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 | CONL723 |
| Module Title | Digital Forensics |
| Level | 7 |
| Credit value | 15 |
| 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 |
|---|---|
| MSc Computer Science with Cyber Security | Core |

## Pre-requisites

None

## Breakdown of module hours

| | |
|---|---|
| Learning and teaching hours | 15 hrs |
| Placement tutor support | 0 hrs |
| Supervised learning e.g. practical classes, workshops | 0 hrs |
| Project supervision (level 6 projects and dissertation modules only) | 0 hrs |
| **Total active learning and teaching hours** | 15 hrs |
| Placement / work based learning | 0 hrs |
| Guided independent study | 135 hrs |
| **Module duration (total hours)** | 150 hrs |

| **For office use only** | |
|---|---|
| Initial approval date | 17/06/21 |
| With effect from date | 28/06/21 |
| Date and details of revision | 27/10/24 Programme revalidation |
| Version number | 2 |

## Module aims

This module will introduce students to the principles of digital forensics to gather and analyse evidence from computer systems and communications. Students will learn the techniques, technologies and tools required to gather information within practical environments, and effectively report the results for consideration within legal and commercial situations.

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

| | |
|---|---|
| 1 | Demonstrate a systematic understanding and critical awareness of a comprehensive range of digital forensics techniques and tools used for discovering information within computer systems. |
| 2 | Make informed judgments by critically evaluating the use of a variety of approaches to digital forensics. |
| 3 | Critically evaluate computer systems and networks to identify and analyse useful information in an ethically sound manner. |
| 4 | Use and adapt digital forensics techniques to analyse existing systems and retrieve pertinent information. |
| 5 | Critically reflect upon, document, and evaluate digital forensics outcomes in a legal, ethical and commercial compliant manner. |

## Assessment

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.

Indicative Assessment Tasks:

Assessment 1 will see students utilise digital forensic techniques within a case study environment in order to understand and report on findings. This will require students to detail processes, findings and recommendations to demonstrate a full understanding of the module content. Assessment 2 will then allow students to demonstrate their further understanding of processes and procedures along with common digital forensics techniques through an in-class test with an indicative length of 90 minutes.

| Assessment number | Learning Outcomes to be met | Type of assessment | Weighting (%) |
|---|---|---|---|
| 1 | 1,2,5 | Coursework | 70% |
| 2 | 3,4 | In-class test | 30% |

## Derogations

None

## Learning and Teaching Strategies

The overall learning and teaching strategy is one of guided independent study requiring ongoing student engagement. Online material will provide the foundation of the learning resources, requiring the students to log in and engage regularly throughout the eight weeks of the module. There will be a mix of suggested readings, discussions and interactive content containing embedded digital media and self-checks for students to complete as they work through the material and undertake the assessment tasks. A range of digital tools via the virtual learning environment and additional sources of reading will also be utilised to accommodate learning styles. There is access to a helpline for additional support and chat facilities through Canvas for messaging and responding.

## Indicative Syllabus Outline

- Introduction to digital forensics
- Acquiring digital evidence
- Operating system forensics
- Web and email forensics
- Antiforensics techniques
- Open source intelligence gathering
- Reporting digital forensics

## Indicative Bibliography:

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

**Essential Reads**

License to access SudoCyber online platform.

**Other indicative reading**

M. Graves, *Digital Archaeology: The Art and Science of Digital Forensics*. Boston, MA: Addison-Wesley Professional, 2013.

A. Årnes, *Digital Forensics*. Wiley-Blackwell, 2017.

T. J. Holt, A. M. Bossler, and K. C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction*, 2nd ed. London, U.K.: Routledge, 2017.

M. Sheward, *Hands-on Incident Response and Digital Forensics*. Swindon, U.K.: BCS, The Chartered Institute for IT, 2018.