Liverpool John Moores University

Title:	PRINCIPLES OF COMPUTER FORENSICS
Status:	Definitive
Code:	**5043COMP** (115975)
Version Start Date:	01-08-2014
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
Thomas Berry	Y
Christopher Wren	

Academic Level:	FHEQ5	**Credit Value:**	24.00	**Total Delivered Hours:**	74.00
Total Learning Hours:	240	**Private Study:**	166		

Delivery Options
Course typically offered: Standard Year Long

Component	Contact Hours
Lecture	24.000
Practical	48.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	An individual report to demonstrate documenting material using forensic tools.	20.0	
Report	AS2	A group report to investigate a simulated crime.	40.0	
Exam	AS3	Examination.	40.0	2.00

Aims

To develop an understanding of the role of computer forensics analyst through the use of existing applications and investigative techniques.

Learning Outcomes

After completing the module the student should be able to:

1 Identify the role of the computer forensics analyst in computing investigations.
2 Explain the structure of files and the metadata contained within them.
3 Demonstrate experience in a number of computer forensic tools as used by practitioners in the field.
4 Identify a range of appropriate methodologies used during an investigation and present the results of the investigation.
5 Describe the theoretical underpinnings of computer forensics.

Learning Outcomes of Assessments

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

Forensic tools	1	2
Group investigation	3	4
Examination	5	

Outline Syllabus

The module will cover the three phases of a computing forensics investigation: Search Phase:

Search preparation, processing the crime or incident scene, securing evidence from the computer, data acquisition and identification of digital evidence sources.

Analysis Phase:

Preparing for a computer investigation, the investigator's environment, computer forensics software needs, current computer forensics software and hardware, the impact of file and operating systems on the investigation, computer forensics analysis, recovery and investigation of digital image (picture) files, network forensics and investigating e-mail.

Presentation Phase:

Reporting the results of the investigation and the role of the expert witness.

Learning Activities

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

References

Course Material	Book
Author	Nelson, B., Phillips, A., Enfinger, F. & Steuart, C.
Publishing Year	2009
Title	Guide to Computer Forensics and Investigations
Subtitle	
Edition	4th Edition
Publisher	Thomson Course Technology
ISBN	978-1435498839

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	0-78214-435-7

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 :Principles and Practice
Subtitle	
Edition	
Publisher	Prentice Hall
ISBN	0-13154-727-5

Notes

This module is intended to build on first year modules to introduce the students to the practicalities of conducting computer forensics investigations.