Introduction to Computer Forensics and Security

Module Information

2022.01, Approved

Summary Information

Module Code	4705YCOM
Formal Module Title	Introduction to Computer Forensics and Security
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 4
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
YPC International College (Kolej Antarabangsa YPC)

Learning Methods

Learning Method Type	Hours
Lecture	22
Practical	22

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
SEP-PAR	PAR	September	12 Weeks

Aims and Outcomes

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.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Identify suitable methods and tools for recovering and analysing data in computer forensic investigations.
MLO2	2	Apply computer forensic methods and tools to undertake an investigation.
MLO3	3	Apply knowledge of a range of topics in computer security.
MLO4	4	Analyse given scenarios to determine potential security issues and respective solutions.

Module Content

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 tothen 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
Module Overview	
Additional Information	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.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Coursework 1	50	0	MLO1, MLO2
Report	Coursework 2	50	0	MLO3, MLO4

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Glyn Hughes	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings