze memory residues to determine the sequence of events.<br>**6.8 Unpack malware that decrypts itself in memory**<br>● Discuss techniques for detecting and handling self-unpacking malware.<br>● Demonstrate dynamic analysis methods to capture decrypted code.<br>● Discuss tools and strategies for analyzing transient code in memory.<br>**6.9 Extract registry data from memory**<br>● Discuss methods to extract and analyze registry hives from a memory dump.<br>● Explain the role of registry data in forensic investigations.<br>● Identify and explain tools for correlating registry artifacts with system activity. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to perform memory forensics as outlined in the assessment criteria and content above.<br>2. Practical assessment on Capturing snapshots of the system's memory, identifying malicious processes running in memory Detecting Injected DLLs or code, identifying active connections in memory, uncovering hidden processes or drivers, Extracting Strings, URLs, or encryption keys from memory, Reconstructing events from memory artifacts, Unpacking malware that decrypts itself in memory, Extracting registry data from memory |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Volatility<br>● FTK Imager<br>● Process Explorer<br>● Process Hacker<br>● Netstat<br>● GMER<br>● Sysinternals RootkitRevealer<br>● Bulk Extractor<br>● Strings<br>● PE-sieve<br>● RegRipper |

| | |
|---|---|
| **Learning Outcome 07** | **INTEGRATE THREAT INTELLIGENCE FROM MULTIPLE SOURCES TO CONTEXTUALIZE MALWARE CAMPAIGNS, CORRELATE INDICATORS, AND ENHANCE INVESTIGATIVE INSIGHTS.** |
| **Assessment Criteria** | **7.1 Compare malware artifacts with known indicators of compromise (IOCs).**<br>**7.2 Classify malware into known families.**<br>**7.3 Identify potential threat actors or groups.**<br>**7.4 Identify techniques, and procedures used by attackers.**<br>**7.4 Update analysis tools with the latest threat data.**<br>**7.5 Share Findings with the cybersecurity community.**<br>**7.6 Identify merging malware trends.**<br>**7.7 Map or link malware to known vulnerabilities.**<br>**7.8 Implement intelligence measure to block future attacks**<br>**7.9 Generate reports for stakeholders and law enforcement.** |
| **Content** | **7.1 Compare malware artifacts with known Indicators of Compromise (IOCs)**<br>● Describe the processes of extracting malware artifacts (file hashes, strings, metadata)<br>● Explain how to use comparison techniques on IOC databases and threat feeds |

| | |
|---|---|
| | ● Describe the process of automating tools to correlate artifacts with known IOCs<br>**7.2 Classify malware into known families**<br>● Overview of malware taxonomy and classification methods<br>● Explain static and dynamic analysis techniques for identifying malware families<br>● Discuss signature-based, heuristic, and behavioral detection approaches<br>**7.3 Identify potential threat actors or groups**<br>● Explain attribution methodologies and threat intelligence analysis<br>● Research on known threat groups and their modus operandi<br>● Describe how to link malware artifacts and infrastructure to specific threat actors<br>**7.4 Identify techniques and procedures used by attackers**<br>● Analyze attack vectors, tactics, techniques, and procedures (TTPs)<br>● Describe how to use frameworks like MITRE ATT&CK for mapping attacker behavior<br>● Describe exploitation methods<br>● Examine exploitation methods, persistence mechanisms, and lateral movement<br>**7.5 Update analysis tools with the latest threat data**<br>● Describe malware analysis and threat intelligence tools<br>● Explain the processes updating tools with real-time threat feeds and databases<br>● Describe the process of integrating automated threat intelligence into security workflows<br>**7.6 Share Findings with the Cybersecurity Community**<br>● Explain best practices for reporting and responsible disclosure<br>● Discuss methods for disseminating threat intelligence and analysis reports<br>● Outline strategies for enhancing information exchange among stakeholders<br>**7.7 Identify merging malware trends**<br>● Identify and explain trend and detect convergence between different malware families<br>● Describe how to monitor emerging attack patterns and cross-over techniques<br>● Evaluate the impact of evolving malware trends on cybersecurity<br>**7.8 Map or link malware to known vulnerabilities**<br>● Discuss techniques for linking malware behavior to specific vulnerabilities (CVEs)<br>● Describe the use of vulnerability databases and mapping tools |

| | |
|---|---|
| | ● Identify and explain exploit methods relative to known security weaknesses<br>**7.9 Implement intelligence measures to block future attacks**<br>● Explain defense strategies<br>● Describe how to implement proactive defense strategies based on threat intelligence<br>● Step by step to configure security systems (IDS/IPS, firewalls) with updated threat indicators<br>**7.10 Generate reports for stakeholders and law enforcement**<br>● Prepare executive-level reports<br>● Explain forensic findings.<br>● Propose actionable recommendations. |
| **Assessment Tasks** | 2. Written and/or oral assessment on the skills and knowledge required to integrate Threat Intelligence. as outlined in the assessment criteria and content above.<br>3. Practical assessment on identifying threat actors or groups, identifying techniques and procedures used by attackers Updating tools with the latest threat data, identifying emerging malware trends, Mapping malware to known vulnerabilities, generating reports for stakeholders and law enforcement, Comparing malware artifacts with known indicators of compromise (IoCs), Classifying malware into known families. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● VirusTotal<br>● MITRE ATT&CK Navigator<br>● ANY.RUN<br>● IDA Pro<br>● Snort<br>● Magnet AXIOM<br>● Nessus<br>● OpenVAS<br>● Metasploit<br>● Shodan<br>● Splunk<br>● HxD (Hex Editor) |

| Learning Outcome 08 | **PRODUCE COMPREHENSIVE TECHNICAL DOCUMENTATION AND FORENSIC REPORTS SUMMARIZING ANALYSIS METHODOLOGIES, FINDINGS, AND REMEDIATION RECOMMENDATIONS.** |
|---|---|
| **Assessment Criteria** | **8.1 Provide a high-level overview of the malware and its impact.**<br>**8.2 Outline analysis of the malware's code and behavior.**<br>**8.3 List indicators of compromise for detection.**<br>**8.4 Articulate steps to remove the malware and prevent reinfection.**<br>**8.5 Employ diagrams, screenshots, and charts to illustrate findings.**<br>**8.6 Organise report to ensure admissibility in court.**<br>**8.7 Ensure the report is peer-reviewed by other experts.**<br>**8.8 Suggest improvements for security policies and tools.**<br>**8.9 Explain examples of similar malware incidents**. |
| **Content** | **8.1 Provide a high-level overview of the malware and its impact.**<br>● Outline malware type and classification (e.g., Trojan, ransomware, etc.)<br>● Explain infection vectors and propagation methods<br>● Evaluate the impact on systems, networks, and data integrity<br>● Discuss operational, financial, and reputational consequences<br>**8.2 Explain malware's code and behavior.**<br>● Explain Static analysis: code structure, embedded strings, file headers<br>● Demonstrate knowledge of performing dynamic analysis in sandbox environments<br>● Demonstrate understanding of reverse engineering insights<br>● Outline Behavioral indicators of modified systems<br>**8.3 List indicators of compromise for detection.**<br>● Describe file hashes<br>● Describe digital finger prints<br>● Describe how to compute file hashes and digital fingerprints<br>● Identify and explain suspicious IP addresses, domain names, and URLs<br>● Explain how to detect registry changes and modified system files<br>● Demonstrate knowledge of indicating unusual network activity and anomalous system behavior<br>**8.4 Articulate steps to remove the malware and prevent reinfection.**<br>● Outline Step-by-step removal procedures (manual and automated)<br>● Describe how to perform patching and updating vulnerable systems<br>● Describe the implementation of robust antivirus and endpoint protection<br>● Describe incident response and prevention strategies<br>**8.5 Employ diagrams, screenshots, and charts to illustrate findings.** |

| | |
|---|---|
| | ● Describe how to generate flowcharts depicting the malware infection process<br>● Step by step on the production of screenshots of forensic tool outputs and code snippets<br>● Describe how graphs and charts showing network traffic and timeline of events are illustrated<br>● Describe visual aids<br>● Demonstrate how visual aids can be used to enhance clarity and support technical findings<br><br>**8.6 Organise report to ensure admissibility in court.**<br>● Describe the procedures for constructing proper documentation of chain-of-custody and evidence handling.<br>● Identify key components necessary for accurate and secure evidence handling.<br>● Outline the steps involved in maintaining a clear, factual, and objective methodology in forensic reporting.<br>● Illustrate compliance with legal standards and forensic best practices to ensure the integrity of the investigation.<br>● Produce a detailed and structured forensic report format, incorporating supporting evidence.<br>● Demonstrate how evidence is collected, stored, and presented in accordance with forensic protocols.<br>● Compare best practices with legal requirements to ensure alignment in forensic reporting.<br>● Summarize the methodology and key findings concisely for stakeholders.<br>● Develop a report template that adheres to forensic industry standards.<br>**8.7 Ensure the report is peer-reviewed by other experts.**<br>● Outline the peer review process and criteria for review<br>● Describe independent verification and validation of findings<br>● Explain the procedure for carrying out the integration of feedback from multiple cybersecurity experts<br>**8.8 Suggest improvements for security policies and tools.**<br>● Describe enhanced patch management and system updates to ensure timely remediation of vulnerabilities.<br>● Identify improved security tools such as IDS/IPS and firewalls to strengthen network defenses.<br>● Develop policy adjustments to mitigate similar threats in the future by implementing security best practices.<br>● Illustrate best practices for network segmentation, access control, and user training to enhance overall security posture. |

| | |
|---|---|
| | **8.9 Explain examples of similar malware incidents.**<br>● Identify similar behaviors and techniques used across different malware attacks.<br>● Compare various attack patterns and evolving threats.<br>● Summarize lessons learned from past incidents<br>● Illustrate the impact of attacks using documented case studies.<br>● Extrapolate how previous security incidents influenced current defense mechanisms and predict potential future trends.<br>● Describe historical or well-known malware attacks by outlining key incidents such as (WannaCry and NotPetya). |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to produce documentation and reports as outlined in the assessment criteria and content above.<br>2. Practical assessment on Listing Indicators of Compromise for Detection, Articulating Steps to Remove Malware and Prevent Reinfection, Employing Diagrams, Screenshots, and Charts to Illustrate Findings, Organising Report to Ensure Admissibility in Court, Suggesting Improvements for Security Policies and Tools, Explaining, Examples of Similar Malware Incidents |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Autopsy<br>● FTK Imager<br>● EnCase<br>● Magnet Axiom<br>● XRY |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Demonstrate foundational and advanced knowledge of malware characteristics, classifications, propagation methods, and evasion techniques | 10% |
| Perform static analysis on malware samples using disassembly, string examination, and binary inspection to identify embedded code and indicators of compromise. | 15% |
| Conduct dynamic analysis in controlled environments to observe malware behavior, system interactions, and network activity in real time. | 15% |
| Analyze source or compiled code according to secure coding and forensic standards to detect malicious functionality and vulnerabilities. | 10% |
| Conduct behavioral analysis to map malware execution flow, persistence mechanisms, and potential impacts on host systems. | 15% |
| Perform memory forensics to extract volatile artifacts, detect in-memory malware, and analyze process-level anomalies using forensic tools. | 15% |
| Integrate threat intelligence from multiple sources to contextualize malware campaigns, correlate indicators, and enhance investigative insights. | 10% |
| Produce comprehensive technical documentation and forensic reports summarizing analysis methodologies, findings, and remediation recommendations | 10% |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

   - **Facilities**
     - Isolated Malware Lab: A dedicated environment to safely analyze malware without affecting production systems.
     - Air-Gapped Network: A physically separated network to prevent malware from communicating with external systems.
     - Secure Storage: Lockable cabinets or encrypted storage for malware samples and analysis reports.
     - Backup and Recovery System: To restore the system in case of corruption or damage.
     - Classroom environment (for theoretical and oral assessments)
     - Simulated work environment (for practical assessments)
     - Workplace environment (for real-world application of skills)
     - Network equipment (routers, switches, access points)
     - Virtual machines (for simulating different operating systems and environments)

   - **Tools**

     **Static Analysis Tools (For analyzing malware without executing it)**
     - IDA Pro – Disassembler for reverse engineering.
     - Ghidra – Open-source reverse engineering tool.
     - PE Explorer – Analyzes Windows executable files.
     - Binwalk – Firmware analysis tool.
     - Strings – Extracts readable text from binaries.

     **Dynamic Analysis Tools (For monitoring malware behavior in a controlled environment)**
     - Cuckoo Sandbox – Open-source automated malware analysis system.
     - Remnux – Linux toolkit for analyzing malware.
     - Procmon (Process Monitor) – Monitors system activity in real-time.
     - Wireshark – Network packet analyzer for monitoring malware communications.
     - Regshot – Captures Windows registry changes before and after malware execution.

     **Memory and Forensic Analysis Tools**
     - Volatility – Memory forensics framework.
     - Rekall – Memory analysis for Windows, Linux, and macOS.
     - Redline – Collects and analyzes endpoint forensic data.

**Code and Scripting Tools**

- Python – Used for scripting and automating malware analysis tasks.
- Radare2 – Open-source reverse engineering framework.
- Hex Editors (HxD, 010 Editor) – For manual binary analysis.

**Online and Cloud-Based Analysis Tools**

- VirusTotal – Online malware scanning service.
- Hybrid Analysis – Cloud-based sandbox for malware behavior analysis.
- Any.Run – Interactive malware analysis sandbox.

- **Equipment**
  - Dedicated Analysis Machine – A high-performance PC or VM for running malware safely.
  - Virtualization Software – VMware, VirtualBox, or Hyper-V for creating isolated test environments.
  - Hardware Write Blocker – Prevents modification of malware samples.
  - USB Forensic Duplicator – Clones storage devices for forensic analysis.
  - Router/Firewall with Logging – Monitors malware network traffic.

- **Materials**
  - Malware Samples – Collected from honeypots, infected machines, or repositories like VX Underground.
  - Digital Forensic Workbooks – Documentation for recording analysis findings.
  - Encrypted Storage Devices – External HDDs/SSDs for safely storing malware samples.
  - Incident Response Playbooks – Guides on handling malware outbreaks.
  - Malware Analysis Reports – Sample reports to compare and validate findings.

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 4. Reference Materials (recommended textbooks, recommended readings)

Sikorski, M. and Honig, A., 2022. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 2nd ed. San Francisco: No Starch Press.

Chapple, M., Seidl, D. and Stawowski, M., 2021. Cybersecurity Threat Intelligence: Collecting, Analyzing, and Evaluating Threat Data. 1st ed. New York: Sybex.

Ligh, M.H., Case, A., Levy, J. and Walters, A., 2021. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. 2nd ed. Indianapolis: Wiley.

Eagle, C., 2020. IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler. 3rd ed. San Francisco: No Starch Press.

Skoudis, E. and Liston, T., 2023. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 3rd ed. Upper Saddle River: Prentice Hall.

Altheide, C. and Carvey, H., 2022. Digital Forensics with Open-Source Tools. 2nd ed. Waltham: Syngress.

Engebretson, P., 2023. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. 4th ed. Waltham: Syngress.

Willems, C., 2021. Malware Analysis Using Cuckoo Sandbox: A Practical Guide to Automated Malware Analysis. 1st ed. Birmingham: Packt Publishing.

Messier, R., 2022. Threat Hunting: A Practical Guide to Detecting and Responding to Cyber Threats. 1st ed. New York: Apress.

Paar, C. and Pelzl, J., 2021. Understanding Cryptography: A Textbook for Students and Practitioners. 2nd ed. Berlin: Springer.

| | |
|---|---|
| **Module Code:** | **682/25/M13** |
| **Module Title:** | **ETHICAL HACKING** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 |
| **Relationship with Qualification Standards:** | Based on Unit Standard Ethical Hacking of Qualification Standard for a Digital Forensics Technician |
| **Pre-requisite modules:** | NONE |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an individual to conduct reconnaissance, scan and enumerate target information, perform network exploitation, conduct post-exploitation, compile reports and documentation and utilize ethical hacking techniques This module is important as it helps mitigate detecting and mitigating vulnerabilities in computer systems and networks. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity |
| **List of Learning Outcomes:** | **LO1: Perform effective reconnaissance on a given target system or network, accurately gathering publicly available information to inform subsequent ethical hacking phases.**<br>**LO2: Scan and enumerate target information from identified systems, precisely identifying open ports, services, and potential vulnerabilities by utilizing appropriate tools and methodologies.**<br>**LO3: Execute various network exploitation techniques against identified vulnerabilities in a controlled lab environment, demonstrating the ability to gain unauthorized access while adhering to ethical guidelines.**<br>**LO4: Conduct post-exploitation activities on compromised systems, effectively maintaining access, escalating privileges, and exfiltrating data without causing system damage to identify and evaluate security risks.**<br>**LO5: Construct comprehensive and clear forensic reports and documentation for all phases of an ethical hacking engagement, ensuring all findings are accurately presented and actionable.**<br>**LO6: Assess the security posture of systems and networks using ethical hacking techniques, while adhering to legal and ethical boundaries.** |

| | |
|---|---|
| **Learning Outcome 01** | **PERFORM EFFECTIVE RECONNAISSANCE ON A GIVEN TARGET SYSTEM OR NETWORK, ACCURATELY GATHERING PUBLICLY AVAILABLE INFORMATION TO INFORM SUBSEQUENT ETHICAL HACKING PHASES** |
| **Assessment Criteria:** | **1.1 Describe the process of performing passive reconnaissance.**<br>**1.2 Conduct active reconnaissance and report findings.**<br>**1.3 Identify network map.**<br>**1.4 Explain OS fingerprinting and illustrate its significance.**<br>**1.5 Analyse running services and classify their functions.**<br>**1.6 Demonstrate information gathering through human interaction and summarize key techniques.**<br>**1.7 Conduct Open-Source Intelligence (OSINT) gathering and report findings** |
| **Content:** | **1.1 Describe the process of performing passive reconnaissance**<br>● Explain passive reconnaissance and its role in cybersecurity and ethical hacking.<br>● Identify and explain techniques for gathering information without direct interaction, distinguishing them from active reconnaissance methods.<br>● Outline sources of passive reconnaissance, including WHOIS, DNS records, social media, and public databases, and explain their significance.<br>● Match tools used for passive reconnaissance, such as Maltego, the Harvester, and Shodan, with their functionalities with examples.<br>● Evaluate different passive reconnaissance techniques based their effectiveness, and how they contribute to the reconnaissance phase of penetration testing.<br>● Show how passive reconnaissance can be used in real-world scenarios, infer its potential risks, and predict its impact on cybersecurity defenses.<br>**1.2 Conduct active reconnaissance and report findings**<br>● Describe the concept of active reconnaissance and its associated risks.<br>● Explain various techniques such as network scanning, ping sweeps, and banner grabbing.<br>● List commonly used tools, including Nmap, Netcat, Metasploit, and hping3, and their functionalities.<br>● Demonstrate how to conduct active reconnaissance using these tools and their effectiveness.<br>● Document findings systematically by tabulating results and key |

| | |
|---|---|
| | observations.<br><br>**1.3 Identify network map**<br>● Describe the importance of network mapping in cybersecurity and IT infrastructure management.<br>● Identify the various methods used for network mapping, such as ARP scanning, subnet scanning, and topology discovery.<br>● Label the key components involved in network scanning and mapping processes.<br>● List commonly used tools for network mapping, including Nmap, Zenmap, Wireshark, and SolarWinds Network Mapper.<br>● Match network scanning methods with the appropriate tools used for each process.<br>● Name specific features of network mapping tools that aid in network visualization.<br>● Outline the steps involved in conducting a successful network scan and mapping operation.<br>● Recall key network parameters that need to be analyzed when interpreting mapping results.<br>● Report findings from a network scan, detailing discovered devices, IP addresses, and network structures<br><br>**1.4 Explain OS fingerprinting and illustrate its significance**<br>● Describe OS fingerprinting as the process of identifying an operating system based on its network behavior and response patterns.<br>● Distinguish active and passive fingerprinting<br>● Explaining how active methods send probes to elicit responses, while passive techniques analyze existing traffic without direct interaction.<br>● Classify OS fingerprinting techniques into TCP/IP stack analysis, TTL values examination, and window size differences to determine OS characteristics.<br>● List tools used for OS fingerprinting, such as Nmap (-O flag) and p0f, which help in security assessments and penetration testing.<br>● Illustrate the significance of OS fingerprinting in cybersecurity by providing examples of how attackers and defenders use it for reconnaissance and system hardening.<br>● Compare various fingerprinting methods and their effectiveness in detecting operating systems in different network environments. |

| | |
|---|---|
| | ● Explain how OS fingerprinting supports penetration testing by aiding vulnerability identification and system profiling.<br>● Summarize the role of OS fingerprinting in security assessments, emphasizing its importance in threat modelling and risk evaluation.<br><br>**1.5 Analyse running services and classify their functions**<br>● Describe service enumeration and its role in cybersecurity.<br>● Identify critical services such as web, database, mail, FTP, and SSH.<br>● List tools used for service enumeration, including Nmap, Netstat, Nessus, and OpenVAS.<br>● Classify services based on their security risks and functions.<br>● Compare different service enumeration techniques and their effectiveness.<br>● Explain how service enumeration aids in vulnerability assessments.<br>● Demonstrate the use of enumeration tools in practical scenarios.<br>● Analyse the impact of misconfigured services on security posture.<br>● Organize services based on their level of exposure and sensitivity.<br>● Summarize best practices for secure service management.<br><br>**1.6 Demonstrate Information Gathering Through Human Interaction and Summarize Key Techniques**<br>Describe social engineering and its impact on cybersecurity.<br>Identify different social engineering techniques, such as phishing, pretexting, baiting, and tailgating.<br>Outline tools and frameworks used in social engineering, including the Social Engineering Toolkit (SET) and OSINT tools.<br>Compare various social engineering techniques to highlight their differences and effectiveness.<br>Illustrate social engineering attacks with real-world examples to demonstrate their practical implications.<br>Examine mitigation strategies against social engineering, explaining how organizations can defend against these threats.<br>Explain the importance of training and awareness programs in preventing social engineering attacks.<br>Propose security policies that help reduce the risks associated with social engineering. |

| | |
|---|---|
| | Summarize best practices for individuals and organizations to detect and prevent social engineering attacks.<br>Evaluate the effectiveness of existing security measures<br>Recommend improvements to counter social engineering threats.<br>**1.7 Conduct Open-Source Intelligence (OSINT) gathering and report findings**<br>● Definition and applications of OSINTTools: Maltego, SpiderFoot, Google Dorking, Shodan<br>● Define Open-Source Intelligence<br>● Explain significance of Open-Source Intelligence in cybersecurity, law enforcement, and threat intelligence.<br>● Illustrate how OSINT is used to gather publicly available data for intelligence purposes.<br>● Categorize the various sources used in OSINT investigations, such as social media, search engines, and public databases.<br>● Name commonly used OSINT tools, including Maltego, SpiderFoot, Google Dorking, and Shodan.<br>● Apply Google Dorking techniques to retrieve information efficiently from search engines.<br>● Explain the importance of structured OSINT reporting for security professionals and investigators. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to Conduct Reconnaissance as outlined in the assessment criteria and content above.<br>2. Practical assessment on Passive Reconnaissance, Active Reconnaissance, Network Mapping, OS Fingerprinting, Service Analysis Skills, Human Interaction and Social Engineering, Open-Source Intelligence (OSINT), Analytical and Problem-Solving. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Nmap (with scripts for service detection and OS fingerprinting)<br>● Masscan (for fast large-scale scans)<br>● Zenmap (GUI for Nmap)<br>● traceroute (Linux/Unix)<br>● tracert (Windows) |

| | |
|---|---|
| | ● MTR (My Traceroute)<br>● Maltego<br>● theHarvester<br>● SpiderFoot<br>● Recon-ng |

| **Learning Outcome 02** | **SCAN AND ENUMERATE TARGET INFORMATION FROM IDENTIFIED SYSTEMS, PRECISELY IDENTIFYING OPEN PORTS, SERVICES, AND POTENTIAL VULNERABILITIES BY UTILIZING APPROPRIATE TOOLS AND METHODOLOGIES** |
|---|---|
| **Assessment Criteria** | **2.1 Describe the results of the port scanning process.**<br>**2.2 Identify vulnerabilities detected in the scanned system.**<br>**2.3 Report findings from the network scanning process.**<br>**2.4 Analyse detailed service information gathered during scanning.**<br>**2.5 Extract and interpret SNMP information from the network.**<br>**2.6 Summarize LDAP detailed information gathered.**<br>**2.7 Differentiate SMB data collected from other network protocols.**<br>**2.8 Retrieve and tabulate DNS records extracted from the system.**<br>**2.9 Examine identified web application vulnerabilities.**<br>**2.10 Demonstrate the results of wireless network scanning and outline key findings**. |
| **Content** | **2.1 Describe the results of the port scanning process**<br>● Define of port scanning and its significance in cybersecurity<br>● List common tools used: Nmap, Masscan, Zenmap<br>● Detect open, closed, and filtered ports<br>● Identify commonly exploited ports (e.g., 80, 443, 22, 3389)<br>● Explain scan types: SYN scan, UDP scan, ACK scan, FIN scan, XMAS scan<br>**2.2 Identify vulnerabilities detected in the scanned system**<br>● Explain vulnerability scanning and its purpose<br>● Outline common tools used: Nessus, OpenVAS, Qualys, Nexpose<br>● Categorise vulnerabilities (e.g., high, medium, low severity)<br>● Explain CVSS (Common Vulnerability Scoring System)<br>● Identify misconfigurations, outdated software, and weak passwords<br>**2.3 Report findings from the network scanning process**<br>● Structure a professional network scan report<br>● Outline elements: discovered hosts, open ports, vulnerabilities, risk |

| | |
|---|---|
| | level<br>● Interpret scan logs and output data<br>● Categorise vulnerabilities based on risk level<br>● Create mitigation strategies for detected weaknesses<br><br>**2.4 Analyse detailed service information gathered during scanning**<br>● Describe the process of extracting banner information to determine service versions.<br>● Identify the tools used for version detection, such as Nmap (-sV), Netcat, and various banner-grabbing techniques.<br>● List vulnerable software versions and their associated exploits based on the retrieved information.<br>● Match identified versions with publicly known vulnerabilities to assess security risks.<br>● Outline the importance of understanding TLS/SSL versions and detecting weak cipher implementations.<br>● Report on the findings from the version detection process and summarize security implications.<br>**2.5 Extract and interpret SNMP information from the network**<br>● Describe the purpose of SNMP (Simple Network Management Protocol) and its role in network management.<br>● Identify tools used for SNMP management such as SNMPwalk, SNMPcheck, and SolarWinds SNMP Scanner.<br>● Interpret OID (Object Identifier) values in SNMP responses.<br>● List common misconfigurations in SNMP settings, such as incorrect or default community strings (public/private).<br>● State the process for detecting misconfigured SNMP settings.<br>● Report on how to identify network devices, retrieve system uptime, and access routing tables through SNMP queries.<br><br>**2.6 Summarize LDAP detailed information gathered**<br>● Explain LDAP (Lightweight Directory Access Protocol)<br>● Tools: ldapsearch, JXplorer, Active Directory Enumeration<br>● Demonstrate how to extract user accounts, group memberships, and organizational units<br>● Identify potential misconfigurations (anonymous binds, weak passwords)<br>● Evaluate Security risks related to LDAP injection attacks<br><br>**2.7 Differentiate SMB data collected from other network protocols**<br>● Explain SMB (Server Message Block) and its role in file sharing<br>● Outline tools for SMB enumeration: enum4linux, smbclient, |

| | |
|---|---|
| | Metasploit auxiliary modules<br>● Identifying vulnerable SMB versions (SMBv1, EternalBlue Exploit - MS17-010)<br>● Analyzing NetBIOS and Windows shares exposure<br><br>**2.8 Retrieve and tabulate DNS records extracted from the system**<br>● Explain the role and significance of DNS in networking, outlining its function in converting human-readable domain names to IP addresses, facilitating the smooth operation of the internet.<br>● Describe the importance of DNS in enabling various online services, including email delivery, website access, and the interaction of devices over the internet.<br>● List common DNS diagnostic tools such as dig, nslookup, host, Fierce, and DNSRecon.<br>● Demonstrate how these tools can be used to query DNS records and troubleshoot issues related to DNS configurations.<br>● Explain the significance of each type of DNS record and its role in ensuring proper internet functionality and security.<br>● Identify vulnerabilities related to DNS enumeration and the potential risks of improperly configured DNS servers.<br>● Discuss the concept of zone transfer (AXFR) attacks and how attackers can exploit misconfigurations to gain sensitive information about a domain.<br>● Demonstrate the process of detecting and preventing AXFR misconfigurations in DNS servers.<br>● Analyse the security implications of subdomains<br>● Identify patterns that might indicate vulnerabilities in a domain's structure.<br>● Explain how these findings can help security professionals assess risks and prevent phishing attacks targeting subdomains.<br><br>**2.9 Examine identified web application vulnerabilities**<br>● Describe the OWASP Top 10 Web Vulnerabilities and explain their significance in web security.<br>● List the tools used for web security testing, including Burp Suite, Nikto, ZAP, SQLmap, and DirBuster, and examine their functionalities.<br>● Identify common vulnerabilities such as SQL Injection, XSS, CSRF, Directory Traversal, and Security Misconfigurations, and explain how they impact web applications.<br>● Compare manual versus automated web application scanning techniques and evaluate their effectiveness in detecting vulnerabilities. |

| | |
|---|---|
| | ● Report on high-risk web security flaws, categorize them by severity, and suggest appropriate mitigation strategies to enhance application security.<br><br>**2.10 Demonstrate the results of wireless network scanning and outline key findings**<br>● Define the concept of wireless security assessment.<br>● Explain the importance of securing wireless networks and common vulnerabilities.<br>● List the tools used in wireless security assessments.<br>● Identify the various Wi-Fi encryption protocols (WEP, WPA, WPA2, WPA3).<br>● Explain the differences between these encryption protocols and their vulnerabilities.<br>● Define rogue access points, hidden SSIDs, and de-authentication attacks.<br>● Demonstrate how to detect rogue access points and hidden SSIDs in a network.<br>● Describe methods to detect deauthentication attacks during wireless security testing.<br>● Explain the concept of Evil Twin attacks and how they are carried out.<br>● Analyse the KRACK attack, its impact, and how it exploits weaknesses in WPA2.<br>● Demonstrate the process of capturing WPA handshakes and the significance for cracking encryption.<br>● Summarize key aspects to consider during a wireless security assessment. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to Scan and Enumerate target information as outlined in the assessment criteria and content above.<br>2. Practical assessment on network scanning & enumeration skills, vulnerability assessment & management, security tools & technologies, operating system & network protocols knowledge, web application security, network security & firewall configuration, data collection & interpretation, reporting & documentation, ethical hacking & penetration testing, wireless security knowledge. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Nmap (with scripts for service detection and OS fingerprinting)<br>● Masscan (for fast large-scale scans)<br>● Zenmap (GUI for Nmap)<br>● traceroute (Linux/Unix)<br>● tracert (Windows)<br>● MTR (My Traceroute)<br>● Maltego<br>● theHarvester<br>● SpiderFoot<br>● Recon-ng<br>● Metasploit<br>● Cobalt Strike<br>● Empire<br>● Hydra<br>● John the Ripper |

| | |
|---|---|
| **Learning Outcome 03** | **EXECUTE VARIOUS NETWORK EXPLOITATION TECHNIQUES AGAINST IDENTIFIED VULNERABILITIES IN A CONTROLLED LAB ENVIRONMENT, DEMONSTRATING THE ABILITY TO GAIN UNAUTHORIZED ACCESS WHILE ADHERING TO ETHICAL GUIDELINES** |
| **Assessment Criteria** | **3.1 Describe the process of deploying custom exploits for specific vulnerabilities.**<br>**3.2 Analyse techniques used to perform privilege escalation in various environments.**<br>**3.3 Demonstrate methods for maintaining access and gather additional intelligence post-exploitation.**<br>**3.4 Apply password cracking techniques to retrieve compromised credentials.**<br>**3.5 Execute penetration testing using ethical hacking tools to assess system security.**<br>**3.6 Illustrate different social engineering attack methods and their impact.**<br>**3.7 Examine web application exploitation techniques and identify** |

| | |
|---|---|
| | **vulnerabilities.**<br>**3.8 Analyse network exploitation methods and differentiate between various attack vectors.**<br>**3.9 Carry out wireless exploitation techniques and interpret their effectiveness.**<br>**3.10 Develop and implement zero-day exploits to simulate advanced threats.**<br>**3.11 Explain how compromised systems can be leveraged to attack other systems within a network.** |
| **Content** | **3.1 Describe the process of deploying custom exploits for specific vulnerabilities**<br>● Identify vulnerabilities in target systems by examining system configurations and assessing potential weaknesses.<br>● Develop custom exploits by creating code that specifically targets identified vulnerabilities.<br>● Demonstrate how to use tools like Metasploit and custom scripts to execute and deploy exploits in a practical scenario.<br>● Perform controlled experiments by reproducing exploit scenarios in a safe environment to assess the impact.<br>● Carry out mechanisms bypass including antivirus programs and firewalls, by modifying your approach to infiltrate these defenses.<br>**3.2 Analyse techniques used to perform privilege escalation in various environments**<br>● Describe the types of privilege escalation, identify the differences between local and remote, as well as vertical and horizontal privilege escalation.<br>● Explain the techniques used for privilege escalation in Windows systems, such as UAC bypass and DLL injection.<br>● Outline the techniques for privilege escalation in Linux/Unix environments, including Sudo manipulation and Kernel exploits.<br>● Analyse file permissions and SUID/SGID vulnerabilities to detect potential privilege escalation risks.<br>● Demonstrate the use of post-exploitation tools like Metasploit for privilege escalation.<br>**3.3 Demonstrate methods for maintaining access and gather additional intelligence post-exploitation**<br>● Describe methods for establishing persistent backdoors such as web shells, reverse shells, and trojans.<br>● Identify common techniques used to create web shells and reverse |

| | |
|---|---|
| | shells for continued access.<br>● List various types of trojans used to maintain persistence.<br>● Name the process of generating SSH keys for secure and continuous remote access.<br>● Demonstrate how SSH keys can be used to bypass password authentication and ensure sustained access to remote systems.<br>● Describe how SSH keys facilitate automated and encrypted communication between compromised systems.<br>● List common remote access tools like Netcat and Meterpreter used for exploiting systems.<br>● Explain how each tool operates for remote command execution and control over compromised systems.<br>● Outline methods of gathering intelligence, such as password dumps, system logs, and network traffic.<br>● Describe the tools and techniques used to collect system information for further exploitation.<br>● Explain how keyloggers and screen capture tools can be deployed to monitor target activities.<br>● Illustrate the process of installing and using keyloggers to capture sensitive data from victims.<br>● Describe how screen capture tools can provide real-time surveillance of the victim's actions.<br>● Demonstrate how these tools help in collecting information for later use or for escalating the attack.<br><br>**3.4 Apply password cracking techniques to retrieve compromised credentials**<br>● Describe password hashing and encryption techniques.<br>● Identify tools like John the Ripper and Hashcat for performing brute force and dictionary attacks.<br>● List methods for creating and using rainbow tables to accelerate password cracking.<br>● Explain the process of cracking LM/NTLM hashes in Windows environments.<br>● Illustrate the steps to crack Unix/Linux password hashes, such as those stored in shadow files.<br><br>**3.5 Execute penetration testing using ethical hacking tools to assess system security**<br>● Describe the penetration testing methodologies (e.g., OSCP, PTES). |

- Identify the common ethical hacking tools (e.g., Nmap, Burp Suite, Wireshark, Metasploit).
- List the steps involved in conducting vulnerability assessments and network mapping.
- Explain the process of exploiting identified vulnerabilities.
- Report the findings from penetration testing and provide remediation recommendations.
- Classify the different penetration testing methodologies and their key features.
- Illustrate the practical applications of tools like Nmap, Burp Suite, and Metasploit in ethical hacking.
- Compare various approaches to vulnerability assessments and network mapping.
- Examine the techniques used for exploiting vulnerabilities found during penetration testing.
- Summarize how findings are reported and what type of remediation actions are recommended.

**3.6 Illustrate different social engineering attack methods and their impact**

- Describe the different types of social engineering attacks, such as phishing, pretexting, baiting, and tailgating.
- Identify the tools and techniques commonly used for conducting social engineering campaigns.
- Explain the use of email spoofing and malicious links in social engineering attacks.
- Analyze the potential impacts on individuals and organizations, including data theft, reputation damage, and financial loss.
- List defensive measures that can be implemented to protect against social engineering attacks.

**3.7 Examine web application exploitation techniques and identify vulnerabilities**

- Describe common web application vulnerabilities, such as SQL Injection, XSS, and CSRF.
- Identify tools like Burp Suite to detect and exploit vulnerabilities in web applications.
- Explain techniques for bypassing authentication and authorization mechanisms in web applications.
- Illustrate the concept of web shells and backdoor implants in web servers.

| | |
|---|---|
| | ● Classify common vulnerabilities based on their impact and exploitability.<br>● Analyse the behaviour of vulnerabilities like SQL Injection, XSS, and CSRF in a real-world context.<br>● Compare the effectiveness of different tools, such as Burp Suite, in identifying web application vulnerabilities.<br>● Demonstrate how to perform an attack using Burp Suite to exploit an identified vulnerability.<br>● Discuss strategies to secure web applications against common vulnerabilities.<br>● Identify potential risks posed by web shells and backdoor implants in web servers.<br>● State best practices for preventing SQL Injection, XSS, and CSRF vulnerabilities.<br>● Summarize the key principles of web application security according to the OWASP Top 10.<br>● Define the role of Burp Suite in penetration testing and web application security assessments.<br>● Examine the implications of bypassing authentication and authorization mechanisms.<br>● Design strategies to mitigate risks associated with web shell implants.<br>● Analyse the structure and exploitation techniques of web shells in web servers.<br><br>**3.8 Analyse network exploitation methods and differentiate between various attack vectors**<br>● Describe network sniffing and man-in-the-middle attacks and their impact on security.<br>● Identify methods of exploiting network services, such as SMB, DNS, and RDP.<br>● List common techniques for Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.<br>● Match potential network misconfigurations (e.g., open ports, weak firewalls) with the risks they pose.<br>● Explain techniques for attacking network protocols, including ARP spoofing and DNS poisoning.<br>● Classify network security issues that arise from misconfigurations and protocol vulnerabilities.<br>● Compare the effectiveness of network sniffing and man-in-the-middle techniques. |

| | |
|---|---|
| | ● Demonstrate the exploitation of network services like SMB and DNS.<br>● Analyse the potential impact of DoS and DDoS attacks on an organization's infrastructure.<br>● Discuss methods of identifying open ports and weak firewalls.<br>● Illustrate how ARP spoofing and DNS poisoning can be executed in network environments.<br>● Perform an assessment of network misconfigurations and propose remediation steps.<br><br>**3.9 Carry out wireless exploitation techniques and interpret their effectiveness**<br>● Describe the process of attacking WEP/WPA and WPA2 encryption using tools like aircrack-ng.<br>● Identify the methods involved in executing evil twin attacks and de-authentication.<br>● List the steps involved in Wi-Fi sniffing and packet capture.<br>● Analyse SSID spoofing and explain how man-in-the-middle attacks operate in wireless networks.<br>● Discuss the effectiveness of wireless attacks and outline the countermeasures that can be implemented.<br><br>**3.10 Develop and implement zero-day exploits to simulate advanced threats**<br>● Describe the concept of zero-day vulnerabilities (unknown vulnerabilities).<br>● List the techniques used in exploit chaining and bypassing multiple security mechanisms.<br>● Outline the methods for detecting and preventing zero-day attacks.<br>● Examine the process of creating and testing proof-of-concept exploits.<br>● Classify the types of security mechanisms bypassed in exploit chaining.<br>● Illustrate techniques for simulating and testing APT attacks.<br>● Apply techniques for simulating APT scenarios in a controlled environment.<br>● Develop and test proof-of-concept exploits for unknown vulnerabilities.<br>● Design a comprehensive approach to exploit chaining and security bypass techniques.<br>● Evaluate the success of advanced persistent threat simulations. |

- Reorganize existing security protocols to defend against zero-day exploits.
- Reconstruct a response plan after an APT attack involving zero-day exploits.

**3.11 Explain how compromised systems can be leveraged to attack other systems within a network**

- Identify the process of pivoting through compromised systems, which allows attackers to extend their reach to additional targets within a network.
- Explain how Command and Control (C&C) infrastructure is set up for large-scale exploitation, facilitating continuous communication between the attacker and the compromised systems.
- State the methods used in data exfiltration and the techniques employed to spread malware across networks, enabling widespread disruption.
- Categorize different lateral movement techniques, comparing them based on their effectiveness and impact on network security.
- Illustrate how internal reconnaissance helps in identifying vulnerable systems, users, and resources that can be exploited for further attacks.
- Analyze the components of C&C infrastructure, discussing how attackers use it to maintain persistent access and control over a compromised network.
- Develop strategies for defending against lateral movement techniques, including securing authentication methods and using network segmentation.
- Demonstrate how data exfiltration can be prevented by implementing encryption and monitoring for unusual network activity.
- Outline a plan for detecting and responding to lateral movement and pivoting activities within a network, focusing on early identification and containment.
- Generate potential scenarios where C&C infrastructure is leveraged, considering different attack vectors and the scale of exploitation.
- Compare different approaches to spreading malware across networks, evaluating their success rates and the necessary mitigations.
- Examine the relationship between internal reconnaissance and the

| | |
|---|---|
| | subsequent stages of an attack, identifying how each contributes to the overall exploitation strategy. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to perform network exploitation as outlined in the assessment criteria and content above.<br><br>2. Practical assessment on reconnaissance and information gathering, vulnerability assessment, exploitation techniques, privilege escalation, post-exploitation, network exploitation, web application security, password cracking, wireless security, social engineering, tool proficiency, security controls & countermeasures, reporting and documentation, ethical hacking best practices, cloud security |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br><br>● Nmap (with scripts for service detection and OS fingerprinting)<br>● Masscan (for fast large-scale scans)<br>● Zenmap (GUI for Nmap)<br>● traceroute (Linux/Unix)<br>● tracert (Windows)<br>● MTR (My Traceroute)<br>● Maltego<br>● theHarvester<br>● SpiderFoot<br>● Recon-ng<br>● Computer Hardware |

| | |
|---|---|
| **Learning Outcome 04** | **CONDUCT POST-EXPLOITATION ACTIVITIES ON COMPROMISED SYSTEMS, EFFECTIVELY MAINTAINING ACCESS, ESCALATING PRIVILEGES, AND EXFILTRATING DATA WITHOUT CAUSING SYSTEM DAMAGE TO IDENTIFY AND EVALUATE SECURITY RISKS** |
| **Assessment Criteria** | **4.1 Describe the persistence mechanisms developed.**<br>**4.2 Identify and report the data exfiltration methods used.**<br>**4.3 Outline and explain how tracks were covered.**<br>**4.4 Analyse and illustrate the privilege escalation techniques performed.**<br>**4.5 Examine and demonstrate in-depth network enumeration processes.**<br>**4.6 Categorize collected forensic artifacts.**<br>**4.7 Interpret detected log manipulation activities.**<br>**4.8 Demonstrate lateral movement techniques.**<br>**4.9 Manipulate data as per operational needs.** |
| **Content** | **4.1 Identify and report the data exfiltration methods used**<br>● Define how attackers move stolen data outside a compromised network.<br>● Explain the process by which attackers access and transfer sensitive data to external locations.<br>● List common exfiltration methods such as HTTP/HTTPS tunneling, FTP, DNS tunneling, email (attachments or links), and cloud storage.<br>● Identify different channels through which data can be exfiltrated.<br>● State the typical signs of data exfiltration, such as unusual traffic patterns, large file transfers, and encrypted traffic.<br>● Outline the information to include in an incident report, such as timestamps, affected systems, and methods used.<br>● Report the findings with the necessary context and evidence to aid further investigation.<br><br>**4.2 Outline and explain how tracks were covered**<br>● Describe how attackers hide their activities to avoid detection.<br>● Identify common techniques used by attackers to cover their tracks.<br>● List the methods attackers use to manipulate logs, delete files, clear command history, and disable security tools.<br>● State the purpose of these techniques in avoiding detection and forensic investigation.<br>● Explain the importance of preserving logs and other evidence to trace malicious activities. |

| | |
|---|---|
| | ● Illustrate the role of digital footprints in forensic investigations.<br>● Discuss strategies to prevent attackers from covering tracks, such as enabling system auditing and retaining logs.<br>● Apply countermeasures like regular log review and the implementation of file integrity monitoring.<br><br>**4.3 Analyse and illustrate the privilege escalation techniques performed**<br>● Describe techniques such as exploiting software vulnerabilities, bypassing authentication controls, exploiting misconfigurations, and utilizing social engineering tactics to gain unauthorized access to higher system privileges.<br>● Differentiate between vertical escalation, which involves elevating user privileges (e.g., gaining admin access), and horizontal escalation, which involves moving laterally within the network to compromise other systems or accounts without altering user roles.<br>● Define how attackers exploit software vulnerabilities (e.g., buffer overflows), crack passwords using methods such as brute force or dictionary attacks, exploit misconfigurations like weak file permissions or sudo misconfigurations<br>● Employ social engineering tactics (e.g., phishing) to gain unauthorized access.<br>● Provide examples of privilege escalation in practice, such as exploiting a kernel vulnerability to gain root access, abusing a misconfigured service to move laterally, or using weak sudo permissions to escalate privileges on a compromised system.<br>● Recommend steps like regularly patching systems, implementing the principle of least privilege, securing configuration files, using multi-factor authentication, and training employees to recognize social engineering tactics to prevent privilege escalation.<br><br>**4.4 Examine and demonstrate in-depth network enumeration processes**<br>● Describe the techniques used to map out and gather information about a network and its devices.<br>● Identify the common tools for network enumeration, such as Nmap, Netdiscover, Netcat, and Wireshark.<br>● State the objectives of enumeration, including the identification of live hosts, open ports, and services, along with the collection of data on network shares and user information.<br>● List the mitigation techniques for preventing successful enumeration, such as segmentation, firewalls, and IDS/IPS. |

| | |
|---|---|
| | ● Illustrate how segmentation, firewalls, and IDS/IPS can effectively mitigate network enumeration attempts.<br>● Demonstrate the use of tools for conducting network enumeration and identifying vulnerabilities.<br>● Design a network environment incorporating countermeasures to thwart enumeration attempts.<br>● Summarize the role of network enumeration in cybersecurity and the countermeasures that can be applied to secure a network.<br><br>**4.5 Categorize collected forensic artifacts**<br>● Describe the types of data that are considered forensic evidence, including logs, registry keys, temporary files, and network traffic.<br>● Identify various forms of forensic artifacts such as system logs, user activity logs, registry entries, file system metadata, network logs, and email headers.<br>● List the techniques used for collecting, preserving, and categorizing forensic artifacts to ensure their integrity and chain of custody.<br>● Match each type of artifact to its appropriate category and purpose in forensic investigations.<br>● Clarify the best practices for collecting forensic artifacts, including the importance of maintaining the integrity and chain of custody during the collection process.<br>● Categorize the techniques used in artifact collection based on their method (e.g., direct collection, remote collection, live collection).<br>● Explain the significance of preserving forensic artifacts during collection to ensure they can be used in legal or investigative processes.<br>● Reproduce the steps involved in collecting and preserving forensic evidence in accordance with best practices.<br>● Demonstrate how to collect system logs, user activity logs, and other artifacts while adhering to the chain of custody.<br><br>**4.6 Interpret detected log manipulation activities**<br>● Describe the process by which attackers alter or delete logs to erase evidence of their actions.<br>● Identify common methods used in log manipulation, including timestamp changes, missing logs, anomalous patterns, and log truncation.<br>● List the key indicators of log manipulation:<br>● Analyse logs by cross-referencing with other data sources to identify inconsistencies.<br>● Examine system events for patterns that might suggest manipulation. |

| | |
|---|---|
| | ● Correlate data from multiple sources (such as firewall, server, and application logs) to identify discrepancies that indicate tampering.<br>● Predict areas of high risk based on historical log data and known attack patterns.<br>● State the steps to take if log manipulation is suspected<br><br>**4.7 Demonstrate lateral movement techniques**<br>● Define lateral movement as the techniques employed by attackers to move across different systems within a network after initial access is gained.<br>● List common techniques used for lateral movement, such as Pass-the-Hash, RDP (Remote Desktop Protocol), SMB exploitation, SSH tunneling, and WMI (Windows Management Instrumentation).<br>● Identify tools commonly associated with lateral movement, including Mimikatz, PsExec, and PowerShell Empire.<br>● Outline countermeasures to prevent lateral movement. These include network segmentation, multi-factor authentication, and application whitelisting.<br><br>**4.8 Manipulate data as per operational needs**<br>● Describe the ways attackers alter or destroy data to achieve operational objectives.<br>● Identify techniques used for data manipulation, including database manipulation, file modification, data corruption, and denial of service (DoS) attacks to prevent access to data.<br>● List indicators of data manipulation, such as monitoring changes in file integrity, abnormal system states, or unusual data flows.<br>● State the ethical considerations surrounding data manipulation, specifying when and how it may be conducted within legal and authorized boundaries, such as during red team exercises or penetration testing. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to Conduct post-exploitation as outlined in the assessment criteria and content above.<br>2. Practical assessment on network security assessment, malware analysis and reverse engineering, log analysis and interpretation, privilege escalation, data exfiltration techniques, forensic data collection, stealth and evasion techniques, incident response and containment, cryptography and encryption, lateral movement and pivoting, cloud security assessment, web application security, social engineering techniques, and operating system hardening. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Nmap (with scripts for service detection and OS fingerprinting)<br>● Masscan (for fast large-scale scans)<br>● Zenmap (GUI for Nmap)<br>● traceroute (Linux/Unix)<br>● tracert (Windows)<br>● MTR (My Traceroute)<br>● Maltego<br>● theHarvester<br>● SpiderFoot<br>● Recon-ng<br>● Computer hardware<br>● Virtual machines |

| | |
|---|---|
| **Learning Outcome 05** | **CONSTRUCT COMPREHENSIVE AND CLEAR FORENSIC REPORTS AND DOCUMENTATION FOR ALL PHASES OF AN ETHICAL HACKING ENGAGEMENT, ENSURING ALL FINDINGS ARE ACCURATELY PRESENTED AND ACTIONABLE** |
| **Assessment Criteria** | **5.1 Summarise the high-level findings, outlining key security concerns and vulnerabilities identified.**<br>**5.2 Analyse and break down technical details of vulnerabilities and exploits, explain their impact, and illustrate methods of exploitation.**<br>**5.3 Assess classes of risks by evaluating their likelihood and potential consequences, compute risk scores, and differentiate between low, medium, and high-risk vulnerabilities.**<br>**5.4 Propose remediation strategies, outline best practices, and illustrate step-by-step mitigation techniques to address identified vulnerabilities.**<br>**5.5 Illustrate visual aids such as charts, graphs, and screenshots to represent security findings effectively.**<br>**5.6 Compile compliance reports by matching security gaps with regulatory standards and demonstrate adherence to industry frameworks.**<br>**5.7 Conduct a peer review by examining, evaluating, and verifying the findings, ensuring accuracy and completeness.**<br>**5.8 Generate actionable insights by interpreting data trends, predicting potential threats, and proposing strategic improvements.**<br>**5.9 Summarize lessons learned, extrapolate future security implications, and outline key takeaways for enhancing security postures.**<br>**5.10 Ensure legal considerations by identifying regulatory requirements, interpreting relevant laws, and demonstrating compliance with legal frameworks**. |
| **Content** | **5.1 Summarize the high-level findings, outlining key security concerns and vulnerabilities identified**<br>● Identify the critical weaknesses found, list them as open ports, insecure protocols, or misconfigured firewalls, and classify them by their severity.<br>● Describe the potential impacts these vulnerabilities may have on the confidentiality, integrity, and availability of systems, illustrating the possible consequences for data protection and system stability.<br>● Summarize the primary security issues uncovered during the |

| | |
|---|---|
| | analysis, highlighting concerns such as network vulnerabilities, weak access controls, and outdated software.<br><br>**5.2 Analyse and break down technical details of vulnerabilities and exploits, explain their impact, and illustrate methods of exploitation**<br>● Identifying key actions that lead to system breaches.<br>● Categorize the various stages of compromise<br>● Analyze identified vulnerability (e.g., buffer overflow, SQL injection), classify the technical details, and explain the underlying issues.<br>● Describe how these vulnerabilities can be exploited<br>● Comparing techniques such as exploitation via Metasploit or Phishing.<br>● Illustrate step-by-step processes of exploitation.<br>● Examine the potential consequences of exploitation.<br>● Clarify risks like unauthorized access, data breach, or DoS attack.<br>● Discuss the severity of these impacts and their implications for security.<br>● Outline the exact steps attackers would take to exploit vulnerabilities.<br><br>**5.3 Assess classes of risks by evaluating their likelihood and potential consequences, compute risk scores, and differentiate between low, medium, and high-risk vulnerabilities**<br>● Classify risks by their likelihood and impact.<br>● Produce risk levels using a risk matrix or tool, such as CVSS scores, to assess the severity of risks.<br>● Categorize vulnerabilities as low, medium, or high based on their severity and potential consequences.<br><br>**5.4 Propose remediation strategies, outline best practices, and illustrate step-by-step mitigation techniques to address identified vulnerabilities**<br>● Describe specific actions to mitigate vulnerabilities (e.g., patching, access control improvements).<br>● Identify the vulnerabilities and state the corresponding fixes.<br>● Outline the priority levels of vulnerabilities and propose suitable remediation steps.<br>● Classify the fixes by type (e.g., technical, procedural, |

| | |
|---|---|
| | organizational) and arrange them in order of implementation.<br>● Explain industry-recognized practices to improve security posture (e.g., least privilege, secure coding).<br>● Provide detailed instructions on how to implement fixes (e.g., applying patches, reconfiguring firewall rules).<br>● Demonstrate the application of patches and configuration adjustments.<br>● Enumerate steps for reconfiguring access controls and show how to test their effectiveness.<br>● List the actions required to remediate each vulnerability, and describe how they contribute to the overall security improvement.<br><br>**5.5 Illustrate visual aids such as charts, graphs, and screenshots to represent security findings effectively**<br>● Illustrate vulnerabilities using charts, graphs, and screenshots to illustrate the severity and potential effects of exploits.<br>● Represent the impact of exploits by showing potential attack vectors or highlighting affected areas with visual aids.<br><br>**5.6 Compile compliance reports by matching security gaps with regulatory standards and demonstrate adherence to industry frameworks**<br>● Compare identified security gaps with relevant regulatory standards (e.g., GDPR, HIPAA).<br>● Match security gaps with applicable compliance requirements.<br>● Outline the necessary actions to bridge the gaps and achieve compliance.<br>● Demonstrate compliance with industry frameworks like ISO 27001, NIST, or PCI DSS.<br>● Classify the organization's adherence to these frameworks.<br>● Identify areas of non-compliance and the steps required for correction.<br>● Create detailed compliance reports that show adherence to regulatory standards and frameworks.<br>● Summarize the current state of compliance and actions for remediation.<br><br>**5.7 Conduct a peer review by examining, evaluating, and verifying the findings, ensuring accuracy and completeness**<br>● Outline the process of reviewing findings and reports with colleagues or experts to ensure accuracy and credibility.<br>● Compare the data and methods used in analysis to validate the findings and ensure consistency. |

| | |
|---|---|
| | ● Examine all aspects of the assessment to ensure they are thoroughly analyzed, properly documented, and in compliance with standards.<br><br>**5.8 Generate actionable insights by interpreting data trends, predicting potential threats, and proposing strategic improvements**<br>● Identify emerging security patterns or trends from the data by analyzing frequent types of attacks and common vulnerability areas.<br>● Predict future security risks based on current findings and trends.<br>● Propose long-term strategies by organizing and synthesizing findings from data trend analysis and predictive threat modelling to address identified security issues and improve overall security measures.<br><br>**5.9 Summarize lessons learned, extrapolate future security implications, and outline key takeaways for enhancing security postures**<br>● Explain Lessons Learned from the analysis and what can be improved in future security assessments.<br>● Discuss how the findings may shape future security efforts, such as preparing for advanced persistent threats (APTs).<br>● Outline recommendations for bolstering defenses and mitigating emerging threats.<br><br>**5.10 Ensure legal considerations by identifying regulatory requirements, interpreting relevant laws, and demonstrating compliance with legal frameworks**<br>● Identify legal standards that apply to the organization (e.g., GDPR, CFAA, HIPAA).<br>● Provide security measures and practices that align with the applicable laws and regulations.<br>● Show Compliance to proof that organizational security measures comply with legal frameworks and industry regulations. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to compiling reports and documentation as outlined in the assessment criteria and content above.<br><br>2. Practical assessment on compiling compliance reports by matching security gaps with regulatory standards and demonstrate adherence to industry frameworks, conducting a peer review by examining, evaluating, and verifying the findings, ensuring accuracy and completeness and generating actionable insights by interpreting data trends, predicting potential threats, and proposing strategic improvements. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 06** | **ASSESS THE SECURITY POSTURE OF SYSTEMS AND NETWORKS USING ETHICAL HACKING TECHNIQUES, WHILE ADHERING TO LEGAL AND ETHICAL BOUNDARIES** |
| **Assessment Criteria** | **6.1 Summarize the high-level overview of the findings.**<br>**6.2 Analyse and differentiate the technical details of vulnerabilities and exploits.**<br>**6.3 Categorize risks associated with identified vulnerabilities.**<br>**6.4 Propose and formulate remediation recommendations based on analysis.**<br>**6.5 Illustrate findings using charts, graphs, and screenshots to enhance understanding**.<br>**6.6 Report on compliance status, ensuring adherence to regulatory frameworks.**<br>**6.7 Conduct a peer review to validate findings and methodologies.**<br>**6.8 Generate actionable insights and extrapolate security improvements.**<br>**6.9 Outline lessons learned to enhance future security strategies.**<br>**6.10 Ensure legal considerations are interpreted and integrated into the findings**. |
| **Content** | **6.1 Summarize the high-level overview of the findings**<br>● Describe the overall findings from the security assessment.<br>● Identify the most critical vulnerabilities and potential threats discovered.<br>● Outline the context of the environment or system under review.<br>● List the key security concerns, including insecure configurations, outdated software versions, unpatched vulnerabilities, and weak access controls.<br>● State the vulnerabilities identified: insufficient encryption, poor password management, exposed sensitive data, absence of multi-factor authentication (MFA), and open ports in the firewall.<br><br>**6.2 Analyse and differentiate the technical details of vulnerabilities and exploits**<br>● Describe specific vulnerabilities identified in the system, including SQL injection, outdated SSL/TLS protocols, and weak hashing algorithms in password storage.<br>● Identify the attack vectors associated with these vulnerabilities, such as the public-facing application and misconfigured web servers.<br>● List the CVE references for the vulnerabilities discovered and |

| | |
|---|---|
| | match them with the relevant technical aspects of the exploits.<br>● Outline how an attacker might exploit misconfigurations in web servers for remote code execution, emphasizing the potential for unauthorized access.<br>● Compare the risk levels between SQL injection and outdated SSL/TLS protocols, showing which presents a higher likelihood of exploitation.<br>● Illustrate the potential consequences of each exploit in real-world scenarios.<br>● Categorize the vulnerabilities into different groups (e.g., injection flaws, encryption weaknesses, and configuration errors).<br>● Discuss possible mitigation strategies for each identified vulnerability, including patching, encryption upgrades, and configuration hardening.<br>● Summarize the exploit techniques and their consequences, rephrasing the details of each to ensure clarity.<br>● Analyze the possibility of preventing exploitation by using modern security practices and applying these to future development efforts.<br><br>**6.2 Categorize risks associated with identified vulnerabilities**<br>● Identify risk categories based on the likelihood and impact of potential vulnerabilities.<br>● Analyze the consequences of each vulnerability in relation to business operations and sensitive data.<br>● Apply risk assessment frameworks such as STRIDE and OWASP Top 10 to evaluate risks.<br>● Label critical risks, such as the exposure of sensitive data due to weak encryption or plaintext storage.<br>● Classify moderate risks, such as privilege escalation through insecure permissions or excessive user privileges.<br>● State low risks, such as information disclosure from debug messages or overly verbose error reporting.<br><br>**6.3 Propose and formulate remediation recommendations based on analysis**<br>● Identify potential threats and use firewalls to block unauthorized access.<br>● Apply security patches to fix known vulnerabilities and implement strong encryption mechanisms to protect sensitive data.<br>● Enforce strong user authentication practices and train employees on security awareness to minimize human error. |

| | |
|---|---|
| | ● Describe the process of securing systems by applying patches, modifying system configurations, and following secure coding practices.<br>● Organize secure coding practices by following guidelines to prevent vulnerabilities such as SQL injection or buffer overflows.<br>● Classify defense mechanisms into physical, technical, and administrative controls.<br>● Discuss how each layer of defense provides complementary protection to mitigate attacks.<br>● Explain remediation techniques, including the application of patches, encrypting sensitive data, and conducting employee security training.<br>● Summarize the benefits of disabling unnecessary services and closing unused ports to reduce attack surfaces.<br>● Organize the steps needed to perform system hardening by adjusting security configurations and removing potential vulnerabilities.<br><br>**6.4 Illustrate findings using charts, graphs, and screenshots to enhance understanding**<br>● Identify vulnerability findings and represent them visually using charts, graphs, and screenshots.<br>● Clarify the data by providing a clear and easily understandable format for stakeholders to interpret<br>● Use visualization tools such as Excel, Power BI, Kali Linux, and Nmap output to illustrate the findings.<br>● Categorize vulnerabilities by severity level and diagram the distribution using bar charts.<br>● Summarize the percentage of high, medium, and low-risk vulnerabilities found through pie charts.<br><br>**6.5 Report on compliance status, ensuring adherence to regulatory frameworks**<br>● Describe the adherence to relevant regulatory frameworks (e.g., GDPR, HIPAA, PCI DSS, ISO 27001) within the organization.<br>● Identify compliance gaps, such as the lack of encryption for data in transit, which violates PCI DSS requirements.<br>● Outline non-compliance issues, including the failure to comply with GDPR's data retention and user consent policies.<br>● List the regulatory risks associated with non-compliance, specifically those related to GDPR and PCI DSS. |

| | |
|---|---|
| | ● Clarify the necessary actions for bridging the compliance gaps, such as implementing encryption for data in transit.<br>● Analyse the potential regulatory risks if these compliance issues are not addressed, particularly the impact on GDPR compliance.<br>● Explain the importance of aligning with PCI DSS and GDPR regulations to avoid legal and financial penalties.<br>● Recommend actions to mitigate compliance gaps, such as updating data retention policies and enhancing data security measures.<br><br>**6.6 Conduct a peer review to validate findings and methodologies**<br>● Describe the peer review process and how it ensures accuracy by cross-checking findings with team members.<br>● Identify overlooked vulnerabilities and areas needing further attention based on peer feedback.<br>● Label the methodologies used to ensure consistency with industry standards and report any discrepancies.<br>● Outline necessary adjustments to methodologies based on peer input to improve assessment thoroughness.<br>● Analyze peer feedback and compare findings with industry standards to detect gaps.<br>● Implement changes to the methodology based on the peer review to enhance assessment accuracy.<br>● Create a refined methodology and report reflecting the peer review findings and adjustments made.<br><br>**6.7 Generate actionable insights and extrapolate security improvements**<br>● Transform findings into actionable insights that enhance the security posture by identifying and addressing immediate vulnerabilities and weaknesses.<br>● Suggest long-term improvements to reduce the risk of future breaches, prioritizing the implementation of measures like multi-factor authentication (MFA) for all critical systems.<br>● Provide strategic advice to strengthen security policies and controls, recommending regular vulnerability scans and penetration tests to identify new vulnerabilities.<br>● Implement multi-factor authentication (MFA) across all critical systems to enhance access control and prevent unauthorized access.<br>● Perform regular vulnerability scans and penetration tests to detect new vulnerabilities, evaluating the effectiveness of current security |

| | |
|---|---|
| | controls and improving future protection measures.<br><br>**6.8 Outline lessons learned to enhance future security strategies**<br>● Describe the lessons learned from the security assessment process: The need to improve early-stage risk assessments and automate patch management for quicker vulnerability remediation.<br>● Identify best practices and areas for improvement: Regular staff training on cybersecurity hygiene and incident response protocols.<br>● Label key improvements: Early-stage risk assessments and automated patch management.<br>● List areas for improvement: Automating vulnerability remediation and improving incident response through continuous staff training.<br>● Match lessons learned to corresponding actions: Faster vulnerability remediation with automated patch management and enhanced incident response with staff training.<br>● State the purpose of the lessons learned: To guide future security assessments and incident responses for better security hygiene.<br>● Summarize recommendations for improvement: Focus on automation for patch management, early detection of vulnerabilities, and regular training on cybersecurity best practices.<br><br>**6.9 Ensure legal considerations are interpreted and integrated into the findings**<br>● Describe the findings in compliance with relevant laws and ethical standards.<br>● Evaluate the impact of vulnerabilities on legal obligations, such as breach reporting requirements.<br>● List the risks associated with failing to secure personally identifiable information (PII) and the potential for regulatory fines.<br>● State the importance of adhering to legal obligations regarding data security.<br>● Outline steps to ensure compliance with GDPR and HIPAA in data management.<br>● Explain the potential legal consequences and financial penalties for mishandling PII.<br>● Illustrate how failure to meet data security standards can lead to significant legal risks.<br>● Examine the risks involved in handling sensitive data and the need to implement strong security measures to mitigate legal repercussions. |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to utilize Ethical Hacking Techniques as outlined in the assessment criteria and content above.<br>2. Practical assessment on compliance auditing and legal knowledge, data privacy and protection, collaboration and peer review, risk assessment, documentation and report writing |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below.<br>● Standards (GDPR, HIPAA, PCI DSS, ISO 27001)<br>● Computer hardware |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Perform effective reconnaissance on a given target system or network, accurately gathering publicly available information to inform subsequent ethical hacking phases | 15% |
| Scan and enumerate target information from identified systems, precisely identifying open ports, services, and potential vulnerabilities by utilizing appropriate tools and methodologies | 20 % |
| Execute various network exploitation techniques against identified vulnerabilities in a controlled lab environment, demonstrating the ability to gain unauthorized access while adhering to ethical guidelines | 20% |

| | |
|---|---|
| Conduct post-exploitation activities on compromised systems, effectively maintaining access, escalating privileges, and exfiltrating data without causing system damage to identify and evaluate security risks | 15% |
| Construct comprehensive and clear forensic reports and documentation for all phases of an ethical hacking engagement, ensuring all findings are accurately presented and actionable | 15 % |
| Assess the security posture of systems and networks using ethical hacking techniques, while adhering to legal and ethical boundaries | 15% |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**
   - **Facilities**
     - Cybersecurity Lab – A dedicated space with isolated networks for ethical hacking practice.
     - High-Speed Internet Connection – Essential for penetration testing and online research.
     - Secured Testing Environment – A sandbox or virtual lab to conduct tests without affecting live systems.
     - Server Room/Data Center – If conducting network security assessments.
     - Whiteboard and Projectors – For discussions, training, and presentations.

- **Tools**

  Reconnaissance Tools (Information Gathering)
  - Nmap – Network scanning and port discovery.
  - Maltego – OSINT and network intelligence gathering.
  - Recon-ng – Web-based reconnaissance automation.

  Vulnerability Assessment Tools
  - Nessus – Vulnerability scanning.
  - OpenVAS – Open-source vulnerability assessment.
  - Nikto – Web vulnerability scanner.

  Exploitation & Penetration Testing Tools
  - Metasploit – Framework for penetration testing.
  - Sqlmap – Automated SQL injection testing.
  - Burp Suite – Web application security testing.
  - BeEF – Browser exploitation framework.

  Password Cracking Tools
  - John the Ripper – Password cracking.
  - Hydra – Brute-force attack tool.
  - Hashcat – Advanced password recovery.

  Wireless Hacking Tools
  - Aircrack-ng – Wireless network penetration testing.
  - Wireshark – Packet analysis and network sniffing.
  - Kismet – Wireless network detector.

  Forensics & Reverse Engineering Tools
  - Autopsy – Digital forensics toolkit.
  - Volatility – Memory forensics.
  - IDA Pro – Reverse engineering software.

  Anonymity & Privacy Tools
  - Tor Browser – Anonymous web browsing.
  - Proxychains – Redirecting traffic through proxies.
  - VPN Services – Secure and encrypted network connections.

- **Equipment**
  - High-Performance Laptop/Desktop – Must support virtualization and heavy processing.
  - External Hard Drives/USBs – For portable storage and bootable hacking tools.
  - Raspberry Pi – Used for network penetration testing and automation.
  - Network Switches & Routers – To set up and simulate network attacks.
  - Wi-Fi Adapters (Alfa AWUS036NH or similar) – For wireless penetration testing.

- Hardware Keyloggers – For testing keystroke security.
- RFID/NFC Readers – To test RFID security.

➢ **Materials**

Operating Systems:

- Kali Linux, Parrot OS, Ubuntu (for ethical hacking).
- Windows Server and Windows 10/11 for testing.

▪ Cybersecurity Frameworks:

- NIST Cybersecurity Framework.
- MITRE ATT&CK.
- OWASP Top 10.

▪ Legal & Ethical Guidelines:

- Cybersecurity Laws & Regulations (e.g., GDPR, HIPAA, PCI-DSS).
- Penetration Testing Rules of Engagement.
- Ethical Hacking Code of Conduct.

▪ Training & Certification Materials:

- CEH (Certified Ethical Hacker) Study Guides.
- OSCP (Offensive Security Certified Professional) Manuals.
- SANS Course Materials

**3. Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

**4. Reference Materials (recommended textbooks, recommended readings)**

**Engebretson, P.** (2021). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* 3rd ed. Syngress.

**Kim, P. and Solomon, M.G.** (2020). *Fundamentals of Information Systems Security*. 4th ed. Jones & Bartlett Learning.

**Oriyano, S.P.** (2020). *Hacker Techniques, Tools, and Incident Handling.* 3rd ed. Jones & Bartlett Learning.

**Gregg, M.** (2021). *Certified Ethical Hacker (CEH) Version 11 Cert Guide.* Pearson IT Certification.

**Weidman, G.** (2020). *Penetration Testing: A Hands-On Introduction to Hacking*. 2nd ed. No Starch Press.

**Stallings, W. and Brown, L.** (2021). *Computer Security: Principles and Practice*. 4th ed. Pearson.

**McClure, S., Scambray, J., and Kurtz, G.** (2020). *Hacking Exposed 7: Network Security Secrets and Solutions.* 7th ed. McGraw-Hill Education.

**Cole, E.** (2021). *Advanced Penetration Testing: Hacking the World's Most Secure Networks.* 2nd ed. Wiley.

**Hadnagy, C.** (2021*). Social Engineering: The Science of Human Hacking.* 2nd ed. Wiley.

**Ozkaya, E.** (2020). *Cybersecurity: The Beginner's Guide*. Packt Publishing

| | |
|---|---|
| **Module Code:** | **682/25/M14** |
| **Module Title:** | **Mobile Device Forensics** |
| **ZNQF Level:** | **5** |
| **Credits:** | 120 |
| **Duration:** | 12 |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Mobile Forensics** of Unit Standards for Digital Forensics Technician |
| **Pre-requisite modules:** | None |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an **individual** to be able demonstrate understanding of mobile device architecture, apply legal and ethical considerations, acquire data on mobile devices, extract and recover data, analyse data collected from mobile devices, analyse malware on mobile devices and perform incidence response for mobile devices.<br>This module is important as provides crucial evidence in criminal investigations, assisting in civil litigation, enhances cybersecurity, and protects national security. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of Learning Outcomes:** | **LO1: Demonstrate understanding of mobile device architecture to accurately describe the functional roles of hardware and software elements within a mobile operating environment**<br>**LO2: Apply legal and ethical considerations to real-world scenarios involving mobile device forensics and security, ensuring all actions adhere to established professional standards and legal requirements.**<br>**LO3: Acquire data on mobile devices utilizing industry-standard tools and methodologies to ensure the integrity and admissibility of collected evidence in a forensic context.**<br>**LO4: Extract and recover deleted, hidden, or fragmented data from mobile devices using advanced data recovery techniques and tools.**<br>**LO5: Reconstruct events and identify relevant information for investigative purposes by analyzing data collected from mobile devices and interpreting findings.**<br>**LO6: Obtain insights into the threat landscape and develop effective mitigation strategies by analyzing malware on mobile devices.**<br>**LO7: Resolve security incidents by executing comprehensive incident response procedures for mobile devices, encompassing** |

| | |
|---|---|
| | **identification, containment, eradication, recovery, and post-incident analysis** |

| | |
|---|---|
| **Learning Outcome 01** | **Demonstrate understanding of mobile device architecture to accurately describe the functional roles of hardware and software elements within a mobile operating environment** |
| **Assessment Criteria:** | **1.1 Identify components of mobile devices**<br>**1.2 Distinguish mobile operating systems**<br>**1.3 Describe mobile devices file systems** |
| **Content:** | **1.1 Identify components of mobile devices**<br>● Outline the hardware components of mobile devices<br>● Group the software components of mobile devices<br>● Classify the peripheral and external components of mobile devices<br>● Describe the emerging technologies in mobile devices<br><br>**1.2 Distinguish mobile operating systems**<br>● Discuss overview of Mobile Operating Systems<br>● Outline major Mobile Operating Systems<br>● Assess market share and popularity of mobile Operating Systems<br>● Analyse the emerging trends and future of mobile Operating Systems<br><br>**1.3 Describe mobile devices file systems**<br>● Describe the mobile device file systems<br>● Explain common mobile file systems<br>● Illustrate file system structure<br>● Describe file system features<br>● Outline file system management |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to identify components of mobile devices, distinguish mobile operating systems and describe mobile devices file systems as outlined in the assessment criteria and content above.<br>2. Practical assessment on demonstrating understanding of mobile device architecture, applying legal and ethical considerations, acquiring data on mobile devices, extracting and recovering data, analysing data collected from mobile devices, analysing malware on mobile devices and performing incidence response for mobile devices based on the performance criteria of the qualification standard Digital Forensics Technician. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:-<br>● Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics |

| | |
|---|---|
| **Learning Outcome 02** | **Apply legal and ethical considerations to real-world scenarios involving mobile device forensics and security, ensuring all actions adhere to established professional standards and legal requirements** |
| **Assessment Criteria** | **2.1 Follow chain of custody procedures for mobile evidence.**<br>**2.2 Ensure compliance with relevant laws and regulations.**<br>**2.3 Obtain proper authorization before accessing mobile data**. |
| **Content** | **2.1 Follow Chain of custody procedures for mobile evidence**<br>● Define chain of custody in digital forensics<br>● Outline the importance of chain of custody in digital forensics<br>● Compute types of mobile evidence (e.g., call logs, messages, GPS data, app data)<br>● Differentiate between mobile evidence and other types of digital evidence<br>● carry out chain of custody documentation<br>● Outline evidence collection procedures<br>● Review evidence transfer and storage procedure<br>● Outline Legal and Ethical Considerations<br>● Identify common challenges and best practices<br>**2.2 Ensure Compliance with relevant laws and regulations**<br>● Define of compliance and its importance<br>● Explain the consequences of non-compliance (e.g., evidence inadmissibility in court) |

| | |
|---|---|
| | ● Rate ethical considerations in compliance<br>● Analyse relevant laws and regulations<br>● Specify emerging trends and challenges<br><br>**2.3 Obtain proper authorization before accessing mobile data.**<br>● Explain Legal Frameworks and Regulations pertaining to authorization before accessing mobile data.<br>● Outline the ethical considerations |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to apply legal and ethical considerations as outlined in the assessment criteria and content above.<br>2. Practical assessment on following chain of custody procedures for mobile evidence, ensuring compliance with relevant laws and regulations and obtaining proper authorization before accessing mobile data based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>Legal Tools and Materials (eg. Data Protection Act, NIST) and Ethical Tools and Materials (e.g., ACM Code of Ethics, IEEE Code of Ethics) |

| | |
|---|---|
| **Learning Outcome 03** | **Acquire data on mobile devices utilizing industry-standard tools and methodologies to ensure the integrity and admissibility of collected evidence in a forensic context** |
| **Assessment Criteria** | **3.1 Use appropriate tools to extract data.**<br>**3.2 Perform logical, physical, and file system acquisitions.**<br>**3.3 Follow write-blocking techniques to prevent data alteration.** |
| **Content** | **3.1 Use appropriate tools to extract data.**<br>● Define mobile forensics<br>● Outline the importance of mobile forensics<br>● Describe types of Mobile Data<br>● Use commercial tools (e.g., Cellebrite, Magnet AXIOM, Oxygen Forensics)<br>● Use open-source tools (e.g., ADB, FTK Imager, Autopsy)<br>● Compare techniques for data extraction ( eg. Logical extraction vs. physical extraction)<br>**3.2 Perform logical, physical, and file system acquisitions.**<br>● Explain data acquisition<br>● Describe types of data acquisition<br>● Outline data acquisition tools<br>**3.3 Follow write-blocking techniques to prevent data alteration.**<br>● Define write-blocking<br>● Explain types of write blocking<br>● Resolve common issues that may arise when using write-blocking techniques |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to acquire data on mobile devices as outlined in the assessment criteria and content above.<br>2. Practical assessment on using appropriate tools to extract data, performing logical, physical, and file system acquisitions and following write-blocking techniques to prevent data alteration based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite |

| | |
|---|---|
| | UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics. |

| **Learning Outcome 04** | **Extract and recover deleted, hidden, or fragmented data from mobile devices using advanced data recovery techniques and tools** |
|---|---|
| **Assessment Criteria** | **4.1 Recover deleted files, messages, and call logs.**<br>**4.2 Extract data from apps.**<br>**4.3 Identify specialized tools to bypass encryption or locked devices**. |
| **Content** | **4.1 Recover deleted files, messages, and call logs.**<br>● Explain how data deletion works<br>● Outline types of data recovery<br>● Describe how challenges like encrypted data, corrupted storage, or overwritten files are handled.<br>● Use data recovery tools (Eg. Dr.Fone, DiskDigger, EaseUS MobiSaver, or PhoneRescue)<br>● Describe data recovery techniques<br>**4.2 Extract data from apps.**<br>● Describe web scrapping<br>● Explain App sandboxing<br>**4.3 Identify specialized tools to bypass encryption or locked devices**.<br>● Describe how encryption works on mobile devices (e.g., AES, RSA)<br>● Explain Device Lock Mechanisms<br>● Use tools to bypass locks |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to extract and recover data as outlined in the assessment criteria and content above.<br>2. Practical assessment on recovering deleted files, messages, and call logs, extracting data from apps and identifying specialized tools to bypass encryption or locked devices based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees. |

| | |
|---|---|
| | 2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:- Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic Elcomsoft iOS Forensic Toolkit, John the Ripper, Hashcat, RIFF Box, Heat Guns and Soldering Tools, EnCase Forensics, FTK (Forensic Toolkit) Imager, Faraday bags, Anti-Static Equipment, |

| **Learning Outcome 05** | **Reconstruct events and identify relevant information for investigative purposes by analyzing data collected from mobile devices and interpreting findings** |
|---|---|
| **Assessment Criteria** | **5.1 Analyse Call logs, SMS, MMS, and email communications.**<br>**5.2 Examine GPS data and location history.**<br>**5.3 Identify patterns or anomalies in the data.** |
| **Content** | **5.1 Analyse Call logs, SMS, MMS, and email communications.**<br>● Classify call logs (incoming, outgoing, and missed)<br>● Identify SMS and MMS messages metadata(e.g., sender, receiver, timestamps**)**<br>● Examine email communication**.**<br>**5.2 Examine GPS data and location history.**<br>● Illustrate how Global Positioning System (GPS) technology functions<br>● Identify types of Location Data<br>● Explain sources of GPS and location Data<br>● Outline factors that affect GPS accuracy<br>**5.3 Identify patterns or anomalies in the data.**<br>● Illustrate types of Data Patterns( Temporal patterns (e.g., timestamps, frequency of activities), Behavioral patterns (e.g., app usage, call logs, messaging habits))<br>● Outline techniques for identifying patterns<br>● Define anomalies<br>● Compute methods for detecting anomalies |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyze data collected from mobile devices as outlined in the assessment criteria and content above.<br>2. Practical assessment on analyzing Call logs, SMS, MMS, and email communications, examining GPS data and location history and identifying patterns or anomalies in the data based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - |

| **Learning Outcome 06** | **Obtain insights into the threat landscape and develop effective mitigation strategies by analyzing malware on mobile devices** |
|---|---|
| **Assessment Criteria** | **6.1 Detect evidence of malware infection.**<br>**6.2 Perform static and dynamic analysis of suspicious apps**.<br>**6.3 Provide findings documented and provide recommendations for mitigation.** |
| **Content** | **6.1 Detect evidence of malware infection.**<br>● Identify different types of malwares targeting mobile devices (e.g., spyware, ransomware, adware, trojans, etc.).<br>● Identify Indicators of compromise.<br>**6.2 Perform static and dynamic analysis of suspicious apps**.<br>● Define Static analysis and dynamic analysis<br>● Illustrate mobile app structure<br>● Describe the static and dynamic analysis techniques<br>**6.3 Provide findings documented and recommendations for mitigation.**<br>● Create a clear, concise, and structured forensic reports<br>● Explain evidence presentation |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyse malware on mobile devices as outlined in the assessment criteria and content above.<br>2. Practical assessment on detecting evidence of malware infection, performing static and dynamic analysis of suspicious apps and providing findings documented and provide recommendations for |

| | |
|---|---|
| | mitigation based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below:- |

| **Learning Outcome 07** | **Resolve security incidents by executing comprehensive incident response procedures for mobile devices, encompassing identification, containment, eradication, recovery, and post-incident analysis** |
|---|---|
| **Assessment Criteria** | **7.1 Identify and contain mobile-related security incidents.**<br>**7.2 Ensure proper forensic collection of logs, files, and metadata from the affected mobile device.**<br>**7.3 Perform remediation** |
| **Content** | **7.1 Identify and contain mobile-related security incidents**.<br>● Explain mobile security threats<br>● Describe how incidents are identified.<br>● Extrapolate containment strategies<br>● State ways of mitigation and recovery from a security incident.<br>● Explain Preventive measures<br><br>**7.2 Ensure proper forensic collection of logs, files, and metadata from the affected mobile device**.<br>● Define logs<br>● Define metadata<br>● Describe ways to maintain data integrity and preservation.<br>● Explain anti-forensic techniques (e.g., data obfuscation, steganography)<br>● State anti-forensic countermeasures<br><br>**7.3 Perform remediation**<br>● Explain how to safely remove malware without compromising data integrity (e.g., factory reset, manual removal, using specialized tools)<br>● Identify security vulnerabilities in mobile devices (e.g., outdated OS, unpatched apps, weak passwords).<br>● Describe data sanitization and secure disposal of mobile devices. |

| | |
|---|---|
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to perform incidence response for mobile devices as outlined in the assessment criteria and content above.<br>2. Practical assessment on identifying and contain mobile-related security incidents, ensuring proper forensic collection of logs, files, and metadata from the affected mobile device and performing remediation based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Demonstrate understanding of mobile device architecture to accurately describe the functional roles of hardware and software elements within a mobile operating environment | 20% |
| Apply legal and ethical considerations to real-world scenarios involving mobile device forensics and security, ensuring all actions adhere to established professional standards and legal requirements | 10 % |
| Acquire data on mobile devices utilizing industry-standard tools and methodologies to ensure the integrity and admissibility of collected evidence in a forensic context | 20% |

| | |
|---|---|
| Extract and recover deleted, hidden, or fragmented data from mobile devices using advanced data recovery techniques and tools | 10% |
| Reconstruct events and identify relevant information for investigative purposes by analyzing data collected from mobile devices and interpreting findings | 20 % |
| Obtain insights into the threat landscape and develop effective mitigation strategies by analyzing malware on mobile devices | 10% |
| Resolve security incidents by executing comprehensive incident response procedures for mobile devices, encompassing identification, containment, eradication, recovery, and post-incident analysis | 10 % |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**
   Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics , Anti-static mats & wrist straps, Forensic-

grade storage (encrypted drives), SD card readers (write-blocked), Spare cables (USB-C/Lightning/Micro-USB), Evidence bags & tamper-proof seals, Faraday Bags (Mission Darkness), Faraday Cage/Box, RF-Shielded Room, RIFF Box / Octoplus Box (JTAG), Hot Air Rework Station (desoldering), NAND/NOR Flash Reader

**3. Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

**4. Reference Materials (recommended textbooks, recommended readings)**


Ayers, R., Jansen, W., Cilleros, N., and Daniellou, R. (2021). **Mobile Device Forensics: A Practical Guide.** 2nd Ed. Boca Raton, FL: CRC Press.

Holt, T.J., Bossler, A.M., and Seigfried-Spellar, K.C. (2022). Cybercrime and Digital Forensics: An Introduction. 3rd Ed. New York: Routledge.

Luttgens, J.T., Pepe, M., and Mandia, K. (2020). Incident Response & Computer Forensics. 3rd ed. New York: McGraw-Hill Education.

Sammons, J. (2021). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. 3rd ed. Waltham, MA: Syngress.

Kävrestad, J. (2020). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. 2nd ed. Cham, Switzerland: Springer.

Reith, M., Carr, C., and Gunsch, G. (2022). Digital Forensics and Incident Response: A Practical Guide to Investigating and Responding to Cyber Attacks. Birmingham, UK: Packt Publishing.

Casey, E. (2021). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. Waltham, MA: Academic Press.

Rogers, M.K. and Seigfried-Spellar, K.C. (2023). Mobile Forensics: Advanced Investigative Strategies. 1st ed. Boca Raton, FL: CRC Press.

Maras, M.H. (2022). Computer Forensics: Cybercriminals, Laws, and Evidence. 3rd ed. Burlington, MA: Jones & Bartlett Learning.

Quick, D. and Choo, K.K.R. (2021). Digital Forensic Investigation of Internet of Things (IoT) Devices. 1st ed. Cham, Switzerland: Springer.

| | |
|---|---|
| **Module Code:** | **682/25/M15** |
| **Module Title:** | **CLOUD FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard Cloud Forensics of Qualification Standard for a Digital Forensics Technician. |
| **Pre-requisite modules:** | None |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by a Digital Forensic Technician to investigate cloud-based cyber incidents, identify threats, collect and analyze digital evidence and ensure legal compliance. This includes identifying cloud threats and attack vectors, acquiring cloud data and collecting evidence, analyzing cloud logs and investigating incidents, recovering and analyzing cloud data, detecting and mitigating cloud threats; and studying cloud forensic cases and emerging trends.<br>The advantages of the module are is allows investigators to analyze various types of digital evidence, including user logs, network traffic, application data, and metadata. Access to this module is open to all target groups, which include the unemployed, youth, men and women willing to develop their country in line with the Education 5.0 Philosophy. |
| **List of Learning Outcomes:** | **LO1: Identify cloud threats and attack vectors to enable informed risk assessment and proactive defense strategies against vulnerabilities in cloud environments.**<br>**LO2: Acquire cloud data and collect forensic evidence following standard procedures for digital investigations within virtualized environments to ensure integrity and admissibility.**<br>**LO3: Analyse cloud system logs to investigate security incidents and trace unauthorized activities.**<br>**LO4: Maintain data integrity by recovering lost or compromised cloud data using appropriate recovery tools and frameworks.**<br>**LO5: Ensure timely intervention and minimal data exposure by detecting ongoing or potential cloud security threats and applying appropriate mitigation strategies and protocols.**<br>**LO6: Explore emerging trends in cloud threat landscapes and digital evidence to foster a deeper understanding of evolving attack strategies, detection methodologies, and** |

| | |
|---|---|
| | **forensic investigation techniques.** |

| Learning Outcome 01 | **Identify cloud threats and attack vectors to enable informed risk assessment and proactive defense strategies against vulnerabilities in cloud environments** |
|---|---|
| **Assessment Criteria:** | **1.1 Analyze cloud security risks.**<br>**1.2 Identify vulnerabilities in cloud infrastructure.**<br>**1.3 Assess risks related to multi-tenancy and shared resources.**<br>**1.4 Identify common cloud threats.**<br>**1.5 Assess attack vectors.**<br>**1.6 Examine cloud malware and ransomware risks.**<br>**1.7 Detect malicious file uploads and cloud-based malware execution.**<br>**1.8 Investigate cloud-native ransomware and data encryption attacks.**<br>**1.9 Monitor cloud network security.**<br>**1.10 Analyze network traffic for suspicious activities.**<br>**1.11 Detect lateral movement and unauthorized access patterns.**<br>**1.12 Investigate cloud log data for anomalies.**<br>**1.13 Analyze AWS CloudTrail, Azure Monitor, Google Cloud Logging.**<br>**1.14 Identify signs of account compromise or credential theft.**<br>**1.15 Evaluate compliance and security gaps.**<br>**1.16 Assess adherence to security frameworks (NIST, ISO 27001, GDPR, HIPAA)**<br>**1.17 Identify non-compliance issues that could expose the cloud environment.**<br>**1.18 Recommend cloud security enhancements.**<br>**1.19 Implement zero trust security policies.**<br>**1.20 Streng IAM policies (MFA, RBAC) and data encryption strategies.** |
| **Content:** | **1.1 Analyze cloud security risks.**<br>● Define key cloud security risks like data breaches, insecure APIs, and account hijacking.<br>● Analyze the impact of attack vectors such as DDoS, insider threats, and misconfigurations.<br>● Explain the shared responsibility model between cloud providers and users.<br>● Describe how open resources (e.g., storage buckets) can lead to |

| | |
|---|---|
| | unauthorized access.<br>● Outline best practices like strong authentication, encryption, and monitoring.<br>● Identify risks from third-party integrations and supply chain vulnerabilities.<br><br>**1.2 Identified vulnerabilities in cloud infrastructure.**<br>● Define vulnerabilities like weak access controls, misconfigured storage, and lack of encryption.<br>● Analyze risks from default configurations and outdated software.<br>● Explain how insecure APIs can lead to unauthorized access.<br>● Describe the impact of poor patch management on cloud security.<br>● Outline the need for regular vulnerability assessments and testing.<br>● Identify risks from excessive permissions and privilege escalation.<br><br>**1.3 Assess risks related to multi-tenancy and shared resources**<br>● Define multi-tenancy and risks from shared cloud resources.<br>● Analyze data leakage and unauthorized access between tenants.<br>● Explain the impact of poor isolation leading to breaches.<br>● Describe how side-channel attacks can exploit shared resources.<br>● Outline best practices like proper isolation and access controls.<br>● Identify risks from over-provisioning shared resources.<br><br>**1.4 Identify common cloud threats.**<br>● Define common cloud threats such as data breaches, DDoS attacks, and insider threats.<br>● Analyze how misconfigured cloud resources can expose systems to security risks.<br>● Explain the threat posed by inadequate authentication |

| | |
|---|---|
| | mechanisms, leading to unauthorized access.<br>● Describe how vulnerabilities in cloud APIs can be exploited to compromise data and services.<br>● Outline the risks of malware and ransomware targeting cloud infrastructure and services.<br>● Identify the threats posed by insecure third-party integrations and supply chain vulnerabilities.<br><br>**1.5 Assess attack Vectors.**<br>● Define common attack vectors like phishing, DDoS, and malware.<br>● Analyze exploitation of weak entry points such as unsecured APIs and weak authentication.<br>● Explain how social engineering attacks like phishing target cloud users.<br>● Describe how MITM attacks can intercept cloud data.<br>● Outline the impact of distributed attacks like botnets and DDoS on cloud services.<br>● Identify risks from compromised credentials and poor access management.<br><br>**1.6 Examine cloud malware and ransomware risks.**<br>● Define cloud malware and ransomware, focusing on their impact in cloud environments.<br>● Analyze how malware spreads across shared resources in the cloud.<br>● Explain ransomware tactics, including data encryption and ransom demands.<br>● Describe risks like data exfiltration and service disruption from cloud malware.<br>● Outline mitigation strategies such as backups, updates, and endpoint protection. |

| | |
|---|---|
| | ● Identify vulnerabilities in cloud configurations that allow malware or ransomware entry.<br><br>**1.7 Identify signs of account compromise or credential theft**<br>● Define account compromise and credential theft in the cloud.<br>● Analyze unusual logins, failed attempts, and unauthorized access.<br>● Explain behavioral changes like unexpected configuration changes.<br>● Describe indicators like phishing, password resets, and unknown devices.<br>● Outline detection measures like MFA and activity monitoring.<br>● Identify risks from weak passwords and credential-stuffing attacks.<br><br>**1.8 Evaluate compliance and security gaps.**<br>● Define compliance requirements and security standards for cloud environments (e.g., GDPR, ISO 27001).<br>● Analyze security gaps by comparing existing controls against industry best practices.<br>● Explain how misconfigurations and weak policies lead to non-compliance and security risks.<br>● Describe the impact of failing to meet regulatory requirements, including legal and financial penalties.<br>● Outline strategies for identifying and mitigating compliance and security gaps.<br>● Identify tools and frameworks used for compliance audits and security assessments.<br><br>**1.9 Assess adherence to security frameworks (NIST, ISO 27001, GDPR, HIPAA).**<br>● Define key security frameworks such as NIST, ISO 27001, GDPR, and HIPAA. |

| | |
|---|---|
| | ● Analyze cloud security policies to determine compliance with these frameworks.<br>● Explain the importance of adhering to security standards for data protection and regulatory compliance.<br>● Describe common gaps in cloud security that may lead to non-compliance.<br>● Outline best practices for aligning cloud security with industry frameworks.<br>● Identify tools and techniques for assessing and improving adherence to security standards.<br><br>**1.10 Identify non-compliance issues that could expose the cloud environment.**<br>● Define non-compliance in cloud security and its potential risks.<br>● Analyze common non-compliance issues, such as weak access controls and lack of encryption.<br>● Explain how misconfigurations and policy violations expose cloud environments to threats.<br>● Describe the impact of non-compliance, including data breaches and legal penalties.<br>● Outline methods for identifying and mitigating non-compliance risks.<br>● Identify security tools and audits used to detect compliance gaps.<br><br>**1.11 Recommend cloud security enhancements.**<br>● Define cloud security enhancements, including encryption, IAM, and zero-trust architecture.<br>● Analyze existing security gaps and areas for improvement in cloud environments.<br>● Explain the benefits of implementing stronger authentication, such as MFA and biometric security.<br>● Describe how continuous monitoring and threat detection tools |

| | |
|---|---|
| | improve cloud security.<br>● Outline best practices for securing cloud workloads, including data protection and compliance measures.<br>● Recommend security frameworks and tools to enhance cloud security posture.<br><br>**1.12 Implement zero trust security policies.**<br>● Define Zero Trust security and its core principles, including "never trust, always verify."<br>● Analyze traditional security models vs. Zero Trust to highlight key differences.<br>● Explain the importance of identity verification, least privilege access, and micro-segmentation.<br>● Describe how multi-factor authentication (MFA) and continuous monitoring enhance Zero Trust.<br>● Outline steps to implement Zero Trust in cloud environments, such as enforcing strict access controls.<br>● Recommend tools and frameworks for adopting a Zero Trust architecture in cloud security.<br><br>**1.13 Strength IAM policies (MFA, RBAC) and data encryption strategies.**<br>● Define Identity and Access Management (IAM) policies, including MFA and Role-Based Access Control (RBAC).<br>● Analyze weaknesses in IAM configurations that could lead to unauthorized access.<br>● Explain how MFA enhances security by requiring multiple authentication factors.<br>● Describe RBAC's role in restricting access based on user roles and responsibilities.<br>● Outline data encryption strategies for securing data at rest, in transit, and during processing. |

| | |
|---|---|
| | ● Recommend best practices for strengthening IAM policies and encryption mechanisms in cloud environments. |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to identify cloud threats and attack vectors as outlined in the assessment criteria and content above.<br>2. Practical assessment on analyzing cloud security risks, identifying vulnerabilities, assessing attack vectors, implementing Zero Trust policies, and strengthening IAM and encryption strategies in a simulated or real-world cloud environment. |
| **Conditions/Context of assessment** | 2. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>3. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>4. The context of the assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 02** | **Acquire cloud data and collect forensic evidence following standard procedures for digital investigations within virtualized environments to ensure integrity and admissibility** |
|---|---|
| **Assessment Criteria** | **2.1 Identify relevant cloud data sources.**<br>**2.2 Utilize cloud forensic tools.**<br>**2.3 Capture cloud storage and VM snapshots.**<br>**2.4 Extract log data from AWS CloudTrail, Azure Monitor, and Google Cloud Logging.**<br>**2.5 Analyze network traffic.**<br>**2.6 Secure and maintain the chain of custody using hashing, time stamping, and digital signatures.**<br>**2.7 Document and store evidence securely using Encryption, classify,** |

| | |
|---|---|
| | **and retain per policy.** |
| **Content** | **2.1 Identify relevant cloud data sources.**<br>● Define cloud data sources, including logs, virtual machines, databases, and storage services.<br>● Analyze the relevance of different data sources for forensic investigations and security monitoring.<br>● Explain how cloud service models (IaaS, PaaS, SaaS) affect data accessibility.<br>● Describe key sources such as access logs, network traffic logs, and API activity records.<br>● Outline best practices for identifying and securing critical cloud data sources for evidence collection.<br>● Identify tools and techniques used to extract and analyze cloud-based data.<br>**2.2 Utilize cloud forensic tools.**<br>● Define cloud forensic tools like EnCase, FTK, and cloud-native logging services.<br>● Analyze how these tools collect and analyze cloud data for evidence.<br>● Explain their role in recovering deleted or encrypted data.<br>● Describe how to capture logs, VMs, and network traffic using forensic tools.<br>● Outline steps to ensure data integrity and legal admissibility during collection.<br>● Identify best practices for integrating cloud forensic tools with other security platforms.<br>**2.3 Capture cloud storage and VM snapshots.**<br>● Define cloud storage and VM snapshots as methods for capturing system data at a specific time.<br>● Analyze the process of preserving evidence through snapshot captures.<br>● Explain the importance of VM snapshots in maintaining system integrity.<br>● Describe how to capture snapshots using APIs, interfaces, and scripts.<br>● Outline best practices for secure and integrity-preserving snapshot captures.<br>● Identify tools for capturing snapshots across different cloud platforms.<br>**2.4 Extract log data from AWS CloudTrail, Azure Monitor, Google** |

| | |
|---|---|
| | **Cloud Logging.**<br>● Define log data in AWS CloudTrail, Azure Monitor, and Google Cloud Logging.<br>● Analyze the role of log data in tracking activities for forensic purposes.<br>● Explain how to extract log data using APIs and interfaces.<br>● Describe the process of filtering, exporting, and storing log data.<br>● Outline best practices for securing and organizing extracted logs.<br>● Identify tools for automating log extraction and analysis.<br>**2.5 Analyze network traffic.**<br>● Define network traffic analysis as monitoring and inspecting data packets in a network.<br>● Analyze key components like IP addresses, protocols, and payloads.<br>● Explain how it helps detect anomalies and threats.<br>● Describe tools for capturing and analyzing traffic (e.g., Wireshark, tcpdump).<br>● Outline steps to identify suspicious traffic during investigations.<br>● Identify best practices for preserving data integrity in traffic analysis.<br>**2.6 Secure and maintain the chain of custody using hashing, time stamping, and digital signatures.**<br>● Define chain of custody as tracking and securing evidence integrity.<br>● Analyze how hashing, time stamping and digital signatures ensure evidence authenticity.<br>● Explain how hashing verifies data integrity with unique values.<br>● Describe time stamping to record collection time and prevent tampering.<br>● Outline digital signatures for validating identity and data authenticity.<br>● Identify best practices for maintaining a secure chain of custody in cloud investigations.<br>**2.7 Document and store evidence securely using Encryption, classify, and retain per policy.**<br>● Define secure evidence storage using encryption and classification to ensure confidentiality.<br>● Analyze encryption's role in protecting evidence in transit and at rest.<br>● Explain how evidence is classified based on sensitivity and policy. |

| | |
|---|---|
| | ● Describe retention policies for maintaining evidence per legal requirements.<br>● Outline best practices for encrypted storage and access management.<br>● Identify tools for automating evidence classification, encryption, and retention. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to acquire cloud data, collect evidence, and maintain its integrity using techniques like encryption, hashing, and digital signatures, as outlined in the assessment criteria and content above.<br>2. Practical assessment on securely capturing, analyzing, and documenting cloud data and evidence, ensuring compliance with security and retention policies. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 03** | **Analyse cloud system logs to investigate security incidents and trace unauthorized activities** |
|---|---|
| **Assessment Criteria** | **3.1 Collect and correlate log data.**<br>**3.2 Identify suspicious activities.**<br>**3.3 Analyze network traffic logs.**<br>**3.4 Detect lateral movement, DDoS, unusual connections.**<br>**3.5 Investigate authentication and IAM logs.**<br>**3.6 Examine API and Application Log.**<br>**3.7 Apply SIEM and forensic tools for log analysis.**<br>**3.8 Generate incident Timeline.**<br>**3.9 Document report findings.** |

| | |
|---|---|
| **Content** | **3.1 Collect and correlate log data.**<br>● Define log data as records documenting cloud system activities and events.<br>● Analyze the process of collecting and correlating log data from various cloud sources.<br>● Explain how correlating log data helps identify patterns and detect anomalies.<br>● Describe log aggregation methods using tools like SIEM for streamlined analysis.<br>● Outline best practices for ensuring log integrity during collection and correlation.<br>● Identify challenges in correlating log data across platforms and solutions.<br>**3.2 Identify suspicious activities.**<br>● Define suspicious activities as deviations from normal behavior that may indicate security threats.<br>● Analyze signs of suspicious activities like unauthorized access or abnormal system behavior.<br>● Explain using log analysis to detect anomalies indicating suspicious activity.<br>● Describe methods like anomaly detection and behavioral analysis for identifying suspicious actions.<br>● Outline steps to investigate suspicious activities, validate findings, and escalate if needed.<br>● Identify tools for detecting suspicious activities in cloud logs.<br>**3.3 Analyze network traffic logs.**<br>● Define network traffic logs as records capturing data packets, IP addresses, ports, and protocols.<br>● Analyze traffic logs to detect unusual patterns, such as unauthorized access or DDoS attacks.<br>● Explain how to spot security breaches like data exfiltration through log analysis.<br>● Describe techniques for filtering and parsing logs to focus on relevant data.<br>● Outline the importance of correlating traffic logs with other logs for incident analysis.<br>● Identify tools like Wireshark and Suricata for analyzing network traffic.<br>**3.4 Detect lateral movement, DDoS, unusual connections.**<br>● Define lateral movement as attackers moving within a network to escalate privileges or compromise more systems.<br>● Analyze logs for signs of lateral movement, like unusual logins or |

| | |
|---|---|
| | communication between unexpected systems.<br>● Explain DDoS attacks as traffic floods that overwhelm systems, detected through traffic spikes and resource strain.<br>● Describe unusual connections, such as strange IP addresses or communication with unknown sources, as potential threats.<br>● Outline methods for detection using behavioral analysis, IDS, and log correlation.<br>● Identify tools like SIEM and traffic analysis for detecting these threats.<br>**3.5 Investigate authentication and IAM logs.**<br>● Define authentication and IAM logs as records of user access, logins, and permission changes in cloud environments.<br>● Analyze logs for irregularities like failed logins or unauthorized role changes, indicating potential security issues.<br>● Explain how IAM logs track user actions to identify suspicious access patterns.<br>● Describe examining authentication logs for signs of credential theft, such as unusual login times or IP anomalies.<br>● Outline correlating IAM and authentication logs with other logs for a full incident view.<br>● Identify tools like SIEM and cloud-native monitoring tools for analyzing these logs.<br>**3.6 Examine API and Application Log.**<br>● Define API and application logs as records of interactions between users, apps, and cloud services, tracking requests, responses, and errors.<br>● Analyze API logs for unauthorized access attempts or unusual request patterns.<br>● Explain how application logs reveal errors or behaviors that could indicate security issues.<br>● Describe examining API logs for traffic spikes or abnormal IPs signaling potential attacks.<br>● Outline correlating API and application logs with other logs for a comprehensive security view.<br>● Identify tools like SIEM platforms for effective log analysis.<br>**3.7 Apply SIEM and forensic tools for log analysis.**<br>● Define SIEM tools as platforms for aggregating and analyzing security data to detect threats in real-time.<br>● Analyze how SIEM correlates logs from multiple sources to identify suspicious patterns and trigger alerts.<br>● Explain integrating forensic tools with SIEM for detailed incident |

| | |
|---|---|
| | investigations and log analysis.<br>● Describe using forensic tools to filter, query, and visualize logs for security threat detection.<br>● Outline steps for configuring SIEM tools to collect and analyze logs in compliance with security policies.<br>● Identify SIEM and forensic tools (e.g., Splunk, QRadar, FTK, EnCase) for cloud log analysis.<br>**3.8 Generate incident timeline.**<br>● Define an incident timeline as a chronological record of events during a security incident.<br>● Analyze logs to reconstruct the sequence of events, from breach to mitigation.<br>● Explain how the timeline helps identify attack vectors and actions.<br>● Describe extracting timestamps from logs to ensure an accurate timeline.<br>● Outline best practices for creating timelines, using tools for time sync and visualization.<br>● Identify tools like TheHive, Splunk, and Kibana for generating incident timelines.<br>**3.9 Document report findings.**<br>● Define documenting report findings as presenting analysis, conclusions, and recommendations from cloud log investigations.<br>● Analyze data to ensure findings are supported by evidence, like suspicious activities or threats.<br>● Explain the need for a structured report for transparency, legal, or compliance purposes.<br>● Describe the report format, including summary, methodology, findings, and recommendations.<br>● Outline the documentation process, capturing relevant logs, timeframes, and events.<br>● Identify key sections, such as incident details, affected systems, and remediation actions. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyze cloud logs, identify suspicious activities, investigate incidents, and document findings, as outlined in the assessment criteria and content above.<br>2. Practical assessment on using forensic tools to analyze cloud logs, detect incidents, create incident timelines, and document findings in a detailed report. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 04** | **Maintain data integrity by recovering lost or compromised cloud data using appropriate recovery tools and frameworks** |
|---|---|
| **Assessment Criteria** | **4.1 Recover deleted or encrypted data.**<br>**4.2 Analyze cloud storage and databases.**<br>**4.3 Extract and inspect metadata.**<br>**4.4 Identify file changes, access history, and timestamps.**<br>**4.5 Decrypt and verify data integrity.**<br>**4.6 Use hashing, encryption keys, and forensic tools.**<br>**4.7 Correlate log and network data.**<br>**4.8 Cross-check recovered data with logs for anomalies.** |
| **Content** | **4.1 Recover deleted or encrypted data.**<br>● Define recovering deleted or encrypted data as retrieving lost or inaccessible information from cloud systems.<br>● Analyze tools and techniques like file carving, decryption, and cloud provider APIs for data recovery.<br>● Explain challenges in recovery, such as data overwriting or encryption strength.<br>● Describe methods like logical recovery (backups) and physical recovery (forensic tools).<br>● Outline recovery steps: identifying data loss cause, selecting tools, and ensuring data integrity.<br>● Identify decryption techniques or vulnerabilities for encrypted data recovery.<br>**4.2 Analyze cloud storage and databases.**<br>● Define cloud storage and databases as remote platforms for managing data, including object storage and databases.<br>● Analyze the structure of cloud storage and databases to identify data loss or unauthorized access.<br>● Explain the differences between cloud storage types and their impact on data recovery.<br>● Describe common cloud databases (e.g., AWS RDS, Azure SQL) and methods for retrieving data. |

| | |
|---|---|
| | ● Outline techniques for analyzing cloud storage and databases, including log queries and integrity checks.<br>● Identify tools used for cloud storage and database analysis, such as AWS CloudTrail and third-party forensic tools.<br>**4.3 Extract and inspect metadata.**<br>● Define metadata as data describing other data, like creation time and file modifications.<br>● Analyze metadata's role in cloud forensics, such as identifying unauthorized changes.<br>● Explain how to extract metadata from cloud storage (e.g., AWS S3, Azure Blob).<br>● Describe common metadata types like file attributes and access logs.<br>● Outline tools and methods for inspecting metadata, including cloud services and forensic tools.<br>● Identify how metadata helps reconstruct user activity and incident events.<br>**4.4 Identify file changes, access history, and timestamps.**<br>● Define file changes, access history, and timestamps as key indicators of cloud data activity.<br>● Analyze how file changes and timestamps help detect unauthorized access or tampering.<br>● Explain the significance of access history in identifying when and who interacted with files.<br>● Describe how to examine file metadata to track modifications and access patterns.<br>● Identify cloud audit logs and forensic tools to monitor file changes and access.<br>**4.5 Decrypt and verify data integrity.**<br>● Define decryption as converting encrypted data back to its readable form.<br>● Explain how data integrity ensures data remains unchanged and accurate.<br>● Describe decryption methods like AES or RSA in cloud environments.<br>● Outline steps to verify data integrity using cryptographic hashes (e.g., SHA256).<br>● Analyze the use of digital signatures for confirming data authenticity.<br>**4.6 Use hashing, encryption keys, and forensic tools.**<br>● Define hashing for data integrity verification. |

| | |
|---|---|
| | ● Explain encryption keys for secure data access.<br>● Outline forensic tools (e.g., FTK Imager, EnCase) for cloud data analysis.<br>● Analyze hash algorithms (e.g., MD5, SHA256) to verify recovered data.<br>● Describe using encryption keys and forensic tools for encrypted data recovery.<br>**4.7 Correlate log and network data.**<br>● Define the process of correlating log and network data for incident investigation.<br>● Analyze network traffic logs alongside cloud logs to detect anomalies and unauthorized activity.<br>● Explain how correlating log and network data enhances understanding of cloud security events.<br>● Describe techniques for mapping network traffic patterns to logs for tracing incidents.<br>● Outline the importance of integrating multiple data sources (logs, network) for comprehensive analysis and evidence collection.<br>**4.8 Cross-check recovered data with logs for anomalies.**<br>● Define cross-checking recovered data with logs to identify anomalies.<br>● Analyze discrepancies between recovered data and logs to detect tampering.<br>● Explain the importance of comparing data and logs for integrity verification.<br>● Describe methods like comparing timestamps and file changes.<br>● Outline how cross-referencing helps uncover hidden issues and breaches. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to recover and analyze cloud data, including the use of forensic tools, metadata inspection, and log correlation as outlined in the assessment criteria and content above.<br>2. Practical assessment on recovering deleted data, analyzing cloud storage, extracting metadata, and correlating log and network data for evidence of anomalies. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, |

| | |
|---|---|
| | equipment and materials listed below. |

| **Learning Outcome 05** | **Ensure timely intervention and minimal data exposure by detecting ongoing or potential cloud security threats and applying appropriate mitigation strategies and protocols** |
|---|---|
| **Assessment Criteria** | **4.1 Monitor cloud logs and traffic.**<br>**5.1 Identify unauthorized access.**<br>**5.2 Detect and block malware.**<br>**5.3 Mitigate Misconfigurations.**<br>**5.4 Secure APIs.**<br>**5.5 Enforce least privilege.**<br>**5.6 Update firewall rules.**<br>**5.7 Implement incident response actions.**<br>**5.8 Isolate affected resources.**<br>**5.9 Patch vulnerabilities.**<br>**5.10 Strengthen Identity and Access Management (IAM) controls.** |
| **Content** | **5.1 Monitor cloud logs and traffic.**<br>● Define the importance of monitoring cloud logs and traffic to detect potential threats and abnormal activity.<br>● Explain how cloud service logs (AWS CloudTrail, Azure Monitor) help identify unauthorized access or suspicious behavior.<br>● Describe types of logs and traffic patterns that indicate security risks, such as failed logins or unusual IPs.<br>● Analyze traffic and logs with SIEM tools to detect anomalies like data exfiltration or DDoS attacks.<br>● Outline setting up automated alerts to detect real-time threats and mitigate risks quickly.<br>● Discuss integrating network traffic monitoring and cloud logs for comprehensive threat detection.<br>**5.2 Identify unauthorized access.**<br>● Define unauthorized access as attempts to access cloud resources without permission, often using stolen credentials or misconfigurations.<br>● Explain indicators like unfamiliar IPs, failed logins, and unrecognized devices.<br>● Analyze cloud logs to spot irregular login patterns or after-hours access.<br>● Describe using MFA and Identity and Access Management (IAM) to strengthen security and detect unauthorized access. |

| | |
|---|---|
| | ● Outline how SIEM tools help monitor and identify access anomalies.<br>● Discuss methods of investigating access by cross-referencing logs and verifying credentials.<br>**5.3 Detect and block malware.**<br>● Define malware as harmful software, such as viruses and ransomware, targeting cloud environments.<br>● Explain detection methods like behavior analysis, signature detection, and machine learning.<br>● Describe blocking techniques, including firewalls, antivirus software, and intrusion prevention systems.<br>● Analyze cloud logs for indicators of compromise (IoC), such as unusual file changes or unexpected server communication.<br>● Outline the need for continuous scanning and regular security updates.<br>● Explain automated incident response for isolating infected systems and preventing malware spread.<br>**5.4 Mitigate Misconfigurations.**<br>● Define misconfigurations as cloud settings that create vulnerabilities, like open ports or weak access controls.<br>● Analyze common misconfigurations, such as improper IAM roles and unsecured storage.<br>● Explain using tools like AWS Config and Azure Security Center to detect misconfigurations.<br>● Describe steps to remediate, including applying least privilege and automating configuration management.<br>● Outline best practices, like regular audits and using Infrastructure as Code (IaC) for consistent settings.<br>● Explain security testing and compliance frameworks, such as CIS benchmarks, for identifying misconfigurations.<br>**5.5 Secure APIs.**<br>● Define API security as protecting APIs from unauthorized access via authentication and encryption.<br>● Analyze common vulnerabilities like injection attacks and broken authentication.<br>● Explain the use of HTTPS and secure protocols to encrypt API traffic.<br>● Describe methods like OAuth 2.0 and API keys for user authentication and authorization.<br>● Outline input validation and output encoding to prevent attacks like SQL injection. |

| | |
|---|---|
| | ● Explain how API gateways enforce security policies and monitor traffic.<br>● Describe regular security testing (e.g., penetration testing) to find vulnerabilities.<br>**5.6 Enforce the principle of least privilege.**<br>● Define least privilege as giving users only necessary access to perform tasks.<br>● Explain how it reduces the attack surface by limiting data and system access.<br>● Analyze RBAC as a tool to implement least privilege in cloud environments.<br>● Describe the need for regular access reviews and updates based on job roles.<br>● Outline temporary access permissions to prevent excessive privileges.<br>● Explain how automation adjusts access dynamically.<br>● Describe using logs and monitoring to detect privilege violations.<br>**5.7 Update firewall rules.**<br>● Define firewall rules as configurations that control inbound and outbound network traffic.<br>● Explain how updating firewall rules prevents unauthorized access and mitigates threats.<br>● Describe the process of reviewing and adjusting rules based on new threats or network changes.<br>● Analyze traffic patterns to identify necessary rule updates for enhanced security.<br>● Outline best practices for firewall rule management, such as least privilege and segmentation.<br>● Explain the use of automated tools for monitoring and updating firewall configurations.<br>● Describe how to test rule changes to ensure they don't disrupt legitimate operations while blocking malicious activity.<br>**5.8 Implement incident response actions.**<br>● Define incident response actions as predefined procedures to address and mitigate security incidents.<br>● Describe the steps in implementing an incident response, such as identification, containment, eradication, and recovery.<br>● Explain the importance of quick, coordinated actions to minimize damage and restore normal operations.<br>**5.9 Isolate affected resources.**<br>● Define isolating affected resources as detaching compromised |

| | |
|---|---|
| | systems to prevent further spread.<br>● Explain the importance of quick isolation to contain threats and protect unaffected systems.<br>● Describe methods like shutting down access to compromised servers or databases.<br>**5.10 Patch vulnerabilities.**<br>● Define patching vulnerabilities as applying updates or fixes to address security gaps in systems or software.<br>● Explain the importance of timely patching to prevent exploitation of known vulnerabilities.<br>● Describe methods for patching, including automated tools or manual updates based on criticality.<br>**5.11 Strengthen Identity and Access Management (IAM) controls.**<br>● Define Identity and Access Management (IAM) controls as policies managing user access in cloud environments.<br>● Explain how strengthening Identity and Access Management (IAM) limits unauthorized access and reduces threats.<br>● Outline strategies like multi-factor authentication (MFA) and role-based access control (RBAC) for enhanced security. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to detect and mitigate cloud threats through techniques like monitoring logs, identifying unauthorized access, blocking malware, and strengthening Identity and Access Management (IAM) controls, as outlined in the assessment criteria and content above.<br>2. Practical assessment on implementing incident response actions, patching vulnerabilities, and isolating affected resources to detect and mitigate cloud threats effectively. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| Learning Outcome 06 | **Explore emerging trends in cloud threat landscapes and digital evidence to foster a deeper understanding of evolving attack strategies, detection methodologies, and forensic investigation techniques** |
|---|---|
| **Assessment Criteria** | **6.1 Analyze high-profile cloud security incidents.**<br>**6.2 Review cases like AWS breaches or data leaks in cloud environments.**<br>**6.3 Identify lessons from past incidents.**<br>**6.4 Evaluate response strategies and improve future cloud forensic practices.**<br>**6.5 Research emerging cloud threats.**<br>**6.6 Update new attack vectors like container vulnerabilities and cloud-native malware.**<br>**6.7 Explore AI and machine learning in forensics.**<br>**6.8 Monitor trends in cloud compliance and regulations.** |
| **Content** | **6.1 Analyze high-profile cloud security incidents.**<br>● Define the impact of high-profile cloud security incidents.<br>● Analyze case studies to identify patterns and vulnerabilities.<br>● Explain the investigative steps taken in response to breaches.<br>● Describe emerging cloud security trends and their implications.<br>**6.2 Review cases like AWS breaches or data leaks in cloud environments.**<br>● Define common causes of AWS breaches and data leaks in cloud environments.<br>● Analyze the impact of these incidents on data security and privacy.<br>● Explain the investigative methods used to uncover vulnerabilities.<br>● Describe how cloud service providers have addressed these issues to improve security.<br>**6.3 Identify lessons from past incidents.**<br>● Identify key takeaways from past cloud security incidents.<br>● Analyze patterns or weaknesses that contributed to these breaches.<br>● Explain how these lessons can inform future cloud security practices.<br>● Outline best practices to prevent similar incidents based on past case studies.<br>**6.4 Evaluate response strategies and improve future cloud forensic practices.**<br>● Evaluate the effectiveness of response strategies used in past cloud forensic cases.<br>● Analyze how these strategies impacted the resolution and detection of incidents.<br>● Explain potential improvements in response protocols based on past experiences. |

| | |
|---|---|
| | ● Outline ways to enhance cloud forensic practices for quicker, more accurate incident resolution in the future.<br>**6.5 Research emerging cloud threats.**<br>● Research emerging cloud threats, such as new attack vectors or evolving malicious techniques.<br>● Analyze trends in cloud security breaches and their impact on cloud infrastructure.<br>● Explain the significance of new threats and their potential risks to cloud environments.<br>● Outline proactive measures and tools that can be implemented to mitigate emerging cloud threats.<br>**6.6 Update new attack vectors like container vulnerabilities and cloud-native malware.**<br>● Define new attack vectors, including container vulnerabilities and cloud-native malware.<br>● Analyze the impact of container vulnerabilities and cloud-native malware on cloud security.<br>● Explain the evolution of these threats and their methods of exploitation in cloud environments.<br>● Outline strategies for identifying and mitigating these vulnerabilities to enhance cloud security.<br>**6.7 Explore AI and machine learning in forensics.**<br>● Define AI and machine learning's role in cloud forensics.<br>● Analyze their impact on improving threat detection and data analysis.<br>● Explain AI's use in automating anomaly detection.<br>● Outline benefits and challenges in cloud forensic practices.<br>**6.8 Monitor trends in cloud compliance and regulations.**<br>● Define key cloud compliance standards and regulations (e.g., GDPR, CCPA, HIPAA).<br>● Analyze trends in regulatory changes and their impact on cloud forensics.<br>● Explain the importance of compliance in cloud data security.<br>● Outline strategies to stay updated with evolving cloud regulations |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to study cloud forensic cases, emerging trends, and assess response strategies as outlined in the assessment criteria and content above.<br>2. Practical assessment on researching and evaluating cloud security incidents, applying forensic techniques, and identifying new attack vectors and compliance trends. |

| | |
|---|---|
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3-hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Identify cloud threats and attack vectors to enable informed risk assessment and proactive defense strategies against vulnerabilities in cloud environments | 20% |
| Acquire cloud data and collect forensic evidence following standard procedures for digital investigations within virtualized environments to ensure integrity and admissibility | 15% |
| Analyse cloud system logs to investigate security incidents and trace unauthorized activities | 15% |
| Maintain data integrity by recovering lost or compromised cloud data using appropriate recovery tools and frameworks | 15% |
| Ensure timely intervention and minimal data exposure by detecting ongoing or potential cloud security threats and applying appropriate mitigation strategies and protocols | 15% |
| Explore emerging trends in cloud threat landscapes and digital evidence to foster a deeper understanding of evolving attack strategies, detection methodologies, and forensic investigation techniques | 20% |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

3. **Learning Resources**

   Relevant training manual (learners' guide) and facilitators' guide

4. **Reference Materials (recommended textbooks, recommended readings)**


   Manuele, F.A., 2013. *On the practice of safety*. 4th ed. Hoboken: John Wiley & Sons, Inc.

   Amazon Web Services (AWS), 2020. *AWS CloudTrail User Guide*. [online] Available at: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/ [Accessed 17 February 2025].

   Cloud Security Alliance, 2019. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. [online] Available at: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ [Accessed 17 February 2025].

European Union, 2016. *General Data Protection Regulation (GDPR)*. [online] Available at: https://gdpr.eu/ [Accessed 17 February 2025].

ISO/IEC, 2013. *ISO/IEC 27001:2013 - Information Security Management Systems*. [online] Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 17 February 2025].

National Institute of Standards and Technology (NIST), 2020. *NIST Cybersecurity Framework*. [online] Available at: https://www.nist.gov/cybersecurity-framework [Accessed 17 February 2025].

Zscaler, 2021. *Zero Trust Architecture: A Secure and Modern Approach to Protecting Applications and Data*. [online] Available at: https://www.zscaler.com/zero-trust [Accessed 17 February 2025].

| | |
|---|---|
| **Module Code:** | **682/25/M16** |
| **Module Title:** | **MEMORY FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 12 |
| **Duration:** | 120 |
| **Relationship with Qualification Standards:** | Based on Unit Standard **Memory Forensics** of Unit Standards for a Digital Forensic Technician |
| **Pre-requisite modules:** | None |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an **individual** to be able to effectively communicate in business. This includes demonstrating knowledge of memory forensics concepts and principles, acquiring memory, analysing memory, detecting and analyse malware present in memory, applying advanced techniques to uncover sophisticated threats, utilizing automated tools in memory forensics and providing incident response for memory forensics.<br>This module is important as it helps detecting, analysing, and mitigating cyber threats by uncovering volatile evidence, such as malware, encryption keys, and unauthorized activities that traditional forensic methods may miss. The module targets individuals who are in the cybersecurity field of work irrespective of gender, age or ethnicity. |
| **List of Learning Outcomes:** | **LO1: Demonstrate knowledge of memory forensics concepts and principles**<br>**LO2: Acquire memory dumps from suspect machines, using industry-standard tools and procedures under forensic lab conditions to ensure completeness, integrity, and chain of custody.**<br>**L03: Extract forensic artifacts such as processes, handles, and network connections by analysing captured memory.**<br>**LO4: Detect and analyse malware embedded in volatile memory using signature-based and behavioral analysis tools to accurately identify indicators of compromise.**<br>**LO5: Uncover stealthy or encrypted threats such as rootkits and fileless malware by applying advanced techniques.**<br>**LO6: Utilize automated tools in memory forensics to** |

| | |
|---|---|
| | **enable rapid memory parsing, anomaly detection, and triage.**<br>**LO7: Provide incident response strategies based on findings from memory forensic analysis during live security breaches to align with organizational protocols and forensic best practices.** |

| Learning Outcome 01 | Demonstrate knowledge of memory forensics concepts and principles |
|---|---|
| **Assessment Criteria:** | **1.1 Capture purpose and importance of memory forensics in digital investigations**<br>**1.2 Describe structure and organization of volatile memory (RAM).**<br>**1.3 Identify types of data that can be extracted from memory.** |
| **Content:** | **1.1 Purpose and importance of memory forensics in digital investigations**<br>● Define memory forensics as the process of capturing and analysing volatile memory (RAM) to uncover digital evidence.<br>● Explain the significance of memory forensics in cybercrime investigations, malware analysis, and incident response.<br>● Describe the role of memory forensics in identifying fileless malware, detecting rootkits, and uncovering unauthorized access.<br>● Analyse the advantages of memory forensics over traditional disk forensics, emphasizing the ability to retrieve live system activity, encryption keys, and volatile data.<br>● Outline real-world applications of memory forensics, such as ransomware investigations, insider threat detection, and advanced persistent threat (APT) analysis.<br>**1.2 Structure and organization of volatile memory (RAM)**<br>● Define volatile memory RAM<br>● Describe the structure of RAM.<br>● Explain the function of kernel space in managing system-level operations, memory allocation, and process execution.<br>● Analyse the role of user space in handling application-level processes, temporary data storage, and software execution.<br>● Describe memory management techniques,<br>● Examine challenges in analysing RAM.<br>**1.3 Types of data that can be extracted from memory**<br>● Identify key memory artifacts<br>● Describe the forensic relevance of running processes and active threads.<br>● Explain the significance of network connections and open ports in tracing external communications and detecting potential data exfiltration.<br>● Describe the forensic value of injected code, malicious payloads, and rootkits.<br>● Outline the impact of data volatility on forensic acquisition. |

| | |
|---|---|
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to perform memory forensics, including acquisition, analysis, and interpretation of memory data, as outlined in the assessment criteria.<br>2. Practical assessment on demonstrating knowledge of capturing the purpose and importance of memory forensics in digital investigations, describing structure and organization of volatile memory (RAM) and identifying types of data that can be extracted from memory. Based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br>● Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics |

| | |
|---|---|
| **Learning Outcome 02** | **Acquire memory dumps from suspect machines, using industry-standard tools and procedures under forensic lab conditions to ensure completeness, integrity, and chain of custody** |
| **Assessment Criteria** | **2.1 Utilize appropriate tools to capture memory.**<br>**2.2 Ensure integrity of memory dumps using hashing algorithms.**<br>**2.3 Document memory acquisition process, including timestamps and system state** |

| | |
|---|---|
| **Content** | **2.1 Utilize appropriate tools to capture memory**<br>● Define memory acquisition tools.<br>● Describe the importance of selecting appropriate tools.<br>● Outline common memory acquisition tools, emphasizing their functionalities and use cases.<br>● Analyse the factors influencing tool selection.<br>● Explain the significance of minimizing system disruption during acquisition.<br>**2.2 Ensure integrity of memory dumps using hashing algorithms**.<br>● Define the concept of data integrity in digital forensics<br>● Describe the use of cryptographic hashing algorithms, in verifying the integrity of memory dumps.<br>● Explain the role of hashing in forensic investigations.<br>● Analyse the risks of compromised integrity.<br>● Outline the process of generating and verifying hash values before and after acquisition to maintain forensic soundness.<br>**2.3 Document memory acquisition process, including timestamps and system state**<br>● Describe the importance of documentation in the memory acquisition process to maintain a clear chain of custody and forensic validity.<br>● Explain the role of timestamps in memory forensics.<br>● Outline the key details recorded during memory acquisition.<br>● Analyse the impact of system state on memory forensics, highlighting how changes in RAM contents may affect evidence reliability.<br>● Describe best practices for documentation. |
| **Assessment Tasks** | 3. Written and/or oral assessment on the skills and knowledge required to acquire memory as outlined in the assessment criteria and content above.<br>4. Practical assessment on utilizing appropriate tools to capture memory, ensuring integrity of memory dumps using hashing algorithms and documenting memory acquisition process, including timestamps and system state based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment |

| | |
|---|---|
| | and materials listed below: -<br>Legal Tools and Materials (eg. Data Protection Act, NIST) and Ethical Tools and Materials (e.g., ACM Code of Ethics, IEEE Code of Ethics) |

| **Learning Outcome 03** | **Extract forensic artifacts such as processes, handles, and network connections by analysing captured memory** |
|---|---|
| **Assessment Criteria** | **3.1 Utilise memory analysis tools**<br>**3.2 Identify running processes, hidden processes, and injected code.**<br>**3.3 Analyse network connections and open sockets to detect suspicious activity.**<br>**3.4 Extract and interpret artifacts such as registry keys, passwords, and encryption keys.** |
| **Content** | **3.1 Utilise memory analysis tools**<br>● Describe memory analysis tools.<br>● Explain the role of memory forensics tools.<br>● Outline commonly used memory analysis tools.<br>● Analyse the importance of choosing the right tool<br>**3.2 Identify running processes, hidden processes, and injected code**<br>● Define running processes.<br>● Describe hidden processes.<br>● Analyse process injection techniques.<br>● Explain the significance of detecting anomalies<br>**3.3 Analyse network connections and open sockets to detect suspicious activity**<br>● Define network connections and open sockets.<br>● Describe methods for examining active network connections to identify unauthorized communication channels and potential command-and-control servers.<br>● Explain how suspicious network activity can be detected.<br>● Explain how attackers use network-based techniques<br>**3.4 Extract and interpret artifacts such as registry keys, passwords, and encryption keys**<br>● Describe memory artifacts<br>● Explain the forensic value of extracting registry keys<br>● Explore password recovery techniques<br>● Outline the process of locating encryption keys within memory to decrypt protected files and communications. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to analyze memory as outlined in the assessment criteria and content |

| | |
|---|---|
| | above.<br>2. Practical assessment on utilizing memory analysis tools, analyzing network connections and open sockets to detect suspicious activity and extracting and interpreting artifacts such as registry keys, passwords, and encryption keys based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of the assessment should include the facilities, tools, equipment and materials listed below: -<br>● Forensic Lab Setup, Virtual Machines, Legal Framework, Cellebrite UFED, MSAB XRY, Magnet AXIOM, Oxygen Forensic Detective, Belkasoft Evidence Center, MOBILedit Frensics, Autopsy,iPhone Backup Analyzer, Elcomsoft iOS Forensic tool kit, Cellebrite UFED Chip-Off, Cellebrite UFED Touch and Camera, SIMcon, Forensic SIM Toolkit, Forensic cables and adapters, Dr.Fone -Data Recovery, Encase Forensics. |

| **Learning Outcome 04** | **Detect and analyse malware embedded in volatile memory using signature-based and behavioral analysis tools to accurately identify indicators of compromise** |
|---|---|
| **Assessment Criteria** | **4.1 Indicators of compromise (IOCs) related to malware in memory identified.**<br>**4.2 Static and dynamic analysis of malicious processes performed.**<br>**4.3 Behaviour and impact of malware found in memory documented.** |
| **Content** | **4.1 Identify indicators of compromise (IOCs) related to malware in memory**<br>● Define indicators of compromise (IOCs)<br>● Describe memory-based IOC.<br>● Analyse how malware leverages volatile memory<br>● Outline methods for identifying IOCs.<br>**4.2 Perform static and dynamic analysis of malicious processes**<br>● Define static analysis.<br>● Describe dynamic analysis<br>● Explain the use of memory forensic tools.<br>● Analyse process injection techniques<br>**4.3 Document behaviour and impact of malware found in memory** |

| | |
|---|---|
| | ● Describe common malware behaviours in memory.<br>● Explain the role of memory-resident malware in advanced persistent threats (APTs), fileless attacks, and in-memory exploitation.<br>● Analyse the impact of memory-based malware on system stability, data integrity, and network security.<br>● Outline documentation techniques for forensic reporting |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to detect and analyse malware present in memory as outlined in the assessment criteria and content above.<br>2. Practical assessment on performing static and dynamic analysis of malicious processes and documenting the behaviour and impact of malware found in memory based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br><br>Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic Elcomsoft iOS Forensic Toolkit, John the Ripper, Hashcat, RIFF Box, Heat Guns and Soldering Tools, EnCase Forensics, FTK (Forensic Toolkit) |

| | |
|---|---|
| | Imager, Faraday bags, Anti-Static Equipment, |

| **Learning Outcome 05** | **Uncover stealthy or encrypted threats such as rootkits and fileless malware by applying advanced techniques** |
|---|---|
| **Assessment Criteria** | **5.1 Detect rootkits and kernel-level malware using memory analysis**<br><br>**5.2 Analyse memory artifacts from virtual machines and cloud environments.**<br>**5.3 Reconstruct attacker activities.**<br>**5.4 Detect and analyse Anti-forensics techniques used by attackers**<br>**5.5 Identify attempts to hide malicious activity in memory**<br>**5.6 Recover evidence from memory regions that have been intentionally corrupted or overwritten.** |
| **Content** | **5.1 Detect rootkits and kernel-level malware using memory analysis**<br>● Define rootkits.<br>● Describe kernel-level malware.<br>● Analyse techniques used to detect rootkits in memory.<br>● Explain the impact of kernel-level threats on system integrity, security controls, and forensic investigations.<br>**5.2 Analyse memory artifacts from virtual machines and cloud environments**<br>● Describe memory forensics in virtualized environments.<br>● Explain differences in memory acquisition techniques for physical machines, virtual machines (VMs), and cloud-based instances.<br>● Analyse challenges in retrieving memory dumps from cloud environments<br>● Outline forensic methods for extracting memory artifacts<br>**5.3 Reconstruct attacker activities**<br>● Define attack reconstruction.<br>● Describe timeline analysis.<br>● Analyse attacker tradecraft.<br>● Explain forensic approaches to mapping attacker activity.<br>**5.4 Detect and analyse anti-forensics techniques used by attackers**<br>● Define anti-forensics techniques.<br>● Describe techniques such as direct kernel object manipulation (DKOM), memory compression, and encrypted payloads that hinder analysis. |

| | |
|---|---|
| | ● Analyse methods for detecting anti-forensics tactics.<br>● Explain countermeasures used to bypass anti-forensic techniques<br>**5.5 Identify attempts to hide malicious activity in memory**<br>● Describe stealth techniques used by malware to evade detection.<br>● Explain how attackers use legitimate system processes (e.g., svchost.exe, explorer.exe) to hide malicious execution in memory.<br>● Analyse forensic methods for detecting hidden activity<br>● Outline detection strategies<br>**5.6 Recover evidence from memory regions that have been intentionally corrupted or overwritten.**<br>● Describe memory corruption techniques<br>● Explain forensic challenges<br>● Analyse memory reconstruction methods<br>● Outline strategies for mitigating evidence destruction |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to apply advanced techniques to uncover sophisticated threats as outlined in the assessment criteria and content above.<br>2. Practical assessment on detecting rootkits and kernel-level malware using memory analysis, analysing memory artifacts from virtual machines and cloud environments, reconstructing attacker activities and recovering evidence from memory regions that have been intentionally corrupted or overwritten based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - |

| Learning Outcome 06 | **Utilize automated tools in memory forensics to enable rapid memory parsing, anomaly detection, and triage** |
|---|---|
| **Assessment Criteria** | **6.1 Demonstrate proficiency with tools.**<br>**6.2 Utilize Open-source tools for supplementary analysis.**<br>**6.3 Diagnose and resolve Common issues encountered during memory acquisition and analysis**<br>**6.4 Remove malicious artifacts and restore affected systems** |
| **Content** | **Demonstrate proficiency with tools**<br>● Describe the role of automated tools in streamlining memory forensics by accelerating data extraction, pattern recognition, and anomaly detection.<br>● Outline commonly used memory forensic tools, (Volatility, Rekall, Redline, and Memoryze).<br>● Explain the benefits of automation<br>● Analyse the limitations of automated tools.<br>**6.2 Utilise open-source tools for supplementary analysis**<br>● Describe open-source tools.<br>● Explain the importance of supplementary tools in complementing proprietary solutions for deeper memory analysis, signature matching, and behavioural detection.<br>● Outline popular open-source tools<br>● Analyse how combining multiple tools improves forensic accuracy<br>**6.3 Diagnose and resolve common issues encountered during memory acquisition and analysis**<br>● Describe challenges in memory acquisition<br>● Explain common errors in memory analysis<br>● Analyse methods for troubleshooting forensic issues<br>● Outline best practices for ensuring successful memory analysis<br>**6.4 Remove malicious artifacts and restore affected systems**<br>● Describe malicious artifacts in memory<br>● Explain methods for isolating and mitigating memory-based threats.<br>● Analyse remediation techniques<br>● Outline post-incident forensic validation |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to **utilize automated tools in memory forensics** as outlined in the assessment criteria and content above.<br>2. Practical assessment on utilising open-source tools for supplementary analysis, diagnosing and resolving common issues encountered during memory acquisition and analysis and removing malicious artifacts and restore affected systems based on the performance criteria of the |

| | |
|---|---|
| | qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: -<br><br>Volatility, Rekall, Redline (by FireEye), Magnet RAM Capture, Belkasoft RAM Capturer, WinPmem, Autopsy, FTK Imager, Process Hacker, Python Scripts, Memory Dumps, Forensic Workstation, Virtual Machines (VMs), Malware Samples, Documentation and Cheat Sheets, Training Datasets, Write Blockers, Forensic Imaging Tools, Operating System Artifacts,<br>Report Templates |

| **Learning Outcome 07** | **Provide incident response strategies based on findings from memory forensic analysis during live security breaches to align with organizational protocols and forensic best practices** |
|---|---|
| **Assessment Criteria** | **7.1 Identify and contain incidents that require memory forensics.**<br>**7.2 Assess the scope and impact of the incident.**<br>**7.3 Capture live memory images.**<br>**7.4 Produce proper documentation for legal and regulatory considerations** |
| **Content** | **7.1 Identify and contain incidents that require memory forensics**<br>● Explore scenarios requiring memory forensics<br>● Assess the role of memory forensics in capturing volatile data.<br>● Describe methods of containing memory-based threats.<br>● Evaluate challenges in incident containment<br>**7.2 Assess the scope and impact of the incident**<br>● Examine the scope of security incidents, identifying affected systems, compromised accounts, and potential data exposure.<br>● Assess indicators of compromise (IOCs) in memory<br>● Interpret the impact of memory-based threats<br>● Review forensic methods used to determine severity<br>**7.3 Capture live memory images**<br>● Investigate techniques for live memory acquisition, considering system state preservation, minimal disruption, and forensic soundness.<br>● Examine the importance of capturing volatile memory. |

| | |
|---|---|
| | ● Evaluate best practices for memory acquisition<br>● Outline challenges in acquiring memory<br>**7.4 Produce proper documentation for legal and regulatory considerations**<br>● Analyse legal and regulatory frameworks that govern digital forensics (GDPR, ISO 27037, and NIST)<br>● Assess the significance of forensic documentation<br>● Investigate methods for maintaining chain of custody<br>● Explain the compliance requirements. |
| **Assessment Tasks** | 1. Written and/or oral assessment on the skills and knowledge required to provide incident response for memory forensics as outlined in the assessment criteria and content above.<br>2. Practical assessment on capturing live memory images and producing proper documentation for legal and regulatory considerations based on the performance criteria of the qualification standard Digital Forensics Technician. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below: - FTK Imager, Magnet RAM Capture, Belkasoft RAM Capturer, DumpIt, WinPmem, AVML (Azure Virtual Memory for Linux), Volatility Framework, Rekall Memory Forensics, Redline (FireEye), Bulk Extractor, LiME for Linux, Wireshark, Zeek (Bro), Suricata, Snort, Arkime (formerly Moloch), Splunk, QRadar, ArcSight, CrowdStrike, SentinelOne, Carbon Black, MISP, VirusTotal, AlienVault OTX), MD5Deep, SHA256sum, HashCalc, CaseNotes, TheHive, Nuix Investigator, Dradis, incident response playbooks, Forensic Investigation Reports (Templates and guidelines), Chain of Custody Forms, external hard drives, encrypted USB drives for storing memory dumps, Regulatory Compliance Documents (GDPR, ISO 27037, NIST standards, etc.) tamper-proof evidence bags, time synchronization tools, live boot forensic OS (CAINE, DEFT, and SIFT Workstation). |

**ASSESSMENT SCHEME**

| MODE OF ASSESSMENT | | WEIGHTING |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | **100%** |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| LEARNING OUTCOME | WEIGHTING |
|---|---|
| Demonstrate knowledge of memory forensics concepts and principles | 20% |
| Acquire memory dumps from suspect machines, using industry-standard tools and procedures under forensic lab conditions to ensure completeness, integrity, and chain of custody | 10 % |
| Extract forensic artifacts such as processes, handles, and network connections by analysing captured memory | 10% |
| Detect and analyse malware embedded in volatile memory using signature-based and behavioral analysis tools to accurately identify indicators of compromise | 20% |
| Uncover stealthy or encrypted threats such as rootkits and fileless malware by applying advanced techniques | 20 % |
| Utilize automated tools in memory forensics to enable rapid memory parsing, anomaly detection, and triage | 10% |
| Provide incident response strategies based on findings from memory forensic analysis during live security breaches to align with organizational protocols and forensic best practices | 10 % |

| | |
|---|---|
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

   FTK Imager, DumpIt, WinPMEM / Rekall, LiME (Linux Memory Extractor), AVML (Azure Virtual Memory forensics tool), Volatility Framework, Rekall, Redline,

   Belkasoft RAM Capturer, MemProcFS, YARA, IDA Pro, Ghidra, Wireshark

**2.1.5 Equipment**

Forensic Workstations, Write-Blockers, External Hard Drives & NAS, Secure USB Devices

**Materials**

Forensic Documentation Templates

Reference Memory Dumps
Incident Response Playbooks

Legal & Compliance Guidelines

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

## 4. Reference Materials (recommended textbooks, recommended readings)

Ligh, M.H., Case, A., Levy, J. and Walters, A. (2014) The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis, IN: Wiley.

Carvey, H. (2014) Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8. 4th edn. Waltham, MA: Syngress.

Altheide, C. and Carvey, H. (2011) Digital Forensics with Open Source Tools. Waltham, MA: Syngress.

Russinovich, M.E., Solomon, D.A. and Ionescu, A. (2012) Windows Internals. 6th edn. Redmond, WA: Microsoft Press.

Carrier, B. (2005) File System Forensic Analysis. Boston, MA: Addison-Wesley Professional.

| | |
|---|---|
| **Module Code:** | **682/25/M17** |
| **Module Title:** | **RESEARCH METHODS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 10 |
| **Duration:** | 100 hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard **RESEARCH METHODS** of Qualification Standard for a Digital Forensics Technician. |
| **Pre-requisite modules:** | NONE |
| **Purpose of Module:** | This module describes the skills, knowledge and attitudes required by an Assistant Business Analytics to understand the principles of research in ICT. This includes explaining the concept of research, performing data collection and analysis, performing hypothesis testing, and applying project management skills to research and apply innovation skills. The advantages of understanding the principles of research in business analytics are that it enhances research skills required. Access to this module is open to all target groups including unemployed youths, women and men wishing to establish or improve SMEs in the networking of computers. |
| **List of Learning Outcomes:** | **LO1: Carry out in-depth research using a variety of research methods to advance knowledge, inform decision-making and solve practical problems**<br>**LO2: Critically analyze and evaluate their own work and that of others to establish the current state of knowledge, identify research gaps, inform research design, and contribute to theoretical development and evidence-based practice in digital forensics.**<br>**LO3: Collect data using data collection methods to gather empirical evidence that is relevant to answering the research questions or testing hypotheses**<br>**LO4: Communicate findings derived from data collection to the intended audience in a clear, accurate, and meaningful manner by using data presentation methods.**<br>**LO5: Ensure that research activities are conducted with integrity, respect for participants' rights, and adherence to established ethical standards by applying ethical principles in research.** |

| Learning Outcome 01 | EXPLAIN THE CONCEPT OF RESEARCH |
|---|---|
| **Assessment Criteria:** | **1.1 Explain what is Research**<br>**1.2 Describe the different types of Research**<br>**1.3 Describe the steps in the research process** |
| **Content:** | **1.1 Explain what Research is.**<br>● Define research<br>● Explain the characteristics of research<br>● Explain the objectives of research<br>● Research and Scientific Method<br><br>**1.2 Describe the different types of Research**<br>● Descriptive versus Analytical Research<br>● Applied versus Fundamental Research<br>● Quantitative versus Qualitative Research<br>● Conceptual versus Empirical Research<br>● Mixed Methods<br><br>**1.3 Describe the steps in the research process**<br>● Selection of the Research Problem<br>● Literature review<br>● Making hypothesis<br>● Preparing the research design<br>● Sampling<br>● Data collection<br>● Data analysis<br>● Hypothesis testing<br>● Generalisation and interpretation<br>● Preparation of report |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to explain the concept of research outlined as follows: explain what is research, describe the different types of research and describe the steps in the research process.<br>2. Practical assessment on explaining the concept of research inclusive of explaining what is research, describing the different types of research and describing the steps in the research process based on the performance criteria of the relevant unit standard. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| | |
|---|---|
| **Learning Outcome 02** | **Collect data using data collection methods to gather empirical evidence that is relevant to answering the research questions or testing hypotheses** |
| **Assessment Criteria:** | **2.1 Describe sampling methods**<br>**2.2 Explain data collection methods**<br>**2.3 Conduct data analysis** |
| **Content:** | **2.1 Describe sampling methods**<br>● Probability versus non-probability<br>● Simple Random Sampling<br>● Stratified Sampling<br>● Systematic Sampling<br>● Cluster Sampling<br>● Purposive Sampling<br>● Quota Sampling<br>● Snowball sampling<br><br>**2.2 Explain data collection methods**<br>● Interviews<br>● Questionnaires<br>● Observation<br>● Document analysis<br><br>**2.3 Conduct data analysis**<br>● Calculate measures of central tendency<br>⇒ Mean<br>⇒ Median<br>⇒ Mode<br>● Calculate measures of dispersion<br>⇒ Range<br>⇒ Variance<br>⇒ Standard deviation<br>● Construct and interpret<br>⇒ Pie Chart<br>⇒ Bar Chart<br>⇒ Histogram<br>⇒ Frequency polygon |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to collect and analyze business data as outlined in the assessment criteria.<br>2. Practical assessment on conducting data analysis based on the performance criteria of the relevant unit standard. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessments can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution. |

| | |
|---|---|
| | 3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 03** | **PERFORM HYPOTHESIS TESTING** |
|---|---|
| **Assessment Criteria:** | **3.1 Calculate probabilities using discrete and continuous probability distributions**<br>**3.2 Test hypothesis** |
| **Content:** | **3.1 Calculate probabilities using discrete and continuous probability distributions**<br>● Binomial distribution<br>● Poisson distribution<br>● Normal distribution<br>**3.2 Test hypothesis**<br>● Formulate null and alternative hypothesis<br>● Perform Z-tests on mean of a population<br>● Perform Z-tests on population proportion |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to perform hypothesis testing as outlined in assessment criteria.<br>2. Practical assessment of calculating probabilities using discrete and continuous probability distributions and test hypothesis based on the performance criteria of the relevant unit standard. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| Learning Outcome 04 | APPLY PROJECT MANAGEMENT SKILLS |
|---|---|
| **Assessment Criteria:** | **4.1 Plan the project**<br>**4.2 Determine project financial implications**<br>**4.3 Generate project schedule**<br>**4.4 Execute project**<br>**4.5 Monitor and control project**<br>**4.6 Implement project management software** |
| **Content:** | **4.1 Plan the project**<br>● Define project scope<br>● Define roles and responsibilities<br>● Explain the process of drawing up a project plan<br>● Analyse a project using work breakdown structures<br><br>**4.2 Determine project financial implications**<br>● Explain the process of<br>✓ Total project cost estimation<br>✓ Drawing up a project budget<br>● Perform cost-benefit evaluation<br>✓ Payback period<br>✓ Net Present Value<br>✓ Return on Investment<br>**4.3 Generate project schedule**<br>● Explain the role of project scheduling<br>● Outline the steps involved in creating a project schedule<br>● Evaluate project scheduling techniques<br>✓ Work Breakdown Structure<br>✓ Critical Path Method<br>✓ Gantt Chart<br>✓ PERT<br>✓ Fast tracking and crashing<br>**4.4 Execute project**<br>● Explain the allocation of project resources<br>● Outline strategies for managing project resources<br><br>**4.5 Monitor and control project**<br>● Explain how to track project effort and cost<br>● Institute strategies to ensure adherence to plan<br>● Maintain project scope<br><br>**4.6 Apply project management software**<br>● Outline the benefits of using project management software<br>● Evaluate project management software |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to apply project management skills as outlined in the assessment criteria. |

| | |
|---|---|
| | 2. Practical assessment on managing projects including the following: SHEQ requirements, the consideration of computer laboratory environmental factors which affect the planning, problem solving, knowledge of development platform, knowledge of software installation and teamwork based on the performance criteria of the relevant unit standard. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution.<br>3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

| **Learning Outcome 05** | **APPLY INNOVATION SKILLS** |
|---|---|
| **Assessment Criteria:** | **5.1 Explain the concept of innovation**<br>**5.2 Discuss the innovation process** |
| **Content:** | **5.1 Explain the concept of innovation**<br>● Define innovation<br>● Explain the difference between radical and incremental innovation<br>● Explain the benefits of innovation<br>**5.2 Discuss the innovation process**<br>● Describe the stages of the innovation process<br>✓ Idea generation (Idea formulation)<br>✓ Idea evaluation (Screening)<br>✓ Concept testing<br>✓ Product development<br>✓ Testing and execution<br>✓ Post-development (Commercialization, Market Introduction)<br>✓ Support and maintenance<br>● Describe the factors that affect the success of an innovation |
| **Assessment Tasks:** | 1. Written and/or oral assessment on the skills and knowledge required to apply innovation skills as outlined in the assessment criteria.<br>2. Practical assessment on application of innovation skills including the following: SHEQ requirements, the consideration of computer laboratory environmental factors which affect the planning, problem solving, knowledge of development platform, knowledge of software installation and teamwork based on the performance criteria of the relevant unit standard. |
| **Conditions/Context of assessment** | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will be conducted in the workplace or simulated work environment in the training institution. |

| | |
|---|---|
| | 3. The context of assessment should include the facilities, tools, equipment and materials listed below. |

**ASSESSMENT SCHEME**

| | | |
|---|---|---|
| 3 hour written examination | A minimum of<br>● 2 Theory Assignments 20%<br>● 2 Practical Assignments 20%<br>● 2 Tests 20% | 100% |

**ASSESSMENT SPECIFICATION GRID**

| No. | TOPIC | WEIGHTING |
|---|---|---|
| LO1 | Explain the concept of Research | 20 |
| LO2 | Perform Data Collection and Analysis | 20 |
| LO3 | Perform hypothesis testing | 20 |
| LO4 | Apply project management skills to research | 20 |
| LO5 | Apply Innovation Skills | 20 |
| | **TOTAL** | **100** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% written examination.
2. Weighting of institution-based and work-based assessment: 50% institution-based assessment and 50%.
3. Oral assessment to be conducted by a panel of two or more assessors.
4. RPL assessment.
5. Portfolio of evidence.
6. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**

All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualifications and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).

2. **Facilities, Tools, Equipment and Materials**

Computers/ Lptops
Stationery

3. **Learning Resources**

Relevant training manual (learners' guide) and facilitators' guide

4. **Reference Materials**

Crashaw, J and Chambers, J. (2014) **Advanced Level Statistics**. Nelson Thornes, Cheltenham.
Creswell, J. (2014) **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 6th Ed.** Sage Publications, London
Kerri Shields (2022). **Leading Innovation**. eCampusOntario, Toronto

Lucey, T. (2014) **Management Information Systems 8th Ed**. London: Gill Macmillan Ltd.
Patton, MQ. (2015) **Qualitative Research & Evaluation Methods 5th Ed.** London: Sage Publications
Schwalbe K. (2015) **Information Technology Project Management 8th Ed.** New Jersey: Prentice Hall

Sekaran, U and Bougie, R.(2016) **Research Methods for Business: A Skill Building Approach 7th Ed.** Wiley and Sons, New Jersey

| | |
|---|---|
| **Module Code:** | **682/25/M17** |
| **Module Title:** | **EMERGING TECHNOLOGIES AND DIGITAL FORENSICS** |
| **ZNQF Level:** | **5** |
| **Credits:** | 10 |
| **Duration:** | 100 Hours |
| **Relationship with Qualification Standards:** | Based on Unit Standard "Emerging Technologies in Digital Forensics" or similar advanced unit standards in Digital Forensics, Cybersecurity, or ICT Digital Forensics Technician qualifications. |
| **Pre-requisite module:** | N/A |
| **Purpose of Module:** | This module describes the skills, knowledge, and attitudes required by a digital forensics specialist to understand, investigate, and adapt to the challenges posed by rapidly evolving technologies. It focuses on equipping learners with the necessary expertise to perform forensic analysis in environments involving Artificial Intelligence, Blockchain, Internet of Things (IoT), Big Data, and other cutting-edge technologies, ensuring they can effectively collect, preserve, analyze, and report on digital evidence from these complex sources. This module aims to prepare learners for the future landscape of digital investigations. |
| **List of Learning Outcomes:** | LO1: Apply Machine Learning algorithms for automated anomaly detection and pattern recognition within large digital forensic datasets.<br>LO2: Conduct forensic investigations of digital evidence originating from blockchain and distributed ledger technologies.<br>LO3: Perform forensically sound data acquisition and analysis from Internet of Things (IoT) devices.<br>LO4: Develop strategies and methodologies for digital forensic investigations in dynamic cloud environments (e.g., serverless, containerized, microservices).<br>LO5: Utilize big data analytics platforms and techniques to process and correlate massive volumes of digital evidence. |

| | |
|---|---|
| | LO6: Evaluate the forensic implications of emerging and future technologies (e.g., quantum computing, advanced AI ethics). |

| **Learning Outcome 01** | **APPLY MACHINE LEARNING ALGORITHMS FOR AUTOMATED ANOMALY DETECTION AND PATTERN RECOGNITION WITHIN LARGE DIGITAL FORENSIC DATASETS** |
|---|---|
| Assessment Criteria: | 1.1 Describe the fundamental concepts of Machine Learning (ML) relevant to digital forensics.<br>1.2 Utilize ML algorithms (e.g., clustering, classification) for anomaly detection in forensic data.<br>1.3 Apply ML for pattern recognition in digital evidence (e.g., identifying malware families, user behavior).<br>1.4 Evaluate the effectiveness and limitations of ML models in forensic contexts. |
| Content: | **1.1 Describe the fundamental concepts of Machine Learning (ML) relevant to digital forensics:**<br>1.1.1 Define ML, Supervised Learning, Unsupervised Learning, Reinforcement Learning.<br>1.1.2 Explain key ML terminology: features, labels, training data, testing data, model, overfitting, underfitting.<br>1.1.3 Discuss the relevance of ML in automating and enhancing forensic processes (e.g., speed, scale, accuracy).<br>**1.2 Utilize ML algorithms (e.g., clustering, classification) for anomaly detection in forensic data:**<br>1.2.1 Explain common anomaly detection techniques (e.g., Isolation Forest, One-Class SVM).<br>1.2.2 Describe how clustering algorithms (e.g., K-Means, DBSCAN) can group similar forensic artifacts and highlight outliers.<br>1.2.3 Apply these algorithms using relevant ML libraries (e.g., scikit-learn) on simulated forensic datasets (e.g., log files, network traffic).<br>1.2.4 Interpret the results of anomaly detection to identify suspicious activities.<br>**1.3 Apply ML for pattern recognition in digital evidence (e.g., identifying malware families, user behavior):**<br>1.3.1 Explain how classification algorithms (e.g., Decision Trees, Support Vector Machines, Neural Networks) can categorize digital evidence.<br>1.3.2 Describe the process of feature extraction from raw forensic data (e.g., PE file headers for malware, command history for user behavior).<br>1.3.3 Implement a basic ML model to classify malware samples or recognize user activity patterns.<br>1.3.4 Analyze the output of pattern recognition models to draw forensic conclusions.<br>**1.4 Evaluate the effectiveness and limitations of ML models in** |

| | |
|---|---|
| | **forensic contexts:**<br>1.4.1 Discuss common ML model performance metrics (e.g., accuracy, precision, recall, F1-score, ROC-AUC).<br>1.4.2 Explain the challenges of applying ML in forensics (e.g., data imbalance, adversarial attacks, explainability/interpretability of results, ground truth availability).<br>1.4.3 Propose strategies to mitigate limitations and improve model reliability for forensic use. |
| Assessment Tasks: | 1. Written and/or oral assessment on the skills and knowledge required to apply Machine Learning algorithms as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using Python with scikit-learn/TensorFlow/PyTorch to build and evaluate a simple ML model for a forensic task (e.g., classifying benign vs. malicious network traffic, clustering user activity logs). |
| Conditions/Context of assessment | 4. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>5. The practical assessment will be conducted in a simulated lab environment with access to Python development tools, ML libraries, and pre-prepared forensic datasets.<br>6. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 02** | **CONDUCT FORENSIC INVESTIGATIONS OF DIGITAL EVIDENCE ORIGINATING FROM BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES.** |
|---|---|
| Assessment Criteria | **2.1 Describe the fundamental concepts of blockchain and DLTs relevant to forensics.**<br>**2.2 Acquire and preserve digital evidence from blockchain networks and related platforms.**<br>**2.3 Analyze blockchain transaction data and identify relevant forensic artifacts.**<br>2.4 **Discuss the legal and ethical challenges of blockchain forensics.** |

| | |
|---|---|
| Content | **2.1 Describe the fundamental concepts of blockchain and DLTs relevant to forensics:**<br>2.1.1 Define blockchain, distributed ledger technology (DLT), cryptocurrencies (e.g., Bitcoin, Ethereum), smart contracts.<br>2.1.2 Explain core concepts: blocks, chains, hashes, consensus mechanisms (e.g., Proof-of-Work, Proof-of-Stake), decentralization, immutability.<br>2.1.3 Discuss the relevance of blockchain in criminal activities (e.g., money laundering, ransomware payments) and legitimate use cases.<br>**2.2 Acquire and preserve digital evidence from blockchain networks and related platforms:**<br>2.2.1 Explain the challenges of evidence acquisition from decentralized and distributed systems.<br>2.2.2 Describe methods for acquiring data from public blockchains (e.g., using blockchain explorers, node synchronization).<br>2.2.3 Discuss techniques for acquiring data from off-chain sources (e.g., cryptocurrency exchange logs, wallet files, user devices).<br>2.2.4 Outline the importance of maintaining chain of custody and ensuring data integrity in a distributed environment.<br>**2.3 Analyze blockchain transaction data and identify relevant forensic artifacts:**<br>2.3.1 Interpret blockchain transaction data (e.g., sender/receiver addresses, amounts, timestamps, transaction IDs).<br>2.3.2 Trace cryptocurrency flows across multiple addresses and transactions.<br>2.3.3 Analyze smart contract code and execution logs for malicious activity or vulnerabilities.<br>2.3.4 Identify and analyze artifacts from associated platforms (e.g., exchange account data, darknet market transactions).<br>**2.4 Discuss the legal and ethical challenges of blockchain forensics:** |

| | |
|---|---|
| | 2.4.1 Explain jurisdictional complexities in cross-border blockchain investigations.<br>2.4.2 Discuss the anonymity/pseudonymity of blockchain users and challenges in attribution.<br>2.4.3 Address legal admissibility of blockchain evidence and the need for new legal frameworks.<br>2.4.4 Discuss ethical considerations related to privacy and data access on public ledgers. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to conduct blockchain forensic investigations as outlined in the assessment criteria and content above.<br>2. Practical assessment involving using a blockchain explorer or a local blockchain node to trace a series of cryptocurrency transactions and identify associated addresses. |
| Conditions/Context of assessment | 4. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>5. The practical assessment will be conducted in a simulated lab environment with access to blockchain explorers, sample wallet files, and relevant analysis tools.<br>6. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 03** | **PERFORM FORENSICALLY SOUND DATA ACQUISITION AND ANALYSIS FROM INTERNET OF THINGS (IOT) DEVICES.** |
|---|---|
| Assessment Criteria | **3.1 Describe the architecture and data sources of various IoT devices relevant to forensics.**<br>**3.2 Acquire digital evidence from IoT devices using appropriate techniques.**<br>**3.3 Analyze data extracted from IoT devices for forensic insights.**<br>**3.4 Discuss the challenges and limitations of IoT forensics.** |

| | |
|---|---|
| Content | **3.1 Describe the architecture and data sources of various IoT devices relevant to forensics:**<br>3.1.1 Define IoT, common IoT device categories (e.g., smart home, wearables, industrial IoT).<br>3.1.2 Explain typical IoT architectures (sensors, gateways, cloud platforms).<br>3.1.3 Identify potential data sources on IoT devices (e.g., internal storage, firmware, volatile memory, external storage) and associated cloud services/mobile apps.<br>3.1.4 Discuss common communication protocols (e.g., Wi-Fi, Bluetooth, Zigbee, MQTT).<br>**3.2 Acquire digital evidence from IoT devices using appropriate techniques:**<br>3.2.1 Explain the challenges of IoT device acquisition (e.g., diverse hardware, lack of standard interfaces, anti-forensics).<br>3.2.2 Describe various acquisition methods: JTAG, Chip-off, ISP (In-System Programming), logical extraction via device interfaces/APIs, cloud acquisition.<br>3.2.3 Outline the steps for forensically sound acquisition, including power management and write protection.<br>3.2.4 Discuss the use of specialized tools for IoT acquisition.<br>**3.3 Analyze data extracted from IoT devices for forensic insights:**<br>3.3.1 Interpret various data formats found on IoT devices (e.g., proprietary logs, SQLite databases, binary files).<br>3.3.2 Reconstruct timelines of user activity or device events from fragmented data.<br>3.3.3 Analyze network traffic generated by IoT devices.<br>3.3.4 Identify user data, device configurations, and communication patterns.<br>**3.4 Discuss the challenges and limitations of IoT forensics:**<br>3.4.1 Explain issues related to data volatility, limited storage, |

| | |
|---|---|
| | proprietary formats, and firmware encryption.<br>3.4.2 Discuss legal and privacy concerns related to data collected by IoT devices.<br>3.4.3 Address the scalability of IoT forensic investigations given the sheer number and diversity of devices.<br>3.4.4 Propose strategies to overcome common IoT forensic challenges. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to perform IoT forensics as outlined in the assessment criteria and content above.<br>2. Practical assessment involving performing a logical or physical acquisition (simulated or on a safe test device) from a common IoT device (e.g., smart speaker, smart plug) and analyzing extracted data for specific artifacts. |
| Conditions/Context of assessment | 4. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>5. The practical assessment will be conducted in a simulated lab environment with access to sample IoT devices, specialized acquisition tools (or emulators), and analysis software.<br>6. The context of assessment should include the facilities, tools, equipment, and materials listed below. |
| **Learning Outcome 04** | **DEVELOP STRATEGIES AND METHODOLOGIES FOR DIGITAL FORENSIC INVESTIGATIONS IN DYNAMIC CLOUD ENVIRONMENTS (E.G., SERVERLESS, CONTAINERIZED, MICROSERVICES).** |
| Assessment Criteria | 4.1 Describe the architectural characteristics and data sources of dynamic cloud environments.<br>4.2 Formulate strategies for evidence collection and preservation in serverless and containerized deployments.<br>4.3 Analyze logs and artifacts from microservices and cloud-native applications.<br>4.4 Discuss the unique challenges of cloud forensics in dynamic environments |

| | |
|---|---|
| Content | **4.1 Describe the architectural characteristics and data sources of dynamic cloud environments:**<br>4.1.1 Define serverless computing (e.g., AWS Lambda, Azure Functions), containers (e.g., Docker), orchestration (e.g., Kubernetes), and microservices.<br>4.1.2 Explain their ephemeral nature, distributed logging, and dynamic scaling.<br>4.1.3 Identify potential data sources: cloud provider logs (CloudTrail, Azure Monitor), container logs, serverless function logs, ephemeral storage, object storage, CI/CD pipelines.<br>**4.2 Formulate strategies for evidence collection and preservation in serverless and containerized deployments:**<br>4.2.1 Explain the "volatile" nature of evidence in these environments and the importance of timely collection.<br>4.2.2 Describe techniques for snapshotting container states, capturing memory from running containers, and preserving serverless function execution logs.<br>4.2.3 Discuss the use of cloud provider APIs and forensic tools for remote acquisition.<br>4.2.4 Outline strategies for maintaining chain of custody in distributed cloud systems.<br>**4.3 Analyze logs and artifacts from microservices and cloud-native applications:**<br>4.3.1 Interpret structured and unstructured logs from various cloud services and microservices.<br>4.3.2 Correlate events across distributed logs to reconstruct incident timelines.<br>4.3.3 Analyze container images and layers for malicious implants or vulnerabilities.<br>4.3.4 Extract configuration data and secrets from cloud environments.<br>**4.4 Discuss the unique challenges of cloud forensics in dynamic environments:**<br>4.4.1 Explain issues related to data volatility, multi-tenancy, shared responsibility model, and legal jurisdiction.<br>4.4.2 Discuss the difficulty of obtaining complete forensic images from highly distributed systems.<br>4.4.3 Address the impact of rapid deployment cycles and continuous integration/delivery on evidence preservation.<br>4.4.4 Propose solutions for effective cloud forensic readiness and incident response in dynamic environments. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to develop cloud forensic strategies as outlined in the assessment criteria and content above.<br>2. Practical assessment involving analyzing simulated cloud logs (e.g., CloudTrail logs, Docker logs) to identify a security incident and outline |

| | |
|---|---|
| | a forensic acquisition plan for a containerized application. |
| Conditions/Context of assessment | 4. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>5. The practical assessment will be conducted in a simulated lab environment (e.g., using Docker, Kubernetes mini-kube, or cloud sandboxes) with access to relevant logging and monitoring tools.<br>6. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 05** | **PROCESS AND CORRELATE MASSIVE VOLUMES OF DIGITAL EVIDENCE UTILIZING BIG DATA ANALYTICS PLATFORMS AND TECHNIQUES.** |
|---|---|
| Assessment Criteria | 5.1 Describe the characteristics of big data in digital forensics and its challenges.<br>5.2 Apply big data processing frameworks for forensic data ingestion and storage.<br>5.3 Utilize big data analytics techniques for correlating diverse digital evidence.<br>5.4 Evaluate the benefits and limitations of big data forensics. |
| Content | **5.1 Describe the characteristics of big data in digital forensics and its challenges:**<br>5.5.1 Define the "Vs" of Big Data (Volume, Velocity, Variety, Veracity, Value) in the context of forensic evidence (e.g., massive log files, network traffic, IoT data).<br>5.5.2 Explain the challenges of traditional forensic tools when dealing with big data (e.g., scalability, processing time, storage).<br>**5.2 Apply big data processing frameworks for forensic data ingestion and storage:**<br>5.2.1 Explain the architecture and components of big data frameworks (e.g., Hadoop, Spark, Elasticsearch).<br>5.2.2 Describe methods for ingesting diverse forensic data sources into big data platforms.<br>5.2.3 Discuss distributed storage solutions (e.g., HDFS, S3-compatible storage) for forensic evidence.<br>5.2.4 Implement basic data loading and transformation processes using a chosen framework.<br>**5.3 Utilize big data analytics techniques for correlating diverse digital evidence:**<br>5.3.1 Explain how big data analytics enables correlation across disparate data sources (e.g., correlating firewall logs with endpoint events and user activity).<br>5.3.2 Describe techniques for searching, filtering, and aggregating |

| | |
|---|---|
| | large datasets (e.g., using SQL-like queries in Spark, Kibana dashboards).<br>5.3.3 Discuss the use of graph databases for visualizing relationships in complex forensic data.<br>5.3.4 Apply analytical queries to identify patterns, anomalies, and relationships indicative of an incident.<br>**5.4 Evaluate the benefits and limitations of big data forensics:**<br>5.4.1 Discuss the advantages of big data approaches (e.g., enhanced scalability, faster processing, deeper insights, improved correlation).<br>5.4.2 Explain the limitations (e.g., infrastructure cost, complexity of setup, skill requirements, data privacy concerns).<br>5.4.3 Propose scenarios where big data forensics is essential. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to utilize big data analytics as outlined in the assessment criteria and content above.<br>2. Practical assessment involving ingesting a large simulated forensic dataset (e.g., a large collection of logs) into a big data platform (e.g., a local Elasticsearch instance or a simple Spark setup) and performing queries to extract specific incident-related information. |
| Conditions/Context of assessment | 4. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>5. The practical assessment will be conducted in a simulated lab environment with access to big data frameworks (e.g., pre-configured Docker containers for Elasticsearch/Kibana, a local Spark installation).<br>6. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

| **Learning Outcome 06** | **EVALUATE THE FORENSIC IMPLICATIONS OF EMERGING AND FUTURE TECHNOLOGIES (E.G., QUANTUM COMPUTING, ADVANCED AI ETHICS).** |
|---|---|
| Assessment Criteria | 6.1 Identify current and future trends in emerging technologies relevant to digital forensics.<br>6.2 Analyze the potential impact of advanced emerging technologies on forensic methodologies.<br>6.3 Discuss the ethical, legal, and societal implications of these emerging technologies in forensics.<br>6.4 Propose strategies for adapting forensic practices to future technological landscapes. |
| Content | **6.1 Identify current and future trends in emerging technologies relevant to digital forensics:**<br>6.1.1 Describe the basics of **Quantum Computing** and its potential impact on cryptography and data security (e.g., breaking current encryption, post-quantum cryptography).<br>6.1.2 Discuss **Advanced AI Ethics and Governance** in forensics (e.g., bias in AI, accountability for AI decisions, explainable AI (XAI)).<br>6.1.3 Explore **Bioinformatics Forensics** (e.g., DNA evidence from digital sources, digital footprints in biological data).<br>6.1.4 Examine **Extended Reality (XR) Forensics** (VR/AR/MR) – data sources, user interactions, and privacy.<br>6.1.5 Identify other relevant emerging areas (e.g., Neuromorphic Computing, Advanced Robotics, Digital Twins).<br>**6.2 Analyze the potential impact of advanced emerging technologies on forensic methodologies:**<br>6.2.1 Explain how quantum computing could challenge current cryptographic evidence and require new forensic tools.<br>6.2.2 Discuss how advanced AI could both enhance forensic capabilities (e.g., hyper-automation) and complicate |

| | |
|---|---|
| | investigations (e.g., AI-generated fake evidence).<br>6.2.3 Analyze the new types of digital evidence that might emerge from XR environments and how they would be acquired/analyzed.<br>6.2.4 Consider how these technologies might be used by adversaries and the forensic challenges they would present.<br>**6.3 Discuss the ethical, legal, and societal implications of these emerging technologies in forensics:**<br>6.3.1 Address ethical dilemmas related to privacy, surveillance, and data ownership in a hyper-connected world.<br>6.3.2 Discuss the legal frameworks needed to address evidence from new technologies and cross-jurisdictional challenges.<br>6.3.3 Examine the societal impact of pervasive data collection and AI-driven investigations on civil liberties.<br>6.3.4 Debate the responsibility and accountability for actions taken by AI systems in forensic contexts.<br>**6.4 Propose strategies for adapting forensic practices to future technological landscapes:**<br>6.4.1 Outline the need for continuous research and development in forensic tools and techniques.<br>6.4.2 Suggest changes in legal and regulatory frameworks to accommodate new technologies.<br>6.4.3 Propose interdisciplinary collaboration between forensic experts, AI researchers, ethicists, and legal professionals.<br>6.4.4 Recommend strategies for professional development and training to equip future forensic practitioners. |
| Assessment Tasks | 1. Written and/or oral assessment on the skills and knowledge required to evaluate the forensic implications of emerging technologies as outlined in the assessment criteria and content above.<br>2. Research project and presentation on a specific emerging technology, analyzing its current state, potential forensic challenges, and proposed |

| | |
|---|---|
| | solutions/strategies for investigation. |
| Conditions/Context of assessment | 1. Written and/or oral assessment can be conducted in a classroom environment. Oral assessment can also be conducted by the assessor during the performance of the practical assessment by the trainees.<br>2. The practical assessment will involve research and critical analysis, potentially using simulation tools or publicly available datasets related to the chosen emerging technology.<br>3. The context of assessment should include the facilities, tools, equipment, and materials listed below. |

**ASSESSMENT SCHEME**

| **MODE OF ASSESSMENT** | | **WEIGHTING 100%** |
|---|---|---|
| **EXAMINATION 40%** | **CONTINUOUS ASSESSMENT 60%** | |
| 3 hour written examination | **2 Practical Assignments**<br>**2 Theory Assignments**<br>**2 Tests** | 100% |

**ASSESSMENT SPECIFICATIONS GRID**

| **LEARNING OUTCOME** | **WEIGHTING** |
|---|---|
| Apply Machine Learning algorithms for automated anomaly detection and pattern recognition within large digital forensic datasets. | 20 |
| Conduct forensic investigations of digital evidence originating from blockchain and distributed ledger technologies. | 15 |
| Perform forensically sound data acquisition and analysis from Internet of Things (IoT) devices. | 15 |
| Develop strategies and methodologies for digital forensic investigations in dynamic cloud environments (e.g., serverless, containerized, microservices). | 15 |
| Utilize big data analytics platforms and techniques to process and correlate massive volumes of digital evidence. | 15 |
| Evaluate the forensic implications of emerging and future technologies (e.g., quantum computing, advanced AI ethics). | 20 |
| **TOTAL** | **100%** |

**Approach to Teaching and Learning:**

1. Observation of adult learning principles.
2. Both institution-based and work-based learning to facilitate the integration of theory and practice.
3. Face-to-face education and learning.
4. Problem-based learning.
5. Online/distance education and learning.
6. Blended/hybrid education and learning.
7. Use of social media for collaborative learning and resource sharing.

**Approach to Assessment:**

1. Weighting of 60% continuous assessment and 40% examination.
2. Oral assessment to be conducted by a panel of two or more assessors.
3. Portfolio of evidence.
4. Assessment of work conducted by both individual learners and teams of learners.

**Resources:**

1. **Qualifications and experience of Trainers, Assessors and Moderators**
   All trainers, assessors and moderators should have undergone ZNQF accredited training programmes and should have qualification and experience recognised by the Zimbabwe National Qualifications Authority (ZNQA).
2. **Facilities, Tools, Equipment and Materials**

   **Facilities**

| Facility | Purpose |
|---|---|
| **Computer Laboratory** | Equipped with modern desktops/laptops to run resource-intensive forensic tools and virtual machines. |
| **Digital Forensics Lab** | A controlled environment for conducting forensic imaging, evidence analysis, and testing. |
| **Smart Classroom/Multimedia Room** | For delivering interactive lessons, showcasing simulations, and playing recorded cybercrime scenarios. |
| **Server Room (optional)** | To host virtual machines, digital forensic databases, and simulate network forensics and cloud environments. |
| **Secure Storage Room** | For storing evidence drives, USBs, and other sensitive digital storage securely and in compliance with chain of custody protocols. |

   **Tools (Software)**

| Tool/Software | Use |
|---|---|
| **Autopsy/Sleuth Kit** | Open-source digital forensic platform for analyzing hard drives and |

| Tool/Software | Use |
|---|---|
| | smartphones. |
| **FTK Imager** | Forensic imaging and evidence acquisition. |
| **EnCase** | Industry-standard digital forensic tool for evidence collection, preservation, and reporting. |
| **Cellebrite UFED** | For mobile forensics and data extraction from smartphones. |
| **Wireshark** | Network protocol analyzer used for network forensics. |
| **Volatility Framework** | Memory forensics tool to analyze RAM dumps. |
| **X-Ways Forensics** | Lightweight forensic software for disk and file analysis. |
| **Magnet AXIOM** | Used to recover and examine digital evidence from computers, cloud, and mobile devices. |
| **Kali Linux (with Metasploit, Nmap, etc.)** | For simulating penetration testing, malware injection, and ethical hacking. |
| **Virtual Machines (VMware/VirtualBox)** | To run isolated environments for testing forensic scenarios. |
| **Cloud platforms (AWS, Azure, Google Cloud)** | For studying cloud forensics and emerging threats in cloud environments. |
| **AI/ML tools (e.g., TensorFlow, RapidMiner)** | To explore how artificial intelligence is used in modern forensic investigations. |

**Equipment (Hardware)**

| Equipment | Use |
|---|---|
| **Workstations with high-performance CPUs, RAM (16GB+), and SSD storage** | To run forensic software and virtual labs efficiently. |
| **Write Blockers (USB, SATA/IDE)** | Prevents alteration of source evidence during acquisition. |

| Equipment | Use |
|---|---|
| **Forensic Duplicators** | Devices used to make bit-by-bit copies of evidence drives. |
| **Mobile Device Forensic Kits** | Extract data from smartphones, SIM cards, and memory cards. |
| **External Hard Drives & SSDs (Encrypted)** | Storage of forensic images and logs. |
| **Faraday Bags** | To isolate mobile devices from network signals during evidence collection. |
| **Digital Cameras** | For documenting evidence and crime scenes. |
| **Projector and Smart Boards** | For delivering visual content in class. |

**Materials**

| Material | Use |
|---|---|
| **Lecture Notes and Textbooks** | Core knowledge resources for foundational and emerging digital forensic topics. |
| **Case Studies and Sample Reports** | Real-life scenarios to develop critical thinking and analysis skills. |
| **Simulated Evidence Samples (disk images, logs, malware)** | Practice material for hands-on investigations. |
| **Standard Operating Procedures (SOPs)** | Guidelines for conducting forensic processes. |
| **Digital Forensics Standards and Frameworks (e.g., NIST, ISO 27037)** | Reference materials for best practices and legal compliance. |
| **Chain of Custody Forms** | For teaching proper evidence handling. |
| **Assessment Rubrics and Lab Manuals** | Structured evaluation of student lab work and theoretical understanding. |

## 3. Learning Resources

Relevant training manual (learners' guide) and facilitators' guide

4. **Reference Materials (recommended textbooks, recommended readings)**


Casey, E. (2011). **Digital evidence and computer crime: Forensic science, computers, and the internet. 3rd ed**. Burlington: Academic Press.

Sammons, J. (2012). **The basics of digital forensics: The primer for getting started in digital forensics. 2nd ed**. Amsterdam: Elsevier.

Nelson, B., Phillips, A. & Steuart, C., 2020. **Guide to Computer Forensics and Investigations. 6th ed**. Boston: Cengage Learning.

Casey, E., 2011. **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed**. London: Academic Press.

Rogers, M. & Seigfried-Spellar, K., 2017. **Digital Forensics and Cyber Crime: 9th International Conference**. Cham: Springer.

Taylor, M., Haggerty, J., Gresty, D. & Lamb, D., 2020. **Digital Forensics Explained. 2nd ed**. London: Routledge.

**National Institute of Standards and Technology (NIST),** 2014. ***NIST SP 800-101 Rev. 1 - Guidelines on Mobile Device Forensics.*** [online] Available at: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final [Accessed 28 Jul. 2025].

**Magnet Forensics,** 2023. ***Emerging Trends in Digital Forensics 2023 Report***. [online] Available at: https://www.magnetforensics.com/resources/ [Accessed 28 Jul. 2025].

**Europol,** 2022. ***Internet Organised Crime Threat Assessment (IOCTA).*** [online] Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2022 [Accessed 28 Jul. 2025].

Sunde, N. & Moen, C., 2021. **Artificial Intelligence and Digital Forensics: Challenges and Opportunities. Journal of Digital Forensics, Security and Law**, 16(2), pp.1–15.

Martini, B. & Choo, K-K.R., 2013. **Cloud Storage Forensics: OwnCloud as a Case Study. Digital Investigation,** 10(4), pp.287–299.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G. & Katos, V., 2018. **A Critical Review of 7 Years of Mobile Device Forensics. Digital Investigation,** 24, pp.66–76.

**MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT**

**HIGHER EDUCATION EXAMINATIONS COUNCIL**

**(HEXCO)**

***QUALIFICATION STANDARD***

**FOR**

# DIGITAL FORENSICS TECHNICIAN

**SECTOR:** **BUSINESS OCCUPATIONS**

**QUALIFICATION FOR** **DIGITAL FORENSICS TECHNICIAN**

**QUALIFICATION CODE:** **TBA**

**LEVEL:** **NATIONAL DIPLOMA**

**DATE OF PROMULGATION:** **TBA**

**Foreword**

This document constitutes the first draft of a standard for the occupation of Digital Forensics Technician which was developed using Occupational Competence Profiles (OCPs) as a basis.

This is in preparation for the registration of the Standards on the Zimbabwe Qualifications Framework (ZQF). The ZQF is expected to be administered by the Zimbabwe Examinations and Qualifications Authority (ZIMEQA) once the ZIMEQA Bill currently before parliament becomes law.

In line with the SADC Protocol on Education and Training, each SADC member state was tasked to come up with its own Qualifications Framework that shall subsequently be linked to the Regional Qualifications Framework (RQF). The development and registration of standards on a qualifications framework is meant to facilitate the upward and horizontal movement of individuals in their occupations, across occupations or in their areas of study – within the country or the SADC region.

As a draft, certain sections have not yet been addressed. These sections are denoted by a [TBA] and will be attended to as information is finalized.

For ease of reference, a definition of terms commonly used in this document is included in the document.

This particular standard, for the occupation of an Administrative Assistant developed with the active participation of expert workers from the industry.

## TABLE OF CONTENTS

## Definition of Terms

| | |
|---|---|
| **Assessment** | A process of collecting evidence of a learner's work to measure and make judgments about the achievement or non-achievement of the specified National Qualifications Framework standards or qualifications. |
| **Certification** | Awarding of approved documentary evidence of a qualification. |
| **Competences required in readiness for assessment** | Critical relevant knowledge, skills and attitudes a learner requires in order to achieve specified outcomes before assessment. |
| **Credit** | The value assigned to a unit completed or a value assigned to a unit standard which reflects the relative time and effort required to complete the outcomes. |
| **Date of promulgation** | Date when standard and qualification have been approved, registered and gazetted. |
| **Duration** | The minimum notional hours required by a learner to attain all the competencies in a unit standard. |
| **Element** | The smallest component of a unit with a meaningful outcome. |
| **Generic skills** | Universal skills that apply to more than one occupation. |
| **Level descriptor** | A specific indicator of competence level on the ZQF. |
| **Occupation** | A group of related economically beneficial work activities performed by a person. |
| **Performance criteria** | A statement of competence or achievement against which the attainment of outcomes is measured. |
| **Qualification** | Formal award of recognition of the achievement of the required competency and/or capability level of the Zimbabwe Qualifications Framework as may be determined by the relevant bodies registered for such purpose by the Authority. |
| **Range statement** | The context or conditions within which a competence is performed and assessed that include tools, equipment, materials and duration. |
| **Review Date** | Date of revision of qualification standard as and when necessary but not later than three years from date of issue. |

| | |
|---|---|
| **Sector** | A section of the economy in which operators produce or provide similar products or services. |
| **Standard** | Registered statement of desired education and training outcomes and their assessment criteria. |
| **Unit** | The smallest combination of work activities capable of being a full-time economically beneficial occupation. |
| **Unit Standard** | Registered statement(s) of desired education and training outcomes, their associated assessment criteria together with administrative information as specified. |
| **ZQF** | National qualifications framework approved by the minister for registration of national standards and qualifications. |

## UNIT TITLES

| NO. | UNIT | CREDITS |
|---|---|---|
| 1 | Business Communication | 8 |
| 2 | Computer Networking | 10 |
| 3 | Hardware Administration | 12 |
| 4 | Legal Aspects in Digital Forensics | 12 |
| 5 | Incident Response | 12 |
| 6 | Nation Studies | 8 |
| 7 | Computer Forensics | 12 |
| 8 | Programming Concepts for Computer and Digital Forensics | 12 |
| 9 | Operating Systems Administration | 12 |
| 10 | Network Forensics | 12 |
| 11 | Entrepreneurial Skills Development | 8 |
| 12 | Database Management, Security and Forensics | 12 |
| 13 | Operating System Forensics | 12 |
| 14 | Malware Forensics | 12 |
| 15 | Ethical Hacking | 12 |
| 16 | Mobile Device Forensics | 12 |
| 17 | Cloud Forensics | 12 |
| 18 | Memory Forensics | 12 |
| 19 | Research and Project Management | 12 |
| 20 | Research Project | |

## SUMMARY OF STANDARD

| UNIT NO. | UNIT TITLE | CREDITS | ELEMENTS |
|---|---|---|---|
| 1 | Business Communication | 8 | |
| 2 | Computer Networking | 12 | |
| 3 | Hardware Administration | 12 | |
| 4 | Legal Aspects in Digital Forensics | 12 | |
| 5 | Incident Response | 12 | |
| 6 | National Studies | 8 | |
| 7 | Computer Forensics | 12 | |
| 8 | Programming Concepts for Computer and Digital Forensics | 12 | |
| 9 | Operating Systems Administration | 12 | |
| 10 | Network Forensics | 12 | |
| 11 | Entrepreneurial Skills Development | 8 | |
| 12 | Database Management, Security and Forensics | 12 | |
| 13 | Operating System Forensics | 12 | |
| 14 | Malware Forensics | 12 | |
| 15 | Ethical Hacking | 12 | |
| 16 | Mobile Device Forensics | 12 | |
| 17 | Cloud Forensics | 12 | |
| 18 | Memory Forensics | 12 | |
| 19 | Research and Project Management | 12 | |
| 20 | Research Project | | |
| | | | |

**Unit 1**

| Title 1: | Business Communication |
|---|---|
| Unit Code | |

**ZQF Level:** **National Diploma**

**Credits:** **10**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to communicate effectively in a business environment.

**ELEMENTS AND PERFORMANCE CRITERIA**

| Element 1.1 | Apply language and writing skills in business |
|---|---|

**Performance Criteria:**
1.1.1 Correct language style selected
1.1.2 Business jargon in appropriate situations utilized
1.1.3 Written material logically organized
1.1.4 Effective method of communication in abusiness context selected and used
1.1.5 Telephone effectively utilized

| Element 1.2 | Write business documents |
|---|---|

**Performance Criteria:**
1.2.1 Business letters produced
1.2.2 Reports generated
1.2.3 Memoranda written using the fully-blocked method
1.2.4 Notices written for the company notice board

| Element 1.3 | Use communication skills to satisfy business needs |
|---|---|

**Performance Criteria:**
1.3.1 Communication style adapted to suit different audiences and situations
1.3.2 Clear and confident verbal messages delivered in meetings, presentations, and conversations

1.3.3 Information communicated correctly in a structured language
1.3.4 Written communication used effectively

| Element 1.4 | Apply effective communication techniques in business |
|---|---|

**Performance Criteria:**
1.4.1 Grammar and pronunciation used according to type of business
1.4.2 Orally information presented interpreted
1.4.3 Digital tools used effectively for business communication

| Element 1.5 | Manage different types of meetings |
|---|---|

**Performance Criteria:**
1.5.1 Engaging and professional presentations planned, organized and delivered.
1.5.2 Modern communication tools and platforms used appropriately
1.5.3 Notes taken from meetings
1.5.4 Meeting documents prepared

**Competences required in readiness for assessment.**
Demonstrate knowledge of:

- Language proficiency
- Digital tools for communication
- Verbal and non-verbal cues
- Report writing
- Persuasion and presentation techniques
- Feedback management

**Generic Skills**

- Critical thinking
- Problem-solving
- Listening skills
- Research skills
- Analytical skills
- Attention to detail
- Incident management
- Report writing
- Time management
- Ethical decision-making

**Range Statement:**

**Tools and equipment**

- Collaboration & Productivity Tools
- Presentation & Content Creation Tools
- Networking & Infrastructure
- Communication Tools
- Visual Aids and Presentation Equipment
- Time Management and Scheduling Tools

**Materials**

- Stationery
- Storage media (USB drives, external hard drives)
- Secure evidence bags
- Documentation templates
- Internet access
- Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

## UNIT 2

| Unit Title | National Studies |
|---|---|
| Unit Code: | |

**Level of Unit:** **National Certificate**

**Credits:** **8**

**Occupation:** **Patriotic Citizen**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

### AIM OF THE UNIT STANDARD

This unit helps people to create informed, responsible and engaged Zimbabweans who contribute to the well-being and progress of their nation.

### ELEMENT AND PERFORMANCE CRITERIA

| Element 2.1 | Maintain a Zimbabwean culture |
|---|---|

**Performance Criteria:**

2.1.1 Cultural heritage preserved
2.1.2 Cultural artefacts conserved
2.1.3 Knowledge of Zimbabwe culture demonstrated
2.1.4 Records of maintaining natural resources of Zimbabwe captured
2.1.5 Indigenous knowledge systems preserved

| Element 2.2 | Preserve Zimbabwean History |
|---|---|

**Performance Criteria:**

2.2.1 Pre-colonial states identified
2.2.2 Precolonial political structure analysed
2.2.3 Achievements of precolonial history recorded
2.2.4 Colonial history recorded
2.2.5 Role of Christian missionaries recorded
2.2.6 Occupation of Zimbabwe recorded
2.2.7 Causes of First /Second Chimurenga traced

| Element 2.3 | Assemble components of colonial effects |
|---|---|

**Performance Criteria:**

2.3.1 New administrative boundaries demarcated
2.3.2 Natural resources exploited (minerals, wildlife, land, water, vegetation etc)
2.3.3 Traditional religion changed
2.3.4 Foreign food crops and livestock introduced
2.3.5 Education systems changed
2.3.6 Capitalistic relations introduced
2.3.7 New legal systems introduced
2.3.8 Forms of trade changed
2.3.9 Human rights violated
2.3.10 Results of colonisation analysed

| **Element 2.4** | **Analyse post-independence socio-economic and political developments** |
|---|---|

**Performance Criteria:**

2.4.1 Socio-economic and political developments examined
2.4.2 Policies formulated
2.4.3 Measures to address colonial injustices adopted

| **Element 2.5** | **Carry out a feasibility study on peace, conflict and resolution** |
|---|---|

**Performance Criteria:**

2.5.1 Conflict and resolution styles demonstrated
2.5.2 3Cs between Zimbabwe and the global community demonstrated
2.5.3 Strategies for sustaining peace analysed
2.5.4 Influence of multi-national companies in developing countries analysed
2.5.5 Benefits of International capital to developing countries examined.

| **Element 2.6** | **Participate in civic responsibilities** |
|---|---|

**Performance Criteria:**

2.6.1 Civic responsibilities undertaken
2.6.2 Participation in disaster management observed
2.6.3 Citizen duties adopted
2.6.4 Sustainable exploitation of resources practices formulated.

| **Element 2.7** | **Assemble components of legal and parliamentary affairs** |
|---|---|

**Performance Criteria:**

2.7.1 Origins of law identified
2.7.2 Constitutional provisions observed
2.7.3 Arms of the state identified
2.7.4 Law making process explained

**COMPETENCIES REQUIRED IN READINESS FOR ASSESSMENT:**

Record keeping skills
Customer care
skills
Management
skills (decision
making, planning,
organising)
Technological
awareness
Problem-solving
skills
Interpersonal
skills
Legal awareness
Mobilisation
skills
Upholding norms,
values and social
aspects of
Zimbabwean
culture.
Patriotism
Environmental awareness skills
Legal awareness
Critical thinking skills
Research skills
Problem-solving skills
Maintaining Zimbabwean culture
Social responsible
Abreast with global current events
Tool handling skills

**GENERIC SKILLS:**

Patriotic
Practical skills
Tolerance skills
Technological
knowledge
Communication
Positive regard
Planning
Organisation
Controlling
Human relation skills
Interpersonal skills
CriticAnalytical skills

Good attitude
Good morals
Acceptance of others
Servant hood
Committed cadre to National Agenda
Quest for more knowledge
Social skills

**RANGE STATEMENT:**

**TOOLS AND EQUIPMENT:**
Generic which are relevant to the type of business.

**MATERIALS:**
Generic which are relevant to the type of business.

**Duration:** **8**0 hours

**ASSESSMENT AND CERTIFICATION:**
In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Accredited assessors will conduct the assessment. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

## UNIT 3

| Unit Title: | Entrepreneurial Skills Development |
|---|---|
| Unit Code | |

**Level of Unit:** **National Certificate**

**Credits:** **8**

**Occupation:** **Patriotic Citizen**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

### AIM OF THE UNIT STANDARD

This unit helps people to start, manage, and grow successful businesses.

### ELEMENT AND PERFORMANCE CRITERIA

| Element 3.1 | Formulate a business |
|---|---|

**Performance Criteria:**

3.1.1 Business idea formulated
3.1.2 Business plan produced
3.1.3 Business market research carried out
3.1.4 Financial plan compiled
3.1.5 Product/service positioned
3.1.6 Survival Strategies Enveloped
3.1.7 Business environment established
3.1.8 Financial resources mobilised

| Element 3.2 | Register a company |
|---|---|

**Performance Criteria:**

3.2.1 Company documents prepared
3.2.2 Business registration processed
3.2.3 Place of business operation secured
3.2.4 Rules and Regulations compiled

| Element 3.3 | Operate a successful business |
|---|---|

**Performance Criteria:**

3.1.1 Business managed according to organization policy
3.1.2 Resources allocated according to line of business
3.1.3 Products costed in line with procedures
3.1.4 Products priced according to company procedures
3.1.5 Records updated and maintained
3.1.6 Stock controlled in line with organization requirements
3.1.7 Market plans formulated
3.1.8 Risks managed in line with organization requirements
3.1.9 Growth Strategies Adopted
3.1.10 Business observed and social responsibility provided
3.1.11 Customer care practiced
3.1.12 Employees motivated in line with organizational requirements

**COMPETENCIES REQUIRED IN READINESS FOR ASSESSMENT:**

Record-keeping skills
Customer care
skills
Management skills (decision-making, planning, organizing)
Technological Awareness
Problem-solving skills
Interpersonal skills
Legal Awareness
Mobilisation skills
Patriotism
Environmental awareness skills
Legal awareness
Critical thinking skills
Research skills
Problem-solving skills
Social responsibility
Abreast with global current events
Tool handling skills

**GENERIC SKILLS:**

Patriotic
Practical skills
Tolerance skills
Technological
knowledge
Communication
Positive regard
Planning
Organisation
Controlling
Human relation skills
Interpersonal skills
Critical thinking skills
Analytical skills

Good attitude
Good morals
Acceptance of others
Servant hood
Committed cadre to National Agenda
Quest for more knowledge
Social skills

**RANGE STATEMENT:**

**TOOLS AND EQUIPMENT:**
Generic which are relevant to the type of business.

**MATERIALS:**
Generic which are relevant to the type of business.

**Duration:** 80 hours

**ASSESSMENT AND CERTIFICATION:**
In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Accredited assessors will conduct assessment. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**UNIT 4**

| | |
|---|---|
| **Title 4:** | **Hardware Administration** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **10**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to assemble, install, troubleshoot, and maintain computer hardware.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 4.1** | **Identify & Assemble Hardware components** |

**Performance Criteria:**
4.1.1 Hardware components identified.
4.1.2 Purposes and uses of various peripheral types identified.
4.1.3 Various hardware components are assembled
4.1.4 Test hardware components and configurations

| | |
|---|---|
| **Element 4.2** | **Maintain workshop practice** |

**Performance Criteria:**
4.2.1 IT workshop regulations are established.
4.2.2 Hardware security measures are enforced.
4.2.3 Precautionary measures and workshops ethics are maintained.
4.2.4 Workshop safety tools are identified.

| | |
|---|---|
| **Element 4.3** | **Recommend hardware requisitions** |

**Performance Criteria:**
4.3.1 Hardware requirements are identified
4.3.2 List of requirements is compiled.
4.3.3 Correct specifications are submitted.

| Element 4.4 | Install hardware |
|---|---|

**Performance Criteria:**
4.4.1 Site is prepared.
4.4.2 Requirements for installation are identified.
4.4.3 Components are assembled
4.4.4 Configuration is done.
4.4.5 Hardware testing is done.

| Element 4.5 | Maintain hardware |
|---|---|

**Performance Criteria:**
4.5.1 Maintenance schedule prepared.
4.5.2 Appropriate maintenance tools and accessories identified.
4.5.3 Users are informed of maintenance schedules.
4.5.4 Hardware maintenance is done.
4.5.5 The operation of the system is checked.

| Element 4.6 | Enforce hardware security measures |
|---|---|

**Performance criteria**
4.6.1 Threats are identified.
4.6.2 Access control measures are enforced.
4.6.3 Disaster recovery plan is established.
4.6.4 Periodic back-ups are done.
4.6.5 IT best practices are put in place.

| Element 4.7 | Maintain inventory |
|---|---|

**Performance criteria**
4.7.1 Inventory list is compiled in accordance with company asset identification procedures.
4.7.2 Routine physical verification of the inventory is performed.
4.7.3 Inventory list is updated periodically.
4.7.4 Reports are compiled.

**Competences required in readiness for assessment.**
Knowledge of:
Troubleshooting skills
Hardware assembling skills
Hardware repairing skills
Hardware installation skills
Hardware configurations skills
Hardware maintenance skills

**Generic Skills**
Computer literacy
Confidence
Change Management

**Range Statement:**

**Tools and equipment**

Computer repair tool kit
Computer hardware

**Materials**
Stationery
Protective clothing

**Duration: 100 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

## UNIT 5

| Title 5: | Computer Networking |
|---|---|
| Unit Code | |

**ZQF Level:** **National Diploma**

**Credits:** **10**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim of the unit standard**

The unit will enable an individual to implement and support computer networks

**ELEMENTS AND PERFORMANCE CRITERIA**

| Element 5.1 | Identify network requirements |
|---|---|

**Performance Criteria:**

5.1.1 Computer networks explained in line with organisational needs
5.1.2 Network types and designs are illustrated
5.1.3 Appropriate networking equipment is identified
5.1.4 Internetworking technologies are described

| Element 5.2 | Implement network requirement solutions |
|---|---|

**Performance Criteria:**

5.2.1 Networking equipment is placed in strategic positions in line with network design
5.2.2 Network devices are configured
5.2.3 Network connectivity is tested
5.2.4 Network documentation generated

| Element 5.3 | Maintain Network Operations |
|---|---|

**Performance Criteria:**

5.3.1 Network performance monitored
5.3.2 Network security measures updated periodically
5.3.3 Network troubleshooting performed
5.3.4 Necessary network repairs performed
5.3.5 Network upgrades implemented
5.3.6 Network hardware serviced

| Element 5.4 | Provide network user support |
|---|---|

**Performance Criteria:**

5.4.1 Help desk system is set up
5.4.2 User queries are collected and/logged
5.4.3 User queries analysed
5.4.4 User queries are attended to accordingly
5.4.5 Routine maintenance is conducted
5.4.6 Ad hoc maintenance is carried out where necessary

| Element 5.5 | Monitor network performance |
|---|---|

**Performance Criteria:**

5.5.1 Monitoring plan developed
5.5.2 Faults isolated in line with problem indicators
5.5.3 Appropriate diagnostic methodology implemented
5.5.4 Fault resolution process documented
5.5.5 Operating performance in line with standards

**Competences required in readiness for assessment**

Knowledge of network equipment
Computer networking
Computer network security
Numeracy
Problem solving
Analytical
Interpretation

**Generic Skills**

SHEQ
Communication
Computer literacy
Problem solving
Innovativeness
Controlling
Human relations
Organising
Supervision
Planning

**Range Statement:**

Tools and equipment

Computer repair toolkit
Software
Computer hardware
Protective clothing
First aid kit
Storage media
Internet
Maps
Computer network tool kit

Materials

Stationery

Duration

100 hours

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors.

**Unit 6**

| Title 6: | Operating Systems Administration |
|---|---|
| Unit Code | |

**ZQF Level:** **National Diploma**

**Credits:** **15**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

The aim of the course is to introduce the students to the concepts of operating Systems (OS) as a guide towards understanding their design and implementation as well as their roles in resource management, enabling the learner to install, configure and manage different types of operating systems.

**ELEMENTS AND PERFORMANCE CRITERIA**

| Element 6.1 | Describe the operation and structure of a computer system |
|---|---|

**Performance Criteria:**

6.1.1 Goals and roles of operating systems are outlined.
6.1.2 Structure of operating is analysed.
6.1.3 Interrupts are handled.

| Element 6.2 | Explain the structure and management of processes |
|---|---|

**Performance Criteria:**

6.2.1 Process management is explained.
6.2.2 CPU scheduling algorithms are applied.
6.2.3 Process synchronization is applied.
6.2.4 Deadlock in operating systems is describe.

| Element 6.3 | Outline the fundamentals of memory management |
|---|---|

**Performance Criteria:**

6.3.1 Memory management techniques are implemented.

6.3.2 Memory swapping is explained.
6.3.3 Memory allocation is implemented.
6.3.4 Paging, fragmentation, and segmentation are implemented in operating systems.
6.3.5 Virtual memory management is explained.

| Element 6.4 | Install and configure a LINUX and Windows operating system |
|---|---|

**Performance Criteria:**
6.4.1 Linux and Windows operating systems organization, components and file systems are described.
6.4.2 Linux operating system is installed and configured.
6.4.3 Windows operating system is installed and configured.

| Element 6.5 | Manage the Linux graphical user interface and command line interface, Windows and MS-DOS to perform standard user and administration tasks |
|---|---|

**Performance Criteria:**
6.5.1 Linux administration is performed
6.5.2 Windows Server administration is performed.
6.5.3 Appropriate tools for administrative tasks for system security, performance, and maintenance applied

| Element 6.6 | Adapt to trends in virtualization, emulation and the increasing use of sophisticated OS in mobile systems |
|---|---|

**Performance Criteria:**
6.6.1 Importance of virtualization and emulation in computer systems is outlined.
6.6.2 Strategies for virtualization and emulation in computer systems are implemented.
6.6.3 Virtualization and emulation used to test applications, debug systems, and optimize performance across platforms

| Element 6.7 | Implement appropriate security and protection mechanisms in operating systems |
|---|---|

**Performance Criteria:**
6.7.1 Importance of computer security at the OS level is outlined.
6.7.2 Methods to implement security and protection in operating systems is established.
6.7.3 Security practices applied to ensure the integrity, confidentiality, and availability of systems.

**Competences required in readiness for assessment.**
Demonstrate knowledge of:

Computer networking
Software development skills
Computer hardware
Knowledge in operating systems
Knowledge in virtualization
Knowledge in mobile operating systems
Knowledge in different development environments

**Generic Skills**
Computer literacy
Problem solving
Interpersonal skills

**Range Statement:**

**Tools and equipment**
Computer Hardware and software
Operating systems

*2.2 Emulators and simulators*

Version control software

**Materials**
Stationery
Internet access
Reference manuals
**Competences required in readiness for assessment**

Demonstrate knowledge of:

Different programming languages
Programming skills
Knowledge of systems methodology
Design and modelling skills

**Generic Skills**

Computer literacy
Communication
Research skills
Management skills
Innovativeness
Interpersonal skills

**Range Statement:**

**Tools and equipment**

Computer hardware and software
Cameras
Scanners
LCD Projector

**Materials**

Stationery
Internet Access

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 7**

| Title: | Cloud Forensics |
|---|---|
| Unit Code | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to investigate cloud-based cyber incidents, identify threats, collect and analyze digital evidence, and ensure legal compliance.

**ELEMENTS AND PERFORMANCE CRITERIA**

| Element 7.1 | Identify Cloud Threats and Attack Vectors |
|---|---|

**Performance Criteria:**

7.1.1 Cloud Security Risks Analyzed
7.1.2 Vulnerabilities in cloud infrastructure Identified
7.1.3 Risks related to multi-tenancy and shared resources Assessed
7.1.4 Common Cloud Threats Identified
7.1.5 Attack Vectors Assessed
7.1.6 Cloud Malware & Ransomware Risks Examined
7.1.7 Malicious file uploads and cloud-based malware execution Detected
7.1.8 cloud-native ransomware and data encryption attacks are Investigated
7.1.9 Cloud Network Security Monitored
7.1.10 Network traffic for suspicious activities Analyzed
7.1.11 Lateral movement and unauthorized access patterns Detected
7.1.12 Cloud Log Data for Anomalies Investigated
7.1.13 AWS CloudTrail, Azure Monitor, Google Cloud Logging Analyzed
7.1.14 Signs of account compromise or credential theft Identified
7.1.15 Compliance & Security Gaps Evaluated
7.1.16 Adherence to security frameworks (NIST, ISO 27001, GDPR, HIPAA) Assessed
7.1.17 non-compliance issues that could expose the cloud environment Identified

7.1.18 Cloud Security Enhancements Recommended
7.1.19 Zero Trust Security policies are Implemented
7.1.20 IAM policies (MFA, RBAC) and data encryption strategies Strengthened

| Element 7.2 | Acquire Cloud Data & collect Evidence |
|---|---|

**Performance Criteria:**

7.2.1 Relevant Cloud Data Sources Identified
7.2.2 Cloud Forensic Tools utilized
7.2.3 Cloud Storage & VM Snapshots Captured.
7.2.4 Log Data Extracted from AWS CloudTrail, Azure Monitor, Google Cloud Logging.
7.2.5 Network Traffic Analyzed.
7.2.6 Chain of Custody Secured & Maintained using Hashing, timestamping, digital signatures.
7.2.7 Evidence is securely Documented & Stored using Encryption, classify, and retain per policy.

| Element 7.3 | Analyse Cloud Log and Investigate Incident |
|---|---|

**Performance Criteria:**

7.3.1 Log Data collected & correlated.
7.3.2 Suspicious Activities Identified.
7.3.3 Network Traffic Logs Analyzed
7.3.4 lateral movement, DDoS, unusual connections detected.
7.3.5 Authentication & IAM Logs Investigated.
7.3.6 API & Application Logs Examined.
7.3.7 SIEM & Forensic Tools applied for log analysis.
7.3.8 Incident Timeline Generated.
7.3.9 Report Findings Documented.

| Element 7.4 | Recover and Analyse Cloud Data |
|---|---|

**Performance Criteria:**

7.4.1 Deleted or Encrypted Data Recovered.
7.4.2 Cloud Storage & Databases Analyzed.
7.4.3 Metadata Extracted & Inspected
7.4.4 File changes, access history, timestamps Identified.
7.4.5 Data Integrity Decrypted & Verified.
7.4.6 Hashing, encryption keys, and forensic tools Used.

7.4.7 Log & Network Data Correlated
7.4.8 Recovered data Cross-checked with logs for anomalies.

| Element 7.5 | Detect and mitigate Cloud Threats |
|---|---|

**Performance Criteria:**

7.5.1 Cloud Logs & Traffic Monitored.
7.5.2 Unauthorized Access Identified.
7.5.3 Malware Detected & Blocked.
7.5.4 Misconfigurations Mitigated
7.5.5 APIs Secure
7.5.6 Least Privilege enforced
7.5.7 Firewall rules updated.
7.5.8 Incident Response Actions Implemented
7.5.9 affected resources Isolated,
7.5.10 vulnerabilities patched,
7.5.11 IAM controls strengthened.

| Element 7.6 | Apply Emerging Trends cloud forensics |
|---|---|

**Performance Criteria:**

7.6.1 High-Profile Cloud Security Incidents Analyzed
7.6.2 Cases like AWS breaches or data leaks in cloud environments Reviewed.
7.6.3 Lessons from Past Incidents Identified.
7.6.4 Response strategies and improve future cloud forensic practices Evaluated.
7.6.5 Emerging Cloud Threats Researched.
7.6.6 New attack vectors like container vulnerabilities and cloud-native malware Stay updated.
7.6.7 AI & Machine Learning in Forensics Explored.
7.6.8 Trends in Cloud Compliance & Regulations Monitored

**Competences required in readiness for assessment.**

Demonstrate knowledge of:

- Knowledge of cloud models, storage, security threats, and regulations
- Cloud evidence acquisition and forensic tool proficiency
- Cloud log analysis, data recovery, and threat mitigation
- Forensic investigation, chain of custody, and incident response
- Understanding of cloud provider policies and forensic standards (ISO, NIST)
- Knowledge of conceptual modeling

**Generic Skills**

- Critical thinking
- Problem-solving
- Communication
- Research skills
- Analytical skills
- Attention to detail
- Incident management
- Report writing
- Time management
- Ethical decision-making

**Range Statement:**

**Tools and equipment**

- Computer hardware and software
- Cloud forensic tools (FTK, Autopsy)
- Network analysis tools (Wireshark)
- Log analysis tools
- Secure storage devices

**Materials**

- Stationery
- Storage media (USB drives, external hard drives)
- Secure evidence bags
- Documentation templates
- Internet access
- Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.
Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 8**

| | |
|---|---|
| **Title:** | **Computer Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to systematically investigate digital evidence, ensuring its integrity and admissibility while applying forensic methodologies to analyze, recover and report on digital artifacts**.**

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 8.1** | **Demonstrate knowledge of computer hardware, software, and file systems** |

**Performance Criteria:**

8.1.1 Computer system components identified.

8.1.2 Structure and functioning of common file systems explained.

8.1.3 How data is stored, accessed, and deleted on storage media is described.

| | |
|---|---|
| **Element 8.2** | **Adhere to legal and ethical standards in computer forensics** |

**Performance Criteria:**

8.2.1 Chain of custody procedures followed to ensure evidence admissibility in court.

8.2.2 Compliance with relevant laws and regulations ensured.

8.2.3 Authorization before accessing and analyzing digital evidence obtained.

| | |
|---|---|
| **Element 8.3** | **Acquire digital evidence** |

**Performance Criteria:**

8.3.1 Write-blocking tools to prevent data alteration during acquisition employed.

8.3.2 Forensic images of storage devices created.

8.3.3 Evidence acquisition process documented
8.3.4 Verify the integrity of acquired evidence using hashing algorithms

| Element 8.4 | Recover and analyze digital evidence from storage media |
|---|---|

**Performance Criteria:**
8.4.1 Deleted files, partitions, and unallocated space recovered.
8.4.2 File metadata analyzed to reconstruct events.
8.4.3 Forensic tools utilized to examine file systems and extract data.
8.4.4 Artifacts identified and analyzed.

| Element 8.5 | Analyze malicious software to understand its behavior and impact |
|---|---|

**Performance Criteria:**
8.5.1 Static and dynamic analysis of malware samples performed.
8.5.2 Purpose and functionality of malware identified.
8.5.3 Actionable recommendations constructed.

| Element 8.6 | Investigate network-based incidents and analyze network traffic. |
|---|---|

**Performance Criteria:**
8.6.1 Network traffic captured and analyzed.
8.6.2 Suspicious network activity identified.
8.6.3 Source of network-based attacks traced.

| Element 8.7 | Prepare clear and concise forensic reports |
|---|---|

**Performance Criteria:**
8.7.1 Document structured according to international standards.
8.7.2 Technical details simplified for non-technical stakeholders.
8.7.3 Recommendations for preventing future incidents provided.

| Element 8.8 | Respond to incidents involving computer systems |
|---|---|

**Performance Criteria:**
8.8.1 Computer-related security incidents Identified and contained.
8.8.2 Scope and impact of the incident triaged/assessed.
8.8.3 Root cause of the incident analyzed
8.8.4 Relevant stakeholders promptly notified

**Competences required in readiness for assessment.**
Demonstrate knowledge of:

- Computer hardware, software and file systems
- Legal and ethical compliances in computer forensics

- Digital evidence acquisition
- Malware analysis
- Effective use computer forensics tools
- Forensic reporting and documentation
- Incident response and investigation

**Generic Skills**

- Problem-solving
- Critical thinking
- Attention to detail
- Time management
- Research skills
- Communication skills
- Collaboration and teamwork

**Range Statement:**

**Tools and equipment**

- Computer hardware and software
- FTK imager
- Autopsy and Slueth Kit
- TestDisk
- IDAPro
- PEiD
- Cellebrite UFED
- Magnet AXIOM
- Oxygen Forensic Suite
- John the ripper
- Hashcat
- Splunk

- Sysinternals Suite
- Ophcrack
- Cain and Abel

**Materials**

- Stationery
- Forensic workstations
- Write Blocks
- External storage devices
- CaseNotes
- Clean isolated environment (Kali, Windows, SIFT)
- Anti-forensics detection tools
- Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 9**

| | |
|---|---|
| **Title:** | **Database Management, Security and Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to understand and apply security, and forensic techniques, including data recovery, analysis, securing database environments, ensuring evidence integrity, and complying with legal and regulatory standards during database-related investigations.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 9.1** | **Analyze Database Models & Architectures** |

**Performance Criteria:**

9.1.1 Different types of database models described.
9.1.2 Centralized, distributed, and cloud-based database architectures compared.
9.1.3 Relational databases queried
9.1.4 The strengths and weaknesses of various database models in forensic investigations evaluated.

| | |
|---|---|
| **Element 9.2** | **Identify Data Storage & Retrieval Mechanisms** |

**Performance Criteria:**

9.2.1 Different types of data storage mechanisms identified.
9.2.2 SQL queries retrieving and manipulating data efficiently used.
9.2.3 The impact of indexing, partitioning, and caching on data retrieval explained.
9.2.4 Forensic techniques to retrieve deleted or hidden records applied.

| | |
|---|---|
| **Element 9.3** | **Implement Authentication & Access Management** |

**Performance Criteria:**

9.3.1 User authentication mechanisms (passwords, MFA, tokens) configured and implemented.

9.3.2 Role-based access control (RBAC) for database users enforced.
9.3.3 Risks associated with privilege escalation identified and mitigated.
9.3.4 Best practices for database access control in forensic scenarios applied.

| Element 9.4 | Apply Database Encryption & Data Protection |
|---|---|

**Performance Criteria:**
9.4.1 Different encryption methods used in database security (tde, aes, hashing) explained.
9.4.2 Encryption mechanisms for securing sensitive database records implemented.
9.4.3 The impact of encryption on database performance assessed.
9.4.4 Decryption techniques for forensic analysis of secured data applied.

| Element 9.5 | Identify & Mitigate Database Attacks |
|---|---|

**Performance Criteria:**
9.5.1 SQL injection vulnerabilities in databases detected and analyzed.
9.5.2 The risks of unauthorized database access through proper configurations mitigated.
9.5.3 Threats posed by insider attacks identified and security measures enforced.
9.5.4 Countermeasures against common database attacks (e.g., privilege escalation, buffer overflow) developed.

| Element 9.6 | Configure Log Monitoring & Anomaly Detection |
|---|---|

**Performance Criteria:**
9.6.1 Database logging mechanisms to capture critical events configured.
9.6.2 Database logs to identify suspicious activities and anomalies analyzed.
9.6.3 Database logs with system and network logs for forensic analysis correlated.
9.6.4 Automated alerting mechanisms for security breaches implemented.

| Element 9.7 | Acquire and preserve forensic data |
|---|---|

**Performance Criteria:**
9.7.1 Relevant database artifacts for forensic investigations identified and acquired.
9.7.2 Industry-standard forensic acquisition tools (FTK, encase) to collect database evidence applied.
9.7.3 Integrity preserved and chain of custody for collected database artifacts maintained.
9.7.4 Compliance with forensic and legal guidelines during evidence acquisition ensured.

| Element 9.8 | Recover Deleted & Modified Data |
|---|---|

**Performance Criteria:**
9.8.1 Forensic tools to recover deleted database records used.
9.8.2 Unauthorized modifications by analyzing database transaction logs identified.

9.8.3 The timeline of changes made to the database reconstructed.
9.8.4 Recovered data validated to ensure accuracy and integrity.

| Element 9.9 | Respond to Database Breaches |
|---|---|

**Performance Criteria:**
9.9.1 An incident response plan specific to database security breaches developed.
9.9.2 Database breaches investigated and compromised data identified.
9.9.3 Ongoing database threats contained and mitigated.
9.9.4 Findings documented and incidents reported to relevant stakeholders.

| Element 9.10 | Conduct Root Cause Analysis & Reporting |
|---|---|

**Performance Criteria:**
9.10.1 Forensic analysis to determine the root cause of database security incidents conducted.
9.10.2 Forensic reports detailing the impact and timeline of the breach generated.
9.10.3 Recommendations for mitigating future security risks provided.
9.10.4 Proper legal documentation for potential court proceedings ensured.

| Element 9.11 | Implement Cloud Database Security & Compliance |
|---|---|

**Performance Criteria:**
9.11.1 Cloud database architectures and their security challenges Explained.
9.11.2 Access controls for securing cloud-based databases Implemented.
9.11.3 Legal and compliance requirements for cloud database forensics Identified.
9.11.4 Cloud database security breaches using forensic tools Investigate.

| Element 9.12 | Identify Cloud Forensic Tools & Data Acquisition methods |
|---|---|

**Performance Criteria:**
9.12.1 Cloud forensic tools to collect and analyze database evidence used.
9.12.2 Cloud-based database logs for forensic investigations acquired and preserved.
9.12.3 Unauthorized access in cloud databases identified and investigated.
9.12.4 Proper documentation and compliance with cloud forensic standards ensured.

| Element 9.13 | Check Real-World Database Forensic Investigations |
|---|---|

**Performance Criteria:**
9.13.1 Case studies of past database forensic investigations analyzed.
9.13.2 Learned techniques to real-world forensic scenarios applied.
9.13.3 Forensic data using hands-on exercises extracted and analyzed.
9.13.4 Findings presented in a structured forensic report.

| Element 9.14 | Provide Advanced Forensic Techniques & Expert Testimony |
|---|---|

**Performance Criteria:**

9.14.1 Advanced forensic techniques to uncover hidden database evidence utilized.
9.14.2 Findings interpreted and correlated with other digital forensic evidence.
9.14.3 Expert witness testimony prepared based on forensic findings.
9.14.4 Proficiency in presenting forensic evidence in legal proceedings demonstrated.

**Competences required in readiness for assessment.**

**Demonstrate knowledge of:**

- Knowledge of database management systems (DBMS)
- Understanding of database security principles and encryption
- Proficiency in SQL queries and database operations
- Knowledge of data recovery techniques
- Understanding of forensic data acquisition and analysis
- Familiarity with regulatory and legal requirements in database forensics
- Ability to detect and mitigate database security threats
- Understanding of database backup and restoration processes

**Generic Skills**

- Analytical thinking
- Problem-solving
- Attention to detail
- Research skills
- Communication
- Time management
- Risk assessment
- Documentation and report writing

**Range Statement:**

**Tools and equipment**

- Database management software (e.g., MySQL, SQL Server, Oracle)
- Forensic analysis tools (e.g., FTK, EnCase, X1 Social Discovery)

- Data recovery tools (e.g., R-Studio, Recuva)
- Backup and restoration tools
- Encryption and decryption tools
- Disk imaging software
- Secure storage devices (e.g., external hard drives, USB drives)

**Materials**

- Stationery
- Data storage media (e.g., USB drives, external hard drives)
- Documentation templates and forms
- Reference books and manuals on database management and security
- Encryption keys or security tokens
- Backup tapes and disks
- Evidence bags for secure data handling

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 10**

| | |
|---|---|
| **Title:** | **Ethical Hacking** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to identify and resolve vulnerabilities, weaknesses, and security flaws in computer systems, networks, and applications in a legally responsible manner.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 10.1** | **Conduct Reconnaissance** |

**Performance Criteria:**

10.1.1 Passive Reconnaissance performed
10.1.2 Active Reconnaissance conducted
10.1.3 Network Map Identified
10.1.4 OS Fingerprinting performed
10.1.5 Running services identified
10.1.6 Information gathered through human interaction
10.1.7 Open-Source Intelligence gathered
10.1.8 Domain Analysis conducted
10.1.9 Emails Harvested
10.1.10 Metadata Extracted
10.1.11 Techniques for covering tracks and avoiding detection explored

| | |
|---|---|
| **Element 10.2** | **Scan and Enumerate target information** |

**Performance Criteria:**

10.2.1 Port Scanned
10.2.2 Vulnerability detected
10.2.3 Network Scanned

10.2.4 Service detailed information gathered
10.2.5 SNMP information Extracted
10.2.6 LDAP detailed information gathered
10.2.7 SMB detailed information gathered
10.2.8 DNS records extracted
10.2.9 Web Application vulnerabilities identified
10.2.10 Wireless Network Scanned

| Element 10.3 | Perform network exploitation |
|---|---|

**Performance Criteria:**
10.3.1 Custom exploits for specific vulnerabilities deployed.
10.3.2 Privilege escalation performed
10.3.3 Access maintained and additional information gathered.
10.3.4 Password cracked
10.3.5 Penetration testing conducted using ethical hacking tools
10.3.6 Social engineering attacks performed
10.3.7 Web application exploitation conducted
10.3.8 Network exploitation carried out
10.3.9 Wireless exploitation done
10.3.10 Zero-day exploits performed
10.3.11 Compromised systems used to attack other systems in the network.

| Element 10.4 | Conduct post-exploitation |
|---|---|

**Performance Criteria:**
10.4.1 Persistence Mechanisms developed
10.4.2 Data Exfiltration contacted
10.4.3 Tracks covered
10.4.4 Privilege Escalation performed
10.4.5 Network Enumeration done in-depth
10.4.6 Forensic Artifact Collected
10.4.7 Log Manipulated
10.4.8 Lateral Movement performed
10.4.9 Data Manipulated

| Element 10.5 | Compile Reports and Documentation |
|---|---|

**Performance Criteria:**
10.5.1 High-level overview of the findings Provided.

10.5.2 Technical Details analysis of vulnerabilities and exploits detailed
10.5.3 Risk Assessed
10.5.4 Remediation Recommendations Suggested
10.5.5 Visual Aids Using charts, graphs, and screenshots to illustrated
10.5.6 Compliance Reporting provided
10.5.7 Peer Review performed
10.5.8 Actionable Insights Provided
10.5.9 Lessons Learned Highlighted
10.5.10 Legal Considerations Ensured

| Element 10.6 | Utilize Ethical Hacking Techniques |
|---|---|

**Performance Criteria:**
10.6.1 High-level overview of the findings Provided.
10.6.2 Technical Details analysis of vulnerabilities and exploits detailed
10.6.3 Risk Assessed
10.6.4 Remediation Recommendations Suggested
10.6.5 Visual Aids Using charts, graphs, and screenshots to illustrated
10.6.6 Compliance Reporting provided
10.6.7 Peer Review performed
10.6.8 Actionable Insights Provided
10.6.9 Lessons Learned Highlighted
10.6.10 Legal compliance ensured

**Competences required in readiness for assessment.**
Demonstrate knowledge of:
Networking
Information/data security
Penetration testing
Exploitation
Ethical hacking methodologies

**Generic Skills**
Computer literacy
Analytical skills
Communication skills
Report writing skills
Research skills
Teamwork and collaboration
Time management
Problem-solving

## Range Statement:

**Tools and equipment**
Kali Linux
Metasploit Frameworks
Wireshark
NMap
Burp Suite
Docker
Virtual Environment

**Materials**
Stationery
Internet access
Workstations/Laptop
Forensic USB drives or external storage devices
Write blockers
Live Acquisition setup
Reference manuals

**Duration: 120 Hours**

## Assessment and Certification:

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 11**

| | |
|---|---|
| **Title:** | **Incident Response** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to detect, investigate, contain, eradicate, and recover from incidents such as data breaches, malware attacks, insider threats, and other cybersecurity events.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 11.1** | **Produce Incident Response Plan** |

**Performance Criteria:**

11.1.1 Incident Response Plan (IRP) developed.

11.1.2 Incident Response Team (IRT) with defined roles and responsibilities established.

11.1.3 Regular training and simulations (e.g., tabletop exercises) conducted.

11.1.4 Tools and technologies for monitoring, detection, and analysis identifiedAn up-to-date inventory of assets and systems maintained

| | |
|---|---|
| **Element 11.2** | **Identify and Detect Incident** |

**Performance Criteria:**

11.2.1 Systems and networks for unusual activity are monitored.

11.2.2 Tools like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) are used.

11.2.3 Logs, traffic, and user behavior for signs of compromise are analyzed.

11.2.4 Incident is validated and its severity is classified.

| Element 11.3 | Contain Incident |
|---|---|

**Performance Criteria:**

11.3.1 Affected systems or networks to prevent further damage isolated

11.3.2 Temporary fixes to allow systems to operate safely while investigation continues applied

11.3.3 Evidence (for forensic analysis) preserved

| Element 11.4 | Eradicate Incident |
|---|---|

**Performance Criteria:**

11.4.1 Malware, unauthorized access removed

11.4.2 Vulnerabilities patched and software are updated

11.4.3 Affected systems are cleaned and restored

| Element 11.5 | Recover from incident |
|---|---|

**Performance Criteria:**

11.5.1 Systems are rebuilt and reconfigured

11.5.2 Systems are tested

11.5.3 Systems reintegrated into the production environment

| Element 11.6 | Document lessons learned |
|---|---|

**Performance Criteria:**

11.6.1 Post-incident review done

11.6.2 The incident response plan is updated based on lessons learned.

11.6.3 Findings are shared with stakeholders

11.6.4 Incident document produced

**Competences required in readiness for assessment.**

Demonstrate knowledge of:
Programming skills
Knowledge of DBMS's
Knowledge of backup & recovery methods
Knowledge of Structured Query Languages
Knowledge of database connectivity
Knowledge in database security
Knowledge of conceptual modeling

**Generic Skills**
Computer literacy
Problem solving

**Range Statement:**

**Tools and equipment**
Computer hardware and software (DBMS)

**Materials**
Stationery
Internet access
Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 12**

| | |
|---|---|
| **Title:** | **Legal Aspects in Digital Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to apply the legal principles, regulations, and ethical considerations that govern digital forensics investigations.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 12.1** | **Adhere to Data Privacy Laws** |

**Performance Criteria:**

12.1.1 Consent for data collection and processing obtained.
12.1.2 Data minimization and purpose limitation implemented.
12.1.3 Data subject rights ensured.
12.1.4 Data breaches reported within mandated timeframes.
12.1.5 Data Protection Impact Assessments (DPIAs) conducted.

| | |
|---|---|
| **Element 12.2** | **Maintain Chain of Custody** |

**Performance Criteria:**

12.2.1 Events Recorded
12.2.2 Data Storage Secured
12.2.3 Cryptographic Hashing used
12.2.4 Access Logs maintained
12.2.5 Tamper-evident seals used
12.2.6 Secure transportation of evidence ensured.
12.2.7 Regularly Verification of evidence integrity conducted.
12.2.8 Audit Trails maintained

12.2.9 Legal standards for admissibility ensured.
12.2.10 Expert Testimony prepared

| Element 12.3 | Produce Admissible Evidence Handling |
|---|---|

**Performance Criteria:**
12.3.1 Forensic Imaging Created
12.3.2 Write-Blocking: Used
12.3.3 Metadata Preserved
12.3.4 Legal Authority Obtained
12.3.5 Documentation done
12.3.6 Findings validated using multiple tools or methods.
12.3.7 Certified forensic experts are used to present evidence.
12.3.8 Chain of Custody Maintained
12.3.9 Standards Compliance ensured
12.3.10 Court Presentation Prepared

| Element 12.4 | Apply Cybersecurity Regulations |
|---|---|

**Performance Criteria:**
12.4.1 Regular risk assessments are conducted.
12.4.2 Access controls and encryption implemented.
12.4.3 Network activity Monitored and logged.
12.4.4 Test incident response plans developed.
12.4.5 Employees trained on cybersecurity best practices.

| Element 12.5 | Notify Incident Response and Breach |
|---|---|

**Performance Criteria:**
12.5.1 Incident response plan developed.
12.5.2 Breaches Identified and contained.
12.5.3 Affected individuals and regulators notified.
12.5.4 Post-incident reviews conducted.
12.5.5 Policies and procedures based on lessons learned updated.

**Competences required in readiness for assessment.**
Demonstrate knowledge of:

- Knowledge of cloud models, storage, security threats, and regulations
- Cloud evidence acquisition and forensic tool proficiency
- Cloud log analysis, data recovery, and threat mitigation
- Forensic investigation, chain of custody, and incident response

- Understanding of cloud provider policies and forensic standards (ISO, NIST)
- Knowledge of conceptual modeling

**Generic Skills**

- Critical thinking
- Problem-solving
- Communication
- Research skills
- Analytical skills
- Attention to detail
- Incident management
- Report writing
- Time management
- Ethical decision-making

**Range Statement:**

**Tools and equipment**

- Computer hardware and software
- Cloud forensic tools (FTK, Autopsy)
- Network analysis tools (Wireshark)
- Log analysis tools
- Secure storage devices

**Materials**

- Stationery
- Storage media (USB drives, external hard drives)
- Secure evidence bags
- Documentation templates
- Internet access
- Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 15**

| | |
|---|---|
| **Title:** | **Memory Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Information & Communication Technology**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to identify, acquire, analyze and interpret volatile memory artifacts to detect security threats, uncover malicious activities and support digital investigations.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 15.1** | **Demonstrate knowledge of memory forensics concepts and principles** |

**Performance Criteria:**

15.1.1 Purpose and importance of memory forensics in digital investigations captured

15.1.2 Structure and organization of volatile memory (RAM) described.

15.1.3 Types of data that can be extracted from memory identified.

| | |
|---|---|
| **Element 15.2** | **Acquire Memory** |

**Performance Criteria:**

15.2.1 Appropriate tools utilized to capture memory.

15.2.2 Integrity of memory dumps using hashing algorithms ensured.

15.2.3 Memory acquisition process, including timestamps and system state documented.

| | |
|---|---|
| **Element 15.3** | Analyse memory |

**Performance Criteria:**

15.3.1 Memory analysis tools utilized

15.3.2 Running processes, hidden processes, and injected code identified.
15.3.3 Network connections and open sockets to detect suspicious activity analyzed.
15.3.4 Artifacts such as registry keys, passwords, and encryption keys extracted and interpreted.

| Element 15.4 | Detect and analyse malware present in memory |
|---|---|

**Performance Criteria:**
15.4.1 Indicators of compromise (IOCs) related to malware in memory identified.
15.4.2 Static and dynamic analysis of malicious processes performed.
15.4.3 Behaviour and impact of malware found in memory documented.

| Element 15.5 | Apply advanced techniques to uncover sophisticated threats |
|---|---|

**Performance Criteria:**
15.5.1 Rootkits and kernel-level malware using memory analysis detected.
15.5.2 Memory artifacts from virtual machines and cloud environments analyzed.
15.5.3 Attacker activities reconstructed.
15.5.4 Anti-forensics techniques used by attackers detected and analyzed
15.5.5 Attempts to hide malicious activity in memory identified
15.5.6 Evidence from memory regions that have been intentionally corrupted or overwritten recovered.

| Element 15.6 | Utilize automated tools in memory forensics |
|---|---|

**Performance Criteria:**
15.6.1 Proficiency with tools demonstrated.
15.6.2 Open-source tools for supplementary analysis utilized.
15.6.3 Common issues encountered during memory acquisition and analysis diagnosed and resolved
15.6.4 Malicious artifacts removed and affected systems restored

| Element 15.7 | Provide Incident Response for memory forensics |
|---|---|

**Performance Criteria:**
15.7.1 Incidents that require memory forensics identified and contained.
15.7.2 Scope and impact of the incident assessed.
15.7.3 Live memory images captured.
15.7.4 Proper documentation for legal and regulatory considerations produced

**Competences required in readiness for assessment.**
Demonstrate knowledge of:
Programming skills
Principles and importance of memory forensics in digital investigations

Structure and organization of volatile memory
Memory acquisition skills
Memory analysis skills
Malware detection and analysis
Threat hunting techniques
Incident response for memory forensics
Troubleshooting
Report and documentation

**Generic Skills**
Computer literacy
Problem solving

**Range Statement:**

**Tools and equipment**
FTK Imager
DumpIt
Linux Memory Extractor
WinPMEM
Volatility framework
X_ways forensics
Redline
VirusTotal
Process explorer
PEStudio
RootKit Hunter
GMER
Hashing and integrity tools
Sleuth Kit (TSK)
SANS SIFT Workstation
Cuckoo Sandbox

**Materials**
Stationery
Internet access
Workstations/Laptop
Forensic USB drives or external storage devices
Write blockers
Live Acquisition setup
Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 16**

| | |
|---|---|
| **Title:** | **Mobile Device Forensics** |
| **Unit Code** | |

**ZQF level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to conduct forensic investigations on mobile devices.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 16.1** | **Demonstrate understanding of mobile device architecture** |

**Performance Criteria:**
16.1.1 Components of mobile devices identified.
16.1.2 Mobile operating systems distinguished.
16.1.3 Mobile devices file systems described.

| | |
|---|---|
| **Element 16.2** | **Apply Legal and Ethical Considerations** |

**Performance Criteria:**
16.2.1 Chain of custody procedures for mobile evidence followed.
16.2.2 Compliance with relevant laws and regulations ensured.
16.2.3 Proper authorization before accessing mobile data obtained.

| | |
|---|---|
| **Element 16.3** | **Acquire data on mobile devices** |

**Performance Criteria:**
16.3.1 Appropriate tools used to extract data.
16.3.2 Logical, physical, and file system acquisitions performed.
16.3.3 Write-blocking techniques to prevent data alteration followed.
16.3.4 Acquisition process documented.

| Element 16.4 | Extract and recover data |
|---|---|

**Performance Criteria:**

16.4.1 Deleted files, messages, and call logs recovered.
16.4.2 Data from apps extracted.
16.4.3 Specialized tools to bypass encryption or locked devices identified.

| Element 16.5 | Analyse data collected from mobile devices |
|---|---|

**Performance Criteria:**

16.5.1 Call logs, SMS, MMS, and email communications analysed.
16.5.2 GPS data and location history examined.
16.5.3 Data from multiple sources correlated to reconstruct events.
16.5.4 Patterns or anomalies in the data identified.

| Element 16.6 | Analyse malaware on mobile devices |
|---|---|

**Performance Criteria:**

16.6.1 Evidence of malware infection detected.
16.6.2 Static and dynamic analysis of suspicious apps performed.
16.6.3 Findings documented and provide recommendations for mitigation provided.

| Element 16.7 | Perform incidence response for mobile devices |
|---|---|

**Performance Criteria:**

16.7.1 Mobile-related security incidents are identified and contained.
16.7.2 Proper forensic collection of logs, files, and metadata from the affected mobile device ensured.
16.7.3 Remediation performed

**Competences required in readiness for assessment.**

Demonstrate knowledge of:
Programming skills
Knowledge of DBMS's
Knowledge of backup & recovery methods
Knowledge of Structured Query Languages
Knowledge of database connectivity
Knowledge in database security
Knowledge of conceptual modeling

**Generic Skills**

Computer literacy
Problem solving

**Range Statement:**

**Tools and equipment**
Computer hardware and software (DBMS)

**Materials**
Stationery
Internet access
Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 17**

| | |
|---|---|
| **Title:** | **Network Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Information & Communication Technology**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to investigate, analyze, and respond to network-based incidents.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 17.1** | **Capture Network Traffic** |

**Performance Criteria:**
17.1.1 Traffic packets captured using network tools
17.1.2 Relevant traffic Filtered and stored for further analysis.
17.1.3 Appropriate tools for capturing network traffic selected

| | |
|---|---|
| **Element 17.2** | **Analyse Network Packets** |

**Performance Criteria:**
17.2.1 Packet headers and payloads analyzed
17.2.2 Suspicious IP addresses, ports, or protocols Identified
17.2.3 Patterns of malicious behavior detected

| | |
|---|---|
| **Element 17.3** | **Analyse logs** |

**Performance Criteria:**
17.3. Anomalies in logs from multiple sources identified.
17.3.2 Unauthorized access or policy violations detected.
17.3.3 Timelines of events during an incident recorded.

| Element 17.4 | Perform Intrusion Detection and Prevention |
|---|---|

**Performance Criteria:**

17.4.1 Attack signatures detected

17.4.2 Intrusion detection systems (IDS) alerts generated and analyzed

17.4.3 False positives and validate true threats detected

| Element 17.5 | Analyse Malware Traffic |
|---|---|

**Performance Criteria:**

17.5.1 Command-and-control (C2) communications detected

17.5.2 DNS queries and HTTP requests for malicious domains analyzed

17.5.3 Data Exfiltration Attempts Detected

| Element 17.6 | Analyse Network Flow |
|---|---|

**Performance Criteria:**

17.6.1 Flow data collected

17.6.2 Unusual traffic patterns detected

17.6.3 Potential botnet activity or data breaches detected

| Element 17.7 | Respond to network incidents |
|---|---|

**Performance Criteria:**

17.7.1 Affected systems Isolated to prevent further damage

17.7.2 Evidence for forensic analysis preserved

17.7.3 Normal operations restored and preventive measures implemented

| Element 17.8 | Enforce Legal Compliance |
|---|---|

**Performance Criteria:**

17.8.1 Chain-of-custody procedures for evidence followed.

17.8.2 Data privacy and compliance with laws done/ensured.

17.8.3 Forensic reports for use in legal proceedings prepared.

| Element 17.9 | Reconstruct Network |
|---|---|

**Performance Criteria:**

17.9.1 Network sessions and transactions recreated.

17.9.2 Attack vector and methods used by the attacker identified.

17.9.3 Scope and impact of the incident determined.

| Element 17.10 | Integrate Threat Intelligence |
|---|---|

**Performance Criteria:**

17.10.1 Threat feeds to identify known malicious IPs, domains, or hashes incorporated
17.10.2 Network traffic for indicators of compromise (IoCs) analyzed.
17.10.3 Emerging threats and attack techniques updated.

| Element 17.11 | Produce reports and documentation |
|---|---|

**Performance Criteria:**

17.11.1 Detailed forensic reports prepared.
17.11.2 Timelines, evidence, and analysis indicated.
17.11.3 Recommendations for improving network security provided

**Competences required in readiness for assessment.**

Demonstrate knowledge of:
Networking
Network forensics
OS and file system analysis
Threat intelligence and Incident response
Packet and log analysis skills
Scripting and automation

**Generic Skills**

Computer literacy
Teamwork and communication
Ethical conduct and integrity
Research skills
Problem solving

**Range Statement:**

**Tools and equipment**

Wireshark
tcpdump
nMap
Tshark
Snort
Splunk
Sysmon

**Materials**

Stationery
Internet access
Gloves, Faraday bags

PPE
Sandboxing tools
Routers, switches, hubs, backup disks, disk drivers
Reference manuals

**Duration: 120 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**Unit 18**

| | |
|---|---|
| **Title:** | **Operating System (OS) Forensics** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **12**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

This unit will enable an individual to analyze and investigate digital evidence related to computer operating systems.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 18.1** | **Analyse image** |

**Performance Criteria:**

18.1.1 File Metadata Analyzed
18.1.2 Deleted File Recovered
18.1.3 File Carving performed
18.1.4 Hidden Files Detected
18.1.5 File Integrity Checked
18.1.6 File System Artifacts analyzed
18.1.7 Encrypted Files: Identified
18.1.8 File Permissions reviewed
18.1.9 File System Logs analyzed
18.1.10 File System Type Analysed

| | |
|---|---|
| **Element 18.2** | **Perform memory forensics** |

**Performance Criteria:**

18.2.1 Snapshot of the system's memory captured.
18.2.2 Process identified
18.2.3 Dll injection detected
18.2.4 Network connections identified

18.2.5 Rootkit detected.
18.2.6 Artifact extracted
18.2.7 Timeline analysed
18.2.8 Malware unpacked
18.2.9 Registry analysed

| Element 18.3 | Analyse logs |
|---|---|

**Performance Criteria:**
18.3.1 Event Logs Analyzed
18.3.2 Login Attempts identified
18.3.3 Account Changes detected
18.3.4 Service Activity reviewed
18.3.5 File Access Logs tracked
18.3.6 Firewall Logs Analyzed
18.3.7 Antivirus Logs Reviewed.
18.3.8 Application Logs Examined.
18.3.9 Log Tampering Detected.
18.3.10 Correlation Analysis performed.

| Element 18.4 | Analyse user activity |
|---|---|

**Performance Criteria:**
18.4.1 Login History tracked
18.4.2 File Access identified
18.4.3 Command History reviewed.
18.4.4 Browser History Analyzed.
18.4.5 USB Device Usage Tracked
18.4.6 Printer Activity Monitored
18.4.7 Clipboard Data Extracted
18.4.8 Scheduled Tasks Reviewed
18.4.9 Remote Desktop Activity Detected
18.4.10 Application Usage Identified

| Element 18.5 | Analyse system registry |
|---|---|

**Performance Criteria:**
18.5.1 Registry Hive Analysed
18.5.2 Startup Programs identified
18.5.3 User Activity tracked
18.5.4 Malware Persistence detected
18.5.5 Shellbags analyzed

18.5.6 Uninstalled Programs Identified
18.5.7 Time Stomping Detected
18.5.8 Browser Artifacts Extracted
18.5.9 Network Settings: Reviewed
18.5.10 Registry Backup Analyzed

| Element 18.6 | Analyse malaware on operating systems |
|---|---|

**Performance Criteria:**
18.6.1 Malware Detected
18.6.2 Behavioural Analysis in a Controlled Environment Done
18.6.3 Persistence Mechanisms Detected
18.6.4 Malware's communication with C2 servers monitored and identified.
18.6.5 File System Changes Tracked
18.6.6 Privilege Escalation Detected
18.6.7 Anti-Forensic Techniques Identified.
18.6.8 Payload Extracted
18.6.9 Rootkit Detected
18.6.10 Impact evaluated

| Element 18.7 | Analyse timeline |
|---|---|

**Performance Criteria:**
18.7.1 Event Correlation performed
18.7.2 Timeline of events leading up to and during the incident noted.
18.7.3 Anomaly Detected
18.7.4 Initial entry point and attack vector Identified.
18.7.5 Scope and impact of the incident assessed.
18.7.6 Graphs or charts put in place to represent the timeline.
18.7.7 Timelines from multiple systems Cross-referenced/compared.
18.7.8 Time Stomping Detected
18.7.9 Historical Analysis performed
18.7.10 Timelines used in Reports generation

| Element 18.8 | Produce documentation and reports |
|---|---|

**Performance Criteria:**
18.8.1 High-level overview of the incident provided.
18.8.2 Detailed analysis of the evidence provided
18.8.3 Visual Aids utilized
18.8.4 Indicators of compromise for detection IOCs listed

18.8.5 Mitigation Strategies recommend
18.8.6 Legal Considerations ensure
18.8.7 Peer Review done
18.8.8 Actionable Recommendations Suggested

**Competences required in readiness for assessment.**

**Demonstrate knowledge of:**

Understanding of OS fundamentals
File system and data management skills
Memory management techniques
Memory management techniques
Process management and scheduling skills
Troubleshooting in OS issues
Security and permission management skills
OS configuration skills
OS installation and updating skills
Scripting and automation skills

**Generic Skills**

Computer literacy
Problem-solving
Time management
Communication skills
Teamwork
Research skills

**Range Statement:**

**Tools and equipment**

Computer hardware and software (DBMS)
Task manager
System monitor
Resource monitor
Disk manager
CHKDSK
Process explorer
Virtual Box
Docker

**Materials**

Stationery
Internet access
Reference manuals

**Duration: 120 Hours**

## Assessment and Certification:

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

**UNIT 19**

| | |
|---|---|
| **Title** | **Research Methods** |
| **Unit Code** | |

**ZQF Level:** **National Diploma**

**Credits:** **20**

**Occupation:** **Digital Forensics Technician**

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**Aim/purpose of the unit standard**

The aim of this module is to provide the student with a range of theoretical and practical skills required to carry out research and manage projects in a specified area appropriate in business analytics.

**ELEMENTS AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 19.1** | **Explain the concept of research** |

**Performance Criteria:**
19.1.1 Research is explained.
19.1.2 Different types of research are described.
19.1.3 Steps in the research process are described.

| | |
|---|---|
| **Element 19.2** | **Collect and analyse business data** |

**Performance Criteria:**
19.2.1 Sampling methods are described.
19.2.2 Data collection methods are explained.
19.2.3 Data analysis is conducted.

| | |
|---|---|
| **Element 19.3** | **Perform hypothesis testing** |

**Performance Criteria:**
19.3.1 Probabilities are calculated using discrete and continuous probabilities.
19.3.2 Correct hypothesis test based on data type and research objective selected
19.3.3 Clear and testable hypotheses for real-world scenarios developed

19.3.4 Hypotheses are tested.

| Element 19.4 | Apply project management skills |
|---|---|

**Performance Criteria:**
19.4.1 Project plan is produced.
19.4.2 Project financial implications are produced.
19.4.3 Project schedule is generated.
19.4.4 Project is executed.
19.4.5 Project is monitored and controlled.
19.4.6 Project management software is implemented.

| Element 19.5 | Apply innovation skills |
|---|---|

**Performance Criteria:**
19.5.1 Innovation is explained.
19.5.2 Innovation process is discussed.
19.5.3 Design thinking principles to develop user-centric innovations applied

**Competences required in readiness for assessment.**
Demonstrate knowledge of:
Computer networking
Software development skills
Computer hardware
Knowledge in scripting languages
Knowledge in Search engine optimization
Knowledge in file transfer protocol
Knowledge in different development environments

**Generic Skills**
Computer literacy
Problem solving
Interpersonal skills

**Range Statement:**

**Tools and equipment**
Computer Hardware and software
Project management tools, e.g. PMBOK
Project scheduling software

**Materials**
Stationery

Internet access
Reference manuals

**Competences required in readiness for assessment**

Demonstrate knowledge of:
Different programming languages
Programming skills
Knowledge of systems methodology
Design and modelling skills

**Generic Skills**

Computer literacy
Communication
Research skills
Management skills
Innovativeness
Interpersonal skills

**Range Statement:**
**Tools and equipment**

Computer hardware and software
Cameras
Scanners
LCD Projector

**Materials**

Stationery
Internet Access

**Duration: 200 Hours**

**Assessment and Certification:**

In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors.

**UNIT 18**

| | |
|---|---|
| **Unit Code** | |
| **Unit Title:** | **Entrepreneurship skills development** |

**Level of Unit:** **National Certificate**

**Credits:** **4**

**Occupation:** ***Records and Information Clerk***

**Date of Promulgation:** **TBA**

**Review Date:** **TBA**

**AIM OF THE UNIT STANDARD**

This unit provides learners with the knowledge, skills, and attitudes needed to recognize business opportunities, develop and execute business plans, and register and operate enterprises ethically and sustainably in dynamic market environments.

**ELEMENT AND PERFORMANCE CRITERIA**

| | |
|---|---|
| **Element 1.1** | **Develop a business plan** |

**Performance Criteria:**

1.1.1 Business concept clearly defined

1.1.2 Comprehensive market research conducted

1.1.3 Marketing strategy clearly outlined

1.1.4 Operational plan developed

1.1.5 Organizational structure established

1.1.6 Financial projections completed

1.1.7 Risk management strategies defined

1.1.8 Sustainability and social impact addressed

1.1.9 Plan is investment-ready or bankable

| | |
|---|---|
| **Element 1.2** | **Formalise a business** |

**Performance Criteria:**

1.2.1 Business structure appropriately selected

1.2.2 Certificate of incorporation or registration obtained

1.2.3 Basic record-keeping systems established

1.2.4 Awareness of legal and regulatory obligations demonstrated

1.2.5 Benefits of formalisation articulated

| Element 1.3 | Manage a Business |
|---|---|

**Performance Criteria:**

1.3.1 Manage a business according to organisation policy
1.3.2 Develop business strategies to ensure effectiveness
1.3.3 Allocate resources according to line of business
1.3.4 Cost products in line with procedures
1.3.5 Price products according to company procedures
1.3.6 Update and maintain records
1.3.7 Control stock in line with organisation requirements
1.3.8 Design day-to-day business processes
1.3.9 Formulate market plans including sales and marketing plans
1.3.10 Manage risks in line with organisation requirements
1.3.11 Observe business ethics and social responsibility
1.3.12 Apply customer care tips
1.3.13 Motivate employees in line with organisational requirements
1.3.14 Formulate standard operating procedures
1.3.15 Compile rules and procedures for the business

| Element 1.4 | Optimize the Business |
|---|---|

**Performance Criteria:**

1.4.1 Analyze business performance to determine growth
1 4.2 Identify business process improvement areas
1.4.3 Develop strategies for enhanced customer care
1.4.4 Evaluate market expansion opportunities
1.4.5 Evaluate resource allocation
1.4.6 Monitor market trends
1.4.7 Track performance indicators (KPIs)
1.4.8 Formulate strategies for sustainable growth and scalability
1.4.9 Maintain records
1.4.10 Develop business continuity plans

**COMPETENCIES REQUIRED IN READINESS FOR ASSESSMENT:**

Accounting skills
Record keeping
Customer care skills
Management skills
(decision making,
planning,
organising)
Marketing skills
Business conduct
Legal awareness
Mobilisation skills
Self-Supervision
Patriotism
Environmental awareness (PESTEL)

**GENERIC SKILLS:**

Creativity
Sense of initiative
Ability to Marshall Resources
Technological knowledge
Communication
Planning
Organization
Controlling

**RANGE STATEMENT:**

**Tools and Equipment**

Filing trays Filing
cabinets Filing racks Pigeon holes
Franking machine
Guillotine Scale Scissors
Date stamp and ink Punch

**Materials**

Postage stamps
Action packs Mail
Registers Envelopes
Stamp pad ink
Correction fluid
Bond paper Pens

**Duration:** 40 hours

**ASSESSMENT AND CERTIFICATION:**
In order to gain credits for this unit standard, a candidate must be assessed and demonstrate competency in all the elements and performance criteria of this unit standard.

Assessment will be conducted by accredited assessors. The results of the assessment will be submitted to ZIMEQA. A candidate can apply to ZIMEQA for documentary evidence of their achievements.

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

INDUSTRY: COMMERCE | TRADE/ OCCUPATION: DIGITAL FORENSIC TECHNICIAN | CLASS/LEVEL: NATIONAL DIPLOMA

**DUTY A: INVESTIGATE CYBERSECURITY INCIDENTS**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **A1: Identify the incident** | i. Monitor logs and alerts<br>ii. Note indicators of compromise<br>iii. Verify alerts | ➢ Incident/ activity type indicated<br>➢ Log-in attempts noted<br>➢ Suspicions/ odd IP address noted<br>➢ Unauthorized file transfers identified | • Digital Forensics & Incident Response (DFIR)<br>• Malware Analysis & Reverse Engineering<br>• Network Security & Traffic Analysis<br>• Threat Intelligence & SIEM<br>• Penetration Testing and Vulnerability Assessment<br>• Cloud Security and Multi-Cloud Forensics<br>• Analytical & Problem-Solving Skills<br>• Programming and Scripting<br>• Legal and Compliance | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management |
| **A2: Contain the incident** | i. Isolate affected system<br>ii. Disable compromised account/ reset credentials<br>iii. Block malicious IP addresses/ domains/ processes<br>iv. Monitor secondary attacks | ➢ Affected systems disconnected from networks<br>➢ Malicious IPs, domains or processes blocked<br>➢ Compromised accounts/ reset/ credentials disabled<br>➢ Follow-up | | |

| | | | | |
|---|---|---|---|---|
| | | attempts listed | Knowledge<br>• Communication and Reporting | |
| **A3: Collect evidence** | i. Preserve the scene/ device<br>ii. Capture volatile data<br>iii. Switch off the machine<br>iv. Image the device | ➢ Device/ Scene secured according to SOPs.<br>➢ Volatile data captured<br>➢ Machine/ device switched off<br>➢ Device imaged<br>➢ Device disconnected from network | | |
| **A4: Analyse evidence** | i. Determine attack vectors<br>ii. Identify exploited vulnerabilities<br>iii. Trace attack timelines | ➢ Attack vectors determined<br>➢ Network traffic analyzed<br>➢ Vulnerability scanning reports provided<br>➢ System and application logs provided<br>➢ Penetration testing reports provided<br>➢ Threat intelligence reports provided<br>➢ Analytical vector diagrams provided | | |

| | | | | |
|---|---|---|---|---|
| | | ➢ Exploited vulnerabilities identified<br>➢ Software vulnerabilities identified<br>➢ Hardware vulnerabilities identified<br>➢ Configuration vulnerabilities identified<br>➢ Human vulnerabilities identified<br>➢ Attack timelines noted. | | |
| **A5: Eradicate the incident** | i. Remove malware from the compromised system<br>ii. Patch vulnerabilities exploited/ reconfigure systems<br>iii. Restore compromised systems<br>iv. Scan hidden threats<br>v. Monitor for re-occurrence | ➢ Specialized malware removal tool utilized<br>➢ Effected system isolated<br>➢ Malicious file deleted<br>➢ Registry changes reset system updated<br>➢ Unknown user deleted<br>➢ System restored<br>➢ System reconfigured<br>➢ Hidden threats scanned | | |
| **A6: Generate a report** | i. Gather case details<br>ii. Document findings<br>iii. Describe actions taken<br>iv. Recommend preventive measures | ➢ Case details gathered<br>➢ Case details documented<br>➢ Incident identified<br>➢ Incident contained<br>➢ System restored<br>➢ Antivirus installed | | |

| | | | | |
|---|---|---|---|---|
| | | ➢ Anti malware installed<br>➢ Intrusion detection/ intrusion prevention systems installed<br>➢ Firewalls installed | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**

Forensic Workstations
Write Blockers
Autopsy / Sleuth Kit
EnCase –
Splunk / ELK Stack
Metasploit
AWS Security Hub / Azure Security Center
Prisma Cloud / Dome9
GPG (GnuPG)
Hash-cat
John the Ripper
Cellebrite UFED
Magnet AXIOM
Oxygen Forensics

**MATERIALS**

Stationery
Cartridges
Bond paper

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**

Physical harm
Electrical shock
Fire hazards

Eye strain and fatigue
Mentalhealth
Sedentary work
Electronic waste
Energy consumption
Data center environmental impact
Follow safety protocols
Take regular breaks to reduce eye strain
Implement sustainable practices
Provide mental health support
Conduct environmental impact assessments

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

INDUSTRY: COMMERCE | TRADE/ OCCUPATION: DIGITAL FORENSIC TECHNICIAN | CLASS/ LEVEL: NATIONAL DIPLOMA

**DUTY B: PROVIDE EXPERT TESTIMONY**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **B1: Prepare for testimony** | i. **Review the case**<br>ii. **Re-examine findings**<br>iii. **Anticipate** | ➢ All evidence, reports, and findings are thoroughly examined.<br>➢ Potential gaps or | • Marketing<br>• Creative Art and Design | • Computer literacy<br>• Communication<br>• Organizing |

| | | | | |
|---|---|---|---|---|
| | **questions** | inconsistencies in the evidence are identified and addressed.<br>➢ Familiarity with courtroom procedures and rules of evidence is demonstrated.<br>➢ Visual aids (e.g., charts, diagrams, slides) are created and align with the evidence.<br>➢ A list of potential questions from both prosecution and defence is prepared. | • Salon Management<br>• Business ethics<br>• Continuous Learning<br>• Case Law and Precedents<br>• Technical Knowledge<br>• Cybersecurity<br>• Digital Forensics | • Analytical<br>• Planning<br>• Creative<br>• Time management |
| **B2: Conduct pre-trial meeting** | i. **Meet with legal teams**<br>ii. **Clarify technical concepts**<br>iii. **Practice testimony**<br>iv. **Illustrate technical concepts** | ➢ A meeting is scheduled<br>➢ An agenda is prepared and shared<br>➢ Key evidence and findings are aligned with the legal team's goals<br>➢ Questions from the legal team are addressed<br>➢ Complex technical concepts are explained in simple, non-technical language.<br>➢ Visual aids (e.g., diagrams, charts, slides) are used to illustrate technical concepts<br>➢ Key technical explanations are documented and shared<br>➢ Mock question and answer sessions are conducted<br>➢ Challenging or adversarial | | |

| | | | | |
|---|---|---|---|---|
| | | questions are handled | | |
| **B3: Provide courtroom testimony** | i. Present findings<br>ii. Answer questions pertaining to findings<br>iii. Utilize visual aids. | ➢ Findings presented<br>➢ Questions answered<br>➢ Charts utilized<br>➢ Diagrams used<br>➢ Screenshots utilized | | |
| **B4: Defend Analysis** | **i. Explain methodology**<br>**ii. Address Challenges** | ➢ Methodologies explained<br>➢ The tools and techniques used are justified<br>➢ Challenges addressed<br>➢ Industry best practices and standards are referenced | | |
| **B5: Conduct post-trial Follow-up** | **i. Provide Additional Information**<br>**ii. Maintain Records** | ➢ Additional information is provided<br>➢ Filing system established<br>➢ Records are updated<br>➢ Digital records are encrypted<br>➢ Physical records are kept in a secure location<br>➢ Index or catalog of records is maintained<br>➢ Records are retained for the required duration<br>➢ Records destroyed in compliance with legal | | |

| | | | | |
|---|---|---|---|---|
| | | provisions<br>➢ Physical records are duplicated or digitized for redundancy | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
EnCase, FTK, Autopsy, Cellebrite, X-Ways Forensics, Microsoft PowerPoint, Tableau, Lucidchart, Forensic Blogs and Forums, Microsoft Word, Adobe Acrobat, LaTeX, Zoom/Teams, Google Workspace/Microsoft 365, Westlaw/LexisNexis, Google Scholar, Write-Blockers and Storage Devices, Laptop/Tablet, Encrypted Storage USB,

**Materials**
Non-Disclosure Agreements (NDAs), Rules of evidence, case law, glossary of terms, professional certifications, Expert witness report, supporting documents, notes, legal subpoenas.

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Wear protective clothing (PPEs), safety gloves, electro-static strips, Air conditioner, Noise sensors, Lighting

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**

Knowledge of Network Security & Digital Forensics
Attention to Detail
Critical Thinking
Ability to Explain Technical Concepts Clearly
Public Speaking & Confidence
Strong Report Writing Skills
Confidentiality & Discretion
Adaptability & Quick Thinking

| | | | |
|---|---|---|---|
| | **MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE & TECHNOLOGY DEVELOPMENT**<br><br>**SKILLS PROFICIENCY SCHEDULE** | | **CODE** |

| INDUSTRY: | TRADE/ OCCUPATION | CLASS/ LEVEL: |
|---|---|---|
| COMMERCE | DIGITAL FORENSIC TECHNICIAN | NATIONAL DIPLOMA |

**DUTY C: SYSTEM SECURITY AUDIT**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **C1:** Gather System Information | i. Collect System Overview<br>ii. Identify Hardware components<br>iii. Analyze Software configuration:<br>iv. Review Network Settings | i. System information collected<br>ii. Hardware components identified<br>iii. System settings and configurations reviewed<br>iv. User accounts privileges | • Communication<br>• Security Frameworks and Standards<br>• Networking and Network Security | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative |

| | | | | |
|---|---|---|---|---|
| | v. Check user accounts and privileges<br>vi. Document system information | checked<br>v. Audit documentation availed | • Operating System Security<br>• Vulnerability and Risk Management<br>• Identity and Access Management (IAM)<br>• Cryptography and Data Protection<br>• Logging, Monitoring, and Incident Response<br>• Penetration Testing and Ethical Hacking<br>• Cloud Security and Multi-Cloud Auditing<br>• Compliance and Legal Knowledge | • Time management<br>• Selling |
| **C2:** Scan Vulnerability | i. Select vulnerability scanning tools<br>ii. Run vulnerability scans<br>iii. Identify vulnerabilities<br>iv. Analyze findings<br>v. Generate a vulnerability report | i. Tools selected<br>ii. Scan type identified<br>iii. Scan settings configured<br>iv. Vulnerabilities identified<br>v. Findings analyzed<br>vi. Vulnerability report availed | | |
| **C3: Check** Backup Security | i. Review backup policies and procedures<br>ii. Check encryption<br>iii. Validate backup integrity<br>iv. Assess backup storage security<br>v. Review backup logs<br>vi. Generate a backup security report | i. Backup procedures noted<br>ii. Encryption identified<br>iii. Backup integrity validated<br>iv. Storage security assessed<br>v. Backup logs reviewed<br>vi. Backup security report produced | | |
| **C4:** Evaluate Compliance | i. Identify applicable regulations and standards<br>ii. Check system and data protection Controls<br>iii. Analyse logging and monitoring<br>iv. Evaluate data privacy measures<br>v. Verify incident response procedures | i. Regulations and standards noted<br>ii. Protection protocols identified<br>iii. Patterns, trends and anomalies identified<br>iv. Data protection measure outlined<br>v. Compliance report generated | | |

| | | | | |
|---|---|---|---|---|
| | vi. Generate a compliance report | | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**

Nessus,
OpenVAS
Splunk,
Metasploit
Burp Suit
EnCase
FTK (Forensic Toolkit) Wire shark
Microsoft Word, Excel,
Printer
Computer
Communication gadgets
Fax machine
Internet facility
Cameras

**MATERIALS**

Stationery
Cartridges
Bond paper

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**

Ventilation
Personal Protective Clothing
Sufficient lighting
First Aid Kit
Fire Fighting Equipment

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**

Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter
Attention to Detail
Analytical Thinking
Confidentiality
Adaptability
Technical Proficiency

| | | | |
|---|---|---|---|
| | **MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT**<br><br>**SKILLS PROFICIENCY SCHEDULE** | | **CODE** |

| | | |
|---|---|---|
| INDUSTRY:<br>COMMERCE | TRADE/ OCCUPATION:<br>DIGITAL FORENSIC TECHNICIAN | CLASS/ LEVEL:<br>NATIONAL DIPLOMA |

**DUTY D: RESEARCH ON DIGITAL AND CYBERSECURITY TRENDS**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **D1:** Identify emerging cyber threats | i. Research current threats<br>ii. Monitor cybersecurity news and reports<br>iii. Track malware and ransomware trends<br>iv. Summarize findings<br>v. Produce a report | i. Cybersecurity threat intelligence platforms visited<br>ii. Cybersecurity news and reports monitored<br>iii. Recent ransomware attacks noted<br>iv. Findings compiled and summarized<br>v. Research reports availed | • Communication<br>• Cybersecurity Knowledge<br>• Threat Intelligence & OSINT Skills<br>• Research & Analytical Skills<br>• Hands-on Security | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management<br>• Selling |

| | | | | |
|---|---|---|---|---|
| **D2:** Explore digital forensics tools | i. Set up a forensics environment<br>ii. Acquire a forensic image<br>iii. Analyze artifacts<br>iv. Compare tools and document Findings | i. Forensics environment and software installed<br>ii. Extracted dumps availed<br>iii. Tool based reports provided<br>iv. Tools comparison reports prepared. | Tools & Techniques<br>• Programming & Scripting Skills<br>• Cloud & Multi-Cloud Security Expertise<br>• Communication & Reporting Skills<br>• Legal & Compliance Awareness | |
| **D3:** Evaluate AI in Forensics | i. Conduct research AI applications in forensics<br>ii. Perform an AI-Based forensic test<br>iii. Compare AI vs. traditional methods<br>iv. Summarize AI's role in digital forensics | i. Advantages and limitations of various AI tools outlined<br>ii. Findings with supporting screenshots, logs, or reports availed<br>iii. Structured comparison provided<br>iv. AI's contribution to data processing, predictive analysis, and automation in forensic cases indicated | | |
| **D4:** Develop Cybersecurity Awareness Programs | i. Identify target audience<br>ii. Create training materials<br>iii. Conduct training<br>iv. Measure effectiveness | i. Employees, students, or general users identified<br>ii. Phishing, password security, malware, social engineering, and safe browsing habits discussed.<br>iii. PowerPoint presentation prepared<br>iv. Phishing simulated<br>v. Real-world cyberattack case study illustrated<br>vi. Post-training surveys conducted<br>vii. follow-up security test through | | |

| | | | | |
|---|---|---|---|---|
| | | phishing simulation performed. | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
Laptop/Workstation
External Hard Drive/Cloud Storage
Shodan
VirusTotal
AlienVault Open Threat Exchange (OTX)
Nessus
OpenVAS
Metasploit Framework
TOR Browser
ChatGPT/Bard
MITRE ATT&CK Navigator
ELK Stack
AWS Security Hub, Azure Security Center, Google Security Command Center
Microsoft OneNote/Evernote
Jupyter Notebook
Maltego

**MATERIALS**
Stationery
Cartridges
Bond paper

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Ventilation

Personal Protective Clothing
Sufficient lighting
First Aid Kit
Fire Fighting Equipment

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter
Attention to Detail
Analytical Thinking
Confidentiality
Adaptability
Technical Proficiency

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

| INDUSTRY: | TRADE/ OCCUPATION: | CLASS/ LEVEL: |
|---|---|---|
| COMMERCE | DIGITAL FORENSIC TECHNICIAN | NATIONAL DIPLOMA |

**DUTY E: ENSURE WORKPLACE SAFETY**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **E1: Identify Potential Hazards** | i. Conduct a risk assessment to identify potential hazards.<br>ii. Inspect work areas, equipment, and procedures for safety risks.<br>iii. Engage employees to | i. Potential hazards identified<br>ii. Work area, equipment and procedures audited.<br>iii. Hazards and safety concerns are reported.<br>iv. Past incidents reviewed.<br>v. Compliance with | ➢ Communication<br>➢ Marketing<br>➢ Creative Art and Design<br>➢ Salon Management<br>➢ Business ethics | ➢ Computer literacy<br>➢ Communication<br>➢ Organizing<br>➢ Analytical<br>➢ Planning<br>➢ Creative<br>➢ Time management<br>➢ Selling |

| | | | | |
|---|---|---|---|---|
| | report hazards and safety concerns.<br>iv. Review past incident reports to identify recurring issues.<br>v. Ensure compliance with workplace safety regulations | workplace safety regulations ensured | | |
| **E2: Develop and Implement Safety Policies** | i. Craft Safety Policies<br>ii. Enforce safety policies and standard operating procedures (SOPs).<br>iii. Maintain safety equipment.<br>iv. Ensure proper signage and hazard warnings are in place.<br>v. Implement emergency response plans and evacuation drills.<br>vi. Monitor compliance with safety protocols through audits and spot checks. | i. Safety policies crafted<br>ii. Safety equipment serviced.<br>iii. Emergency plan created<br>iv. Signage and hazard warnings are put in place.<br>v. Conducted evacuation drills<br>vi. Spot checks implemented | | |
| **E3: Provide Safety Training & Awareness** | i. Organize regular safety training sessions for employees.<br>ii. Provide specialized training for high-risk tasks (e.g., machinery operation, fire safety). | i. Training sessions conducted.<br>ii. Fire drills conducted<br>iii. Safety manuals crafted.<br>iv. Safety manuals and instructional materials distributed. | | |

| | | | | |
|---|---|---|---|---|
| | iii. Distribute safety manuals and instructional materials.<br>iv. Conduct safety quizzes or drills to reinforce learning.<br>v. Encourage a culture of safety awareness and reporting. | v. Safety quizzes reinforced. | | |
| **E4: Monitor Workplace Conditions** | i. Conduct Regular Safety Inspections<br>ii. Use Monitoring Tools and Equipment<br>iii. Track Employee Safety and Compliance<br>iv. Maintain Incident and Near-Miss Reports<br>v. Respond to Identified Risks. | i. Safety Inspections conducted<br>ii. Tools and equipment assessed<br>iii. Identified risk attended.<br>iv. CCTV installed<br>v. air quality sensors installed<br>vi. Lighting improved | | |

**TOOLS, MATERIALS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**

EnCase, Autopsy, FTK (Forensic Toolkit).
Wireshark, Kali Linux
SIEM Solutions (Splunk, Security Onion)
Secure Data Wiping Tools (DBAN, BCWipe)
Multi-Factor Authentication (MFA) Devices (YubiKey, Google Authenticator)
Secure Password Managers (Bitwarden, KeePass, LastPass)
Faraday Bags and Cages
Lockable Storage Cabinets & Safes
Chain of Custody Forms & Labeling Kits

CCTV & Surveillance Systems
Biometric Access Control (Fingerprint, RFID)
UPS (Uninterruptible Power Supply) Systems
Fire & Electrical Safety
Fire Suppression Systems (CO2 Fire Extinguishers, FM-200 Gas Systems)
Cable Management Tools & Surge Protectors

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Electrical Hazards
Trip & Fall Hazards
Ergonomic Risks
Fire Safety Risks
Ventilation
Personal Protective Clothing
Sufficient lighting
First Aid Kit
Fire Fighting Equipment

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

| INDUSTRY: | TRADE/ OCCUPATION: | CLASS/ LEVEL: |
|---|---|---|
| COMMERCE | DIGITAL FORENSIC TECHNICIAN | NATIONAL DIPLOMA |

**DUTY F: DATABASE SECURITY**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **F1: Implement Database Access Controls.** | i. Define and enforce user roles and permissions based on the principle of least privilege.<br>ii. Configure and manage authentication methods.<br>iii. Regularly review and update user access | i. User roles and permissions defined and enforced.<br>ii. Authentication methods configured and managed.<br>iii. User access and reviewed and updated based on job responsibilities and audit results. | • Communication<br>• Marketing<br>• Creative Art and Design<br>• Salon Management<br>• Business ethics | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management |

| | | | | |
|---|---|---|---|---|
| **F2: Securing Database Backups.** | i. Encrypt database backups to prevent unauthorized access during storage and transmission.<br>ii. Store backups in secure locations, preferably offsite or in cloud environments with strong encryption.<br>iii. Automate backup processes to ensure regular and timely backups. | i. Database backups encrypted.<br>ii. Secure offsite locations implemented.<br>iii. Backup processes automated.<br>iv. Data integrity and availability ensured by automating backups. | | |
| **F3: Monitor Database Activity.** | i. Implement real-time monitoring tools to track database access and modifications.<br>ii. Set up alerting mechanisms for unusual or unauthorized activities.<br>iii. Review logs to detect potential security breaches. | i. Real-time monitoring tools implemented.<br>ii. Alerting mechanisms configured.<br>iii. Potential security breaches detected. | | |
| **F4: Patch and Update Databases.** | i. Check for database security patches and updates from the vendor.<br>ii. Test patches in a staging environment before applying them to production systems.<br>iii. Apply patches and updates to ensure | i. Database security patches and updates installed.<br>ii. Patches tested.<br>iii. Patches and updates applied. | | |

| | | | | |
|---|---|---|---|---|
| | protection against known vulnerabilities. | | | |
| **F5: Encrypt Sensitive Data.** | i. Identify sensitive data and ensure encryption both at rest and in transit.<br>ii. Implement encryption protocols for sensitive data storage and transmission.<br>iii. Review encryption standards and update. | i. Sensitive data at rest and in transit encrypted.<br>ii. Encryption protocols implemented.<br>iii. Encryption standards reviewed and updated based on current practices. | | |
| **F6: Assess Database Vulnerability.** | i. Select tools for the assessment<br>ii. Perform regular vulnerability assessments to identify potential weaknesses in the database environment.<br>iii. Use automated tools or manual methods to scan for security vulnerabilities.<br>iv. Address identified vulnerabilities promptly through patching or configuration changes. | i. Vulnerability assessment tools selected<br>ii. Vulnerability assessments performed.<br>iii. Weaknesses identified.<br>iv. Vulnerabilities patched. | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
Computer/Laptop
Database Management System (DBMS) Software
Database Security Tools
Vulnerability Assessment Tools

Encryption & Key Management Tools
Auditing & Monitoring Software
Backup and Recovery Software
Network Security Tools
Compliance & Security Policy Tools

**MATERIALS**
Notebooks
Printed Security Policies
Audit Reports
User Access Logs
Compliance Checklists

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Data Encryption
Access Control Systems
Fire Fighting Equipment
System Monitoring Tools
Ventilation (for server room cooling)

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Attention to Detail
Analytical Thinking
Confidentiality
Adaptability
Technical Proficiency
Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness

Accuracy
Precise
Goal-getter

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

INDUSTRY: COMMERCE | TRADE/ OCCUPATION: DIGITAL FORENSIC TECHNICIAN | CLASS/ LEVEL: NATIONAL DIPLOMA

**DUTY G: NETWORK SECURITY**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **2.2.1 G1:** Assess network vulnerabilities | i. **Identify assets**<br>ii. **Conduct vulnerability scans**<br>iii. **Analyse results**<br>iv. **Prioritize risks** | i. All network assets are identified and documented.<br>ii. Vulnerability scans are completed.<br>iii. High-risk vulnerabilities are accurately identified.<br>iv. Risks are prioritized based on severity and impact. | ➢ Communication<br>➢ Marketing<br>➢ Creative Art and Design<br>➢ Salon Management<br>➢ Business ethics | ➢ Computer literacy<br>➢ Communication<br>➢ Organizing<br>➢ Analytical<br>➢ Planning<br>➢ Creative<br>➢ Time management |
| **2.2.2 G2:** Implement security measures | i. **Configure Firewalls**<br>ii. **Deploy Intrusion Detection/Prevention Systems (IDS/IPS)**<br>iii. **Apply Encryption**<br>iv. **Enable Logging and** | i. Firewalls are configured according to security policies.<br>ii. IDS/IPS systems are deployed and functioning correctly.<br>iii. Encryption protocols are | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Monitoring** | implemented and tested.<br>iv. Logging and monitoring tools are operational and alerting properly. | | |
| **2.2.3** | **G3:** Manage Access Controls | i. **Define access policies**<br>ii. **Implement authentication mechanisms**<br>iii. **Enforce least privilege**<br>iv. **Regularly review access logs** | i. Access policies are clearly defined and documented.<br>ii. MFA is implemented and enforced.<br>iii. Least privilege principles are applied across the network.<br>iv. Access logs are regularly reviewed and anomalies are addressed. | | |
| **2.2.4** | **G4:** Conduct Regular Security Audits | i. **Schedule audits**<br>ii. **Perform audits**<br>iii. **Document findings**<br>iv. **Implement improvements** | i. Audits are scheduled and conducted regularly.<br>ii. Audit tools and checklists are used effectively.<br>iii. Findings are documented and reported accurately.<br>iv. Improvements are implemented in a timely manner. | | |
| **2.2.5** | **G5:** Respond to Security Incidents | i. **Detect incidents**<br>ii. **Contain the threat**<br>iii. **Investigate the incident**<br>iv. **Apply remediate actions**<br>v. **Report and document** | i. Incidents are detected promptly.<br>ii. Network segmented into smaller VLANs to limit the spread of malware<br>iii. Network is is divide into smaller subnets to reduce the attack surface.<br>iv. Investigations are thorough | | |

| | | | | |
|---|---|---|---|---|
| | 2.2.6 | and accurate.<br>v. Remediation actions are completed successfully.<br>vi. Incidents are documented and reported comprehensively. | | |
| **2.2.7** G6. Educate and Train Staff<br>2.2.8 | i. **Develop training programs**<br>ii. **Conduct training Sessions**<br>iii. **Simulate phishing attacks**<br>iv. **Evaluate training effectiveness** | i. Training programs are developed and implemented.<br>ii. Staff participation in training sessions is high.<br>iii. Simulated phishing attacks show improved awareness.<br>iv. Training effectiveness is evaluated and improvements are made | | |

**TOOLS, MATERIALS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**

Forensic Workstations (e.g., FRED, Dell Precision)
Write Blockers (e.g., Tableau TX1, CRU WiebeTech)
Portable Storage Devices (e.g., IronKey, Kingston DataTraveler)
Network Taps & Packet Capture Devices (e.g., Garland Technology, NetScout OptiView XG)
Hardware Encryption Devices (e.g., Apricorn Aegis Padlock, YubiKey)
Faraday Bags & Cages (e.g., Mission Darkness, EDEC)
Incident Response Kits (e.g., Paraben Field Kit, Logicube Falcon-NEO)
RF Signal Jammers
Portable Power Backup (e.g., APC Smart-UPS, CyberPower UPS)
EnCase
Autopsy/Sleuth Kit
FTK (Forensic Toolkit)
Wireshark
NetworkMiner
TShark
Hashcat

John the Ripper
Ophcrack
VMware Workstation
VirtualBox
Hyper-V
Maltego
Shodan
the Harvester

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Electrical & Fire Hazards
Trip & Fall Hazards

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

| INDUSTRY: | TRADE/ OCCUPATION: | CLASS/ LEVEL: |
|---|---|---|
| COMMERCE | DIGITAL FORENSIC TECHNICIAN | NATIONAL DIPLOMA |

DUTY H: Scripting

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **H1: Write Forensic Scripts.** | i. Identify the problem or task to automate.<br>ii. Choose an appropriate programming language.<br>iii. Write the script to automate processes.<br>iv. Test the script to ensure accuracy and efficiency. | i. Problem to automate identified.<br>ii. Appropriate programming language selected.<br>iii. Automation script wrote.<br>iv. Script tested for functionality | • Communication<br>• Marketing<br>• Creative Art and Design<br>• Salon Management<br>• Business ethics | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management |
| **H2: Debug and Optimize Scripts.** | i. Review and debug existing scripts that may not be performing as expected.<br>ii. Identify performance bottlenecks or logical | i. Existing scripts reviewed and debugged<br>ii. Performance bottlenecks identified and solved.<br>iii. Code optimized for speed and efficiency.<br>iv. Script wrote as per standards. | | |

| | | | | |
|---|---|---|---|---|
| | errors.<br>iii. Optimize code for speed and efficiency without sacrificing accuracy.<br>iv. Ensure the script complies with forensic standards. | | | |
| **H3: Develop Custom Forensic Tool.** | i. Identify the need for a custom forensic tool.<br>ii. Design the tool's architecture and features.<br>iii. Program the tool, ensuring it interacts with forensic systems and databases.<br>iv. Test the tool. | i. Need for the tool identified.<br>ii. Tool's architecture and features designed.<br>iii. Tool interacted with forensic systems.<br>iv. Tool testedin real-world scenario. | | |
| **H4: Automate Data Processing and Reporting.** | i. Implement automated reporting features that compile key findings and data into readable formats.<br>ii. Validate automated reports for accuracy. | i. Automated reporting implemented.<br>ii. Report validated for accuracy | | |
| **H5: Script for Evidence Integrity Checks** | i. Develop scripts to automatically perform integrity checks on collected evidence.<br>ii. Create logs and alerts for any detected anomalies in evidence integrity.<br>iii. Run regular checks during investigations. | i. Integrity checked using hash values<br>ii. Anomalies detected<br>iii. Regular checks run during investigations to ensure that data has not been tampered with. | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
Integrated Development Environment (IDE)
Version Control Systems
Scripting Languages
Code Debuggers
Text Editors
Compilers/Interpreters
Automation Tools
Cloud Platforms
Database Management Systems (DBMS) for integration with scripts

**MATERIALS**
Code Documentation
Scripting Tutorials and Guides
API Documentation
Version Control Logs
Error/Debugging Logs

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Eye Strain
Repetitive Strain Injuries (RSI)
Mental Fatigue
Data Breaches
Security Vulnerabilities

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Problem-Solving Skills
Attention to Detail
Creativity
Persistence
Logical Thinking

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION, INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|
| | | | |

INDUSTRY: COMMERCE | TRADE/ OCCUPATION: DIGITAL FORENSIC TECHNICIAN | CLASS/ LEVEL: NATIONAL DIPLOMA

**DUTY I: MAINTAIN OPERATING SYSTEM**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **I1:** Install and configure the operating system | i. Identify system requirements and compatibility.<br>ii. Acquire the appropriate OS installation media.<br>iii. Configure BIOS/UEFI settings for installation.<br>iv. Perform a clean installation or upgrade.<br>v. Install required drivers and updates.<br>vi. Configure user accounts, permissions, and security policies. | i. System requirements identified<br>ii. Compatible OS acquired<br>iii. OS installed<br>iv. BIOS/UEFI configured<br>v. Default settings set<br>vi. Installation media provided<br>vii. Installation settings customized<br>viii. OS issues troubleshooted<br>ix. Drivers and updates applied.<br>x. User accounts configured | • Communication<br>• System Administration Skills<br>• Security & Compliance Skills<br>• Network Administration Skills<br>• Troubleshooting & Problem-Solving Skills<br>• Automation & Scripting Skills<br>• Virtualization & Cloud Skills | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management |

| | | | | |
|---|---|---|---|---|
| | vii. Verify installation and system stability. | | • Communication & Documentation Skills | |
| **I2:** Perform System Updates and Patch Management | i. Monitor OS for updates and patches.<br>ii. Assess update impact and compatibility.<br>iii. Schedule updates to minimize disruptions.<br>iv. Apply updates using manual or automated methods.<br>v. Install software patches | i. Updates identified<br>ii. Updates installed<br>iii. Automatic updates and troubleshoot settings applied<br>iv. Software Patches installed | | |
| **I3:** Monitor and Optimize System Performance | i. Use system monitoring tools to assess performance.<br>ii. Identify resource bottlenecks<br>iii. Optimize startup programs and background processes.<br>iv. Adjust virtual memory and storage configurations.<br>v. Perform disk cleanup, defragmentation, and optimization. | i. Built-in tools like task manager used to monitor performance<br>ii. System logs analyses reports provided<br>iii. System configurations performed<br>iv. System performance improved<br>v. Performance tuning automated. | | |
| **I4:** Implement Security Measures | i. Configure firewalls and security policies.<br>ii. Enable and update antivirus/endpoint protection.<br>iii. Manage user permissions and access controls. | i. Basic security settings enabled<br>ii. Antivirus scans performed<br>iii. Access controls logs monitored and configured.<br>iv. Advanced security policies and conduct forensic analysis implemented | | |

| | | | | |
|---|---|---|---|---|
| | iv. Apply security hardening best practices.<br>v. Audit logs and detect anomalies.<br>vi. Implement backup and disaster recovery measures. | | | |
| **I5:** Troubleshoot and Resolve System Issues | i. Identify symptoms and collect diagnostic data.<br>ii. Use built-in troubleshooting tools and logs.<br>iii. Apply known fixes or rollback recent changes.<br>iv. Test and validate system functionality.<br>v. Document issues and resolutions. | i. Troubleshooting guides followed<br>ii. Restart services.<br>iii. Logs analyzed<br>iv. Root causes identified<br>v. Fixes applied.<br>vi. Troubleshooting scripts developed | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
Computer/Laptop
OS Installation Media
Patch Management Software
System Monitoring Tools
Backup and Recovery Software
Configuration Management Tools
Virtualization Software

**MATERIALS**
Stationery
Cartridges
Bond paper

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**

Ventilation
Personal Protective Clothing
Sufficient lighting
First Aid Kit
Fire Fighting Equipment

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**

Time conscious
Patience
Team work
Humble
Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter
Attention to Detail
Analytical Thinking
Confidentiality
Adaptability
Technical Proficiency

| | MINISTRY OF HIGHER AND TERTIARY EDUCATION,INNOVATION, SCIENCE AND TECHNOLOGY DEVELOPMENT<br><br>SKILLS PROFICIENCY SCHEDULE | | CODE |
|---|---|---|---|

INDUSTRY: COMMERCE | TRADE/ OCCUPATION: DIGITAL FORENSIC TECHNICIAN | CLASS/ LEVEL: NATIONAL DIPLOMA

**DUTY J: MAINTAIN HARDWARE**

**Pre-requisites:** **Approval Date:** **Review Date:**

| TASK | STEPS | PROFICIENCY INDICATORS | RELATED KNOWLEDGE | WORKPLACE ESSENTIAL SKILLS |
|---|---|---|---|---|
| **J1:** Inspect hardware components | i. Check hardware components for faults<br>ii. Check cables and connections for signs of wear or loose connections.<br>iii. Ensure all hardware is clean and free of dust buildup. | i. Physical damage or wear on hardware identified.<br>ii. Inspections Consistently according to schedule.<br>iii. Faults and repairs Documented. | • Communication<br>• Hardware Components and Functionality<br>• Troubleshooting and Diagnostics<br>• Storage and Data Management<br>• Networking and Connectivity<br>• Security and Protection<br>• Preventive Maintenance & Cleaning<br>• Power and Electrical Knowledge | • Computer literacy<br>• Communication<br>• Organizing<br>• Analytical<br>• Planning<br>• Creative<br>• Time management |
| **J2:** Troubleshoot and Repair hardware | i. Diagnose hardware and software issues reported by users.<br>ii. Repair or replace | i. Hardware and software issues functionality restored.<br>ii. Hardware problems and downtime minimized<br>iii. Fault hardware replacement. | | |

| | | | | |
|---|---|---|---|---|
| | faulty hardware components.<br>iii. Restore data and configurations as necessary. | | | |
| **J3:** Document and Report findings | i. Maintain records of hardware inventory, repairs, and maintenance activities.<br>ii. Generate reports on hardware performance and maintenance history.<br>iii. Document procedures and updates for future reference. | i. Accuracy and completeness of documentation prepared<br>ii. Inventory and maintenance logs updated.<br>iii. Clear and concise reports to management provided | | |
| **J4:** Conduct hardware maintenance Training | i. Provide training to users on proper hardware usage and care.<br>ii. Offer technical support and troubleshooting guidance.<br>iii. Communicate updates and maintenance schedules to relevant stakeholders. | i. Feedback from trained users provided.<br>ii. Trouble shooting manuals prepared<br>iii. Maintenance schedules and updates documented.<br>iv. Training registers updated | | |

**TOOLS AND EQUIPMENT NECESSARY TO COMPLETE THIS DUTY:**
Screwdrivers
Anti-static Wrist Strap & Mat
Tweezers & Precision Tools
Multimeter
Cable Testers
Compressed Air Canister or Electric Duster
Isopropyl Alcohol & Microfiber Cloths
Thermal Paste & Spreader
External Hard Drives / SSDs
USB Flash Drives with Bootable Tools
RJ45 Crimping Tool & Connectors
Wi-Fi Analyzer Tool

**MATERIALS**
Stationery
Cartridges
Bond paper

**SAFETY, HEALTH AND ENVIRONMENTAL ISSUES RELATED TO THIS DUTY:**
Ventilation
Personal Protective Clothing
Sufficient lighting
First Aid Kit
Fire Fighting Equipment

**SPECIFIC WORKER TRAITS REQUIRED TO COMPLETE THIS DUTY:**
Time conscious
Patience
Team work
Humble

Honesty/Integrity
Punctual
Neatness
Accuracy
Precise
Goal-getter
Attention to Detail
Analytical Thinking
Confidentiality
Adaptability
Technical Proficiency