TEQSA ID PRV:14323
CRICOS Provider Code: 03866C

MIT623 DIGITAL FORENSICS

Unit Outline

Important Update:	Our aim is to provide you with an optimal learning experience, regardless of how this unit is delivered. Teaching will be delivered in line with the most current COVID Safe health guidelines. This may include a mix of online and face-to-face. Please check the learning management system for announcements and updates. Thank you for your flexibility and commitment to studying with Sydney Institute of Higher Education.
Enrolment Modes:	Year 2, Semester 2.
Credit Point(s):	12.5
EFTSL Value:	0.125
Prerequisites:	MIT508 Cyber Security
Typical study commitment:	Students will on average spend 10 hours per week over the teaching period undertaking the teaching, learning and assessment activities for this unit.
Scheduled learning activities:	4 timetabled hours per week, 6 personal study hours per week.
Other resource requirements:	Students will need access to lab computers or will need their own laptops to carry out lab exercises and assignments. Students will need to use open-source Digital Forensics tools to carry out the labs. Some devices like mobile phones, USB hard drives will also be needed for forensic analysis.

Unit description

This unit provides a comprehensive study of principles, procedures and methodologies that are currently used to carry out Digital Forensics. This unit will prepare students to conduct a digital investigation in an organized and systematic way. Ethical and legal issues in Digital Forensics will be discussed in this unit. Students will use various open-source tools to recover digital evidence from a variety of devices. Unit will also focus on issues related to the Digital Forensics of Internet of Things (IoT) and Cloud Computing.

Unit learning outcomes (ULO)

	On the successful completion of this unit student will be able to:
ULO1	Discuss the basic principles, procedures, and methodologies of Digital Forensics.
ULO2	Demonstrate understanding of the current legal and ethical issues related to Digital Forensics.
ULO3	Demonstrate understanding of principles and procedures associated with the Digital Forensics of Mobile Devices, Internet of Things (IoT) and Cloud Computing.
ULO4	Analyse and evaluate various tools that are currently used for Digital Forensics.
ULO5	Apply Digital Forensics tools and techniques to recover data from various sources.

Topics to be included in the unit

1.	Introduction to Digital Forensics
2.	Data Acquisition
3.	Processing Crime and Incident Scenes
4.	Current Digital Forensics Tools
5.	Working with Windows and CLI Systems
6.	Linux and Macintosh File Systems
7.	Recovering Graphic Files
8.	Digital Forensics Analysis and Validation
9.	Email and Social Media Investigations
10.	Mobile Device Forensics
11.	Digital Forensics in Internet of Things (IoT)
12.	Cloud Forensics and Revision

Assessment

Assessment Description	**Grading and weighting (% total mark for unit)**	**Due date**
Assessment 1: Class Participation	10%	Weeks 2-11
Assessment 2: Online Quiz	10%	Week 7
Assessment 3: Lab	20%	Weeks 3-10
Assessment 4: Report	30%	Week 12
Assessment 5: Final Exam	30%	Final exam week