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

Online Forensics (Computing and Mathematics)

Online Forensics (A14037)

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

Description of Module / Aims

This module aims to provide students with the skills to uncover information that is found in online environments. Such environments may include cloud environments, electronic mail messages, web pages, web servers, web browsers and messaging applications. It also introduces the area of Open Source Intelligence. The module has a significant practical component where the student will use various analysis tools and techniques to explore the areas listed above.

Programmes

		stage/semester/status
COMP-0673	BSc (Hons) in Applied Computing (WD_KACCM_B)	4 / 7 / E
COMP-0673	BSc (Hons) in Applied Computing (WD_KCOMP_B)	4 / 7 / E
COMP-0673	BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	4 / 7 / M
COMP-0673	BSc (Hons) in Computer Science (WD_KCMSC_B)	4 / 7 / E

Indicative Content

- Web forensics: HTTP headers; cookies; browser / server log analysis; proxy servers; capturing web pages; web forms; server-side data; web activity reconstruction
- Email forensics: E-mail activity reconstruction; message headers; message attachments; tracing online e-mail
- Internet domain names and addresses: internet address tools – dig, whois, nslookup; domain name system; anatomy of a URL
- Cloud environments: Issues with gathering data from cloud environments; examples of different cloud environments and their types of data
- Open source intelligence: sources of intelligence; gathering data; common analysis techniques

Learning Outcomes

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

1. Utilise appropriate tools to analyse and understand various log and configuration files on both clients and servers.
2. Reconstruct web based activity.
3. Trace e-mail.
4. Interpret DNS Ownership.
5. Assess issues with cloud based evidence and extract data from certain cloud environments.
6. Integrate Open Source Intelligence.

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	
Practical	36	
Independent Learning	87	

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
Assignment	50%	1,2,3
Assignment	50%	4,5,6

Assessment Criteria

<40%: Unable to interpret and describe key concepts of the specific knowledge domain.

40%–49%: Be able to interpret and describe key concepts of the specific knowledge domain(s). Gather basic evidence types. Reconstruct basic events.

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 reconstruct online based evidence and interpret it.

60%–69%: Be able to solve problems within the specific knowledge domain(s) by experimenting with the appropriate skills and tools. Be able to attempt alternative methods or tools for the extraction and interpretation of information from gathered data.

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.

Supplementary Material(s)

- Bazzell, M. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* United States: CreateSpace Independent Publishing Platform, 2015.
- Golbeck, J. *Introduction to Social Media Investigation: A Hands-on Approach.* United States: Syngress, 2015.
- Hadnagy, C and P Wilson. *Social Engineering: The Art of Human Hacking.* United States: Wiley, 2010.
- Jones, R. *Internet Forensics.* United States: O'Reilly Media, 2005.
- Layton, R and P Watters. *Automating Open Source Intelligence: Algorithms for OSINT (Computer Science Reviews and Trends).* United States: Syngress, 2015.

Requested Resources

- Computer Lab: BYOD Lab