MODULE **DESCRIPTOR**

MODULE TITLE	Digital Evidence and Incident Response		
MODULE CODE	CO2517 (L5)	**CREDIT VALUE**	20 credits / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

1. To enhance the students' understanding of computer hardware
2. To develop skills in planning subject to incident response
3. To foster a rigorous approach to evidence recovery
4. To develop skills necessary for dead-box/live acquisition of evidence
5. To make students aware of legal and ethical issues surrounding evidence handling

MODULE **CONTENT**

Evidential Standards & Tools

Acquisition tools (such as Guymager, DD, or LinEN), chain of custody, evidence labelling, working with Law Enforcement (or their agents), best practice methods (e.g. ACPO Good Practice Guide for electronic-based evidence, ISO 27037)

Hardware

Disk interfaces (e.g. SCSI, ATA, SATA). Host protected area, device configuration overlay, addressing modes and their limitations, solid state drives, device configuration, jumper settings.

Incident Response & Forensic Readiness

Identifying threats, prioritising threats through risk assessment, incident response lifecycle, creating an incident response plan, testing an incident response plan, system use policies, forensic readiness plans, information management

Operating System

Operating systems use: Linux & Windows, system use policies, file system data structures, disaster recovery, data recovery, common artefacts (e.g. web browser artefacts)

Legal and ethical issues

Computer Misuse Act 1990, Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016, Communications Act 2003, Computer Crime, forensic readiness, trust.

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Critically evaluate digital evidence created by computer-based filing system
2. Evaluate digital evidence acquisition techniques
3. Use appropriate techniques to develop, monitor, control and test an incident response plan
4. Discuss the legal and ethical issues relevant to incident response

TEACHING METHODS

A combination of lectures and practical work will be used. Where possible, the material will be presented with an emphasis on the relevance to digital investigations. For example, an analysis of the boot sector could be used to demonstrate a hex editor and the representation of machine code and data; file recovery will motivate the study of file systems.

Diagrams will be used to help understand the mapping of a file system to disk blocks and the artefacts left after deletion.

Lectures will introduce components and their operation.

Practical work will use a distribution of Linux used by digital forensic investigators (e.g., CAINE). The command line interface and hex editors will be used to explore the operation of data persistence in different file systems. These skills will be used to investigate file system artefacts with a view to the recovery of digital data. Evidence acquisition processes will be evaluated and practical experience with the four principles of the ACPO Good Practice Guide for electronic-based evidence. The gained knowledge will be employed to develop, test and evaluate incident response procedures (e.g., to perform a dead-box evidence accusation).

The coursework allows the student to demonstrate practical skills and to integrate techniques explored in the practical. It is designed to evenly assess the students' comprehension of both theoretical topics relevant to digital evidence acquisition and incident response planning, and practical elements including tools and methods needed to acquire digital evidence and evaluate the effectiveness of incident response procedures.

ASSESSMENT METHODS

This module is assessed through a report (50%) and an examination (50%).