Liverpool John Moores University

Title:	INTRODUCTION TO COMPUTER FORENSICS AND SECURITY
Status:	Definitive
Code:	**4015COMP** (119650)
Version Start Date:	01-08-2014
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
Robert Askwith	Y
Thomas Berry	

Academic Level:	FHEQ4	**Credit Value:**	24.00	**Total Delivered Hours:**	72.00
Total Learning Hours:	240	**Private Study:**	168		

Delivery Options

Course typically offered: Standard Year Long

Component	**Contact Hours**
Lecture	24.000
Practical	24.000
Tutorial	24.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Group-based report	40.0	
Artefacts	AS2	Security case study: project proposal	60.0	

Aims

To introduce the student to a range problem solving skills in computing and the associated tools and techniques used by practitioners in computer digital forensics and cyber security.

Learning Outcomes

After completing the module the student should be able to:

1 Identify suitable methods and tools for developing solutions to problems in computer forensics.
2 Demonstrate knowledge of the investigative skills in computer forensics.
3 Present the results from a computer forensics investigation.
4 Apply the appropriate tools and techniques to practical aspects of computer security.
5 Identify practical solutions to problems in computer security

Learning Outcomes of Assessments

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

Group Report	1	2	3
Security case study	4	5	

Outline Syllabus

Forensics:
-Identify the types of crime that may be committed on a computer.
-Explain that evidence may be contained on a number of devices such as PC's, tablets, mobile phones, iPods, etc.
-Demonstrate the three phases of an investigation from seizure to analysis and finally presentation of results.
-Explain the chain of evidence required to ensure any evidence recovered is admissible in court.

Security:
-Basic terminology for security: threat, vulnerability, attacks, privacy, trust, etc.
-C.I.A model – Confidentiality, Integrity, Availability
-Understanding the security problem: Why do bad things happen? How big is the security problem?
-Looking at what security practitioners do
-Understanding the attacker
-Challenges and solutions: technical, management, social
-Authentication, Access Control, Authorisation

Learning Activities

Lectures will typically include theoretical and practical components, which will prepare the student for the follow up tutorial and guided lab session.

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	Sammons, J.
Publishing Year	2012
Title	The Basics of Digital Forensics
Subtitle	The Primer for Getting Started in Digital Forensics
Edition	
Publisher	Syngress
ISBN	978-1597496612

Course Material	Book
Author	Andress, J.
Publishing Year	2011
Title	The Basics of Information Security
Subtitle	
Edition	
Publisher	Syngress
ISBN	978-1597496537

Notes

This module provides the student with the basic concepts, methods, techniques and experience of computer forensics and security.