Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

IT Forensics

School Responsible:	School of Computing

Module Overview:
The use of modern technologies has substantially increased in the last few decades. This has led computers, mobile devices and communications systems being able to create and store unprecedented amount of digital information. However, as we use modern technologies, far more information is retained on these devices than most people would realize. The information retained is usually called electronics evidence (e-evidence). To make matters worse rarely are users aware that their activities have left multiple trails of evidence. In most cases users make insufficient or no attempt to delete those trails regardless of how incriminating they may be. Even techno-savvy users who want to go undetected may not be able to completely delete or disguise all trails of their activities or artefacts. And in some cases, deleting evidence may not be possible. Therefore, Forensics provides a new set of technological investigative skills and tools. The number of different cases and crimes found in today's digital world indicate with certainty that Forensics will be needed in most types of investigations. The e-evidence can be used not only to prove straightforward charges such as illegal possession of pirated software, but also to imply motive or intent by forming a "digital profile or dossier" of an individual or the circumstances surrounding a lawsuit or case. The module aims to develop an understanding of the range of approaches used in computer forensics. This requires an understanding of three phases for recovering evidence from a computer system or storage medium. The three phases are acquiring data; analysing data and reporting on the analysis. It is necessary that students have a clear understanding of how data is stored on a range of computer systems as well as being able to discuss the relevant legal issues involved in the collection and the documentation of evidence in a computer forensics investigation

Learning Outcomes (LO):	
On Completion of this module, the learner will be able to	
1	Understand the laws and regulations affecting Forensic Investigations
2	Understand the significance and importance of evidence admissibility

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

3	Learn how to perform case management and report writing
4	Research modern techniques used in anti-forensics
5	Learn how to use digital forensic tools
6	Perform Digital Forensics analysis on various media i.e. network, email, cloud

Indicative Syllabus:

The Anatomy of A Digital Investigation

- A basic model for investigators
- Understanding the Scope of the Investigation
- Identifying the stakeholders

The Laws Affecting Forensic Investigations

- Constitutional Implications of Forensic Investigation
- The right to privacy
- The expert witness
- Search warrants and subpoenas

The admissibility of evidence

- ˇWhat makes evidence admissible
- Keeping evidence authentic
- Defining the scope of the search
- When the laws and regulations do not apply

The role of the Digital Investigator

- Forensics and Computer Science
- Controlling the Scene of the Crime
- Handling Evidence

Data Acquisition

- Order of volatility
- Memory and running processes
- Acquiring Media

Find Lost Files

- File Recovery
- The Deleted File
- Data Carving

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

Document Analysis

- File Identification
- Understanding Metadata
- Mining the Temporary Files
- Identifying alternate hiding places of data

Email Forensics

- Email Technology
- Information Stores
- The Anatomy of an E-Mail
- The approach to Email Analysis

Web Forensics

- Internet Addresses
- Web Browsers
- Web Servers
- Proxy Servers

Searching the Network

- An eagle's eye view
- Initial Response
- Proactive collection of evidence
- Post incident collection of evidence
- Router and Switch Forensics

Excavating a Cloud

- What is cloud computing
- Shaping the cloud
- The implications of cloud forensics
- On Virtualisation
- Legal Issues

Mobile Device Forensics

- Challenges of Mobile Device Forensics
- How mobile phones work
- Data storage on mobile phones
- Acquisition and storage
- Legal Aspects of Mobile Device Forensics

Fighting Anti Forensics

- Artefact Destruction
- Hiding Data on the System
- Covert Data

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

Case Management and report writing

- Managing a case
- Writing Reports

Tools of the Digital Investigator

- Software tools
- Working with court approved tools
- Hardware tools

Nontechnical Tools

Learning and Teaching Methods:	
This module can be delivered either through standard delivery or blended delivery. In standard delivery this module is delivered through a series of lectures with associated practical assignments. In blended delivery this module is delivered through a series of live and recorded lectures with associated laboratory work and practical assignments. Both blended and standard delivery have the same overall number of teaching and self-directed learning hours.	
Total Teaching Contact Hours	39
Total Self-Directed Learning Hours	61

Module Delivery Duration:
This module is delivered over one semester

Assessment		
Assessment Type	**Weighting (%)**	**LO Assessment (No.)**
Final Exam	50%	1-6

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

In Class Assessment	50%	1-6
Module Specific Assessment Arrangements (if applicable)		
(g) Derogations from General Assessment Regulations		
(h) Module Assessment Thresholds		
(i) Special Repeat Assessment Arrangements		

Essential Reading: (author, date, title, publisher)

Marjie T. Britz (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson Education. ISBN 978-0-13-303609-1.

Darren R. Hayes (2014). *A Practical Guide to Computer Forensics Investigations*. Pearson Education. ISBN 978-0-13-275615-0.

Supplemental Reading: (author, date, title, publisher)

Eoghan Casey (2009). *Handbook of Digital Forensics and Investigation*. Academic Press. ISBN 978-0-08-092147-1.

Clint P Garrison (2010). *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*. Syngress. ISBN 978-1-59749-538-7.

Bill Nelson; Amelia Phillips; Christopher Steuart (2014). *Guide to Computer Forensics and Investigations*. Cengage Learning. ISBN 978-1-305-17608-9.

Marie-Helen Maras (2014). *Computer Forensics*. Jones & Bartlett Publishers. ISBN 978-1-4496-9223-0.

Version No:		**Amended By**	
Commencement Date		**Associated Programme Codes**	

# Modules that are to be offered as Stand-Alone CPD Programmes must have an NFQ level assigned

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					

*Details of the assessment schedule should be contained in the student handbook for the programme stage.

Date of Academic Council approva……………………..

Module Code	Pre-requisite Module codes	Co-Requisite Modules code(s)	ISCED Code	Subject Code	ECTS Credits	NFQ Level (CPD)#
CMPU4028					10	8
Module Title	IT Forensics					