MODULE **DESCRIPTOR**

MODULE TITLE	CYBER DEFENCE		
MODULE CODE	CO4710 (L7)	**CREDIT VALUE**	20 CREDITS / 10 ECTS
CAMPUS	UCLAN CYPRUS		
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

The aims of this module are to:

- Provide an in depth understanding of theoretical and practical aspects of network defence and network forensics.
- Identify systems and appliances used for cyber defence and network forensic purposes.
- Apply network packet analysis and network forensic analysis to identify and address security attacks and vulnerabilities.
- Improve analytical skills by critically interpreting network evidence.

MODULE **CONTENT**

- Foundation:
  - Security attacks, real world cases, security objectives, footprints, network forensics, investigative methodology (OSCAR)
- Network evidence
  - Sources of Network-Based Evidence (i..e.: Switches, routers, DHCP servers, DNS servers, IDS, IPS, firewalls)
  - Evidence acquisition: Physical interception, traffic acquisition software, active acquisition
  - Packet Analysis: Protocol analysis tools and techniques, packet analysis tools, case study
  - Event Log Aggregation Correlation and Analysis: Sources of logs, log architecture, collecting and analyzing evidence, case study
- Understanding wireless security
  - Security concerns of wireless networking, common attacks, secure WLAN implementation, wireless security solutions, wireless network forensics, wireless passive evidence acquisition
- Layered defense strategy
  - Security policies and incident handling
  - Access controls
  - Firewalls, web proxies
  - Intrusion detection and prevention systems
  - Network tunneling: IPSec, TLS, SSL
  - Malware forensics: trends, categories, propagation, countermeasures

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:	
1.	Identify and assess tools and techniques for cyber defence, network evidence acquisition and evidence handling.
2.	Conduct network packet and network forensics analysis.
3.	Critically discuss and evaluate evidence collection.
4.	Research and report on security attacks, cyber defence techniques and tools.

TEACHING **METHODS**

The theoretical material will be delivered during the lectures. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to the acquisition and evaluation of network evidence. During the workshops, students will be introduced to cyber defence and network forensic tools and techniques. Furthermore, the students will be asked to conduct network packet and network forensics analysis. Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss the students' practical findings. As a result of the discussions, additional directed reading may be required. There will be occasions when speakers from leading security organisations will be invited to share their industry experiences with the students.

Distance Learning

The module tutor will deliver the theoretical material through live online lectures in 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 posted by the module tutor asynchronously, through a Blackboard discussion forum. The tutor will provide appropriate feedback to students' comments posted on the discussion board. Students will also be provided with relevant further reading, web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

Workshops will be delivered through live Adobe Connect sessions,short pre-recorded videos, discussion forums or virtual laboratories. Discussion forums will be utilized to provide the opportunity to students to present their views on different cyber defence topics. 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 worksheets from Blackboard and they are expected to follow the instructions included in the practical worksheets to complete the lab work. The practical worksheets will be accompanied by short videos to explain the purpose and requirements of the exercise. 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 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, Adobe Connect, 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 a written exam.