Module Specification

Module Summary Information

1	**Module Title**	Computer Forensics Tools and Techniques
2	**Module Credits**	20
3	**Module Level**	5
4	**Module Code**	CMP5328

5	**Module Overview**

This module develops comprehensive practical skills and theoretical knowledge for the forensic examination of personal computer systems using proprietary and open-source software tools. You will acquire the keys skills necessary in conducting and auditing a systematic forensic investigation of a computer system for user activity, operating system operation and configuration and connectivity.

The module is delivered through a truly 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 each week's lab session, there will be an accompanying video taking you step-by-step through the solutions of the practical lab exercises. In addition to the lab-based analytical experiments, each lab session will also provide you a short set of experiments which are to be conducted on your virtual machine in your own time allowing you to explore the broader aspects of the topic being investigated during the scheduled lab session to help reinforce your learning.

Where appropriate, additional surgeries may be held to provide additional guidance, support and feedback.

6	Indicative Content
Windows Disk Image Acquisition Software and hardware imaging Signature and hash analysis Common file structure and metadata analysis Keywords, searching and filtering cases Registry analysis Recovering deleted files Recycle bin analysis and file recovery Operating system artefacts Volatile data (memory), Pagefile, and unallocated space analysis Windows Event Logs Timeline analysis and events correlation Password attacks Disk encryption and decryption	

7	Module Learning Outcomes On successful completion of the module, students will be able to:	
	1	Administer a comprehensive forensic examination of computer files, metadata, common operating system artefacts and processes on a computer system.
	2	Compare and apply computer forensic examination tools based on the specific requirements of a given scenario in a forensically sound manner.
	3	Assemble key findings to generate a forensic report for a computer forensic investigation.

8	Module Assessment		
Learning Outcome			
	Coursework	**Exam**	**In-Person**
1, 2, 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	48
Private Study (PS) includes preparation for exams	104
Total Study Hours:	200