MODULE TITLE	**Mobile Forensics**				**CREDIT VALUE**	3
MODULE CODE			**MODULE CONVENOR**			
DURATION	**TERM**	**First semester**	**Second semester**		**Number Students Taking Module (anticipated)**	**20**
	WEEKS	16				

DESCRIPTION – summary of the module content (100 words)
Mobile forensics is one of the modern branches of digital forensics, focused on analysing mobile devices to recover digital evidence. This course is designed to provide the student with the required theoretical knowledge and practical experience to conduct mobile forensics investigation in accordance with the current body of knowledge. Students will be exposed to the technology behind mobile devices and cellular networks in addition to the process, methods and techniques of mobile forensics. Moreover, the course will teach the practical aspect of performing a mobile forensics investigation using state-of-the-art commercial solutions, the open-source tools as well.
PREREQUISITES – previous courses required to take this course
This course assumes that the student has a theoretical understanding of the fundamentals of digital forensics investigation, procedures, laws, standards and ethics taught in modules: Foundation of Digital Forensics, Digital Forensic Procedures, Digital Investigation Techniques and Tools, and Network Forensics. Furthermore, the student should be familiar with the fundamental topics in computer science including operating systems, networking and security.
MODULE AIMS – intentions of the module
This course aims to provide the students with the knowledge needed to carry out a mobile forensics investigation in a professional and scientifically sound manner. Furthermore, the course aims to expose the students to the various tools used in mobile forensics especially the de-facto commercial solutions, thus preparing them to compete in the professional market.
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 Understanding the various type of information that can be extracted from a mobile device
2 Collect and analyse artefacts from different mobile devices, Apps and smart cards
3 Validate the results of mobile forensics solutions
Discipline Specific Skills and Knowledge:
4 Demonstrate a solid understanding of the various mobile enabling technologies, forensics process, methods, techniques and tools
5 Perform a complete and comprehensive mobile forensic investigation
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. Fundamentals of Mobile Devices and Cellular Network 1.1. Cellular Network 1.1.1. Evolution of Cellular Network and its History 1.1.2. Cellular Network Architecture and Technologies 1.1.3. Introduction to AT/AT+ Commands 1.2. Mobile Device Hardware 1.2.1. Evolution of Mobile Device and its History 1.2.2. Mobile Device Architecture and Technologies 1.2.3. Mobile Operating Systems 1.3. Smart Cards 1.3.1. Subscriber Identification Module (U/SIM)

1.3.2. U/SIM File Management
1.3.3. U/SIM Security
1.4. Standards, Societies and Body of Knowledge
2. Mobile Forensics Process, Methods and Techniques
2.1. Mobile Forensics Process
2.1.1. Evidence Preservation
2.1.2. Evidence Collection
2.1.3. Evidence Examination and Analysis
2.2. Acquisition Methods
2.2.1. Manual Acquisition
2.2.2. Logical Acquisition
2.2.3. Physical Acquisition
2.2.4. File-system Acquisition
2.2.5. JTAG and Chip-Off Forensics
2.3. Mobile Forensics Techniques
3. Mobile Forensic Tools
3.1. Cellebrite UFED
3.2. Oxygen Forensics Detective
3.3. MSAB XRY and XAMN
3.4. MAGNET IEF
3.5. Open-Source Mobile Forensic Tools
4. Mobile Device Forensics
4.1. Android, BlackBerry, iOS and Windows Mobile Forensics
4.2. Artefacts Extraction
4.2.1. Contacts and Phone Call Artefacts
4.2.2. SMS Artefacts
4.2.3. Network and Location Artefacts
4.2.4. System Artefacts
4.2.5. Multimedia Files Artefacts
4.3. Data and File Carving
4.4. Deleted Files Recovery
4.5. Bypassing Security Controls
5. U/SIM Cards Forensics
5.1. U/SIM Card Artefacts Extraction
5.1.1. Integrated Circuit Card Identifier (ICCID)
5.1.2. International Mobile Subscriber Identity (IMSI)
5.1.3. Mobile Station International Subscriber Directory Number (MSISDN)
5.1.4. Abbreviated Dialling Numbers (ADN)
5.1.5. Fixed Dialling Numbers (FDN)
5.1.6. Last Number Dialled (LND)
5.1.7. Location Information
5.1.8. Phonebook
5.1.9. Messages
5.2. U/SIM Card Cloning
5.3. U/SIM Card Forensic Tools
5.4. Bypassing U/SIM Card Security Controls
5.5. APDU Commands

LEARNING AND TEACHING

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

Scheduled Learning & Teaching activities	48	Guided independent study	140	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	40	Revision for lab and written exam
Guided independent study	40	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	1-7	Oral, written

SUMMATIVE ASSESSMENT (% of credit)

Coursework	40%	Written exams	30%	Practical exams	30%

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of credit	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Lab exam	30%	3 hours	1-3	Online
Assignment	40%	12 weeks	1-7	Online
Written exam	30%	3 hours	4	Online + 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	Week #16-17
Written Exam	Written Exam	4	To be announced

RE-ASSESSMENT NOTES

Re-assessment will be calculated as per the following:

- Lab Exam Re-assessment: 30% of the total points shall be given to this assessment.
- Written Exam Re-assessment: 30% 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:
  1. Mobile Forensics (FORC developed textbook).
  2. Lecture Handouts.
- References:
  1- Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation.
  2- Mobile Forensics: Advanced Investigative Strategies.
- Online resources:
  1. Forensics Wiki, https://forensicswiki.org
  2. Digital Corpora, http://digitalcorpora.org
  3. SANS DFIR, https://digital-forensics.sans.org

CREDIT VALUE	3	**ECTS VALUE**	
PRE-REQUISITE MODULES	1. Operating Systems. 2. Computer Networks. 3. FORC Courses: 3.1. Foundation of Digital Forensics.		

	3.2. Digital Forensic Procedures. 3.3. Digital Investigation Techniques and Tools. 3.4. Network Forensics.		
CO-REQUISITE MODULES	N/A		
NQF LEVEL (FHEQ)	(4th Year Level)	**AVAILABLE AS DISTANCE LEARNING**	No
ORIGIN DATE	**23/04/2018**	**LAST REVISION DATE**	**04/10/2018**
KEY WORDS SEARCH	Mobile forensics, Cellular Networks, Cellebrite, U/SIM.		