Liverpool John Moores University

Title:	COMPUTER FORENSICS
Status:	Definitive
Code:	**7002ESE** (120629)
Version Start Date:	01-08-2016
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Denis Reilly	Y

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	38
Total Learning Hours:	200	**Private Study:**	162		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	12
Practical	12
Tutorial	12

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Computer Forensics Analysis and Investigation.	40	
Exam	AS2	Examination.	60	2

Aims

To develop a critical appreciation of both the theoretical and practical issues in the field of computer forensics.
To develop the knowledge of various computer systems and technologies and understand their importance to computer forensics investigations.
To place the field of computer forensics in the wider field of computer science, the

judicial system and national security.
To develop the necessary skills, methodologies and processes to conduct a basic computer forensics investigation within an organisation.

Learning Outcomes

After completing the module the student should be able to:

1 Explain fundamental technical concepts, implementation, and restrictions of computer forensics.
2 Critically analyse and evaluate computer forensics evidence.
3 Explain the role of computer forensics in the wider fields of computer science, the organisation, the judicial system and national security.
4 Critically evaluate recent advances in the field of computer forensics to assess their applicability to an investigation.

Learning Outcomes of Assessments

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

Analysis and investigation	2		
Examination	1	3	4

Outline Syllabus

Computer forensics fundamentals to include:
-Introduction to digital forensics
-Hard drives and storage media
-Computer forensics in law enforcement
-Process models and evidence handling

Computer forensics in practice, to include:
-Investigation of Windows hosts
-File-systems and file analysis
-Data hiding and fraud investigation
-Passwords analysis

Network forensics, to include:
-Network forensic fundamentals
-Investigating networks
-GPS forensics

Contemporary topics in digital forensics
-Examination of several current digital forensics topics

Learning Activities

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

Notes

The purpose of the course is to cover the fundamental technical concepts combined with practical skills and contemporary research essential for computer forensic investigations within the organisation, law enforcement or national security.