MODULE DESCRIPTOR

Module Title

Digital Forensics and Analysis

Reference	CM4141	Version	1
Created	November 2023	SCQF Level	SCQF 10
Approved	July 2016	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

This module aims to provide students with knowledge and comprehension of digital forensics principles, along with the skills to proficiently gather, analyze, and evaluate digital evidence utilizing forensic tools and techniques.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Demonstrate critical comprehension of the principles underlying digital forensic techniques.
2	Examine the legal and ethical requisites associated with forensic evidence collection.
3	Apply forensic tools effectively to retrieve data from diverse sources.
4	Critically evaluate collected digital evidence.
5	Compose comprehensive reports for communicating collected evidence to relevant parties.

Indicative Module Content

Definitions and conceptual models; Forensic analysis of computer systems, operating system analysis, main memory forensics, application forensics, network and cloud forensics; Introduction to forensic collection and investigation techniques; Professional and ethical challenges with the forensic process; Exploring data recovery and file content carving; Artifact analysis; Examining file systems, memory, system and event logs, system registries, and network traces; Utilizing open-source tools for forensic investigation; Adhering to standards and best practice guides, such as ISO 27001, ISO 27005, ISO 17020, and ISO 17025.

Module Delivery

This module is taught using a structured programme of lectures, lab sessions and student centred learning.

Module Ref:	CM4141 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4, 5
Description:	Coursework consisting of both practical and theoretical elements covering all learning outcomes of the module.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1.
B	The student needs to achieve a B in Component 1.
C	The student needs to achieve a C in Component 1.
D	The student needs to achieve a D in Component 1.
E	The student needs to achieve an E in Component 1.
F	The student needs to achieve an F in Component 1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM2134 Operating Systems & Virtualisation Security CM2135 Securing Networks CM2136 Cryptography CM3145 Web & Mobile Security CM3146 Ethical Hacking CM3148 Software Security & Malware Analysis
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CM4141 v1

INDICATIVE BIBLIOGRAPHY

1	Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction. Routledge.
2	Kavrestad, J. (2020). Fundamentals of Digital Forensics. Springer International Publishing.
3	Boddington, R. (2016). Practical digital forensics. Packt Publishing Ltd.
4	Chen, L., Takabi, H., & Le-Khac, N. A. (Eds.). (2019). Security, privacy, and digital forensics in the cloud. John Wiley & Sons.
5	Gogolin, G. (Ed.). (2021). Digital forensics explained. CRC Press.
6	Hassan, N. A. (2019). Digital forensics basics: A practical guide using Windows OS. Apress.
7	Sammons, J.,(2016). Digital Forensics with the AccessData Forensic Toolkit (FTK). McGraw-Hill Education
8	Datt, S., (2016). Learning Network Forensics. Packt Publishing