MODULE TITLE	**Emerging Trends & Special Topics in Digital Forensics**				**CREDIT VALUE**	3
MODULE CODE	8			**MODULE CONVENOR**		
DURATION	**TERM**	**1**	**2**	**3**	**Number Students Taking Module (anticipated)**	**20**
	WEEKS		16			

DESCRIPTION – summary of the module content (100 words)

This course teaches the students the emerging trends and the new technologies in digital forensics. Moreover, this course teaches how these new technologies and emerging trends can be applied in the forensic investigation process including evidence collecting, analysis and presentation. This course will cover several topics and challenges in digital forensics such as audio/video, internet of things, cloud, big data, social networks and cryptocurrency. This course need to be continuously updated to address the new challenges and advances in digital forensics.

MODULE AIMS – intentions of the module

The aim of this course is to cover new trends and special topics in computer science and explain their effects on digital forensics in particular. The course teaches students how to apply digital forensic techniques on new topics such Internet of Things, cloud computing and digital currencies.

PREREQUISITES – previous courses required to take this course

This course assumes that the students took the courses: Digital Investigation Techniques and Tools and Network Forensic. Students should have a theoretical understanding of the fundamentals of digital forensics investigation, procedures, laws, standards and ethics taught in previous modules. Furthermore, the student should be familiar with the fundamental topics in computer science including operating systems, database, artificial intelligence, networking and security.

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	Identifying and presenting indicators that a cyber-security incident has occurred in new computer scenarios.
2	Analysing forensic cases in new computer scenarios and presenting evidences
3	Apply new technologies to the digital forensic field for achieving better investigations
4	Demonstrating an understanding of forensic principles within an emerging computing environment
Discipline Specific Skills and Knowledge:	
5	Explain the role of digital forensic in the overall context of computer emerging trends.
Personal and Key Transferable/ Employment Skills and Knowledge:	
6	Work effectively in a team.

7	Communicate security-relevant findings in a clear and concise manner both orally and in written form.

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

Module Syllabus

1. Internet of Things Forensics
2. Social Networks Forensics
3. Big Data Forensics
4. Introduction to Cloud Computing forensics
5. Cloud Forensic techniques and tools
6. Cryptocurrency Forensics
7. Digital Forensics reverse engineering fundamentals
8. Selected Research Areas in Digital Forensic
9. Audio/Video Forensics

Weekly laboratory practical sessions reinforce concepts introduced in lectures.

LEARNING AND TEACHING

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

Scheduled Learning & Teaching activities	48	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	24	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
Lab (practical)	12 x 2 hours	1 – 5	Oral, Written report

SUMMATIVE ASSESSMENT (% of credit)

Coursework	15%	Written exams	60%	Practical exams	25%

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of	Size of the	ILOs assessed	Feedback method

	credit	assessment e.g. duration/length		
Lab exam	15%	2 hours	1 – 3	Written + oral
Assignment	15%	6 weeks	4 – 7	Written + Online
Written exam	70%	3 hours	1 – 5	Written + oral

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	1 – 3	To be announced
Written Exam	Written Exam	1 – 5	To be announced

RE-ASSESSMENT NOTES –

Re-assessment will be calculated as per the following:

- Lab Exam Re-assessment: 15% of the total points shall be given to this assessment
- Written Exam Re-assessment: 70% 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: Emerging Trends & Special Topics in Digital Forensics

Web based and electronic resources:

1- EMERALD Database
2- EBSCO Database
3- KNOVEL Database
4- Other databases

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	**ECTS VALUE**	**5**
PRE-REQUISITE MODULES	Digital Investigation Techniques and Tools, Network Forensic, Operating Systems, Database, and Fundamental of Computer networks		
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	(4th Year Level)	**AVAILABLE AS DISTANCE LEARNING**	No
ORIGIN DATE	**11/3/2018**	**LAST REVISION DATE**	**23/6/2018**
KEY WORDS SEARCH	Cloud forensic, IoT forensics, AI in forensics, digital currency		