Liverpool John Moores University

Title:	Network Forensics
Status:	Definitive
Code:	**6202COMP** (128002)
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
Alex Akinbi	

Academic Level:	FHEQ6	**Credit Value:**	20	**Total Delivered Hours:**	44
Total Learning Hours:	200	**Private Study:**	156		

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	Report investigating a topic in network forensics	50	
Report	AS2	Forensic analysis of traffic capture	50	

Aims

To develop a critical appreciation of both the theoretical issues of computer networks and their impact on digital forensic investigations.
To explore the emergence of new networking technologies and how they will impact on network forensics.
To develop a practical understanding of network forensics as it applies to common

applications or services.
To build 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	Compare and contrast how the fundamental concepts in computer networking can both help and hinder network forensics.
2	Critically evaluate recent advances in network technologies to assess their impact and applicability to network forensics.
3	Critically interpret network forensics data evidence.
4	Design and plan a forensic investigation of network traffic.

Learning Outcomes of Assessments

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

Investigation report	1	2
Forensic analysis	3	4

Outline Syllabus

Network forensics basics: network forensics fundamentals, understanding network protocols, communications, and the networking environment. Explore common attack vectors and identifying key sources of evidence within a network investigation. Understand common network services such as web and email and investigate how to conduct forensic analysis in an organisational environment. The network forensic process and the key steps that and investigation will progress through. New and emerging technologies.
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, social network analysis, live response, attack detection and incident response.

Learning Activities

Students will participate in lectures and practical lab sessions.

Notes

Computer networking is now a ubiquitous feature of modern life with the applications and services that we rely on daily being supported by the Internet. Conversely, as the services become more fundamental, the number and range of attacks leveled

against them have increased both in severity and frequency. As such, modern digital forensics investigations are increasingly including some element of network investigation and network operators are increasingly employing forensic techniques to effectively manage their infrastructures.