Network Forensics

Module Information

2022.01, Approved

Summary Information

Module Code	6102COMP
Formal Module Title	Network Forensics
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 6
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
Computer Science and Mathematics

Learning Methods

Learning Method Type	Hours
Lecture	33
Practical	22

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
JAN-CTY	CTY	January	12 Weeks

Aims and Outcomes

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.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Compare and contrast how the fundamental concepts in computer networking can both help and hinder network forensics.
MLO2	2	Critically evaluate recent advances in network technologies to assess their impact and applicability to network forensics.
MLO3	3	Critically interpret network forensics data evidence.
MLO4	4	Design and plan a forensic investigation of network traffic

Module Content

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 a 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.
Module Overview	
Additional Information	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 levelled 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 manager their infrastructures.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Network forensics research	50	0	MLO1, MLO2
Report	Analysis of Network Traffic	50	0	MLO3, MLO4

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Michael Mackay	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings