MODULE **DESCRIPTOR**

MODULE TITLE	DIGITAL FORENSIC INVESTIGATION		
MODULE CODE	CO4507 (L7)	**CREDIT VALUE**	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

•To inculcate a systematic, impartial approach to the preservation and extraction of all relevant overt and covert information from a computer.
•To discuss the challenges facing forensic computer experts.
•To enhance critical thinking through the discussion and analysis of various real and hypothetical situations that illustrate the variety of decisions involved in an investigation: determining what to analyse, selecting appropriate tools, and evaluating interpretations of the information uncovered.
•To extend communication skills in the presentation of complex ideas to people with a non-technical background.

MODULE **CONTENT**

INVESTIGATIVE PROCEDURES AND LEGAL ISSUES

Gathering, preserving and documenting evidence, seizure and acquisition; planning, documenting and reporting investigations, discussions of ethics, guidelines and legislation relevant to IT and forensic investigation. Researching relevant technical information.

INVESTIGATIVE TECHNIQUES

Internet investigations (e-mail, web pages, chat rooms, etc.); IP address and domain names; Reconstruction of electronic crime scenes;

Exploring system artefacts: caches, spool files, swap files, unallocated disk space, backup media. File systems on Unix and Windows. Analysis of file access, modification, and creation time. Reverse engineering of file structures. Hashing algorithms to find and confirm the identity of files and disks.

Searching for and retrieving information. Password recovery. Cracking software protection. Determining file types. Detecting copying: watermarks, plagiarism and detection tools.

TOOLS

Network utilities: network traffic analysis, ping, traceroute.

Specialist forensic utilities for file system acquisition and analysis e.g. CAINE, EnCase, FTK Imager.

Validation of results from utilities

ANALYSIS

Determining significance, reconstructing fragments of data and drawing conclusions based on evidence found. Hypothesis generation and confirmation.

PRESENTATION

Summarising and explaining conclusions to experts and laypeople.

INTENDED **LEARNING OUTCOMES**

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

1.	Analyse evidence discovered during forensic investigation.
2.	Critically evaluate interpretations of evidence.
3.	Communicate the findings of a forensic analysis in written and verbal form appropriate to a professional computing forensic analyst.
4.	Critically evaluate ethical, legal, and procedural issues relating to the forensic analysis of digital systems.

TEACHING METHODS

It is impossible to teach the students about every possible system or form of evidence that they might encounter. Moreover, forensic investigation is a dynamic area of computing: systems are updated and, new tools and techniques become available. To adapt to these changes, the students must be able to use published information and documentation effectively. The teaching approach will encourage the students to adopt an independent learning style, acquiring and applying new knowledge based on an understanding of key concepts.

Lectures will present concepts illustrated by examples of current systems, techniques and tools. Practical classes will provide the opportunity to reinforce the concepts and develop skills in interpreting technical literature through the application of tools and techniques to a variety of problems. The students will tackle problem-based investigations and use a variety of methods in a limited time. Also, they will be encouraged to discuss and explain their investigations and methodology.

Distance Learning
The module tutor will deliver live online lectures through Adobe Connect. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in the live lectures will have the opportunity to answer and reflect on guided questions. in the subsequent live lectures or participate asynchronously on the discussion board. Where appropriate, students will also be provided with relevant further reading, web links and resources for independent study.

Virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. Students will be provided with access to virtual laboratories through which they will be able to complete the practical components of the module. The students will obtain the practical sheets from Blackboard, and they are expected to follow the instructions included in the practical sheets to complete the lab work. If students have difficulties with a particular exercise, they are expected to contact the module tutor or post a question on the discussion forum, where the module tutor and/or their peers can provide feedback. Different means of communication will be utilized by the tutor to offer support to the students based on the reported issue, i.e. email, Skype, MS Teams, virtual laboratory, etc.

Through the virtual laboratories, the students are expected to apply their theoretical knowledge to solve security problems in a professional and legal way. Feedback to the students will be provided asynchronously through Blackboard. If the need arises, the module tutor will schedule live sessions to provide further feedback to the students.

ASSESSMENT METHODS

This module is assessed through a report and an examination.