Liverpool John Moores University

Title:	NETWORK FORENSICS
Status:	Definitive
Code:	**7055COMP** (103314)
Version Start Date:	01-08-2011
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team emplid	Leader
Michael Mackay	Y

Academic Level:	FHEQ7	**Credit Value:**	15.00	**Total Delivered Hours:**	36.00
Total Learning Hours:	150	**Private Study:**	114		

Delivery Options

Course typically offered: Semester 2

Component	Contact Hours
Lecture	12.000
Practical	12.000
Tutorial	12.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Review of network forensic techniques and a practical forensic analysis of network data.	100.0	

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:

Network forensic review	1	2	3	4

Outline Syllabus

The course outline includes:
Overview of network forensics: network forensics fundamentals, legal considerations and the role of network forensics in law enforcement, the organisation and national security.
The network environment: protocols, communications, how computers communicate with one another, wireless versus the wired environment, the Windows network environment and identifying key sources of evidence within a network investigation.
Hard drives and servers: investigating traces of network evidence residing on networked hosts and servers.
Email 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: VoIP applications and their relevance to network investigations, Peer-to-Peer networking and its impact on the investigation and ubiquitous computing.
Mobile phones and PDAs: the mobile phone architecture, analysis of mobile phones and PDAs, embedded GPS data and its importance to the investigation and data sources.
Exploiting the network for investigative purposes: identify tools and techniques that an examiner could use for passive network information gathering.
Social network analysis: identification of analysis tools for investigating social networks, the dynamics of relationships in a networked environment and graph theory as a means of adding analysis and context.
Live response in a volatile world: volatile data sources, finding evidence in memory, identification and preparation of network forensics tools and registry evidence.
Attack detection and incident response: the identification of key networked devices for the provision of networked evidence, attack types and signatures, responding to an incident and the limitations of security countermeasures in network forensic

investigations.

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.

References

Course Material	Book
Author	Anson, S. & Bunting, S.
Publishing Year	2007
Title	Mastering Windows Network Forensics and Investigation
Subtitle	
Edition	
Publisher	John Wiley & Sons
ISBN	0-470-09762-0

Course Material	Book
Author	Di Pietro, R. & Mancini, L.V.
Publishing Year	2008
Title	Intrusion Detection Systems
Subtitle	
Edition	
Publisher	Springer
ISBN	0-387-77265-0

Course Material	Book
Author	Jones, K.J., Bejtlich, R. & Rose, C.W.
Publishing Year	2005
Title	Real Digital Forensics: Computer Security and Incident Response
Subtitle	
Edition	
Publisher	Addison-Wesley
ISBN	0-321-24069-3

Course Material	Book
Author	Jones, R.
Publishing Year	2005
Title	Internet Forensics
Subtitle	
Edition	

Publisher	O'Reilly
ISBN	0-596-10006-X

Course Material	Book
Author	Wasserman, S. & Faust, K.
Publishing Year	1994
Title	Social Network Analysis: Methods and Applications
Subtitle	
Edition	
Publisher	Cambridge University Press
ISBN	0-521-38707-8

Course Material	Journal / Article
Author	
Publishing Year	
Title	In addition, students are encouraged to access the latest research publications from international conferences and journals such as 'Journal of Digital Investigations', 'IEEE Security and Privacy' and 'Computer Security and Law Report'.
Subtitle	
Edition	
Publisher	
ISBN	

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.