MODULE TITLE	Foundations of Digital Forensics			CREDIT VALUE	
MODULE CODE		MODULE CONVENOR			
DURATION	TERM	1	2	3	Number Students Taking Module (anticipated)
	WEEKS				

DESCRIPTION – summary of the module content (100 words)

This course provides a general introduction to the field of Digital Forensics. It covers a number of topics fundamental to the area of digital forensics investigation. Such topics include an overview of computer hardware and digital media and storage formats, data acquisition and validation techniques, forensic methodologies, network traffic analysis, legal issues surrounding forensic investigation, professionalism and ethics, and future development in the field. In addition, the course promotes and strengthens important generic skills, such as communication, analysis, problem-solving, both independent- and group-work as well as professionalism and social responsibility. The course assumes a basic knowledge of IT systems.

MODULE AIMS – intentions of the module

This course fosters those skills essential for ethical hacking as well as acting as an expert witness in legal cases requiring digital forensic investigation. Employers in law enforcement and the digital forensics industry require graduates with such skills. Students taking this course will be introduced to the process of managing a digital forensic case and conducting technical examination and interpretation of digital-based evidence. The course aims to equip students with the professional skills required for problem-solving, working individually or in a team.

INTENDED LEARNING OUTCOMES (ILOs) (see assessment section below for how ILOs will be assessed)
On successful completion of this module **you should be able to**:

Module Specific Skills and Knowledge:	
1	Explain the role of digital forensics in criminal and corporate investigations, auditing, and in the general area of IT security.
2	Describe how digital data is stored both locally and in the cloud and explain how to retrieve such data.
3	Implement current industry best practices for the analysis of digital evidence when presented with hypothetical and real cases.
Discipline Specific Skills and Knowledge:	
4	Plan a digital forensic investigation, including data acquisition and validation, evidence discovery, analysis, and presentation of findings using a variety of digital forensics tools.
Personal and Key Transferable/ Employment Skills and Knowledge:	
5	Perform independent research in a specific area in the field of forensic computing.
6	Display generic skills, such as effective communication, analysis, problem-solving, the ability to work independently and in a group, professionalism and social responsibility.

SYLLABUS PLAN – summary of the structure and academic content of the module

1. Fundamentals of digital forensics investigation
2. Overview of computer crime
3. Foundations of electronic evidence acquisition – legal compliance and requirements
4. Review of forensic laws
5. Overview of the digital forensics process
6. Overview of common tools for digital forensics
7. Fundamentals of file systems

8. Forensics file recovery and file carving
9. Windows System forensics artefacts
10. Network forensic artefacts

LEARNING AND TEACHING

LEARNING ACTIVITIES AND TEACHING METHODS (given in hours of study time)

Scheduled Learning & Teaching activities	42	Guided independent study	102	Placement/study abroad	

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled learning and teaching	42	Lectures
Guided independent study	36	Assignments
Guided independent study	42	Preparation for lectures
Guided independent study	24	Revision for written exam

ASSESSMENT

FORMATIVE ASSESSMENT - for feedback and development purposes; does not count towards module grade

Form of Assessment	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Activities during the lectures	8 x 2 hours	1-4	Oral

SUMMATIVE ASSESSMENT (% of credit)

Coursework	40	Written exams	60	Practical exams	0

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of credit	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Assignments	30	2 x 6 weeks	1-6	LMS, graded report
Written exams	60	1 x 3 hours	1-4, 6	Graded report
Quizzes (oral & written)	10	4 x 1 hours	1-4, 6	Oral, comments on paper

RESOURCES

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener.

Basic reading:

1. *Computer Forensics and Cyber Crime: An Introduction (3rd Edition)* by Marjie T. Britz, 2013.
2. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory* (1st Edition). By Michael Hale Ligh, Andrew Case, Aaron Walters.

Web-based and electronic resources:

1. https://www.memoryanalysis.net/amf
2. Computer Forensics World: http://www.computerforensicsworld.com/
3. Computer Forensic Services: http://www.computer-forensic.com/

4. Digital Forensic Magazine: http://www.digitalforensicsmagazine.com/

CREDIT VALUE		**ECTS VALUE**	**5**
PRE-REQUISITE MODULES			
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	6	**AVAILABLE AS DISTANCE LEARNING**	
ORIGIN DATE	October 2018	**LAST REVISION DATE**	
KEY WORDS SEARCH	Fundamentals of digital forensics, digital file systems		