Module Specification

Module Summary Information

1	**Module Title**	Unix Systems Forensic Analysis
2	**Module Credits**	20
3	**Module Level**	7
4	**Module Code**	CMP7176

5	**Module Overview**

Whilst Microsoft Windows is the predominant operating system installed on desktop PCs, there are a variety of alternative operating systems that can be used on desktop PCs and server applications. Many of these operating systems are based on a Linux or UNIX kernel. Being able to acquire and navigate these operating systems is important in a digital forensic investigation.

This module is designed to provide you with the essential knowledge and skills required to understand the concepts, features and operation of UNIX based operating systems such as Linux and Mac OS X on a variety of hardware platforms in the context of forensic analysis. It will focus on developing knowledge and practical skills to enable you to analyse file systems and operating system artefacts in Linux/UNIX environments. This module will also cover Apple Mac OS. This module aligns with the programme's philosophy of wider appreciation of conducting digital forensic analysis on alternative devices and operating systems.

Alignment with Programme Philosophy and Aims
The programme aims to emphasise the important technical skills associated with analysing digital evidence where this module enhances knowledge of the UNIX and Linux operating systems. The module also enables you to develop your confidence in gaining important technical skills and become an independent problem solver willing to take on new challenges and experiences

Learning and Teaching Strategy
The main approach to learning is practically based where you will get 'hands-on' experience of the UNIX/Linux operating system environment. Practical sessions will be augmented with mini-lectures and tutorials covering important concepts that underpin UNIX/Linux operating system concepts. In addition, there will be opportunities to gain formative feedback on analyses carried out in sessions and on the assessment.

Assessment Strategy
This module is assessed by a technical report comprising solutions to a number of problems involving the analysis of distributions and configurations of UNIX/Linux operating systems. For example analysing UNIX/Linux installed on desktop PCs and server computers configured based on realistic scenarios and data. The report assesses your ability to analyse a UNIX/Linux operating system and articulate the results obtained.

6	Indicative Content

- UNIX/Linux fundamentals.
- UNIX/Linux file systems.
- Imaging a UNIX/Linux system.
- File and metadata analysis.
- Apple Mac OS fundamentals.
- HFS+ analysis.
- UNIX/Linux BOOT process.
- Kernel and process operation.
- User privileges.
- Recovering and interpreting user activity.
- Browser analysis.
- Live and memory analysis.
- Establishing a timeline.

7	Module Learning Outcomes On successful completion of the module, students will be able to:	
	1	Formulate, with justification, a forensic analysis of a Unix/Linux/Mac OS installation.
	2	Administer a live analysis of a UNIX/Linux system.
	3	Administer a post mortem analysis of a UNIX/Linux system.
	4	Critically evaluate the process and findings of a digital forensic investigation in a structured report.

8	Module Assessment		
Learning Outcome			
	Coursework	Exam	In-Person
1-4	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