INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

Approved:

2025 y. «___» _____

Programme	**LEVEL 5 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 9 DIGITAL FORENSICS AND INCIDENT RESPONSE**		
Cohort Code:	L05DFIR-U9		
Unit Level	Level 5		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	To equip students with the skills and knowledge necessary to perform digital forensics investigations and effectively respond to security incidents. This module covers the methodologies and tools used in digital forensics, as well as the legal and ethical considerations involved.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:- 1. Progressive tasks 2. Digital resources 3. Verbal support 4. Variable outcomes

	5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials** • "Digital Forensics and Incident Response: Incident Response Techniques and Procedures" by Gerard Johansen. • "Incident Response & Computer Forensics" by Chris Prosise and Kevin Mandia. • "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters. • "Practical Forensic Imaging: Securing Digital Evidence with Linux Tools" by Bruce Nikkel.

Learning Outcome	Assessment Criteria
LO1. Understand the fundamental principles and methodologies of digital forensics.	**1. Written Assessments:** 1.1 Explain key concepts and terminologies used in digital forensics. 1.2 Describe the steps involved in a digital forensics investigation. 1.3 Identify various types of digital evidence and their sources.
LO2. 2. Develop skills in forensic tools and techniques for evidence collection and analysis.	**2. Practical Assessments:** 2.1 Use forensic tools to collect digital evidence from different devices. 2.2 Analyze collected evidence to identify relevant information. 2.3 Document and report the findings from the forensic analysis.
LO3. 3. Understand the principles and processes of incident response.	**3. Written Assessments:** 3.1 Explain the key stages of an incident response process. 3.2 Describe the roles and responsibilities of an incident response team. 3.3 Identify common types of security incidents and appropriate response strategies.
LO4. 4. Develop skills to effectively plan and execute incident response activities.	**4. Practical Assessments:** 4.1 Develop an incident response plan for a given scenario. 4.2 Execute incident response procedures during a simulated security incident. 4.3 Evaluate the effectiveness of the incident response and identify areas for improvement.
LO5. 5. Understand the legal and ethical considerations in digital forensics and incident response.	**5. Research and Analysis Assessments:** 5.1 Research and explain the legal frameworks governing digital forensics. 5.2 Analyze ethical issues related to digital forensics investigations. 5.3 Evaluate case studies to understand the application of legal and ethical principles in real-world scenarios.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Digital Forensics**	**Introduction to Digital Forensics** Definition, objectives, and forensic investigation lifecycle	LO1: Digital Forensics Fundamentals	
2	**Digital Evidence & Chain of Custody**	**Digital Evidence & Chain of Custody** Types (volatile/non-volatile), preservation, legal admissibility	LO1: Digital Forensics Fundamentals	
3	**Forensic Investigation Process**	**Forensic Investigation Process** Identification, collection, analysis, reporting (NIST SP 800-86)	LO1: Digital Forensics Fundamentals	
4	**File Systems & Data Recovery**	**File Systems & Data Recovery** NTFS, FAT, EXT4; carving deleted files (Autopsy, FTK)	LO1: Digital Forensics Fundamentals	
5	**Case Studies**	**Case Studies** Enron, Silk Road, forensic challenges in cloud/IoT	LO1: Digital Forensics Fundamentals	
6	**Disk Imaging & Write Blockers**	**Disk Imaging & Write Blockers** dd, FTK Imager, hardware write blockers	LO2: Forensic Tools & Techniques	
7	**Memory Forensics**	**Memory Forensics** Volatility framework, RAM analysis for malware	LO2: Forensic Tools & Techniques	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Network Forensics**	**Network Forensics** Wireshark, NetworkMiner, detecting lateral movement	LO2: Forensic Tools & Techniques	

10	**Mobile Device Forensics**	**Mobile Device Forensics** Cellebrite, Oxygen Forensics, iOS/Android artifacts	LO2: Forensic Tools & Techniques	
11	**Cloud Forensics**	**Cloud Forensics** AWS/Azure logs, SaaS application investigations	LO2: Forensic Tools & Techniques	
12	**Incident Response Lifecycle**	**Incident Response Lifecycle** NIST SP 800-61 (Preparation → Lessons Learned)	LO3: Incident Response Principles	
13	**Incident Response Team (IRT)**	**Incident Response Team (IRT)** Roles: CSIRT, SOC analysts, legal liaisons	LO3: Incident Response Principles	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	Midterm	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		
16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Incident Classification**	**Incident Classification** Malware, DDoS, insider threats, APTs	LO3: Incident Response Principles	
18	**Threat Intelligence Integration**	**Threat Intelligence Integration** MITRE ATT&CK, TTPs (Tactics, Techniques, Procedures)	LO3: Incident Response Principles	
19	**Case Study: SolarWinds Breach**	**Case Study: SolarWinds Breach** IR failures and best practices	LO3: Incident Response Principles	
20	**IR Plan Development**	**IR Plan Development** Templates, tabletop exercises, stakeholder alignment	LO4: Incident Response Execution	

21	**Containment Strategies**	**Containment Strategies** Short-term (network isolation) vs. long-term (patch deployment)	LO4: Incident Response Execution	
22	**Eradication & Recovery**	**Eradication & Recovery** Root cause analysis, system restoration	LO4: Incident Response Execution	
23	Review	**Project** Full investigation report + expert testimony simulation		
24	**Post-Incident Activities**	**Post-Incident Activities** Forensic imaging, evidence preservation for litigation	LO4: Incident Response Execution	
25	**Simulated IR Drill**	**Simulated IR Drill** Ransomware attack scenario with team roles	LO4: Incident Response Execution	
26	**Legal Frameworks**	**Legal Frameworks** CFAA, GDPR, ECPA, Fourth Amendment implications	LO5: Legal & Ethical Considerations	
27	**Ethical Dilemmas**	**Ethical Dilemmas** Privacy vs. investigation, expert witness responsibilities	LO5: Legal & Ethical Considerations	
28	**Case Law Analysis**	**Case Law Analysis** United States v. Doe (encryption), Apple vs. FBI	LO5: Legal & Ethical Considerations	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	