COIT20267 *Computer Forensics*
Term 2 - 2020

All details in this unit profile for COIT20267 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

The continual integration of computers and the Internet into business and personal activities is creating opportunities for crimes utilising these technologies. The investigation of these electronic crimes requires specialised computer-based techniques to collect and analyse evidence. This unit equips you with a broad understanding of how electronic crimes are conducted, as well as in-depth knowledge of computer forensic investigations. Through the use of industry-leading digital forensic tools in a laboratory environment, you will develop practical skills applicable to all phases of forensic investigations. You will learn different approaches for identifying, gathering and analysing digital evidence, as well as addressing legal issues in computer forensic investigations.

Details

Career Level: *Postgraduate*
Unit Level: *Level 9*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites

Pre-requisite: COIT20261 Network Routing and Switching
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 - 2020

- Brisbane
- Melbourne
- Online
- Sydney

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 Postgraduate 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. **Written Assessment**
Weighting: 35%
2. **Written Assessment**
Weighting: 45%
3. **Online Quiz(zes)**
Weighting: 20%

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 Students feedback and teachers reflection

Feedback
Enjoyed practical lab exercises and assessment tasks using forensic tools.

Recommendation
Continue using practical lab exercises using Virtual Lab, MindTap, etc.

Feedback from Students feedback

Feedback
Some parts of Assignment 3 are unclear or hard to follow

Recommendation
Improve the clarity of the assignment specifications by breaking them down into smaller tasks

Unit Learning Outcomes

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

1. Discuss the different types of electronic crime and the need for a computer forensics investigation
2. Analyse the role of computer forensic professionals in enabling successful investigation and prevention of electronic crime in business environments
3. Apply a systematic approach in a digital investigation through the conduct of computer forensics procedures and the use of computer forensic tools
4. Apply the necessary steps required for collecting, storing, analysing and validating digital evidence
5. Explain the legal issues involved in a computer forensic investigation
6. Evaluate current industry best practices for analysing computer forensic case scenarios.

Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is in use in over 100 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 at
https://www.acs.org.au/professionalrecognition/mysfia-b2c.html
This unit contributes to the following workplace skills as defined by SFIA. The SFIA code is included:

- Information Security (SCTY)
- Digital forensics (DGFS)
- Data analysis (DTAN)
- Testing (TEST)
- Network Support (NTAS)
- Application Support (ASUP).

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	6
1 - Online Quiz(zes) - 20%	●	●			●	
2 - Written Assessment - 35%	●	●	●	●		●
3 - Written Assessment - 45%			●	●	●	●

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes					
	1	2	3	4	5	6
1 - Knowledge	○	○	○	○	○	○
2 - Communication	○	○	○	○	○	○
3 - Cognitive, technical and creative skills		○	○	○	○	○
4 - Research	○	○	○	○	○	○
5 - Self-management						
6 - Ethical and Professional Responsibility	○	○	○	○	○	○
7 - Leadership						○
8 - Aboriginal and Torres Strait Islander Cultures						

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes							
	1	2	3	4	5	6	7	8
1 - Online Quiz(zes) - 20%	○	○						
2 - Written Assessment - 35%	○	○		○		○		
3 - Written Assessment - 45%	○	○		○		○	○	

Textbooks and Resources

Textbooks
COIT20267

Prescribed

Guide to computer forensics and investigations
Edition: 6th edn
Authors: Nelson, B., Phillips, A., and Steuart, C.
ISBN: 9781337568944
Binding: Hardcover
COIT20267

Supplementary

Lab Manual for Nelson / Phillips / Steuart Guide to Computer Forensics and Investigations
Edition: 5th edn
Authors: Blitz, A.
ISBN: 9781285079080
Binding: Paperback

Additional Textbook Information
If you prefer to study with a paper copy, they are available at the CQUni Bookshop here: http://bookshop.cqu.edu.au (search on the Unit code). eBooks are available at the publisher's website.

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 student data files (with "Lab Manual for Guide to Computer Forensics and Investigations (4th ed)" by A. Blitz)
- MindTap - Cloud based virtual lab integrated in 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

Santoso Wibowo Unit Coordinator
s.wibowo1@cqu.edu.au

Schedule

Week 1 - 13 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic
Understanding the Digital Forensics Professional and Investigation	Chapter 1	

Week 2 - 20 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic

| The Investigator's Office and Laboratory | Chapter 2 | |

Week 3 - 27 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic
Data Acquisition	Chapter 3	

Week 4 - 03 Aug 2020

Module/Topic	Chapter	Events and Submissions/Topic
Processing Crime and Incident Scenes	Chapter 4	

Week 5 - 10 Aug 2020

Module/Topic	Chapter	Events and Submissions/Topic
Current Digital Forensics Tools	Chapter 6	

Vacation Week - 17 Aug 2020

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 24 Aug 2020

Module/Topic	Chapter	Events and Submissions/Topic
Digital Forensics Analysis and Validation	Chapter 9	**Assessment Item 1 - Comparative Study** Due: Week 6 Friday (28 Aug 2020) 11:45 pm AEST

Week 7 - 31 Aug 2020

Module/Topic	Chapter	Events and Submissions/Topic
Working with Windows and CLI Systems	Chapter 5	

Week 8 - 07 Sep 2020

Module/Topic	Chapter	Events and Submissions/Topic
Linux and Macintosh File System & Recovering Graphics Files	Chapters 7 & 8	

Week 9 - 14 Sep 2020

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	

Week 10 - 21 Sep 2020

Module/Topic	Chapter	Events and Submissions/Topic
Mobile Device Forensics and the Internet of Anything	Chapter 12	

Week 11 - 28 Sep 2020

Module/Topic	Chapter	Events and Submissions/Topic
Cloud Forensics and Report Writing for High-Tech Investigation	Chapter 13 and Chapter 14	

Week 12 - 05 Oct 2020

Module/Topic	Chapter	Events and Submissions/Topic
Expert Testimony in Digital Investigation & Ethics for the Expert Witness	Chapters 15 & 16	**Assessment Item 2 - Written Assignment - Case Study** Due: Week 12 Friday (9 Oct 2020) 11:45 pm AEST

Review/Exam Week - 12 Oct 2020		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
		Assessment Item 3 - Online Quiz Due: Review/Exam Week Friday (16 Oct 2020) 11:45 pm AEST
Exam Week - 19 Oct 2020		
Module/Topic	**Chapter**	**Events and Submissions/Topic**
This is no exam in this unit.		

Term Specific Information

Unit Coordinator:
Dr Santoso Wibowo
Email: s.wibowo1@cqu.edu.au

Assessment Tasks

1 Assessment Item 1 - Comparative Study

Assessment Type
Written Assessment

Task Description
This assignment requires you to research existing computer forensic tools and apply a selected computer forensic tool to evaluate a real case problem. More specifically, you will be asked to:
1. Identify different computer forensics tools for computer investigations.
2. Analyse the strengths and weaknesses of computer forensics tools.
3. Demonstrate the suitability of the chosen computer forensic tool in the real case scenario.
4. Submit a written report.
Students have the choice to work in a group of 2 or 3, or they may work individually.

Assessment Due Date
Week 6 Friday (28 Aug 2020) 11:45 pm AEST
Online

Return Date to Students
Week 8 Friday (11 Sept 2020)
Online

Weighting
35%

Assessment Criteria
You will be assessed mainly against:
1. Providing a thorough analysis on available computer forensic tools.
2. The justification of using a specific computer forensic tool.
3. Discussion on the application of the computer forensic tool for dealing with the real case problem.
4. Presenting the analysis and findings in the report.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
Submit as per instructions on the Moodle unit website.

Learning Outcomes Assessed

- Discuss the different types of electronic crime and the need for a computer forensics investigation
- Analyse the role of computer forensic professionals in enabling successful investigation and prevention of

electronic crime in business environments
- Apply a systematic approach in a digital investigation through the conduct of computer forensics procedures and the use of computer forensic tools
- Apply the necessary steps required for collecting, storing, analysing and validating digital evidence
- Evaluate current industry best practices for analysing computer forensic case scenarios.

Graduate Attributes

- Knowledge
- Communication
- Research
- Ethical and Professional Responsibility

2 Assessment Item 2 - Written Assignment - Case Study

Assessment Type
Written Assessment

Task Description
You are to produce a forensic analysis and report for a given case study. In this assessment, you will be specifically asked to:
1. Apply the computer forensics methodologies.
2. Write an analysis of a case study.
3. Prepare an outline of a professional computer forensic plan.
Details of the case study, the questions, what you are required to submit and guidelines for approaching the assignment will be available on the Moodle unit website.
Students may work and submit in a group of 2 or 3, or they may work individually.

Assessment Due Date
Week 12 Friday (9 Oct 2020) 11:45 pm AEST
Online

Return Date to Students

Result will be released after certification

Weighting
45%

Assessment Criteria
You are assessed mainly against:
1. The justification of using the computer forensic methodology and approach.
2. Providing the resources required for a digital forensic investigation, including the skill set of team members and the tools.
3. Outlining an approach for evidence identification and acquisition.
4. Outlining the steps to be taken during the analysis phase.
5. Presenting the full investigative report.
Further details are available on Moodle.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
Submit as per instructions on the Moodle unit website.

Learning Outcomes Assessed

- Apply a systematic approach in a digital investigation through the conduct of computer forensics procedures and the use of computer forensic tools
- Apply the necessary steps required for collecting, storing, analysing and validating digital evidence
- Explain the legal issues involved in a computer forensic investigation
- Evaluate current industry best practices for analysing computer forensic case scenarios.

Graduate Attributes

- Knowledge

- Communication
- Research
- Ethical and Professional Responsibility
- Leadership

3 Assessment Item 3 - Online Quiz

Assessment Type
Online Quiz(zes)

Task Description
You will complete an online quiz in Moodle containing a variety of questions covering material from weeks 1 to 12 of the unit. The quiz is open book, has a duration of 60 minutes, and only a single attempt is allowed.
This assessment is to be done on an individual basis.

Number of Quizzes

Frequency of Quizzes

Assessment Due Date
Review/Exam Week Friday (16 Oct 2020) 11:45 pm AEST

Return Date to Students
Exam Week Monday (19 Oct 2020)

Weighting
20%

Assessment Criteria
1. Each quiz question will be multiple choice, which is randomly drawn from a large question bank.
2. The quiz will be available on the Unit Website on Moodle in Week 13. It has been set to automatically open at 9:00 am on Monday of Week 13 and automatically close at 11:45 pm on Friday of Week 13.
3. Detailed instructions about the quiz will be provided on the Unit Website on Moodle.
4. As a quiz solution will be released shortly after the quiz closing time, no late submissions will be accepted. The quiz will close on the deadline. Therefore if you have not attempted the quiz before the deadline, you will receive 0 marks.

Referencing Style

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

Submission
Online

Submission Instructions
Online

Learning Outcomes Assessed

- Discuss the different types of electronic crime and the need for a computer forensics investigation
- Analyse the role of computer forensic professionals in enabling successful investigation and prevention of electronic crime in business environments
- Explain the legal issues involved in a computer forensic investigation

Graduate Attributes

- Knowledge
- Communication

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