Module Specification

Forensic Computing Practice

Version: 2024-25, v3.0, 20 May 2024

Contents

Part 1: Information

Module title: Forensic Computing Practice

Module code: UFCFC5-15-3

Level: Level 6

For implementation from: 2024-25

UWE credit rating: 15

ECTS credit rating: 7.5

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: Forensic Computing Practice draws together the knowledge gained from Computer Crime and Digital Evidence and Security and Forensic tools in the final core, Digital Forensics input on the award.

Students will be equipped with vital, practical skills that will assist them in becoming Digital Forensic Practitioners as they look to enter industry at the end of the academic year.

Features: Not applicable

Educational aims: The overall educational aim for the module is to initially review and formatively assess foundational knowledge from Computer Crime and Digital Evidence and Security and Forensics Tools.

As the module progresses the students will be taught practical skills to secure and process digital evidence from a live digital crime scene.
Students will be introduced to new digital forensics concepts and artefacts not yet discussed on the course such as mobile device forensics and non-windows based Operating Systems.

Soft, professional skills that will prepare students to become digital forensic practitioners will also feature across the module i.e. Technical CV writing and competency-based interview techniques (STAR).

The module will culminate in a practical skills test that will allow students to demonstrate their proficiency in identifying and capturing evidence from a live crime scene.

Outline syllabus: As with many project modules there is no particular syllabus content other than that covered by earlier modules, in particular the pre-requisite modules. The aim here is for students to apply their technical knowledge and put into practice the skills developed earlier in the programme in realistic computer crime scenarios.

Students will be introduced to all-encompassing live crime scene procedures and processes that will then shift focus to instances where digital evidence may be present. The "Order of volatility" will be reintroduced to the students from earlier modules and practical skills will be taught that will enable them to confidentially identify and secure evidence from volatile and non-volatile sources on a live crime scene.
The module will progress to include areas of digital forensics that have not yet be covered i.e. Mobile Device Forensics with content provided from the Magnet Forensics/AXIOM academic programme.

The module aims to expose the students to every day activities that a Digital Forensics Examiner may encounter in the everyday practice of evidence preservation and analysis.

Part 3: Teaching and learning methods

Teaching and learning methods: Scheduled learning:
Laboratory sessions.

Over the course of the academic year students should expect to spend approximately:
36 hours contact time
114 hours in independent study, including time spent in their teams working on the assignment.
(150 hours in total)

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

MO1 Demonstrate ability to identify and secure crime scene artefacts.

MO2 Demonstrate ability to process and preserve digital evidence.

MO3 Critically appraise processes of digital evidence collection.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 0

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/ufcfc5-15-3.html

Part 4: Assessment

Assessment strategy: The assessment strategy will involve group work in teams of 4 - 5 students.

The teams will produce a framework for securing a live crime scene that will need to be signed off prior to commencement of the practical skills test. This will detail steps and procedures that the team will follow should they encounter volatile evidence or dead box artefacts. The document will contain a critical appraisal of how potential actions may impact digital evidence.

The teams will be required to process, document and seize digital evidence on scene. The students will be observed and assessed on their efficiency and effectiveness of securing the crime scene.

The team will then produce and "MG11 witness statement" detailing their actions on scene. The statement will be cross checked with their framework to ensure that the process that they have followed aligns to their proposed framework.

The resit strategy will be the same as the first sit.

Assessment tasks:

Report (First Sit)
Description: A team based practical skills assessment.

Students will identify and secure digital evidence in a live digital crime scene setting.

Following the execution of the crime scene investigation the team will collectively provide a formal written account of their actions via an MG11 witness statement.
Weighting: 100 %
Final assessment: Yes
Group work: Yes

Learning outcomes tested: MO1, MO2, MO3

Report (Resit)
Description: A team based practical skills assessment.

Students will identify and secure digital evidence in a live digital crime scene setting.

Following the execution of the crime scene investigation the team will collectively provide a formal written account of their actions via an MG11 witness statement.
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Information Technology {Top-Up} [Gloscoll] BSc (Hons) 2024-25

Information Technology {Top-Up} [Gloscoll] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

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

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Cyber Security and Digital Forensics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Feb][FT][GCET][4yrs] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Oct][FT][GCET][4yrs] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Feb][SW][GCET][5yrs] BSc (Hons) 2020-21

Forensic Computing and Security {Foundation} [Sep][SW][Frenchay][5yrs] - Not Running BSc (Hons) 2020-21

Cyber Security and Digital Forensics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2020-21

Computer Security and Forensics {Foundation} [Oct][SW][GCET][5yrs] BSc (Hons) 2020-21

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2024-25

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2023-24

Information Technology {Dual}[Taylors] BSc (Hons) 2022-23