



COIT12201 *Electronic Crime and Digital Forensics*

Term 2 - 2023

Profile information current as at 08/05/2024 01:12 pm

All details in this unit profile for COIT12201 have been officially approved by CQUniversity and represent a learning partnership between the University and you (our student). The information will not be changed unless absolutely necessary and any change will be clearly indicated by an approved correction included in the profile.

General Information

Overview

This advanced unit provides you with a broad understanding of electronic crime and digital forensics in investigations of electronic criminal activities. In this unit, you will learn digital forensics procedures and tools, methods of using digital evidence in justice and legal issues in digital forensics. You will use industry leading software tools to conduct your own forensics investigation on realistic case studies. Completion of this unit enables you to pursue careers within an electronic crime investigation unit of law enforcement agencies, government departments, and businesses.

Details

Career Level: *Undergraduate*

Unit Level: *Level 2*

Credit Points: 6

Student Contribution Band: 8

Fraction of Full-Time Student Load: 0.125

Pre-requisites or Co-requisites

Pre-requisite: (COIT11233 or COIT11238) and (COIT13147 or COIT12206)

Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the [Assessment Policy and Procedure \(Higher Education Coursework\)](#).

Offerings For Term 2 - 2023

- Brisbane
- Cairns
- Melbourne
- Online
- Rockhampton
- Sydney
- Townsville

Attendance Requirements

All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

Website

[This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.](#)

Class and Assessment Overview

Recommended Student Time Commitment

Each 6-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 hours for the unit.

Class Timetable

[Regional Campuses](#)

Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

[Metropolitan Campuses](#)

Adelaide, Brisbane, Melbourne, Perth, Sydney

Assessment Overview

1. **In-class Test(s)**

Weighting: 20%

2. **Written Assessment**

Weighting: 40%

3. **Online Test**

Weighting: 40%

Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the [University's Grades and Results Policy](#) for more details of interim results and final grades.

CQUniversity Policies

All University policies are available on the [CQUniversity Policy site](#).

You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the [CQUniversity Policy site](#).

Previous Student Feedback

Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

Feedback from Student Unit and Teaching Evaluations (SUTE) feedback and Unit Coordinator's reflection.

Feedback

The textbook does not address the Australian legal frameworks relevant to electronic crime and digital forensics, which is a topic of significant interest for students.

Recommendation

Include Australian legal frameworks associated with electronic crime and digital forensics in the unit.

Feedback from SUTE feedback and Unit Coordinator's reflection.

Feedback

The group assessment weighting does not adequately reflect the necessary effort required to enhance student dedication and the quality of their work.

Recommendation

Review the weighting of the assessments and adjust them to better reflect the effort required for the group-based assessment, while also ensuring that the weightage of the individual component is appropriately balanced.

Unit Learning Outcomes

On successful completion of this unit, you will be able to:

1. Define electronic crime and digital forensics
2. Describe the role of digital forensic professionals in investigation and prevention of electronic crime in business environments
3. Apply a systematic approach to the capture, recording, and analysis of events in a digital forensic investigation
4. Discuss the legal issues involved in a forensic investigation and in current professional forensic practice
5. Prepare a design and report for a digital forensic investigation.

The Australian Computer Society (ACS), the professional association for Australia's ICT sector, recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments, and individuals in many countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles. ACS members can use the tool [MySFIA](#) to build a skills profile.

This unit contributes to the following workplace skills as defined by [SFIA 8](#) (the SFIA code is included):

- Digital forensics (DGFS)
- Network Support (NTAS)
- Penetration testing (PENT)
- Problem Management (PBMG)
- Incident Management (USUP)
- Information security (SCTY)

The National Initiative for Cybersecurity Education ([NICE](#)) Framework defines knowledge, skills and tasks needed to perform various cyber security roles. Developed by the National Institute of Standards and Technology (NIST), the NICE Framework is used by organisations to plan their workforce, including recruit into cyber security positions.

This unit helps prepare you for roles within electronic crime investigation unit of law enforcement agencies, government departments, and businesses, contributing to the following knowledge and skills:

- K0003 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0117 Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
- K0622 Knowledge of controls related to the use, processing, storage, and transmission of data.

Alignment of Learning Outcomes, Assessment and Graduate Attributes

 N/A Level	 Introductory Level	 Intermediate Level	 Graduate Level	 Professional Level	 Advanced Level
---	--	--	--	--	--

Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
1 - In-class Test(s) - 20%	•			•	
2 - Written Assessment - 40%		•	•	•	•
3 - Online Test - 40%	•	•	•		•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	5
1 - Communication	•			•	•
2 - Problem Solving			•		•
3 - Critical Thinking		•	•		
4 - Information Literacy				•	•
5 - Team Work					•
6 - Information Technology Competence	•		•		
7 - Cross Cultural Competence				•	
8 - Ethical practice		•		•	•
9 - Social Innovation					
10 - Aboriginal and Torres Strait Islander Cultures					

Textbooks and Resources

Textbooks

COIT12201

Prescribed

Guide to Computer Forensics and Investigations

Edition: 6th edn (2018) (2018)

Authors: B Nelson, A Phillips, C Steuart

Cengage Learning

Florence , KY , USA

ISBN: 9781337568944

Binding: Paperback

[View textbooks at the CQUniversity Bookshop](#)

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- Computer forensic software and data files (included in MindTap- a cloud-based virtual lab integrated into Moodle unit website)

Referencing Style

All submissions for this unit must use the referencing style: [Harvard \(author-date\)](#)

For further information, see the Assessment Tasks.

Teaching Contacts

Jahan Hassan Unit Coordinator

j.hassan@cqu.edu.au

Schedule

Week 1 - 10 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Understanding the Digital Forensics Profession and Investigations	Chapter 1	

Week 2 - 17 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Forensic Investigation Examples and the Investigator's Office and Laboratory	Chapter 1 and Chapter 2	

Week 3 - 24 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Data Acquisition	Chapter 3	Assessment 1(In-class test): Online Quiz 1

Week 4 - 31 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
--------------	---------	------------------------------

Processing Crime and Incident Scenes Chapter 4

Week 5 - 07 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Digital Forensics Tools	Chapter 6	Assessment 1(In-class test): Online Quiz 2

Vacation Week - 14 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
--------------	---------	------------------------------

Week 6 - 21 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Understanding Windows, Linux and Macintosh Systems	Chapter 5 and Chapter 7	

Week 7 - 28 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Recovering Graphic Files	Chapter 8	Assessment 1(In-class test): Online Quiz 3

Week 8 - 04 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Digital Forensics Analysis and Validation	Chapter 9	

Week 9 - 11 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Virtual Machine Forensics, Live Acquisitions, and Network Forensics E-mail and Social Media Investigations	Chapter 10 and Chapter 11	Assessment 1(In-class test): Online Quiz 4

Week 10 - 18 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Mobile Device Forensics, Ethics	Chapter 12 and Chapter 16	Assessment 2 (Written Assessment) Digital Forensic Investigation Due: Week 10 Friday 11:45 PM AEST Digital Forensics Investigation Due: Week 10 Friday (22 Sept 2023) 11:45 pm AEST

Week 11 - 25 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Cloud Forensics and Report Writing	Chapter 13 and Chapter 14	Assessment 1(In-class test): Online Quiz 5

Week 12 - 02 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
Reflection and Exam Overview	Reflection of topics covered in Weeks 1-11, and exam advice	

Review/Exam Week - 09 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
--------------	---------	------------------------------

Exam Week - 16 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
--------------	---------	------------------------------

Term Specific Information

For any term-specific information, please contact your Unit coordinator via E-mail.

Unit Coordinator: Dr Jahan Hassan

E-mail: j.hassan@cqu.edu.au

Assessment Tasks

1 ONLINE QUIZZES

Assessment Type

In-class Test(s)

Task Description

The online quizzes are to complement the theoretical knowledge you learn from the lectures/textbook. These exercises will enhance your understanding and improve your skills in the related topics of Electronic Crime and Digital Forensics.

- There are five (5) weekly online quizzes arranged on weeks 3, 5, 7, 9, and 11.
- Each quiz is worth 4% of the total grade.
- The quizzes are open book, implying that you are allowed to consult the prescribed textbook, lab manuals, lecture notes, and notes you prepare for.
- You will be required to complete such tasks within a time limit.

More details of quiz instruction will be available through the Moodle unit website.

Assessment Due Date

Due in the same week (3, 5, 7, 9, 11) for each quiz. More details will be provided in the online quiz specification through Moodle unit website.

Return Date to Students

Immediately after the quizzes close.

Weighting

20%

Assessment Criteria

You are assessed against your abilities to:

- Understand the weekly content covered in lectures,
- Identify the links between lecture contents and lab exercises,
- Determine the best course of action for a specific investigation scenario.

Extensions are not allowed for the quizzes, because the answers will be released after the due date. If you miss attempting the quizzes, you cannot do it later.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online

Submission Instructions

Quizzes are to be attempted and submitted as individual assessment items.

Learning Outcomes Assessed

- Define electronic crime and digital forensics
- Discuss the legal issues involved in a forensic investigation and in current professional forensic practice

2 Digital Forensics Investigation

Assessment Type

Written Assessment

Task Description

This is a group task that comprises two separate parts:

Part A (25% - individual mark): In this part, each student will independently perform and report on a practical investigation. They will be responsible for completing this part individually, recording their findings in the group report.

Part B (15% - group mark): The second part of the task entails a comprehensive written analysis that incorporates the individual investigations conducted by each group member. This analysis also integrates collaborative group discussions, with a focus on exploring the individual investigations within the broader context of the group's discussion. Together, this assessment combines the practical investigation, collaborative group discussion, and derived findings to generate a comprehensive written report.

Assessment Due Date

Week 10 Friday (22 Sept 2023) 11:45 pm AEST

One report per group, to be submitted via Moodle submission link.

Return Date to Students

Week 12 Friday (6 Oct 2023)

Assessments will be returned through Moodle. Late submissions with or without extension approvals may be returned after the above date.

Weighting

40%

Assessment Criteria

You will be assessed against your abilities to:

- Apply suitable digital forensics methodologies,
- Use appropriate tools and techniques,
- Identify legal and ethical issues in the given case,
- Investigate in a formal process,
- Report the findings in a clear and cohesive manner.

More details of the marking criteria will be available through the Moodle unit website.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online Group

Submission Instructions

Online group submission via Moodle.

Learning Outcomes Assessed

- Describe the role of digital forensic professionals in investigation and prevention of electronic crime in business environments
- Apply a systematic approach to the capture, recording, and analysis of events in a digital forensic investigation
- Discuss the legal issues involved in a forensic investigation and in current professional forensic practice
- Prepare a design and report for a digital forensic investigation.

3 Online Test

Assessment Type

Online Test

Task Description

The final assessment will be an online Moodle Quiz.

The guidelines for this test will be accessible on the Moodle unit website starting from Week 6.

Assessment Due Date

The online test will be held during the examination period. Specific date and time will be advised via Moodle.

Return Date to Students

Overall results become available on Certification Date (see Academic Calendar).

Weighting

40%

Assessment Criteria

Your answers will be marked based on the correct choice from a range of options, and for short answer items on technical correctness, completeness, clarity, originality, and relevance. Originality means the work is your own and is expressed in your own words. An answer is unacceptable (zero marks) if it is composed mostly or solely of quoted materials from other sources.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online

Submission Instructions

Refer to Moodle unit website for details.

Learning Outcomes Assessed

- Define electronic crime and digital forensics
- Describe the role of digital forensic professionals in investigation and prevention of electronic crime in business environments
- Apply a systematic approach to the capture, recording, and analysis of events in a digital forensic investigation
- Prepare a design and report for a digital forensic investigation.

Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the [Student Academic Integrity Policy and Procedure](#). This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

What is a breach of academic integrity?

A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

Why is academic integrity important?

A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

Where can I get assistance?

For academic advice and guidance, the [Academic Learning Centre \(ALC\)](#) can support you in becoming confident in completing assessments with integrity and of high standard.

What can you do to act with integrity?



Be Honest

If your assessment task is done by someone else, it would be dishonest of you to claim it as your own



Seek Help

If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)



Produce Original Work

Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem