Liverpool John Moores University

Title:	Introduction to Computer Forensics and Security
Status:	Definitive
Code:	**4205COMP** (127966)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Thomas Berry	Y
Sorren Hanvey	
Kirsty Lever	
Nathan Shone	

Academic Level:	FHEQ4	**Credit Value:**	20	**Total Delivered Hours:**	44
Total Learning Hours:	200	**Private Study:**	156		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	22
Practical	22

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Computer Forensics Investigation	50	
Report	AS2	Computer Security Case Study	50	

Aims

To develop students' problem-solving skills in computing and apply them using 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 recovering and analyzing data in computer forensic investigations.
2	Apply computer forensic methods and tools to undertake an investigation.
3	Apply knowledge of a range of topics in computer security.
4	Analyse given scenarios to determine potential security issues and respective solutions.

Learning Outcomes of Assessments

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

Coursework 1	1	2
Coursework 2	3	4

Outline Syllabus

Computer Forensics:
-Identify the types of crime that may be committed on a digital device.
-Explain that evidence may be contained on a number of devices such as PC's, tablets, mobile phones, IoT devices, 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.
-Look at the storage on digital devices and recover any data that may exist on them. This data may then be analysed to
then be used as evidence in an investigation.

Computer Security:
- Security theory and key terminology: threat, vulnerability, attacks, privacy, trust, etc.

- Security goals (e.g. CIA model)
- Common attack techniques and threat sources
- Common defence elements and strategies
- Introduction to cryptography
- Threat intelligence and future security issues

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. Students apply their knowledge and develop practical skills in the assessments by undertaking a digital forensic investigation and a security analysis of a case study.