Module Specification

Computer Crime and Digital Evidence

Version: 2023-24, v5.0, 23 May 2023

Contents

Part 1: Information

Module title: Computer Crime and Digital Evidence

Module code: UFCFP4-30-1

Level: Level 4

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Delivery locations: Not in use for Modules

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Not applicable

Features: Not applicable

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.

Part 3: Teaching and learning methods

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.

Module Learning outcomes: On successful completion of this module students will achieve the following 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.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 204 hours

Face-to-face learning = 96 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcfp4-30-1.html

Part 4: Assessment

Assessment strategy: 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.

Assessment components:

Portfolio (First Sit)

Description: Portfolio
Weighting: 50 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2

Report (First Sit)
Description: Technical Report
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO3, MO4, MO5, MO6

Portfolio (Resit)
Description: Portfolio
Weighting: 50 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2

Report (Resit)
Description: Technical report
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO3, MO4, MO5, MO6

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2023-24

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2022-23

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2022-23