Liverpool John Moores University

Title:	NETWORK FORENSICS
Status:	Definitive
Code:	**7135COMP** (122203)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Michael Mackay	Y

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	36
Total Learning Hours:	200	**Private Study:**	164		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	12
Practical	12
Tutorial	12

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	A review of current network forensic techniques and a critical analysis of state-of-the-art in a specific application domain.	50	
Practice	AS2	A portfolio of forensic reports based on practical analysis of network traffic data.	50	

Aims

To develop a critical appreciation of both the theoretical and practical issues in the field of network forensics.

To critically appraise the use of computer networks and their importance to computer forensics investigations.
To develop the necessary skills, methodologies and processes to conduct a basic network forensics investigation within an organisation.

Learning Outcomes

After completing the module the student should be able to:

1	Explain the technical concepts, implementation and restrictions of network forensics in a variety of situations.
2	Critically evaluate recent advances in network technologies to assess their impact and applicability to a network forensics investigation.
3	Assess the role of network forensics in the wider fields of networks, computer security, law and computer science.
4	Critically analyse and evaluate network forensics data evidence.

Learning Outcomes of Assessments

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

Critical Review	1	2	3
Forensic portfolio	4		

Outline Syllabus

Introduction to the network environment
Forensic protocol control
Network analysis using wireshark
Network forensics report
Network protocol and malware forensics
Web forensics
Email forensics
Network intrusion detection and incident response
Mobile and wireless network forensics
Future challenges – Cloud Computing

Learning Activities

Formal lectures will introduce core topics. Practical labs will provide an opportunity to inspect and analyse network traffic and become familiar with attack signatures.

Notes

This advanced course is intended for post-graduate students interested in the field of network forensics. The purpose of the course is to provide the fundamental technical

concepts and research issues essential for network forensics investigations within the organisation, law enforcement or national security.