Module Specification

Computer Crime and Digital Evidence

Version: 2024-25, v5.0, 07 Jun 2024

Contents

Part 1: Information

Module title: Computer Crime and Digital Evidence

Module code: UFCFP4-30-1

Level: Level 4

For implementation from: 2024-25

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

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: This exciting module is an introduction to the world of "Cyber Crime" and "Digital Forensics".

The module covers the problems posed by modern Cyber Crime, Criminals and their impact on society.

The module progresses from theoretical discussions to practical based lab work that

outlines the forensic principles and tools used to preserve and extract digital evidence.

Features: Not applicable

Educational aims: The overall educational aims of the module are to furnish the student with fundamental knowledge so that they can confidentially define and identify Cyber Criminals and their associated criminal activities.

By the end of the module not only will the students be able to confidently discuss the activities related to Cyber Crime but they will also be able to identify "Digital Evidence" that may be left behind following an attack. Students will use Tools, Techniques and Procedures (TTP's) adopted by law enforcement and the military to solve real world problems and scenarios that forensic investigators face on a day to day basis.

The practical and theoretical skills and knowledge gained in the completion of this module serve as the foundation for all other Digital Forensics content that the students will encounter on the programme.

Outline syllabus: TB1: The module will start with introducing students to cyber crime global, regional and local landscapes with specific focus on factors contributing to evolution of cyber crime over decades. Students will gain an understanding of intricacies associated with computer-enabled and computer-dependent crime. Key actors and practices tackling computer-crime will be explored.

TB2: The students will be introduced to the fundamental concepts of Digital Forensics, the principle frameworks and methodologies that underpin this forensic science. The students will be provided with an overview of the key legislation and accreditation standards that are synonymous with Digital Forensic investigaitons. The use of case studies and introduction to the high level use of Forensic tools will take place in the first few weeks of TB2.

Teaching will then shift focus to the Forensic tools and techniques that are utilised in real world investigations to preserve and recover Digital Evidence. Students will learn how low level information structures are represented and identified by forensic

tools, as well as pertinent Computer Artefacts left behind as a result of User interaction.

The module will culminate with the practical testing, documentation and validation of forensic tools and techniques to recover potential Forensic Artefacts of evidential interest.

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. Good communication and presentation skills are of particular importance, when presenting evidence and additional occasional lectures will focus on communication, modelling and analysis.

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

Formative feedback will be delivered with use of digital tools for learning i.e. Menti.

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

MO1 Evaluate, evidence and communicate information related to cyber crime and forensics.

MO2 Assess tools and techniques for investigating computer crime.

MO3 Evaluate appropriate forensic computing investigative strategies and select appropriate tools.

MO4 Clearly document Standard Operating Procedures (SOPs) for the validation and deployment of forensic tools.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 204 hours

Face-to-face learning = 96 hours

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: Students will work in groups towards a presentation. The presentation will require students to identify a cyber crime issue and relevant audience. Students will be required to provide a security briefing to the targeted audience.

Create a Forensic toolkit to investigate specific computer crimes. This is a portfolio of work that will contain the validation and testing of the forensic tool with a SOP implementation document.

The resit strategy is the same as the first sit.

Assessment tasks:

Presentation (First Sit)
Description: Security Briefing
Weighting: 50 %
Final assessment: No
Group work: Yes
Learning outcomes tested: MO1

Portfolio (First Sit)
Description: Forensic Tool Kit Creation.
Weighting: 50 %

Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3, MO4

Presentation (Resit)
Description: Security Briefing
Weighting: 50 %
Final assessment: No
Group work: Yes
Learning outcomes tested: MO1

Portfolio (Resit)
Description: Forensic Tool Kit Creation.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

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

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2024-25

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2024-25

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

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

Computer Security and Forensics {Foundation} [GCET] DipHE 2023-24