University of Essex

Online

Module code	PDFCYL_PCOM7E	NQF level	7
Credit value	20	Study duration	12 weeks

Principles of Digital Forensics and Cyber Law

Module description

This module introduces students to key aspects of law and the legal system, designed to be non-jurisdiction specific. Students will also be introduced to the principles of evidence collection and forensic analysis, different types of evidence and methods of evidence presentation, in a cyber security context. The central consideration of this module is the need to be aware of common legal principles which apply to Cyberspace, to provide a solid foundation in ethics, rights and regulatory challenges which can be applied to a range of situations and jurisdictions, common legal principles which apply to forensics and expert evidence, and to provide a solid foundation in evidence gathering and analysis which can be applied to a range of situations and jurisdictions.

This module aims to:

- Introduce students to the foundational legal concepts and terminologies relevant to digital forensics, with an emphasis on evidence and proof
- Outline the relevant global legal and regulatory environment, including the GDPR and the obligations it imposes
- Discuss cyber harms and digital rights
- Introduce students to ethics in cyber work
- Examine the challenges and opportunities of regulating and policing cyberspace
- Explain different types of evidence and evidence collection and the underlying principles of verifiability, continuity and presentation7.Examine the range of investigations cyber security professionals carry out and the challenges of investigation

Learning outcomes

On completion of this module, students will be able to:

- critically appraise the global legal and regulatory environment as it applies to cyberspace, and compliance requirements, including the GDPR and the obligations it imposes
- critically appraise ethical considerations and the rights that people may or may not have in cyberspace, and understand the debates in this area
- explore the challenges and opportunities of regulating and policing cyberspace
- critically evaluate different types of evidence and collection and presentation techniques, underpinned by the principles of continuity of evidence and reliability of analytical tools and techniques

Syllabus

- Introducing the law and legal systems
- Introducing principles of evidence and proof
- Regulating cyberspace
- What is ‘evidence’ anyway?
- Continuity and reliability
- Virtual crimes and tangible harms
- Rights in cyberspace
- Policing in a digital landscape
- Investigative pitfalls
- The investigative context
- The ethics of cyber work
- The expert witness

Learning and teaching methods

The module will be delivered through the provision of specified reading materials on the virtual learning platform, which shall be supported by specified online discussion forums and lecturecasts. The flexible and participative approach of the module will develop a collaborative research inquiry in the advancement of computing, enabling them to accelerate in their chosen career.

Students will demonstrate their ability and strengths through evidence and reflections by maintaining an e-portfolio. The e-portfolio will also act as a means for assessment on evidence of personal growth and CPD.

Synchronous sessions will give students the opportunity to interact with fellow students and for tutor contact. The sessions will include live coding sessions to help students contextualise their knowledge. These synchronous sessions will be recorded in order to ensure that all students can access the material in their own time.

At pre-arranged days and agreed times during the module (usually weekly, prior to a synchronous session), the module tutor will be available for a drop in telephone or preparatory learning liaison session. This is to give students the opportunity to ask specific and general questions relating to the week’s learning opportunities and enable them to contextualise their learning.

For team activities in this module, students will be grouped according to time zones to ensure team members can communicate easily with each other. Details on the process for team activities and peer assessment will be made available to students at the outset of the module.

Description of unit of assessment	Length/Duration	Submission date	Weighting
Case study 1 - presentation	15 minutes	Unit 6	40%
Case study 2 - blog post	500 words	Unit 9	20%
Case study 3 - expert report	2,500 words	Unit 12	40%