MODULE TITLE	Digital Forensics Procedures			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 introduces students to the methodology, procedures and legal issues associated with managing a digital forensic investigation. The course covers procedures for investigating computer and cybercrime, techniques for the collection, analysis, recovery and preservation of forensic evidence. Students will work with various operating systems, including DOS, Windows, MacOS, and Linux. Other topics covered include the boot process, disk structures, data acquisition, file recovery, network forensics, acting as an expert witness, and reporting investigation results. The course incorporates demonstrations and laboratory exercises to reinforce course material through practical applications and requires independent research into digital forensics procedures. A prerequisite for this course is Foundations of Digital Forensics.

MODULE AIMS – intentions of the module

This course aims to provide students with hands-on experience of the methods, technologies, and challenges relevant to effectively conducting a computer forensics investigation and response, as well as to provide students with professional skills in the areas of problem-solving, working individually and in a professional 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	Summarize important laws pertinent to computer forensics investigation.
2	Describe various computer crimes and how they are investigated.
3	Explain techniques for hiding and encrypting data and enumerate appropriate approaches for the recovery of such data.
4	Compare various types of digital forensics methodologies.
Discipline Specific Skills and Knowledge:	
5	Employ a standard digital forensic methodology and use standard forensic software.
6	Describe incident and intrusion response.
7	Analyze trends and locate resources for digital forensics.
Personal and Key Transferable/ Employment Skills and Knowledge:	
8	Perform independent research in a specific area in the field of forensic computing.
9	Display generic skills, such as effective communication, problem-solving, independent- and group-work, and professionalism and social responsibility.

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

1. Overview of evidence-gathering and digital forensic techniques
2. Applying forensics methods
3. Collecting and protecting evidence
4. Techniques for hiding and scrambling digital artifacts
5. Data recovery
6. E-mail forensics
7. Documenting and reporting investigation results

LEARNING AND TEACHING

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

Scheduled Learning & Teaching activities	42	Guided independent study	104	Placement/study abroad	

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled learning and teaching	21	Lectures
Scheduled learning and teaching	21	Labs
Guided independent study	36	Assignments
Guided independent study	24	Lab write-ups
Guided independent study	44	Lecture preparation and revision

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
Labs	8 x 2 hours	5-9	Oral

SUMMATIVE ASSESSMENT (% of credit)

Coursework	30	Written exams	40	Practical exams	30

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	1-7	LMS
Labs	30	8 x 2 hours	5-9	Graded report
Written exams	40	1 x 3 hours	1-7	Graded exam

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. System Forensics, Investigation, and Response, 3rd Edition, by Easttom, published by Jones & Bartlett Learning, 2017
2. Guide to Computer Forensics and Investigations (4th edition). By B. Nelson, A. Phillips, F. Enfniger, C. Steuart. ISBN 0-619-21706-5, Thomson, 2009.
3. 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. Journal of Digital Forensic Practice: http://www.tandf.co.uk/15567281
2. Electronic Crime Scene Investigation: A Guide for First Responders: http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm
3. Scientific Working Group on Digital Evidence: http://ncfs.org/swgde/index.html

CREDIT VALUE		**ECTS VALUE**	**5**
PRE-REQUISITE MODULES	Foundations of Digital Forensics		
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	6	**AVAILABLE AS DISTANCE LEARNING**	
ORIGIN DATE	October 2018	**LAST REVISION DATE**	
KEY WORDS SEARCH	Digital forensics procedures, forensics methods		