COMP2310

Digital Forensics

Session 1, In person-scheduled-weekday, North Ryde 2023

School of Computing

Contents

General Information

Unit convenor and teaching staff
Muhammad Ikram
muhammad.ikram@mq.edu.au

Convener and Lecturer
Benjamin Zhao
ben_zi.zhao@mq.edu.au

Credit points
10

Prerequisites
(COMP1010 or COMP125) and (COMP1350 or ISYS114)

Corequisites
COMP2250 or COMP247

Co-badged status

Unit description
This unit provides an introduction to digital forensics and incident response methods, techniques and tools. Strong emphasis is given to ethics, the laws and procedures as students are exposed to forensics techniques used to collect and recover data. Students are taught how to conduct digital investigations following the process of preserving, acquiring, analysing and presenting digital evidence.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

ULO1: Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.

ULO2: Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.

ULO3: Use appropriate tools and techniques to collect and recover data from a variety of digital sources.

ULO4: Communicate effectively the results of an investigation following professional standards.

General Assessment Information

Late Assessment Submission Penalty

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark of the task) will be applied for each day a written report or presentation assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. The submission time for all uploaded assessments is **11:55 pm**. A 1-hour grace period will be provided to students who experience a technical concern.

For any late submission of time-sensitive tasks, such as scheduled tests/exams, performance assessments/presentations, and/or scheduled practical assessments/labs, please apply for Special Consideration.

Assessments where Late Submissions will be accepted

Weekly Taks -- Yes, Standard Late Penalty applies

Module exams and Assignment 1 & 2 -- NO, unless Special Consideration is granted

Special Consideration

The Special Consideration Policy aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment.

Written Assessments: If you experience circumstances or events that affect your ability to complete the written assessments in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

Weekly practice-based tasks: To pass the unit you need to demonstrate ongoing development of skills and application of knowledge in 8 out of 10 of the weekly practical classes. If you miss a weekly practical class due to a serious, unavoidable and significant disruption, contact your convenor ASAP as you may be able to attend another class that week.

If it is not possible to attend another class, you should still contact your convenor for access to class material to review in your own time.

Note that a Special Consideration should **only be applied for** if you miss more than three of the weekly practical classes.

Weekly Tasks

Assessment Type[1]: **Quiz/Test**

Indicative Time on Task[2]: **15 hours**

Due: Weekly
Weighting: 10%

This is a hurdle assessment task (see Assessment Policy, mentined above, for more information on hurdle assessment tasks)

Each week, a set of exercises will be available online. Some require written submissions, while some are multiple choice. Your solutions should be submitted electronically via iLearn before the deadline specified in the text.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations

Assignment 1

Assessment Type[1]: **Project**

Indicative Time on Task[2]: **15 hours**

Due: **Week 6**

Weighting: **15%**

This assignment deals with the recovery of digital evidence and is due on week 6. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Assignment 2

Assessment Type[1]: **Project**

Indicative Time on Task[2]: **15 hours**

Due: **Week 12**

Weighting: **15%**

This group assignment deals with the response to an incident. It involves following defined procedures to recover and present evidence. It features the submission of a report and a

presentation . It is due on week 12. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #1

Assessment Type[1]: **Examination**

Indicative Time on Task[2]: **10 hours**

Due: **Week 5**

Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 1 to 4.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #2

Assessment Type[1]: **Examination**

Indicative Time on Task[2]: **10 hours**

Due: **Week 9**

Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 5 to 8.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.

- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #3

Assessment Type[1]: **Examination**

Indicative Time on Task[2]: **10 hours**

Due: **Week 13**

Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 9 to 12.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Requirements to Pass this Unit

To pass this unit you must:

- Achieve a total mark equal to or greater than 50%, and
- Participate in, and undertake all hurdle activities for, a minimum of 8 of the 10 weekly workshops, and

[1] If you need guidance or support to understand or complete this type of assessment, please contact the Learning Skills Team

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Assessment Tasks

Name	Weighting	Hurdle	Due
Assignment 2	15%	No	Week 12
Assignment 1	15%	No	Week 6

Name	Weighting	Hurdle	Due
Module Exam #1	20%	No	Week 5
Weekly Tasks	10%	Yes	Weekly
Module Exam #3	20%	No	Week 13
Module Exam #2	20%	No	Week 9

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 15 hours
Due: **Week 12**
Weighting: **15%**

This group assignment deals with the response to an incident. It involves following defined procedures to recover and present evidence. It features the submission of a report and a presentation . It is due on week 12. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 15 hours
Due: **Week 6**
Weighting: **15%**

This assignment deals with the recovery of digital evidence and is due on week 7. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 5**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 1 to 4.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Communicate effectively the results of an investigation following professional standards.

Weekly Tasks

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 15 hours
Due: **Weekly**
Weighting: **10%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Each week, a set of exercises will be available online. Some require written submissions, while some are multiple choice. Your solutions should be submitted electronically via iLearn before the deadline specified in the text.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 13**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 13 during practical class. This will test your understanding of material covered in weeks 9 to 12.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

Module Exam #2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 9**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 9 during practical class. This will test your understanding of material covered in weeks 5 to 8.

On successful completion you will be able to:

- Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
- Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
- Communicate effectively the results of an investigation following professional standards.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

Please note that COMP2310 is a **BYOD** (Bring Your Own Device). You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the workshop, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

CLASSES

Each week you should complete any assigned readings and review the lecture slides in order to prepare for the lecture. There are two hours of lectures and a one-hour workshop every week. The hands-on exercises in works help to reinforce concepts introduced during the lectures. You should have chosen a practical on enrollment. You will find it helpful to read the workshop instructions before attending - that way, you can get to work quickly! For details of days, times and rooms consult the timetables webpage.

Note that Workshops commence in week 1.

You should have selected a practical at enrollment. Please note that you will be required to submit work every week. Failure to do so may result in you failing the unit or being excluded from the exam.

METHODS OF COMMUNICATION

This unit makes use of discussion boards hosted within iLearn. Please post questions there; they are monitored by the staff on the unit.We will communicate with you via your university email or through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to their email address from your **university email** address.

RECOMMENDED TEXTS

- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, 6th edition, Cengage Learning, 2019.
- Digital Forensics and Investigations People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 1st edition, 2018.

TECHNOLOGY USED

iLearn is a Learning Management System that gives you access to lecture slides, lecture recordings, forums, assessment tasks, instructions for practicals, discussion forums and other resources.

COVID INFORMATION

For the latest information on the University's response to COVID-19, please refer to the Coronavirus infection page on the Macquarie website: https://www.mq.edu.au/about/coronavirus-faqs. Remember to check this page regularly in case the information and requirements change during semester. If there are any changes to this unit in relation to COVID, these will be communicated via iLearn.

Unit Schedule

Module 1 **(Weeks 1 to 4)**	• Computer Forensics and Investigation Processes • Understanding Computing Investigations • The Investigator's Office and Laboratory • Data Acquisitions • Processing Crime and Incident Scenes
Module 2 **(Weeks 5 to 8)**	• Working with Windows and DOS Systems • Computer Forensics Tools • File Systems • Recovering Graphics Files • Recovering data from memory/hardware • Digital Forensics Analysis and Validation
Module 3 **(Weeks 9 to 13)**	• Virtual Machines, Network Forensics, and Live Acquisitions • E-mail Investigations • Cell Phone and Mobile Device Forensics • Cloud Forensics • Report Writing for High-Tech Investigations • Expert Testimony in High-Tech Investigations • Ethics and High-Tech Investigations

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policie

s.mq.edu.au). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Assessment Procedure
- Complaints Resolution Procedure for Students and Members of the Public
- Special Consideration Policy

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

The Writing Centre

The Writing Centre provides resources to develop your English language proficiency, academic writing, and communication skills.

- Workshops
- Chat with a WriteWISE peer writing leader
- Access StudyWISE
- Upload an assignment to Studiosity
- Complete the Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and processes

Student Enquiries

Got a question? Ask us via AskMQ, or contact Service Connect.

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Changes since First Published

Date	Description
05/02/2023	addressed comments from Xuyun Zhang.