Liverpool John Moores University

Title:	ADVANCED TOPICS IN COMPUTER FORENSICS
Status:	Definitive
Code:	**7074COMP** (120333)
Version Start Date:	01-08-2019

Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Christopher Wren	Y
William Hurst	

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	36
Total Learning Hours:	200	**Private Study:**	164		

Delivery Options

Course typically offered: Semester 2

Component	Contact Hours
Lecture	12
Seminar	12
Tutorial	12

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Produce a research paper relating to a contemporary computer forensics problem.	100	

Aims

To develop advanced theoretical and practical research skills in computer forensics.
To develop a critical appreciation of both the theoretical and practical issues in the field of computer forensics.
To provide critical evaluation of research methods in the development of new computer forensics methodologies, tools, techniques and applications.

To provide students with an opportunity to practise research skills, such as scientific writing, presentations, and proposal writing.

Learning Outcomes

After completing the module the student should be able to:

1   Conduct research relating to Computer Forensics.
2   Display advanced knowledge of one or more issues within Computer Forensics.
3   Demonstrate expertise in applying knowledge to Computer Forensics problems.
4   Demonstrate skills in the communication of research findings.

Learning Outcomes of Assessments

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

Research paper   1   2   3   4

Outline Syllabus

Topics will reflect the current research in computer forensics, including that being undertaken within the school, and may include (but are not limited to):

- Advanced hard drive and storage media analysis,
- Issues in current practice and evidence handling,
- Operating system (Windows/UNIX) advanced analysis techniques,
- Advanced file analysis approaches,
- Network forensics,
- Mobile device (e.g. mobile phone or embedded systems) computer forensics,
- Data hiding and hostile code,
- Encryption and forensics,
- Computer forensics in virtual environments (e.g. virtual machines, the cloud),
- Incident response and live computer forensic analysis,
- Combining computer forensics investigations with other evidentiary material,
- Automation of digital forensic procedures,
- Database and big data forensics,
- Computer forensics approaches for social networks,
- Forensic investigation of peer-to-peer applications and networks.

Learning Activities

Lectures will be supported by tutorials. Students will engage in seminar sessions to present and discuss the results of their research work.

Notes

The focus of the module is on examining current research issues and agendas within Computer Forensics. Students are encouraged to develop their research skills, through conducting literature investigations and proposing ideas in a seminar setting.