MODULE TITLE	Digital Forensics Investigation: Techniques and Tools			CREDIT VALUE	3
MODULE CODE	5			MODULE CONVENOR	
DURATION	TERM	1	2	3	Number Students Taking Module (anticipated)	20
	WEEKS	16				

DESCRIPTION – summary of the module content (100 words)

Digital Forensics Investigation refers to the scientific and systematic methodology applied to the collection, analysis, preservation, storage, transportation and presentation of the digital evidence in courtrooms with respect to both criminal and civil laws. This course is designed to build on the student's theoretical understanding of the principles, methodologies, laws and standards of digital forensics. Specifically, it will develop the students' ability to carry out a complete forensics investigation using industry-leading digital forensic solutions to solve hypothetical cases that mimics the ones that they might face in the real world. This course will focus mainly on the techniques and tools for conducting investigations on operating systems, databases and memory forensics.

PREREQUISITES – previous courses required to take this course

This course assumes that students have theoretical understanding of the fundamentals of digital forensics investigation, procedures, laws, standards and ethics taught in modules (Foundation of Digital Forensic, Digital Forensic Procedures, Legal Aspects of Digital Forensic, Business Aspects of Digital Forensic). Furthermore, the student should have a full comprehension of the hard disk structures and the major File Systems including FAT, NTFS, ReFS, HPFS/APFS, EXT and ZFS, in addition to having a prior knowledge of the main concepts of operating systems and database.

MODULE AIMS – intentions of the module

This course aims to provide the student with the practical skills required to conduct a complete forensics investigation whether in criminal and civil cases. Upon completion of the course, students should be able to apply their knowledge of digital forensics and use several digital forensic solutions to collect and analyse the digital evidence then present it as part of a digital forensic report. Students are expected to be able to perform operating system forensics including Windows, Linux and Mac OS, in addition to perform memory and database forensics.

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	Effectively and efficiently work with various digital forensics solutions
2	Conduct live, traditional and memory forensic acquisition & analysis
3	Analyse evidence collected from Windows, Linux, Mac OS, database and memory
4	Handle forensics hardware tools such as write-blockers, bridges, adapters and forensic workstations
Discipline Specific Skills and Knowledge:	
5	Demonstrate a solid understanding of the various digital forensics investigation techniques and tools
6	Perform a complete and comprehensive digital forensic investigation
7	Prepare and present a thorough digital forensics report
Personal and Key Transferable/ Employment Skills and Knowledge:	
8	Apply critical thinking and interpersonal skills to work in digital forensics investigation teams

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

Module Syllabus

1. Introduction to Digital Forensics Investigation
    a. Hard disk structure
    b. File systems (Journal vs. Non-journaling)
    c. Forensics software
    d. Forensics hardware
2. Digital Forensics Evidence Acquisition
    a. Traditional forensics acquisition
    b. Triage forensics acquisition
    c. Memory forensics acquisition
3. Digital Forensics Techniques
    a. Live forensics analysis
    b. Data Recovery
    c. Data & file curving
    d. Data hiding and Anti-forensics (steganography, cryptography, slack space, …)
    e. Searching and Filtering (files, emails, documents, images, …)
    f. Metadata and Timeline analysis
4. Internet investigation
    - How the Internet Works
    - Introduction to Internet Crime
    - Collecting and Documenting Online Evidence
    - Using Internet Investigating Tools
    - Working Hidden On the Internet
    - Investigation websites and WebPages
    - Prevention of Internet Crimes
    - Summary
5. Introduction to Database Forensics
    - Importance and Aims of Database Forensic
    - mathematical representation of data
    - Database Threats
    - Database Threats Control Methods
    - Database Security in the Web Environment
    - Database forensic techniques and tools
    - Detecting and Analysis Database Attacks Using Digital Forensics Tools
    - Data recovery
    - Summary
6. Windows Artifacts
    a. Windows registry analysis
    b. Volume shadow copy analysis
    c. User activities analysis
    d. System configurations analysis
    e. Applications analysis
    f. Devices analysis
    g. Events and logs analysis
7. Linux Artifacts
    a. Volume snapshots analysis
    b. User activities analysis
    c. System configurations analysis
    d. Applications analysis
    e. Devices and Log analysis
8. Memory Analysis

LEARNING AND TEACHING

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

Scheduled Learning & Teaching activities	38	Guided independent study	100	Placement/study abroad	0

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled learning and teaching	14	Lectures
Scheduled learning and teaching	24	Lab (practical)
Guided independent study	36	Assignments
Guided independent study	24	Labs write-up
Guided independent study	20	Revision for lab and written exam
Guided independent study	20	Preparation for lectures

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
Coursework (quizzes, assignments)		2 – 8	Oral, Written
Written exam		1, 5	Written
Lab (practical)	12 x 2 hours	2 – 8	Written

SUMMATIVE ASSESSMENT (% of credit)

Coursework	15%	Written exams	15%	Practical (report)	70%

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of credit	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Lab	70%	3 hrs	2 – 8	Oral, Written
Assignment	15%	6 weeks	2 – 8	Written, Online
Written exam	15%	2 hrs	1,5	Oral, Written

DETAILS OF RE-ASSESSMENT (where required by referral or deferral)

Original form of assessment	Form of re-assessment	ILOs re-assessed	Time scale for re-assessment
Lab Exam	Lab Exam	2 – 8	To be announced
Written Exam	Written Exam	1, 5	To be announced

RE-ASSESSMENT NOTES

Re-assessment will be calculated as per the following:

9. Lab Exam Re-assessment: 70 % of the total points shall be given to this assessment
10. Written Exam Re-assessment: 15 % of the total points shall be given to this assessment.

Re-assessment for assignments is not available.

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: Digital Investigation Techniques and Tools

Web based and electronic resources:

1- EMERALD Database
2- EBSCO Database
3- KNOVEL Database
4- Others

Other resources:

1. Computer Forensic Training Center Online http://www.cftco.com/
2. Computer Forensics World http://www.computerforensicsworld.com/
3. Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

CREDIT VALUE	3 Credits	**ECTS VALUE**	**5**
PRE-REQUISITE MODULES	Operating Systems, Database, and Fundamental of Computer networks		
CO-REQUISITE MODULES	Computer Security		
NQF LEVEL (FHEQ)	(4th Year Level)	**AVAILABLE AS DISTANCE LEARNING**	NO
ORIGIN DATE	11– 03 - 2018	**LAST REVISION DATE**	**23/6/2018**
KEY WORDS SEARCH	Digital Investigation, Forensic Tools, Network Forensic, Mobile Forensic, Database Forensics		