Liverpool John Moores University

Title:	DIGITAL FORENSICS
Status:	Definitive
Code:	**5105COMP** (121227)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Thomas Berry	Y
Aine MacDermott	

Academic Level:	FHEQ5	**Credit Value:**	20	**Total Delivered Hours:**	57
Total Learning Hours:	200	**Private Study:**	143		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	22
Practical	33

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	A report to investigate a simulated crime.	50	
Exam	AS2	Examination	50	2

Aims

To develop an understanding of the role of computer forensics analyst through the use of existing applications and investigative techniques.

Learning Outcomes

After completing the module the student should be able to:

1 Explain the structure of files and the metadata contained within them.
2 Apply practical knowledge of a number of computer forensic tools as used by practitioners in the field.
3 Compare a range of appropriate methodologies used during an investigation and present the results of the investigation.
4 Interpret the theoretical underpinnings of computer forensics.

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Forensic Investigation	1	2	3
Exam	1	4	

Outline Syllabus

The module will cover the three phases of a computing forensics investigation:
Search Phase:
Search preparation, processing the crime or incident scene, securing evidence from the computer, data acquisition and identification of digital evidence sources. Need to ensure that the ACPO guidelines on Computer Forensics investigations are followed correctly.
Analysis Phase:
Preparing for a computer investigation, the structure and tools required in an investigator's environment, computer forensics software needs, current computer forensics software and hardware, the impact of file and operating systems on the investigation, computer forensics analysis, recovery and investigation of digital image (picture) files and investigating e-mail.
Presentation Phase:
Presenting and reporting the results of a Computer Forensics investigation.

Learning Activities

Lectures and practical work. The practical work builds on core forensic computing concepts covered in the lectures. This involves laboratory and user demonstrations of computer forensic techniques.

Notes

This module is intended to build on first year modules to introduce the students to the practicalities of conducting computer forensics investigations.