INFO 3014 DIGITAL INVESTIGATIONS AND FORENSICS

Credit Points 10

Legacy Code 102701

Coordinator Farhad Ahamed (https://directory.westernsydney.edu.au/search/name/Farhad Ahamed/)

Description This subject focuses on the concepts, theories, and practice of digital investigations and forensics. More specifically, it focuses on using a detailed hands-on approach to the use of computer technology in investigating and demonstrating that particular digital media contains incriminating evidence. With topics ranging from data acquisition, file systems examination, social media, email and network investigations, mobile and cloud forensics, a working knowledge of how to approach digital investigations and utilise various forensic tools to collect, analyse and present digital evidence will be gained. In this subject, digital investigations and forensics is covered from both a theory-based and applied understanding of how to recover admissible legal evidence after an incident, or proactively as a key defence to reduce the likelihood of cyber attacks.

School Social Sciences

Discipline Security Science

Student Contribution Band HECS Band 2 10cp

Check your fees via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 3 subject

Pre-requisite(s) INFS 1002 AND
INFO 2001 OR
INFO 2004

Assumed Knowledge

A basic understanding of computer systems, architecture, infrastructure, internet protocols and networking protocols. A basic understanding of core theories related to social and cognitive psychology is desirable.

Learning Outcomes

On successful completion of this subject, students should be able to:

1. Explain the process of digital investigations and forensics on digital media.
2. Design a proactive digital investigation process to detect and prevent exposure to cyber attacks in organisations.
3. Identify and recover key evidence from digital media using a variety of forensic tools.
4. Conduct and manage digital investigations and forensics involving digital media
5. Demonstrate an understanding of the ethical principles and practice for digital forensic investigators.
6. Present clear evidence and conclusions of a digital investigation in report form.
7. Define the methods, theories, and terms related to digital investigations and forensics.

Subject Content

Fundamentals of digital investigations and forensics
Processing attack and incident scenes
Data acquisition, analysis, and validation
Network, mobile and cloud forensics
Email and social media forensic investigations
Current digital forensics tools
Digital evidence and report writing for high-tech investigations
Ethical issues for digital investigations and forensics

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Type	Length	Percent	Threshold	Individual/ Group Task
Quiz	10 x 10 MCQ ea	10	N	Individual
Report	2,000 words	30	N	Group
Practical	10 lab projects	20	N	Individual
Final Exam	2 hours	40	N	Individual

Prescribed Texts

- Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to computer forensics and investigations: Processing digital evidence. Cengage Learning.

Teaching Periods

Autumn (2024)

Parramatta - Victoria Rd

On-site

Subject Contact Farhad Ahamed (https://directory.westernsydney.edu.au/search/name/Farhad Ahamed/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3014_24-AUT_PS_1#subjects)

WSU Online TRI-3 (2024)

Wsu Online

Online

Subject Contact Rosalind Priestman (https://directory.westernsydney.edu.au/search/name/Rosalind Priestman/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO3014_24-OT3_OW_2#subjects)