# **Liverpool** John Moores University

Title: ADVANCED FORENSIC COMPUTING

Status: Definitive

Code: **7004CCTV** (118647)

Version Start Date: 01-08-2011

Owning School/Faculty: Computing and Mathematical Sciences Teaching School/Faculty: Computing and Mathematical Sciences

Team	Leader
Christopher Wren	Υ

Academic Credit Total

Level: FHEQ7 Value: 15.00 Delivered 36.00

**Hours:** 

Total Private

Learning 150 Study: 114

**Hours:** 

**Delivery Options** 

Course typically offered: Runs Twice - S1 & S2

Component	Contact Hours
Lecture	12.000
Seminar	24.000

**Grading Basis:** 40 %

### **Assessment Details**

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Analysis/evaluation of current research directions in computer forensics 4,000 - 6,000 words).	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:

- 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 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**

Attend online lectures, tutorials and practical work. 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
Subtitle	Computer Security and Incident Response
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	

Course Material	Book
Author	Sammes, A.J. & Jenkinson, B.
Publishing Year	2007
Title	Forensic Computing
Subtitle	A Practitioner's Guide'
Edition	2nd Edition
Publisher	Springer
ISBN	1-846-28397-3

Course Material	Book
Author	Haggerty, J. & Merabti, M.
Publishing Year	
Title	Proceedings of EC2ND
Subtitle	
Edition	
Publisher	LJMU
ISBN	1-90256-015-9

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