Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM663
Module Title	Digital Forensics
Level	6
Credit value	20
Faculty	FACE
HECoS Code	100385
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core
Stand-alone module aligned to BSc (Hons) Cyber Security for QA and assessment	Option

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	12 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	12 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**24** hrs
Placement / work based learning	0 hrs
Guided independent study	176 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2026
Date and details of revision	

For office use only	
Version number	1

Module aims

This module aims to equip students with the necessary knowledge and skills to effectively investigate and analyse digital evidence in the context of legal proceedings or cybersecurity incidents. The primary objective is to provide a comprehensive understanding of the principles and methodologies employed in the field of digital forensics. The module aims to foster critical thinking and problem-solving abilities, allowing students to apply forensic techniques to real-world scenarios and challenges. Additionally, it aims to promote ethical and professional conduct in handling digital evidence, emphasizing the importance of maintaining integrity, confidentiality, and impartiality throughout the investigative process.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Compare and contrast the concepts, principles, and legal frameworks related to digital forensics.
2	Evaluate and outline the various types of digital evidence and their relevance in different investigative contexts.
3	Analyse and interpret the integrity and reliability of digital evidence, considering potential challenges and limitations.
4	Critically evaluate the effectiveness of digital forensic techniques and tools in different investigative scenarios.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment strategy for the digital forensics' module encompasses both theoretical understanding and practical skill development. The coursework assignments aim to reinforce the acquired knowledge and demonstrate students' comprehension of digital forensics principles, concepts, and legal frameworks. They will also assess the students' ability to evaluate forensic tools, techniques, and methodologies. These assignments may include tasks such as preparing reports, analysing case studies, or conducting practical investigations.

Students will have a two-hour in-class test. This test will evaluate students' theoretical knowledge of digital forensics, requiring them to demonstrate their understanding of key concepts, terminology, and principles within a specified timeframe. The test aims to assess students' theoretical knowledge and comprehension of the subject matter, providing them with an opportunity to showcase their understanding and alignment with industry-level certification standards.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2	Coursework	30%
2	3,4	In-class test	70%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

The learning methodology for this module adopts a blended approach, integrating both theoretical and practical components. Students will engage in a series of workshops and practical sessions, which combine theory-based lectures with hands-on activities. These activities will involve students working on simulated problems and developing solutions.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Cybercrime
- Computer Forensics Fundamentals
- Computer Forensics Investigation Process
- Hard Disks and File Systems
- Data Acquisition and Duplication
- Anti-forensics Techniques
- OS Forensics
- Network Forensics
- Web Attacks
- Email Crimes
- Malware Forensics

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

N/A

Other indicative reading

G. Johansen, *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response*, 3rd Edition. Packt Publishing. 2022.

Shiva V.N. Parasram, *Digital Forensics with Kali Linux.* Shiva V.N. Parasram. 2nd Edition. Packt Publishing. 2020.