Liverpool John Moores University

Title:	COMPUTER FORENSICS
Status:	Definitive
Code:	**7056COMP** (103315)
Version Start Date:	01-08-2011
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
Christopher Wren	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 1

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	analysis/discussion of research in the area.	100.0	

Aims

To develop a critical appreciation of both the theoretical and practical issues in the field of computer forensics.
To develop the knowledge of various computer systems and understand their importance to computer forensics investigations.
To place the field of computer forensics in the wider field of computer science, the judicial system and national security.
To develop the necessary skills, methodologies and processes to conduct a basic

computer 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 computer forensics in law enforcement, national security and the organisation.
2	Critically evaluate recent advances in the field of computer forensics to assess their applicability to an investigation.
3	Assess the role of computer forensics in the wider fields of computer science, the organisation, the judicial system and national security.
4	Critically analyse and evaluate physical and computer forensics data evidence.

Learning Outcomes of Assessments

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

Research analysis /discussion	1	2	3	4

Outline Syllabus

The course outline includes:
Overview of computer forensics: computer forensics fundamentals, the computer crime classification and the role of computer forensics in law enforcement, the organisation and national security.
Computer forensics in law enforcement: forensics principles and methodologies in law enforcement and their relationship to the ACPO Guide for Forensic Practitioners.

Legislation: relevant UK and international laws that will impact on the investigation within judicial and organisational investigations.
The basics of hard drives and storage media: the generic computer models, hard drive architectures, partitions and deleted data analysis.
Reporting and documentation processes: extracting the evidence from a crime scene, search preparation, the ACPO Guidelines for search and seizure, lab evidence considerations and documentation.
Investigating electronic files: the file structure, embedded meta-data analysis and advanced research techniques for file analysis.
Windows advanced analysis techniques: the boot sequence and file changes, Windows view of the hard drive, File Allocation Table (FAT) file system analysis, New Technology File System (NTFS) analysis, volatile and non-volatile data and the registry as an investigative resource.
Linux/Mac advanced analysis techniques: the boot sequence and file changes, Linux file system structure with inodes, the X Windows environment and volatile and non-volatile data.

Learning Activities

Lectures, tutorials and practical work. The practical work builds on core computer forensics concepts covered in the lectures. This involves laboratory and user demonstrations of computer forensics techniques.

References

Course Material	Book
Author	Bryant, R.P.
Publishing Year	2008
Title	Investigating Digital Crime
Subtitle	
Edition	
Publisher	Wiley Blackwell
ISBN	0-470-51601-1

Course Material	Book
Author	Carrier, B.
Publishing Year	2005
Title	File System Forensic Analysis
Subtitle	
Edition	
Publisher	Addison-Wesley
ISBN	0-321-26817-2

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	Nelson, B.
Publishing Year	2007
Title	Guide to Computer Forensics and Investigations
Subtitle	
Edition	3rd Edition
Publisher	Delmar 1
ISBN	418-06733-4

Course Material	Book
Author	Sammes, A.J. & Jenkinson, B.

Publishing Year	2007
Title	Forensic Computing: A Practitioner's Guide
Subtitle	
Edition	2nd Edition
Publisher	Springer
ISBN	1-846-28397-3

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 forensic computing. The purpose of the course is to provide the fundamental technical concepts and research issues essential for computer forensic investigations within the organisation, law enforcement or national security.