2024 / 25

School of Science and Computing
☎ +353 (0)51 302037
✉ Eleanor.Reade@setu.ie
🌐 www.wit.ie/schools/science_computing

SETU

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Module Descriptor

Introduction to Security and Forensics (Computing and Mathematics)

Introduction to Security and Forensics (A14022)

Short Title: Intro to Security & Forensics
Department: Computing and Mathematics
Credits: 5 **Level:** Introductory

Description of Module / Aims

This module aims to make the student security aware. By the end of the module the student will be conscious of threats to their data and their person, technologies that can be used to help protect them and how to respond to issues that can occur. They will also be familiar with digital forensics and the process that occurs at each of its stages.

Programmes

		stage/semester/status
COMP-0641	BSc (Hons) in Applied Computing (WD_KACCM_B)	1 / 2 / E
COMP-0641	BSc (Hons) in Applied Computing (WD_KCOMP_B)	1 / 2 / E
COMP-0641	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	1 / 2 / M
COMP-0641	BSc (Hons) in Computer Science (WD_KCMSC_B)	1 / 2 / E

Indicative Content

- Introduction
- Threats – threats to data; online threats; device threats
- Security Awareness – security services; security systems
- Security Technologies – physical security; digitally secured systems; security systems
- Digital Evidence - types of evidence; chain of custody; crime scene searching
- Digital Forensic Investgiations – evidence cloning; evidence analysis; evidence recovery; forensic documentation

Learning Outcomes

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

1. Recognise threats to digital data and resources.
2. Use security technologies to create digitally secure systems or security systems.
3. Search a crime scene for evidence.
4. Recover deleted data in a forensically sound manner.
5. Demonstrate findngs of a forensic investigation.

Learning and Teaching Methods

- This module will be presented by a combination of lectures and practicals.
- The lectures will be used to introduce new topics and their related concepts.
- The practical element allows the student to put into practice the theoretical concepts covered in the lectures.

Learning Modes

Learning Type	F/T Hours	P/T Hours
Lecture	12	
Lab	36	
Independent Learning	87	

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
Assignment	50%	1,2
Assignment	50%	3,4,5

Assessment Criteria

<40%: Unable to interpret and describe key concepts of the specific knowledge domain(s). Unable to define threats or implement security technologies. Unable to outline the steps of a forensic investigation.

40%–49%: Be able to interpret and describe key concepts of the specific knowledge domain(s). Identify relevant threats, perform basic tasks for security.

50%–59%: Ability to discuss key concepts of the specific knowledge domain and ability to discover and integrate related knowledge in other knowledge domains. Ability to match specific threats and implement security technologies to combat these. Recover data in a forensic investigation.

60%–69%: Be able to solve problems within the specific knowledge domain(s) by experimenting with the appropriate skills and tools. Produce high quality documentation for a forensic investgation.

70%–100%: All the above to an excellent level. Be able to analyse and design solutions to a high standard for a range of both complex and unforeseen problems through the use and modification of appropriate skills and tools.

Essential Material(s)

- "Forensic Focus." www.forensicfocus.com
- Williams, J. *ACPO Good Practice Guide for Digital Evidence.* United Kingdom: ACPO, 2012.

Supplementary Material(s)

- "SANS." www.sans.org
- Altheide, C and H Carvey. *Digital Forensics with Open Source Tools.* United States: Syngress, 2011.
- Andress, J. *The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice.* United States: Syngress, 2014.
- Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition.* United States: Academic Press, 2011.
- Casey, E. *Handbook of Digital Forensics and Investigation.* United States: Academic Press, 2009.
- Nelson, B, A Philips and C Steuart. *Guide to Computer Forensics and Investigations.* United States: Course Technology, 2015.
- Ollam, D. *Practical Lock Picking, Second Edition: A Physical Penetration Tester's Training Guide.* United States: Syngress, 2012.
- Sammons, J. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* United States: Syngress, 2012.
- Schwartz, M. *Arduino for Secret Agents.* United States: Packt Publishing, 2015.
- Sjogelid, S. *Raspberry Pi for Secret Agents.* United States: Packt Publishing, 2015.
- Solomon, M, K Rudolph, E Tittel, N Broom and D Barrett. *Computer Forensics JumpStart.* United States: Sybex, 2011.

Requested Resources

- Computer Lab: BYOD Lab