MODULE DESCRIPTOR

Module Title

Incident Management And Forensics

Reference	CMM519	Version	4
Created	January 2023	SCQF Level	SCQF 11
Approved	August 2017	SCQF Points	15
Amended	June 2023	ECTS Points	7.5

Aims of Module

To provide students with the ability to evaluate and apply the methods, tools and techniques used in intrusion response and forensics.

Learning Outcomes for Module

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

1	Evaluate and apply the techniques and tools used in intrusion analysis.
2	Appraise the methods used in incident handling and management.
3	Apply the techniques used in collecting, processing and preserving digital evidence.
4	Analyse and appraise the procedures used in preparing a forensics report and expert testimony.

Indicative Module Content

Incident identification: unauthorised access, denial of service, malicious code, improper usage, and scans/probes. Analysis of malware signatures and behaviour. Incident handling, containment and recovery. Understanding of legislation and legal constraints for digital forensics. Evidence gathering rules and techniques: collecting, processing and preserving digital evidence. Device forensics; Memory forensics; File systems forensics; Network forensics; Malware forensics; handheld device forensics; Anti-forensic techniques. Forensic report writing and expert testimony.

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

Module Ref:	CMM519 v4

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	30
Non-Contact Hours	120	120
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
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
Description:	This is a coursework where students will be appraising the various methods of incident handling and preparing a forensics investigation 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 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	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM519 v4

INDICATIVE BIBLIOGRAPHY

1	Street, J., 2015, Dissecting the Hack: The V3rb0ten Network. Springer.
2	Zeigler, A., 2016, Preserving Electronic Evidence for Trial: A team approach to the litigation hold, data collection, and preservation of digital evidence. Elsevier.
3	SAMMONS, J., 2016, Digital Forensics: Threatscape and best practices. Elsevier.
4	Leighton, J., 2014 Computer incident response and forensics team management conducting a successful incident response. Syngress.
5	Malin, C., 2014, Malware Forensic Field Guide For Linux/Windows systems. Elsevier.
6	Hassan, N.A., 2019. Digital forensics basics: a practical guide using Windows OS. Springer.