Liverpool John Moores University

Title:	MOBILE SYSTEMS AND FORENSICS
Status:	Definitive
Code:	**6058COMP** (117472)
Version Start Date:	01-08-2018
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Michael Mackay	Y
Robert Askwith	

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	12
Seminar	12
Tutorial	24

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Design of a Wireless Networking Infrastructure supporting specific application requirement.	50	
Report	AS2	Forensic analysis of traffic captures.	50	

Aims

To provide an in-depth study of the application and network requirements of wireless and mobile communications systems.

To develop an advanced understanding of the theory and practice of building modern mobile and wireless systems.

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

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	Critically review and identify the fundamental technical requirements of applications and network infrastructures supporting modern wireless systems.
2	Apply creative skills concerning the development of applications and network infrastructures of modern wireless systems.
3	Critically evaluate recent advances in network technologies to assess their impact and applicability to a network forensics investigation.
4	Critically analyse and evaluate network forensics data evidence.

Learning Outcomes of Assessments

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

Design	1	2
Forensic analysis	3	4

Outline Syllabus

Wireless Networking Infrastructures: Application and Network Requirements, Wireless Network Architectures; WLAN infrastructure, Bluetooth ad hoc, Protocols and Internetworking issues; wireless Internet, Mobile IP, MIPv6, Cellular IP, WAP, Wireless QoS, Middleware for wireless, adaptation, security, MAC schemes, TDMA/CDMA/FDMA, Applications; location-based services, networked appliances, sensor networks

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

Students will participate in lectures, tutorials, and practical lab sessions.

Notes

The module provides advanced communications networks skills by looking at wireless and mobile systems and forensics analysis of networked systems.