MODULE SPECIFICATION

Part 1: Information			
Module Title	Security and Forensic Tools		
Module Code	UFCFJ6-30-2	Level	Level 5
For implementation from	2018-19		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Contributes towards			
Module type:	Standard		
Pre-requisites	Computer Crime and Digital Evidence 2018-19		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Educational Aims: The module provides a more advanced, coherent and detailed investigation of a number of some common security and forensic software and hardware tools together with a set of technical knowledge and experience regarding computer systems. The principal aim is to reinforce and build on concepts and practical knowledge introduced at Level 1 to give students the practical and theoretical knowledge base required for them to take up placement opportunities in their specialist fields and to progress to Level 3 study. The main emphasis is on Microsoft Windows operating systems, though Linux/Unix will be covered where appropriate.

Outline Syllabus: N.B. The following content list is organised by topic and is not intended to be in chronological order of presentation.

The module will be regularly updated to cover new tools and techniques. The following is an indicative list of content:

Case practice:
Review of incident response procedures

Digital Evidence acquisition methods and procedures
Report writing and presentational skills
Security and Forensic case studies and practice

Computer-based forensics and security:
Search techniques (inc. GREP) and strategies
EnCase: advanced concepts and internals
FTK: concepts and internals
Indexing and searching
Malware analysis
Virus checkers

Network-based forensics and security:
Network-based tools (e.g. netcat, ping, vulnerability assessment tools etc.)
Network packet sniffers (e.g. Wireshark)
Intrusion detections systems – e.g. Snort
Penetration testing: theory, ethics and practice

e-Discovery and e-Disclosure:
Context
Tools and Techniques
Database topics for e-Discovery

Computer systems internals:
Review of Boot Process, Partitions and File Systems
Review of data formats
FAT internals
NTFS internals
Windows and Linux OS artifacts and evidence locations

Databases for Forensics and Security:
SQL
XML
Data mining fundamentals
Scripting languages

Teaching and Learning Methods: Scheduled learning
Lectures are used to present basic concepts and context and provide an introduction to the laboratory work and independent learning. Laboratory sessions provide space for students to initiate practice on the materials deriving from the lectures whilst being able to receive personal support as required. These sessions also provide an opportunity for staff and students to interact regarding the case studies.

Independent learning
Students are expected to work outside scheduled classes on practice and assignment work.

Part 3: Assessment

Assessment will consist of online exercises, individual report, and a group presentation. The assessment is designed to encourage student engagement, and provide opportunities for feedback to the students, during the module. In this way, students will have the opportunity to reflect on their progress and further develop their understanding of the material presented.

Report: the report will be based upon the examination of a forensic case study. This will show not only report writing skills, but also knowledge of the technical aspects of forensic recovery and analysis. It will also include contemporaneous notes, enabling development of the professional responsibilities associated with forensic analysis. The nature of the case study will require the students to apply knowledge of tools and techniques gained in lectures and laboratory sessions to a simulated real-world scenario. The assessment is designed to extend skills developed in year 1 and to prepare students for more intensive case work in year 3.

Exercises: a series of light-weight individual on-line exercises, for example Blackboard quizzes, each of which must be completed within a time period and will give the students immediate feedback. Each exercise will attract equal marks.

Group presentation: this will require students to work within a group, analysing and evaluating a security based tool, to propose new or enhanced features for the tool. The presentation will include a demonstration of the tool being used. Students will present their findings to the lecturer and fellow students.

The following will be assessed on an individual basis (80%)
1. The materials produced by an individual.
2. The content of the individual's section of the presentation.
3. The reflection and critical analysis demonstrated by the individual.
4. The individual's presentational skills.

The overall structure and coherence of the presentation will be assessed on a group basis (20%).

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Report - Component B	✓	48 %	Individual written report on a forensic case study.
Presentation - Component A		40 %	Group work analysis, evaluation and demonstration of a security based tool, presenting to the lecturer and fellow students.
In-class test - Component B		12 %	Series of in-class exercises
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Report - Component B	✓	48 %	Individual written report on a forensic case study
Portfolio - Component B		12 %	Portfolio of individual exercises
Examination - Component A		40 %	Seen examination (3 hours)

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will be able to:

	Module Learning Outcomes
MO1	Understand, select and utilise an extensive range of forensic and security tools appropriate to the case study environments encountered
MO2	Self-manage investigations of cases
MO3	Organise and present information via written or oral reports
MO4	Evaluate existing tools and tool market sectors to identify strengths and weaknesses and develop proposals for new tools or enhancements to existing tools

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	228
Total Independent Study Hours:	228
Scheduled Learning and Teaching Hours:	
Face-to-face learning	72
Total Scheduled Learning and Teaching Hours:	72
Hours to be allocated	300
Allocated Hours	300

Reading List

The reading list for this module can be accessed via the following link:

https://uwe.rl.talis.com/modules/ufcfj6-30-2.html