Liverpool John Moores University

Title:	COMPUTER AND NETWORK FORENSICS
Status:	Definitive
Code:	**6063COMP** (117507)
Version Start Date:	01-08-2019
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Michael Mackay	Y
Thomas Berry	

Academic Level:	FHEQ6	**Credit Value:**	24	**Total Delivered Hours:**	72
Total Learning Hours:	240	**Private Study:**	168		

Delivery Options
Course typically offered: Standard Year Long

Component	Contact Hours
Lecture	24
Practical	24
Tutorial	24

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Computer forensics investigation	50	
Report	AS2	Forensic analysis of traffic captures	50	

Aims

To develop a critical appreciation of both the theoretical and practical issues in the field of computer and network forensics.
To critically appraise the use of computer and communication networks and their importance to computer forensics investigations.

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

Learning Outcomes

After completing the module the student should be able to:

1	Critically review fundamental technical concepts, implementation, and restrictions of computer and network forensics.
2	Critically evaluate computer and network forensics problems.
3	Critically evaluate recent advances in network technologies to assess their impact and applicability to a network forensics investigation.
4	Apply creative skills relating to analysis of network forensics data evidence.

Learning Outcomes of Assessments

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

Computer forensics	1	2
Forensic analysis	3	4

Outline Syllabus

The course outline includes:
Computer forensics: computer forensics fundamental, network forensics fundamentals, legal considerations and the role of computer and network forensics in law enforcement, the organisation and national security.

Network forensics basics: network forensics fundamentals, understanding network protocols, communications, the Windows network environment and identifying key sources of evidence within a network investigation, networked storage and servers,

Network analysis: email as source of contextual information and evidence, identifying communications path evidence, Web-based email versus client applications and legal considerations when investigating emails, advances in network applications e. g. VoIP, mobile phones and PDAs, social network analysis, live response, attack detection and incident response.

Learning Activities

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

Notes

This advanced course is intended for students interested in the field of computer and network forensics. The purpose of the course is to provide the fundamental technical concepts and research issues essential for computer and network forensics investigations within an organisation, law enforcement or national security.