Liverpool John Moores University

Title: FORENSIC COMPUTING
Status: Definitive
Code: **7002CCTV**   (118645)
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:** 38.00
Total Learning Hours: 150	**Private Study:** 112	

Delivery Options
Course typically offered: Runs Twice - S1 & S2

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	Coursework - analysis/discussion of research in the area (4,000 - 6,000 words).	50.0	
Exam	AS2	Examination	50.0	2.00

Aims

To develop an understanding of the theory and practice of computer forensics.

Learning Outcomes

After completing the module the student should be able to:

1. Demonstrate a critical understanding of technical concepts, implementation, and restrictions of computer forensics in the organisation and law enforcement.
2. Develop practical and advanced research skills in computer forensics.
3. Critically analyse and evaluate physical and forensic computing data evidence.

Learning Outcomes of Assessments

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

Analysis   1   2

Examination   3

Outline Syllabus

The course outline includes:
Overview of computer forensics, the basics of hard drives and storage media, reporting and documentation processes, forensic computing in law enforcement and national security, 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) forensic computing, data hiding and hostile code, encryption and forensics, investigation of fraud, and future research directions of the field.
The practical laboratory exercises will develop skills in data and evidence collection from both Windows and UNIX computers.

Learning Activities

Attend online lectures, tutorials and practical work. The practical work builds on core forensic computing concepts covered in the lectures. This involves 4-day laboratory and user demonstrations of forensic computing techniques at the end of the module.

References

Course Material	Book
Author	Nelson, B., Phillips, A., & Steuart, C
Publishing Year	2007
Title	Guide to Computer Forensics and Investigations
Subtitle	
Edition	3rd Edition
Publisher	Thomson Course Technology
ISBN	978-1418067335

Course Material	Book

Author	Bunting, S.
Publishing Year	2007
Title	EnCE The Official Encase Certified Examiner
Subtitle	
Edition	2nd Edition
Publisher	John Wiley & Sons
ISBN	978-0470181454

Course Material	Book
Author	Prosise, C. & Mandia, K.
Publishing Year	2003
Title	Incident Response and Computer Forensics
Subtitle	
Edition	
Publisher	McGraw Hill
ISBN	0-072-22696-X

Course Material	Book
Author	Carvey, H.
Publishing Year	2004
Title	Windows Forensics and Incident Recovery
Subtitle	
Edition	
Publisher	Addison Wesley
ISBN	0-32120-098-5

Course Material	Book
Author	Anzaldua, R., Godwin, J. & Volonino, L
Publishing Year	2006
Title	Computer Forensics
Subtitle	Principles and Practice
Edition	
Publisher	Prentice Hall
ISBN	0-13154-727-5

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.