Module Specification

Module Summary Information

1	**Module Title**	Advanced Techniques in Digital Forensics
2	**Module Credits**	20
3	**Module Level**	7
4	**Module Code**	CMP7164

5	**Module Overview**

This module covers advanced topics in digital forensics. The module will begin with an introduction to the detection and analysis of obfuscated data and anti-forensic techniques; this will progress on to advanced steganographic and steganalytic techniques for media formats. Further topics covered include Root-Kit and Malware analysis using sophisticated specialist techniques that require access to intricate operating system features. The module will also address the inspection of computer peripheral devices such as printers; digital camera equipment as well as biometric data capture devices as they become ever more prevalent in computer based devices. The module will also introduce the concept of image content analysis, which also links to pattern recognition and analysis techniques beyond simple string and keyword matching algorithms used in conventional forensic analysis.

This module emphasises a “hands-on” approach to learning forensic computing techniques using open-source and commercial forensic tools. The module will teach you the fundamental data structures applicable to computer forensics and how various tools can be exploited to analyse these structures in a variety of case types.

The module is delivered through a flipped methodology placing significant emphasis on the development of practical skills supported by blended learning and a variety of learning activities including lectures, seminars, practice-led, self-directed and experiential learning; in person and online through Virtual Learning Environments (VLE).

Each practical session comprises a series of hands-on analytical experiments to progressively unpack the more advanced aspects of the topic being investigated. All practical sessions will be hosted in the specialist Computer Forensics Laboratory.

The post session activities for each week will comprise a short formative Moodle quiz which will provide instant feedback on the theoretical material covered. For practical session, there will be an accompanying video taking you step-by-step through the solutions of the practical lab exercises.

6	Indicative Content
Evidence manipulation and Anti-Forensics of Multimedia Data and Countermeasures Steganography and Multimedia File Manipulation Memory and Process Forensics Malware Analysis Virtual Machine Forensics Forensic Authentication of Digital Audio and Video Files and Digital Camera Identification Image Content Analysis Techniques Printer, Scanner and Computer Peripheral Forensics Use of Biometrics in Digital Forensics	

7	Module Learning Outcomes On successful completion of the module, students will be able to:	
	1	Evaluate applied anti-forensic techniques in order to extract digital forensic evidence.
	2	Formulate and administer techniques for the examination of digital camera, printer and other computer peripheral devices and media as a source of digital evidence.
	3	Critically analyse advanced operating system features and operations for malicious techniques used to compromise system security and provide unauthorised access to system resources and data.

8	Module Assessment			
Learning Outcome				
	Coursework	Exam	In-Person	
1-3	X			

9	Breakdown Learning and Teaching Activities	
Learning Activities		Hours
Scheduled Learning (SL) includes lectures, practical classes and workshops, peer group learning, Graduate+, as specified in timetable		48
Directed Learning (DL) includes placements, work-based learning, external visits, on-line activity, Graduate+, peer learning, as directed on VLE		92
Private Study (PS) includes preparation for exams		60
Total Study Hours:		200