Module Specification

Digital Forensics for Cyber Security

Version: 2023-24, v1.0, 21 Mar 2023

Contents

Part 1: Information

Module title: Digital Forensics for Cyber Security

Module code: UFCE3Y-15-M

Level: Level 7

For implementation from: 2023-24

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: Global College of Engineering and Technology (GCET)

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: DForCySec provides a comprehensive overview of the fundamental methodologies, key principles, tools and techniques that underpin a digital forensic investigation. Theoretical knowledge is consolidated with lab-based practical's that are designed in line with scenarios that an investigator will commonly encounter in real world scenarios.

Features: Not applicable

Educational aims: The module begins with an introduction to the key methodologies and principles that provide the foundational knowledge of how to deal with “Live” and “Deadbox” forensics in order to prove evidential integrity. Students will learn of the contemporary challenges and problems that real investigators face in the field of digital forensic casework.

As the module progresses students will know how to identify, extract and process both volatile and non-volatile digital evidence, by critically appraising and selecting the appropriate tools.

At the end of the module the students will be able to identify, extract, items of evidential importance and record their findings in a forensically sound manner.

Outline syllabus: The module will cover the following threshold concepts and topics:

Digital forensic fundamentals: The module begins with an introduction to forensic science it’s overall aim and how digital forensics is derived from this. The topic progresses to explain evidence exchange theory and the similarity between physical and digital domain. Suitable forensic methodologies and frameworks will be highlighted via the reading list and key forensic principles will be referenced as a foundation to build upon. Students will learn how to record their investigative actions in a forensically sound, impartial manner.

The topic will culminate in a brief overview of legislation, legislating bodies (UKCAS – ISO 17025/FSR Codes of practice) and how these impact the field of digital forensics. Current challenges will be highlighted with a review of reports such as the Forensic Science Strategy, authored by the “Forensic Capability Network.”

Forensic strategies for investigation: Strategies for forensic investigations are the “silver thread” that run throughout the module. Students will learn suitable approaches to conducting investigations as a case progresses and evolves (System Profiling, identifying indicators of compromise and Identifying user, file system interaction).

An introduction to digital evidence: The foundational knowledge from the introduction is built upon with the discussion of forensic artefacts, their composition, sources and how they can be leveraged to answer the questions that forensic science aims to answer (Who, What, Where, When, Why and How) (Registry, Internet, E-mail, .LNK files, Log files, Prefetch, Volatile data etc).

Forensic tooling: Students are introduced to an open-source forensic toolkit that can be used to extract, process and present digital evidence from its “raw” format. Students will gradually be introduced to tools and how they operate in weekly lab sessions that relate to the subject matter that features for that week (Autopsy, KAPE, SIFT, RegRipper, OphCrack, Volatility, HashCat,FTK Imager).

Part 3: Teaching and learning methods

Teaching and learning methods: Students will be provided the opportunity to consolidate their theoretical knowledge delivered in tutor led sessions on weekly basis. Students will subsequently take part in activity led learning sessions that will be conducted in a lab environment. Situated learning will take place where authentic labs, based on real world problems faced by investigators will be solved, allowing the cohort to put into practice what they have learned.

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

MO1 Explain the implications of investigative actions inline with the core concepts and principles that pertain to Digital Forensic Investigations and Digital Evidence.

MO2 Critically evaluate and employ suitable methodologies and tools to facilitate the capture of digital evidence.

MO3 Identify, extract, and analyse digital evidence from a range of sources.

MO4 Capture and present investigative actions in line with key digital forensic principles

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

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: The overall aim of the module is to provide the student with the critical skills to identify, preserve, capture and record digital evidence in a forensically sound manner.

These skills will be assessed through a series of In Class Tests (ICT). The assessment will follow the format of an evolving cyber-attack. The student will be provided with a data set (image) that becomes increasingly populated with digital evidence after each test. Students will have to answer a series of questions based on their findings and provided a record of their actions of how they have arrived at their conclusion (contemporaneous record).

The overall assessment will have three key themes that will satisfy the module outcomes, each theme is synonymous with digital forensic “Incident response”:

ICT1 (20%): System Profiling, students will be expected to profile a windows computer system, identifying user accounts, system activity and critical configuration information.

ICT2 (20%): Cyber attack! The students will be provided with the same image, with additional seeded evidence that contain “Indicators of compromise”. The additional artefacts will be synonymous with a system that has been accessed by a threat actor and are more complicated to identify and analyse.

ICT3 (60%): Compromise, The students will have to identify file system and file artefacts to determine if/how files have been exfiltrated proving, unauthorised, criminal activity in the process.

Each in class test will increase in difficulty and will cover different facets and specialist techniques of a forensic investigation. ICT will be marked automatically.

Students will be required to keep a contemporaneous log (notes) of their actions for each investigation but will submit their notes on ICT3 for marking, the notes will be weighted and class as a percentage towards the final test. Formative feedback can be provided to the cohort regarding notes after ICT 1 and 2 from observations of notes across the class.

Formative assessment will take place with the aid of digital tools (Menti) to capture the cohorts understanding of key concepts. Further diagnostic assessment will be used to follow up on this in lab sessions should there be any gaps in knowledge that have been identified.

The resit structure is the same as the first sit.

Assessment tasks:

In-class test (First Sit)
Description: In-Class test (ICT1) 90 minutes
Weighting: 20 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

In-class test (First Sit)
Description: In-class test (ICT2) 90 minutes
Weighting: 20 %
Final assessment: No
Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

In-class test (First Sit)

Description: In-class test 3 (ICT3) 90 minutes

Weighting: 60 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

In-class test (Resit)

Description: In-Class test (ICT1) 90 minutes: Resit

Weighting: 20 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

In-class test (Resit)

Description: In-Class test (ICT2) 90 minutes: Resit

Weighting: 20 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

In-class test (Resit)

Description: In-Class test (ICT3) 90 minutes: Resit

Weighting: 60 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [GCET] MSc 2023-24

Cyber Security [Frenchay] MSc 2022-23