Computer Forensics

Module Information

2022.01, Approved

Summary Information

Module Code	7130COMP
Formal Module Title	Computer Forensics
Owning School	Computer Science and Mathematics
Career	Postgraduate Taught
Credits	20
Academic level	FHEQ Level 7
Grading Schema	50

Teaching Responsibility

LJMU Schools involved in Delivery
Computer Science and Mathematics

Learning Methods

Learning Method Type	Hours
Lecture	12
Practical	12
Tutorial	12

Module Offering(s)

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

Aims and Outcomes

Aims	To develop a critical appreciation of both the theoretical and practical issues in the field of computer forensics.To develop the knowledge of various computer systems and technologies and understand their importance to computer forensics investigations.To place the field of computer forensics in the wider field of computer science, the judicial system and national security.To develop the necessary skills, methodologies and processes to conduct a basic computer forensics investigation within an organisation.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Explain fundamental technical concepts, implementation, and restrictions of computer forensics.
MLO2	2	Critically analyse and evaluate computer forensics evidence.
MLO3	3	Explain the role of computer forensics in the wider fields of computer science, the organisation, the judicial system and national security.
MLO4	4	Critically evaluate recent advances in the field of computer forensics to assess their applicability to an investigation.

Module Content

Outline Syllabus	Computer forensics fundamentals to include:-Introduction to digital forensics-Hard drives and storage media-Computer forensics in law enforcement-Process models and evidence handlingComputer forensics in practice, to include:-Investigation of Windows hosts-File-systems and file analysis-Data hiding and fraud investigation-Passwords analysisNetwork forensics, to include:-Network forensic fundamentals-Investigating networks-GPS forensicsContemporary topics in digital forensics-Examination of several current digital forensics topics
Module Overview	The purpose of the course is to cover the fundamental technical concepts combined with practical skills and contemporary research essential for computer forensic investigations within the organisation, law enforcement or national security. It aims to: develop a critical appreciation of both the theoretical and practical issues in the field of computer forensics develop the knowledge of various computer systems and technologies and understand their importance to computer forensics investigations place the field of computer forensics in the wider field of computer science, the judicial system and national security develop the necessary skills, methodologies and processes to conduct a basic computer forensics investigation within an organisation
Additional Information	The purpose of the course is to cover the fundamental technical concepts combined with practical skills and contemporary research essential for computer forensic investigations within the organisation, law enforcement or national security.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping

Essay	Analysis and investigation	40	0	MLO2
Centralised Exam	Examination	60	2	MLO1, MLO3, MLO4

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Thomas Berry	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings