UWE Bristol | University of the West of England

MODULE SPECIFICATION

Part 1: Information			
Module Title	Computer Crime and Digital Evidence		
Module Code	UFCFP4-30-1	Level	Level 4
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	Forensic Computing and Security [Sep][SW][Frenchay][4yrs] BSc (Hons) 2018-19 Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] BSc (Hons) 2018-19 Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] BSc (Hons) 2018-19 Forensic Computing and Security [Sep][SW][Frenchay][4yrs] BSc (Hons) 2018-19		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description
Educational Aims: See Learning Outcomes **Outline Syllabus:** Legal matters Categories of computer crime: offences against confidentiality and integrity; computer-related offences (e.g. fraud, forgery, copyright etc.); content-related offences (e.g. child pornography). Law pertaining to computer crime: Computer Misuse Act 1990; EU CyberCrime Convention 2003; applicable international law may also be presented. Law relating to evidence: Police and Criminal Evidence Act 1984; Regulation of Investigatory

Powers Act 2000; Data Retention and Investigatory Powers Act 2014; challenges in applying existing legislation to forensic computing.

Responsibilities of Forensic Computing practitioner: securing evidence; ensuring continuity of evidence; use of auditable procedures when investigating evidence; admissibility of evidence specifically legally-admissible report writing; the need for impartiality; regulation and licensing.

Computer Crime investigation and incident response forms of digital evidence: emails, documents, images, residual information. Investigative strategies for digital evidence and computer crime scenes. Relationships between people, organisations, information systems and information technology. Differing roles, expectations and activities.

Introduction to investigative tools: Generic: hex editors, search tools etc.; Professional: EnCase. To include practical experimentation and preliminary investigation with these tools.

Search and retrieval, especially e-documents and other data. Classification, meaning and interpretation in different social and legal contexts. Ordering and sorting. Evaluating information sources. Creating a criminal profile from digital evidence - statistical analysis of probabilities.

Low-level information structures: hard disk formats: Windows: DOS, FAT, NTFS; Unix; Apple/Mac. partitions and free space. File structures and formats, file compression.

Teaching and Learning Methods: The module will have two lecture strands. In one strand, theoretical information and good working practices will be presented, whilst the second strand will be more practically based, possibly working through the complete solution to a problem. Good communication and presentation skills are of particular importance to when presenting evidence and additional occasional lectures will focus on communication, modelling and analysis.

Practical sessions will enable the students individually to become proficient and self-sufficient in all aspects of forensic computing and computer security under the guidance of the teaching staff.

Part 3: Assessment

The assessment is designed to assist the students transition into higher education, and to encourage student engagement through the course of the module. The assessment will consist of an individual report and a portfolio.

The Report will take place in the first semester. This will be an individual report on the forensic analysis of a case, showing not only report writing skills but also a knowledge of the technical aspects of forensic recovery and analysis, and the use of contemporaneous notes. Students will take the skills developed in the first semester in writing contemporaneous notes, and demonstrate these further in their portfolio via a weekly log.

The Portfolio will take place in the second semester and will be based around the legal context of computer crime and digital evidence. This portfolio based component is designed to facilitate an assessment for learning approach, and will provide opportunities for feedback to the students during the module, allowing students to reflect on their progress and further develop their understanding of the material presented. The portfolio will allow for a range of activities. For example; minutes and agendas from meetings, the application of legislation to the forensic case studied in semester 1, a group teaching session on a legal case which allows their peers the opportunity to provide feedback, a discussion and comparison of two legal cases, a weekly log in contemporaneous notes format.

Referral assessment will consist of an examination and /or coursework. The introduction of a resit examination allows students who have not successfully achieved the learning outcomes via a portfolio based approach, the opportunity to demonstrate their understanding via a different assessment mechanism.

First Sit Components	Final Assessment	Element weighting	Description
Report - Component B		50 %	Technical Report
Portfolio - Component A	✓	50 %	Portfolio
Resit Components	Final Assessment	Element weighting	Description
Report - Component B		50 %	Technical report
Examination - Component A	✓	50 %	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 — Demonstrate a detailed knowledge of laws pertaining to computer crime and digital evidence. MO2 — Evaluate the significance and likely impact of new and emerging law and regulations with respect to acquiring and assimilating new knowledge in both legal and computing fields. MO3 — Assess tools and techniques for investigating computer crime enabling the identification of low level information structures and hardware file formats. MO4 — Evaluate appropriate forensic computing investigative strategies and select available tools based on their appropriateness for a given investigation. MO5 — Understand how to use software tools to investigate the contents of electronic storage devices. MO6 — Create reports that use a language and format appropriate to their use in a court of law.
Contact Hours	**Contact Hours** **Independent Study Hours:** Independent study/self-guided study — 204 **Total Independent Study Hours:** — 204 **Scheduled Learning and Teaching Hours:** Face-to-face learning — 96

	Total Scheduled Learning and Teaching Hours:	96
		4
	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/ufcfp4-30-1.html	