Module Definition Form (MDF)

Module code: MOD006611	**Version:** 19 **Date Amended:** 24/Feb/2020

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 will build on student knowledge, learnt from the previous module “Digital Forensics”. Students are shown an advanced level of Digital Forensics, from the latest version of the Windows operating system.
As malicious software is becoming more advanced, in this module, students will learn transferable and desirable skills that security researchers/Analysts require for a job in this sector.
Students will gain theory of how Malware is written, deployed and infects a victim’s device. The students will go on to learn practical methods of reverse engineering malicious code.
Malware such as WannaCry has cost the NHS, billions in lost income. Students will learn how to control such Malware/infected files in a sandboxed environment and determine what has happened in a case study scenario.

This module will then lead into the module “Software Security”, in the following trimester.

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	Understand and critically appraise malware, how it infects machines at an operating systems level and report their findings appropriately.
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**
2025/6	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					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
010	Coursework	1-3	20 (%)	Fine Grade	30 (%)
DEMONSTRATION – 600 WORDS					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
011	Coursework	1-4	80 (%)	Fine Grade	30 (%)
ASSIGNMENT – 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]