2024 / 25

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

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Module Descriptor

Computer Forensics (Computing and Mathematics)

Computer Forensics (A14039)

Short Title: Computer Forensics
Department: Computing and Mathematics
Credits: 5 **Level:** Advanced

Description of Module / Aims

This module provides the essentials of computer forensics. Students will explore the area of digital forensics through file system forensics, network/online forensics and media forensics. Students will be introduced to the different stages of the forensic process, issues relating to digital evidence and will use a selection of forensic tools.

Programmes

		stage/semester/status
COMP-0654	BSc (Hons) in Information Technology Management (WD_KITMA_B)	1 / 8 / E
COMP-0654	BSc (Hons) in Information Technology (WD_KINTE_B)	4 / 2 / E

Indicative Content

- The forensic process
- File systems and recovery of data
- Live response
- Network data: types of data; collecting and analysing data from a network
- Web forensics: HTTP headers; cookies; browser/server log analysis; proxy servers; capturing web pages/web forms server-side data; web activity reconstruction; DNS
- Email forensics: e-mail activity reconstruction; message headers; message attachments; tracing online e-mail
- Mobile device forensics

Learning Outcomes

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

1. Utilise forensic tools to analyse a file system and recover deleted data.
2. Perform a live response and gather network data.
3. Investigate web based services/applications.
4. Trace email data.
5. Collect electronic evidence from modern devices such as smart phones or tablets.

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%	1,5
Assignment	50%	2,3,4

Assessment Criteria

<40%: Unable to effectively use relevant tools. Unable to differentiate stages of the forensic process.

40%–49%: Can conduct basic computer forensic investigations.

50%–59%: In addition to the above, can conduct computer forensic investigations using appropriate controls and recover deleted data.

60%–69%: In addition, can interpret evidence extracted during a forensic investigation and corroborate it with other sources of evidence.

70%–100%: All of the above to an excellent level. Can evaluate the appropriateness of different forensic tools and approaches.

Essential Material(s)

- Willams, D. *ACPO Good Practice Guide for Digital Evidence.* United Kingdom: ACPO, 2012.

Supplementary Material(s)

- "Forensic Focus." www.forensicfocus.com
- Altheide, C and H Carvey. *Digital Forensics with Open Source Tools.* United States: Syngress, 2011.
- Sammons, J. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* United States: Syngress, 2012.
- Solomon, M, K Rudolph, E Tittel, N Broom and D Barrett. *Computer Forensics JumpStart.* United States: Sybex, 2011.

Requested Resources

- Computer Lab: BYOD Lab