MODULE TITLE	Network Forensics				**CREDIT VALUE**	3
MODULE CODE	D2			**MODULE CONVENOR**	**Dr. Mohammad Ababneh / PSUT**	
DURATION	**TERM**	**1**	**2**	**3**	**Number Students Taking Module (anticipated)**	**20**
	WEEKS		16			

DESCRIPTION – summary of the module content (100 words)

This course introduces the methodology and procedures associated with digital forensic analysis in a network environment. Students will develop an understanding of the fundamental protocols, tools, equipment and applications required to conduct forensic analysis in a network environment. Students will learn about the importance of network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. The course will incorporate laboratory exercises and case studies to reinforce practical applications of course instruction.

MODULE AIMS – intentions of the module

The aim of this module is to equip students with the skills required to carry out network forensic analysis. In today's increasingly interconnected world such skills are in high-demand from employers. Through team-based assignments, seminars, and problem-based learning. Students will confront a range of real world network forensics issues and implement approaches for dealing with them.

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	Perform network forensics and extract evidence.
2	Appropriately apply some industry standard forensics tools.
3	Perform network protocol analysis
Discipline Specific Skills and Knowledge:	
4	Apply knowledge of network forensics to respond to network security threats and attacks
5	Apply network forensics to professionally respond to legal challenges and provide irrefutable evidence
Personal and Key Transferable/ Employment Skills and Knowledge:	
6	Analyze logs and other traces left on compromised computers.
7	Analyze and interpret TCP/IP traffic
8	Use open source forensic tools to retrieve forensic artefacts
9	Use network forensics techniques to extract network evidence from sources
10	Differentiate between normal traffic and anomaly traffic

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

1. Introduction to Network Forensics
2. Network Foundations and Protocols
3. Traffic Analysis
4. Network Systems Forensics
5. Network Evidence Collection and Examination

LEARNING AND TEACHING

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

Scheduled Learning & Teaching activities	48	Guided independent study	88	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 (12x2)	Labs
Guided independent study	24	Assignments
Guided independent study	24	Lab write-ups
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
Labs	8 x 2	1-4	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	12	1-10	LMS, Paper
Labs	30	8 x 2	1-10	Graded report
Written Exams	40	1 x 40%	1-10	Graded Exam

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

RE-ASSESSMENT NOTES –

re-assessment 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: Network Forensics, FORC Book, 2018.

Other resources:

- Davidoff, S., Ham, J. (2012) Network Forensics- Tracking Hackers through Cyberspace. ISBN: 0132564718
- Brunty, J., Helenek, K. (2012). Social Media Investigation for Law Enforcement. ISBN: 1455731358
- Datt, S. (2016) Learning Network Forensics. ISBN: 9781785282126.

CREDIT VALUE	3	**ECTS VALUE**	**5**
PRE-REQUISITE MODULES	Digital Forensics, Network Security, Computer Networks		
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	4th year	**AVAILABLE AS DISTANCE LEARNING**	NO
ORIGIN DATE		**LAST REVISION DATE**	**22/06/2018**
KEY WORDS SEARCH	**Network Forensics, Traffic Analysis, Logging, SIEM**		