Module Definition Form (MDF)

Module code: MOD007376	**Version:** 3 **Date Amended:** 16/Jul/2026

1. Module Title
Principles of Digital Forensics

2a. Module Leader
Steven Shepherd

2b. School
School of Computing and Information Sciences

2c. Faculty
Faculty of Science and Engineering

3a. Level
5

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions

Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	BSc (Hons) Cyber Security BSc (Hons) Cyber Security and Digital Forensics		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

Digital forensics is a vital component of modern policing, corporate security, and cybercrime investigation. This module introduces the principles and practices that underpin digital investigative work, including identification of evidence sources, lawful powers of seizure, secure handling procedures, relevant policy and legislation, and established methods for the examination of digital evidence. You will also explore how digital evidence is presented within the criminal justice system, ensuring a balanced understanding of both the technical and procedural dimensions of forensic practice.

Teaching is delivered through a combination of lectures and practical sessions, designed to build a secure theoretical foundation while developing applied competence. You will be introduced to established scientific methods and professional standards that support effective digital forensic investigation.

You will gain hands-on experience using industry-relevant tools and techniques employed in real-world investigations. This practical focus prepares you for careers in law enforcement, corporate security, and specialist roles such as digital forensic analyst, forensic consultant, or e-discovery practitioner. By the end of the module, you will have developed a strong foundation in digital forensics and a clear understanding of its role and importance in an increasingly connected digital environment.

6b. Outline Content

An introduction to the issues pertaining to digital and cyber-crime in the UK and worldwide.

Evidential procedures in relation to identification, seizure and storage of digital evidence.

Legislative and regulatory requirements in relation to digital and cyber-crime.

Digital forensics fundamentals, which can include the Interpretation of:

- File formats such as Microsoft Office files & PDFs to audio/visual media
- File systems such as NTFS & FAT
- Forensic Techniques such as carving, parsing and Windows artefact collection
- Hidden and Deleted Data recovery
- Timeline analysis
- Analysis in static, live and virtual environments
- eDisovery

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

Computer labs with admin rights and the ability to use virtualisation via a tool such as VMware Workstation.

Specialist Digital Forensics Hardware/software and Netlab facilities.

Access to a programming language such as Python.

7. Learning Outcomes (threshold standards)		
No.	**Type**	**On successful completion of this module the student will be expected to be able to:**
1	Knowledge and Understanding	Recognise and define what digital evidence is, and the role it plays in investigations
2	Knowledge and Understanding	Discuss the legislative and regulatory requirements in relation to digital forensics
3	Intellectual, practical, affective and transferrable skills	Analyse complex data and Identify key evidential elements, relating to digital forensics
4	Intellectual, practical, affective and transferrable skills	Construct results in appropriate formats to be comprehensible to a varied audience

8a. Module Occurrence to which this MDF Refers				
Year	**Occurrence**	**Period**	**Location**	**Mode of Delivery**
2026/7	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	**Hours**	**Learning Outcomes**	**Details of Duration, frequency and other comments**
Lectures	12	1-4	12 x 1 Hr(s) Lecture
Other teacher managed learning	24	1-4	12 x 2 Hr(s) Practical
Student managed learning	114	1-4	Self-directed study
TOTAL:	150		

9. Assessment for the above Module Occurrence

The assessment for some modules includes a presentation (see below for details on how this particular module is assessed). We recognise that presenting, especially to a large group, can cause significant anxiety or distress for some students. If this may affect you, please contact your Module Leader or the Disability and Neurodiversity Service as early as possible. We will work with you to consider appropriate reasonable adjustments. Depending on your individual needs, these might include, for example, presenting to a smaller group or presenting only to a member of academic staff.

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Coursework	1-4	100 (%)	Fine Grade	30 (%)
Case Study (equivalent to 3000 words)					

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]