This Version is No Longer Current

The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Digital Forensics and Analysis

Reference	CM4100	Version	3
Created	November 2021	SCQF Level	SCQF 10
Approved	July 2016	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

The aim of the module is to provide students with a knowledge and understanding of the principles of computer, digital and network forensics, and the skills to gather, analyse and evaluate digital evidence using forensic tools and techniques.

Learning Outcomes for Module

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

1 Analyse and critically discuss the principles of computer and network forensic techniques.

2 Effectively employ forensic tools to capture and recover forensic data from different sources.

3 Analyse, evaluate and report on digital evidence from multiple sources.

4 Critically discuss and appraise the correct procedures and processes when performing a forensic investigation.

5 Explain the legal and ethical requirements of forensic evidence gathering and apply these to real world situations.

Indicative Module Content

Forensic analysis of computer, network and cloud data. Introduction to forensic collection and investigation techniques. Professional and Ethical challenges with the forensic process. Analysis of File systems, Memory, System and Event logs, System Registries and Network traces. The use of open-source tools for forensic investigation. Standards and Best Practice Guides: ISO 27001, ISO 27005, ISO 17020, ISO 17025.

Module Delivery

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

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:	Written report.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. 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 C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1 Learning Network Forensics (2016), Datt. Packt Publishing

2 Davidoff & Ham. Hall, P. Network Forensics: Tracking Hackers Through Cyberspace(2012)

3 Bejtlich, R., 2013. The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press

4 Sammons, S. 2012. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Syngress. 2nd ed.

5 Altheide, C., Carvey, H., 2011. Digital Forensics with Open Source Tools. Syngress.

6 Hayes. D., 2014. A Practical Guide to Computer Forensics Investigations, Pearson.

7 Sammons, J., 2016. Digital Forensics with the AccessData Forensic Toolkit (FTK), McGraw-Hill Education