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

File System Forensics (Computing and Mathematics)

File System Forensics (A14027)

Short Title: File System Forensics
Department: Computing and Mathematics
Credits: 5 **Level:** Introductory

Description of Module / Aims

The aims of this module are to provide students with an understanding of how computer file systems organize and store data. Students will learn how different operating systems arrange data. The student will use tools to extract and forensically analyse these kinds of data.

Programmes

		stage/semester/status
COMP-0119	BSc (Hons) in Applied Computing (WD_KACCM_B)	2 / 3 / E
COMP-0119	BSc (Hons) in Applied Computing (WD_KCOMP_B)	2 / 3 / E
COMP-0119	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	2 / 3 / M
COMP-0119	BSc (Hons) in Computer Science (WD_KCMSC_B)	2 / 3 / E

Indicative Content

- Introduction: data analysis & organisation; the booting process
- Hard Disk Acquisition: Host Protected Areas (HPAs); write blockers; cryptographic hashes
- Volume Analysis: partitioning schemes
- File System Analysis: file system category; content category; metadata category; filename category; application category
- File Systems

Learning Outcomes

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

1. Describe the concepts of partitions.
2. Demonstrate an awareness of issues surrounding the creation of forensic duplicates.
3. Analyse file systems of various kinds of operating systems.
4. Use a forensic toolkit.
5. Demonstrate how to retrieve deleted data.
6. Examine the conceptual types of data associated within a file system and how these conceptual types of data are implemented in common file systems.

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. Practical work will include the student working with an industry standard forensic toolkit.

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%	1,2,3,4,5
Assignment	50%	3,4,5,6

Assessment Criteria

<40%: Unable to describe concepts of file systems. Unable to use and explain system forensics tools and related OS utilities.

40%–49%: Can describe in detail major concepts of file systems. Able to use and explain system forensics tools and related OS utilities.

50%–59%: All of the above and in addition can compare and contrast various different file systems and data formats.

60%–69%: In addition, be capable of demonstrating an in depth understanding of different file systems.

70%–100%: All above to an excellent level.

Essential Material(s)

- Carrier, B. *File System Forensic Analysis*. New York: Addison-Wesley, 2005.

Supplementary Material(s)

- "Digital Investigation." http://www.sciencedirect.com/science/journal/17422876
- Altheide, C and H Carvey. *Digital Forensics with Open Source Tools*. United States: Syngress, 2011.

Requested Resources

- Computer Lab: BYOD Lab