



# COIT20267 Computer Forensics

## Term 1 - 2017

Profile information current as at 19/05/2022 10:41 pm

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 rapid growth of the Internet and computers usage have led to various electronic crimes that require the urgent need for computer investigations. This unit equips students with a broad understanding of electronic crimes and computer forensics investigation. The content is structured so as to provide students with the practical knowledge of computer forensics and to enable students develop the necessary skills in investigating electronic criminal activities using available digital forensics tools. Specific topics including electronic crime, digital forensics procedures and tools, methods of using digital evidence in justice, and legal issues in digital forensics are covered in the unit. If you have successfully completed unit COIS23002 you cannot take this unit.

### 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 1 - 2017

- Brisbane
- Distance
- Melbourne
- 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. **Online Quiz(zes)**

Weighting: 20%

#### 2. **Practical and Written Assessment**

Weighting: 35%

#### 3. **Practical and Written Assessment**

Weighting: 45%

### 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 Self-reflection

**Feedback**

No extension on the first assessment item

**Recommendation**

Indicate in the unit profile, in the Task Description component, that extensions cannot be granted for the online quiz assessment because answers will be released to students upon completion of the quiz.

#### Feedback from Self-reflection and student feedback

**Feedback**

Australia and U.S. Jurisdiction

**Recommendation**

The unit should highlight and compare the differences between U.S. and Australian laws on criminal procedure and privacy.

## 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. Analyse the necessary steps required for collecting, storing, analysing and validating digital evidence.
5. Critically evaluate the different methods of recovering evidence from files and explain how to determine feasible methods.
6. Identify the legal issues involved in a computer forensic investigation.
7. Apply 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:

- Data analysis (DTAN)
- Database/repository design (DBDS)
- Testing (TEST)
- Network Support (NTAS)
- Application Support (ASUP).

## Alignment of Learning Outcomes, Assessment and Graduate Attributes



### Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes						
	1	2	3	4	5	6	7
1 - Online Quiz(zes) - 20%	•	•		•		•	
2 - Practical and Written Assessment - 35%	•	•	•	•	•	•	•
3 - Practical and Written Assessment - 45%	•	•	•	•	•	•	•

### Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes						
	1	2	3	4	5	6	7
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 - Practical and Written Assessment - 35%	◦	◦				◦		
3 - Practical and Written Assessment - 45%	◦	◦				◦		

## Textbooks and Resources

### Textbooks

COIT20267

#### Prescribed

#### **Guide to Computer Forensics and Investigations: Processing Digital Evidence**

Edition: Fifth (2016)

Authors: Nelson, B., Phillips, A. and Steuart, C.

Cengage Learning

Boston , MA 02210 , United States of America

ISBN: 9781285060033

Binding: Hardcover

#### **Additional Textbook Information**

[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)

## 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](mailto:s.wibowo1@cqu.edu.au)

## Schedule

### **Week 1 - 06 Mar 2017**

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to digital forensics	Chapter 1	

### **Week 2 - 13 Mar 2017**

Module/Topic	Chapter	Events and Submissions/Topic
Digital investigation environments	Chapter 2	

### **Week 3 - 20 Mar 2017**

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

### **Week 4 - 27 Mar 2017**

Module/Topic	Chapter	Events and Submissions/Topic
Processing crime and incident scenes	Chapter 4	

<b>Week 5 - 03 Apr 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Digital forensics tools	Chapter 6	
<b>Vacation Week - 10 Apr 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
<b>Week 6 - 17 Apr 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Digital forensics analysis and validation	Chapter 9	<b>Online Quiz</b> Due: Week 6 Friday (21 Apr 2017) 11:45 pm AEST
<b>Week 7 - 24 Apr 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Understanding Windows and DOS Systems	Chapter 5	<b>Written Assignment 1 - Presentation and Comparative Study</b> Due: Week 7 Friday (28 Apr 2017) 11:45 pm AEST
<b>Week 8 - 01 May 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Understanding UNIX/Linux Systems and Recovering Graphics Files	Chapter 7 & 8	
<b>Week 9 - 08 May 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Mobile Device and Cloud Forensics	Chapter 12 & 13	
<b>Week 10 - 15 May 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
E-mail and social media investigations	Chapter 11	
<b>Week 11 - 22 May 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Digital forensics report and professionalism	Chapter 14 & 16	
<b>Week 12 - 29 May 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
Expert Testimony	Chapter 15	<b>Written Assignment 2 - Case Study</b> Due: Week 12 Friday (2 June 2017) 11:45 pm AEST
<b>Review/Exam Week - 05 Jun 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic
<b>Exam Week - 12 Jun 2017</b>		
Module/Topic	Chapter	Events and Submissions/Topic

## Assessment Tasks

### 1 Online Quiz

#### Assessment Type

Online Quiz(zes)

#### Task Description

This quiz has 40 multiple choice questions relating to the unit material of Weeks 1 to 5, covering Chapters 1, 2, 3, 4, and

6 of the prescribed textbook. The quiz is open book implying that the students are allowed to consult the prescribed textbook, lecture notes and their own notes.

**Number of Quizzes**

1

**Frequency of Quizzes****Assessment Due Date**

Week 6 Friday (21 Apr 2017) 11:45 pm AEST

**Return Date to Students**

Week 7 Friday (28 Apr 2017)

**Weighting**

20%

**Assessment Criteria**

1. The quiz will be available on the Unit Website on Moodle in Week 6.
2. Detailed instructions about the quiz will be provided on the Unit Website on Moodle.

**Referencing Style**

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

**Submission**

Online

**Submission Instructions**

Attempt 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.
- Analyse the necessary steps required for collecting, storing, analysing and validating digital evidence.
- Identify the legal issues involved in a computer forensic investigation.

**Graduate Attributes**

- Knowledge
- Communication

## 2 Written Assignment 1 - Presentation and Comparative Study

**Assessment Type**

Practical and Written Assessment

**Task Description**

This assignment has two parts.

The first part requires you to research on existing computer forensic tools and apply the suitable 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 the computer forensics tools.
3. Demonstrate the suitability of the chosen computer forensic tool to evaluate a real case scenario.

The second part requires you to carry out a comparative study on Australian and American laws on criminal procedure and/or privacy.

A detailed assignment specification will be made available on Moodle from Week 4.

**Assessment Due Date**

Week 7 Friday (28 Apr 2017) 11:45 pm AEST

**Return Date to Students**

Week 9 Friday (12 May 2017)

**Weighting**

35%

**Assessment Criteria**

You are 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.
5. Knowledge and understanding on criminal procedural and privacy laws.

### Referencing Style

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

### Submission

Online

### 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.
- Analyse the necessary steps required for collecting, storing, analysing and validating digital evidence.
- Critically evaluate the different methods of recovering evidence from files and explain how to determine feasible methods.
- Identify the legal issues involved in a computer forensic investigation.
- Apply current industry best practices for analysing computer forensic case scenarios.

### Graduate Attributes

- Knowledge
- Communication
- Ethical and Professional Responsibility

## 3 Written Assignment 2 - Case Study

### Assessment Type

Practical and Written Assessment

### Task Description

The purpose of this assignment is to produce a report based on 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 Moodle unit website.

### Assessment Due Date

Week 12 Friday (2 June 2017) 11:45 pm AEST

### Return Date to Students

Written assignment 2 marks will be released at the Certification of Grades.

### 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

**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.
- Analyse the necessary steps required for collecting, storing, analysing and validating digital evidence.
- Critically evaluate the different methods of recovering evidence from files and explain how to determine feasible methods.
- Identify the legal issues involved in a computer forensic investigation.
- Apply current industry best practices for analysing computer forensic case scenarios.

**Graduate Attributes**

- Knowledge
- Communication
- Ethical and Professional Responsibility

## 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