Liverpool John Moores University

Title:	INTRODUCTION TO COMPUTER FORENSICS AND SECURITY
Status:	Definitive
Code:	**4605YCOM** (125483)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	YPC International College (Kolej Antarabangsa YPC)

Team	Leader
Thomas Berry	Y
Nathan Shone	

Academic Level:	FHEQ4	**Credit Value:**	20	**Total Delivered Hours:**	55
Total Learning Hours:	200	**Private Study:**	145		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	33
Practical	11
Tutorial	11

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Computer Forensics based report	50	
Report	AS2	Computer Security case study	50	

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 computer 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 and security
2	Demonstate knowledge of a range of topics in computer security
3	Indentify and apply the appropriate tools and techniques to practical aspects of computer forensics.

Learning Outcomes of Assessments

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

Coursework 1	1	3
Coursework 2	1	2

Outline Syllabus

Computer 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.

Computer 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 practical and guided lab session.

Notes

This module provides the student with the basic concepts, methods, techniques and

experience of computer forensics and security.