Module 4: Computer Forensics

Stage				1			
Semester				1			
Module Title				Computer Forensics			
Module Number				4			
Module Status				Mandatory			
Module ECTS Credits				10			
Module NFQ level				9			
Pre-Requisite Module Titles				None			
Co-Requisite Module Titles				None			
Capstone Module?				No			
List of Module Teaching Personnel				Dr Mark Scanlon			
Contact Hours				**Non-contact Hours**			**Total Effort (hours)**
72				**128**			**200**
Lecture	**Practical**	**Tutorial**	**Seminar**	**Assignment**	**Placement**	**Independent Work**	
48		24		60		68	
Allocation of Marks (Within the Module)							
	Continuous Assessment	**Project**	**Practical**	**Final Examination**			**Total**
Percentage Contribution	**40**			**60**			**100**

Intended Module Learning Outcomes

On successful completion of this module the learner will be able to:

1. Discuss the importance of the integrity of digital evidence
2. Evaluate common digital forensic investigative methods and associated tools
3. Identify where to locate digital evidence across a range of devices
4. Evaluate the techniques used to track cybercriminals online
5. Integrate knowledge of various technologies to identify malware and network attacks
6. Analyse state-of-the-art digital forensic techniques and methodologies

Module Objectives

This module introduces the learner to the concepts of computer forensics. They encounter various techniques used in digital forensic investigations and the tools required for these investigations. Learners also gain an exposure to the practical digital evidence gathering process. Current trends in Computer Forensics, such as network and cloud forensics are introduced through the use of academic papers.

Module Curriculum

- **Admissibility of Electronic Evidence**
  Forensic Evidence and Crime Investigation
  Computer Forensics and Digital Detective Work

- **Preparing for Digital Evidence Collection and Preservation**
  Tools, Environments, Equipment, and Certifications
  Policies and Procedures
  Data, PDA, and Mobile Phone Forensics

- **Forensic Examination of Computers and Digital and Electronic Media**
  Operating Systems and Data Transmission Basics for Digital Investigations
  Investigating Windows, Linux, and Graphics Files
  E-Mail and Webmail Forensics

- **Detecting Intrusions, Malware, and Fraud**
  Internet and Network Forensics and Intrusion Detection
  Tracking Down Those Who Intend to Do Harm on a Large Scale
  Fraud and Forensic Accounting Investigation

Recommended Reading

Volonino L, Anzaldua R, Godwin J, 2007, *Computer Forensics: Principles and Practice*, Prentice Hall

Graves M W, 2014, *Digital Archaeology: The Art and Science of Digital Forensics*, Addison-Wesley

Secondary Reading

Various Authors, 2014, *Proceedings of DFRWS Conferences**, Elsevier

Various Authors, 2014, *Proceedings of ICDF2X Conferences**, Springer

Various Authors, 2014, *Digital Investigation Journal**, Elsevier

*available online

Additional reading as recommended by lecturer, appropriate to topic.

Module Learning Environment

Accommodation

Lectures are carried out in class rooms / lecture halls in the College. Computer Labs throughout the Campus are accessible for the purpose of completing assignments. There is no specific software required to deliver the programme.

Library

All learners have access to an extensive range of physical and electronic (remotely accessible) library resources. The library monitors and updates its resources on an on-going basis, in line with the College's Library Acquisition Policy. Lecturers update reading lists for this course on an annual basis as is the norm with all courses run by Griffith College.

Module Teaching and Learning Strategy

Each week, there are three classes:

Classes are used to explain the concepts, exemplify the techniques, and solve (in workshop style) a series of exercises and problems. Some classes involve the discussion of seminal research papers in the IR domain. Learners are expected to read the material prior to class.

In addition to classes, the learners need to put in at least four hours of study and homework each week.

Module Assessment Strategy

Element No.	Weighting	Type	Description	Learning Outcomes Assessed
1.	20%	Report	For this assignment learners are required to research a specific topic in Computer Forensics identifying the best practises, tools and cases where this topic has proved advantageous in the conviction of criminals.	1,2,6
2.	20%	Assignment	For this assignment, learners are required to emulate a real-world digital investigation. Learners will be required to document their recovery of digital evidence from a suspect device. The resultant evidence must be documented and analysed to retrieve “court admissable” evidence.	2,3,5
3.	60%	Examination	The examination will test the learners understanding of the theoretical aspects of the coursework.	all