



Module Specification

Security and Forensic Tools

Version: 2021-22, v2.0, 06 Oct 2021

Contents

Module Specification	1
Part 1: Information	2
Part 2: Description	2
Part 3: Teaching and learning methods	4
Part 4: Assessment.....	5
Part 5: Contributes towards	7

Part 1: Information

Module title: Security and Forensic Tools

Module code: UFCFJ6-30-2

Level: Level 5

For implementation from: 2021-22

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: Frenchay Campus, Taylors University

Field: Computer Science and Creative Technologies

Module type: Standard

Pre-requisites: Computer Crime and Digital Evidence 2021-22

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: 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

Part 3: Teaching and learning methods

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.

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

MO1 Understand, select and utilise an extensive range of forensic and security tools appropriate to the case study environments encountered On successful completion of this module students will achieve the following learning outcomes.

MO2 Self-manage investigations of cases On successful completion of this module students will achieve the following learning outcomes.

MO3 Organise and present information via written or oral reports On successful completion of this module students will achieve the following learning outcomes.

MO4 Evaluate existing tools and tool market sectors to identify strengths and weaknesses and develop proposals for new tools or enhancements to existing tools

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 hours

Total = 300

Reading list: The reading list for this module can be accessed at [readinglists.uwe.ac.uk](https://uwe.rl.talis.com/modules/ufcfj6-30-2.html) via the following link <https://uwe.rl.talis.com/modules/ufcfj6-30-2.html>

Part 4: Assessment

Assessment strategy: Assessment will consist of online exercises, individual report, and a 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.

Presentation: this will require students to analyse and evaluate 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.

The resit strategy takes a similar approach as for the main sit.

Assessment components:

Report - Component B (First Sit)

Description: Individual written report on a forensic case study.

Weighting: 48 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3

Presentation - Component A (First Sit)

Description: Pre-recorded presentation of the analysis, evaluation and demonstration of a security based tool.

Weighting: 40 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO3, MO4

In-class test - Component B (First Sit)

Description: Series of in-class exercises

Weighting: 12 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3

Presentation - Component A (Resit)

Description: Pre-recorded presentation of the analysis, evaluation and demonstration of a security based tool.

Weighting: 40 %

Final assessment: No

Group work: No

Learning outcomes tested:

Portfolio - Component B (Resit)

Description: Portfolio of individual exercises

Weighting: 12 %

Final assessment: No

Group work: No

Learning outcomes tested:

Report - Component B (Resit)

Description: Individual written report on a forensic case study

Weighting: 48 %

Final assessment: Yes

Group work: No

Learning outcomes tested:

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Forensic Computing and Security [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Forensic Computing and Security [Sep][FT][Frenchay][3yrs] BSc (Hons) 2020-21

Cyber Security and Digital Forensics [Sep][FT][Frenchay][3yrs] BSc (Hons) 2020-21

Cyber Security and Digital Forensics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Computer Security and Forensics {Foundation} [Feb][FT][GCET][4yrs] BSc (Hons)
2019-20

Computer Security and Forensics {Foundation} [Oct][FT][GCET][4yrs] BSc (Hons)
2019-20

Forensic Computing and Security {Foundation} [Sep][SW][Frenchay][5yrs] BSc
(Hons) 2019-20

Forensic Computing and Security {Foundation} [Sep][FT][Frenchay][4yrs] BSc
(Hons) 2019-20