Module Definition Form (MDF)

Module code: MOD006611	**Version:** 10 **Date Amended:** 18/Sep/2026

1. Module Title
Digital Forensics and Malware Science

2a. Module Leader
Andrew Moore

2b. School
School of Computing and Information Sciences

2c. Faculty
Faculty of Science and Engineering

3a. Level
6

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:	None		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

This module introduces the principles and practice of malware analysis within the broader context of contemporary cyber threat intelligence and incident response. You'll explore how malicious software operates, how modern cyber threats are constructed and deployed, and how security professionals interpret and respond to real-world attacks. Case studies are used throughout to ground theory in practice, including the 2024 Qilin ransomware incident affecting NHS pathology services, which caused major disruption across London hospitals and the cancellation of thousands of appointments alongside the theft of sensitive patient data, and the Mirai botnet, which demonstrated the large-scale exploitation of insecure Internet of Things devices such as cameras and routers.

You'll develop practical skills in both static and dynamic malware analysis. Static analysis focuses on examining code structure and binary artefacts without execution, while dynamic analysis involves observing behaviour in controlled sandbox environments. You'll use these approaches to understand malware functionality, identify indicators of compromise, and reconstruct attack behaviour in a safe and systematic way.

The module culminates in a group investigation where you will select a contemporary malware strain or campaign, perform structured analysis, and produce both a technical report and presentation. This includes reverse engineering key behaviours, mapping attack chains, and delivering a threat intelligence briefing in a format consistent with professional security operations practice.

The module emphasises applied analytical skills and professional practice, including secure laboratory procedures, critical interpretation of evidence, and clear communication of technical findings. By the end of the module, you'll be equipped with the skills required for roles in cybersecurity analysis, digital forensics, and security operations environments.

6b. Outline Content

Introduction to Digital forensics concepts

Scientific evidence gathering

Windows 10 & NTFS artefacts

Introduction to Malware Investigation

Process tree and reverse analysis of potential Malware

Producing quality documents, ready for court

6c. Key Texts/Literature

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

6d. Specialist Learning Resources

"Students will be given access to hardware/software write blockers, appropriate tools, toolkits and Virtual Machines via the VMware Academy Program."

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	Demonstrate an in depth understanding of the role of a digital forensics investigator, courts and professional standards.
2	Knowledge and Understanding	Critically appraise malware, including how it infects machines at an operating system level, as an example of a complex engineering challenge, and report findings in a way that considers societal impact, EDI, and is accessible to a varied, non-specialist audience.
3	Intellectual, practical, affective and transferrable skills	Take on a scientific investigation to preserve evidence, understand malware related artefacts and produce a timeline analysis.
4	Intellectual, practical, affective and transferrable skills	Scientifically analyse malware, infection processes and reverse engineer code.

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	1-2	1 hour per week – interactive session
Other teacher managed learning	24	3-4	Practical session
Student managed learning	114	1-4	Background reading of course texts and completing lab exercises
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	Practical	4	20 (%)	Fine Grade	30 (%)
Demonstration (600 words)					

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
011	Practical	1-3	80 (%)	Fine Grade	30 (%)
Demonstration (2400 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]