Module Specification

Cyber Security Forensics

Version: 2024-25, v1.0, 11 Jul 2023

Contents

Part 1: Information

Module title: Cyber Security Forensics

Module code: UFCE53-30-2

Level: Level 5

For implementation from: 2024-25

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field:

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 module will offer you an insight into the realm of cybercrime investigation as a pursuit through a landscape of potential evidence, leveraging an assortment of contemporary digital forensics tools and methodologies.

Features: Not applicable

Educational aims: This module aims to endow students with fundamental knowledge and skills in identifying and investigating cybercrimes, appreciating the

nuances that inform methodological decisions, selecting and deploying appropriate digital forensics tools, and critically evaluating and refining their investigative approach.

It also seeks to foster an understanding of the ethical, legal, and regulatory considerations arising from the practice of cyber forensics and the use of forensic tools for data recovery and threat analysis

Outline syllabus: Role of a cyber forensics investigator, and common tools used

Wireshark, Foremost, Linux, Bash scripting

Legal, ethical, and regulatory aspects of cyber forensics

Regulations like GDPR, Computer Misuse Act, Digital Millennium Copyright Act

Principles and methodologies in digital forensics

Chain of custody, incident response, evidence acquisition and preservation

Application of network analysis in detecting cyber threats

Network traffic analysis, intrusion detection and prevention

Hands-on forensic investigations in a virtualised environment

Use of VMs, digital evidence search and recovery

Principles of file access controls and audit procedures

User permissions, audit logs, intrusion detection systems

Case studies on real-life cyber incidents

Network breach, malware infection, insider threat investigation, phishing incident analysis

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching will be conveyed through a mix of methods, encompassing in-person lectures, supplementary readings, and forensic tool practice guides. Students will engage in on-campus dialogue and hands-on sessions, where they'll be motivated to delve into and expand on the ideas and concepts originating from lecture content. In addition, students will receive assistance in completing practical exercises using forensics tools, which will enhance their proficiency in undertaking module assignments.

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

MO1 Critically evaluate the role of a cyber forensics investigator, the tools and techniques employed in the field, and the ethical, legal, and regulatory aspects of the profession.

MO2 Explain the principles of file access controls and audit procedures for safeguarding business assets and understand the lockdown and isolation procedures in response to security breaches.

MO3 Critically assess the current state-of-the-art in digital forensics, including network analysis and data recovery techniques, to evaluate the strengths and weaknesses of existing methodologies.

MO4 Demonstrate practical skills that indicate a definitive career path into cyber forensics, including proficiency in network analysis, digital evidence recovery, breach response, and contextualisation of cyber threats.

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 via the following link

Part 4: Assessment

Assessment strategy: Exam (online) - 1 hour
Portfolio - Digital Forensics Investigation

The Cyber Security Forensics module is assessed using a combination of a written exam and a practical portfolio.

The multiple-choice exam will gauge students' understanding and proficiency in the various topics covered in the syllabus. It will assess their grasp of cyber forensics concepts, techniques, and legal aspects.

The practical portfolio requires students to apply their knowledge of cyber forensics concepts and tools to investigate, analyse, and respond to specified cybercrimes using a provided VM. This hands-on task allows students to demonstrate their skills in areas like network analysis, digital evidence recovery, and breach response. All completed tasks should adhere to industry best practices and highlight students' ability to apply forensic techniques to real-life cyber incidents.

Throughout the module, tutor-led formative feedback will be provided to assist students in their learning and development.

The resit opportunity should follow a similar format to the first assessment. A re-work of the first assessment may be considered.

Assessment tasks:

Examination (Online) (First Sit)
Description: Cyber Forensics Principles and Practice Multiple-choice exam (1 hour)

Weighting: 30 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO3

Portfolio (First Sit)
Description: Digital Forensics Investigation
Weighting: 70 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO4

Examination (Online) (Resit)
Description: Cyber Forensics Principles and Practice Multiple-choice exam (1 hour)
Weighting: 30 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO3

Portfolio (Resit)
Description: Digital Forensics Investigation
Weighting: 70 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Digital and Technology Solutions (Cyber Security Analyst) {Apprenticeship-UCW} [UCW] BSc (Hons) 2023-24