Liverpool John Moores University

Title:	ADVANCED TOPICS IN COMPUTER FORENSICS
Status:	Definitive
Code:	**7046COMP** (103305)
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 2

Component	Contact Hours
Lecture	12.000
Seminar	24.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Essay	AS1	Analysis and evaluation of current research directions in computer forensics.	100.0	

Aims

To develop advanced theoretical and practical research skills in computer forensics.
To develop a critical appreciation of both the theoretical and practical issues in the field of digital forensics.
To provide critical evaluation of research methods in the development of new computer forensics methodologies, tools, techniques and applications.

Learning Outcomes

After completing the module the student should be able to:

1 Demonstrate the technical concepts, implementation, and restrictions of computer forensics in the organisation, law enforcement and national security.
2 Demonstrate practical and advanced research skills in computer forensics.
3 Critically analyse and evaluate physical and computer evidence using advanced computer forensics and research-based techniques.
4 Critically evaluate the impact of future research issues on the field of computer forensics.

Learning Outcomes of Assessments

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

Analysis and evaluation	1	2	3	4

Outline Syllabus

The course outline includes:
Advanced hard drive and storage media analysis, reporting and documentation processes, forensic computing for the organisation and national security, issues in current practice and evidence handling, operating system (Windows/Unix) advanced analysis techniques, advanced file analysis approaches, network forensics, mobile device (e.g. mobile phone or embedded systems) computer forensics, data hiding and hostile code, encryption and forensics, combining computer forensics investigations with other evidentiary material, P2P applications, encrypted network traffic, identification of computer forensics artefacts on the hard drive or in the file system, analysis of social networks and other advanced topics.

Learning Activities

Lectures and seminars. The seminars build on core computer forensics concepts covered in the lectures. It is envisaged that this course will empower the post-graduate student by giving them the responsibility to self-manage and self-organise lectures and seminars around their research interests in computer forensics.

References

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	Mohay, G., Anderson, A., Collie, B., De Vel, O. & McKemmish, R.
Publishing Year	2003
Title	Computer and Intrusion Forensics
Subtitle	
Edition	
Publisher	Artech House
ISBN	Artech House

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	Book
Author	Blyth, A. & Sutherland, I.
Publishing Year	2007
Title	Proceedings of EC2ND
Subtitle	
Edition	
Publisher	Springer-Verlag
ISBN	1-84628-749-9

Course Material	Book
Author	Haggerty, J. & Merabti, M.
Publishing Year	2006
Title	Proceedings of ACSF
Subtitle	
Edition	
Publisher	LJMU
ISBN	1902560159

Course Material	Journal / Article
Author	
Publishing Year	
Title	In addition, material will be used from journal and conference papers, such as Computer Fraud and Security, Digital Investigations Journal,
Subtitle	International Journal of Digital Evidence, IEEE Network,

	IEEE Security and Privacy, IEEE Internet Computing,
Edition	
Publisher	
ISBN	

Notes

This advanced module is intended for post-graduate students to discuss and analyse the current situation and future directions of the computer forensics field. It ideally would prepare a student for a career either as a practitioner in the computer forensics field or for further post-graduate study.