Liverpool John Moores University

Title:	Digital Forensics
Status:	Definitive
Code:	**5205COMP** (127984)
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:**	46
Total Learning Hours:	200	**Private Study:**	154		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	22
Practical	22

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	To investigate a simulated crime and report the results	50	
Exam	AS2	Examination	50	2

Aims

To develop an understanding of the role of computer forensics investigator/analyst using existing applications and investigative techniques.

Learning Outcomes

After completing the module the student should be able to:

1 Apply practical knowledge of computer forensic tools as used by practitioners in the field.
2 Compare a range of appropriate methodologies used by an investigation team and present the results of the investigation as a team.
3 Interpret the theoretical underpinnings of computer forensics.
4 Apply computer forensics techniques to theoretical scenarios.

Learning Outcomes of Assessments

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

Forensic Investigation	1	2
Examination	3	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 digital devices, data acquisition and identification of digital evidence sources. The requirement 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 and the current Computer Forensics software and hardware. The impact of file and operating systems on the investigation. Computer Forensics analysis, recovery and investigation of data such as the suspects files, internet history, e-mail, registry, unallocated space, etc.

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. Students will learn to work as an investigation team on their assessment to simulate a work-based scenario.

Notes

This module is intended to build the core computer forensics skills required by the

student to work in the Computer Forensics industry. These skills will be applied to conducting a simulated Computer Forensics investigation.