COMP2310

Digital Forensics

Session 1, Special circumstances 2021

School of Computing

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to timetable viewer. To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

General Information

Unit convenor and teaching staff
Convenor, Lecturer
Muhammad Ikram
muhammad.ikram@mq.edu.au
Contact via +61 2 9850 8439
Room 286, BD Building 4RD

Lecturer
Alireza Jolfaei
alireza.jolfaei@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 Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Weekly Tasks

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

Indicative Time on Task[2]: **5 hours**

Due: Weekly

Weighting: 10%

This is a hurdle assessment task (see Assessment Policy, bellow, 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]: **7 hours**

Due: **Week 7**

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.

Assignment 2

Assessment Type[1]: **Project**

Indicative Time on Task[2]: **8 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.

[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
Weekly Tasks	10%	Yes	Weekly
Assignment 1	15%	No	Week 7
Assignment 2	15%	No	Week 12
Module Exam #1	20%	No	Week 5
Module Exam #2	20%	No	Week 9
Module Exam #3	20%	No	Week 13

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.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 15 hours
Due: **Week 7**
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.

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 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.

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.

---

[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 three 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.

DISCUSSION BOARDS

This unit makes use of discussion boards hosted within iLearn. Please post questions there; they are monitored by the staff on the unit.

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.

Unit Schedule

The topics covered in this unit are as follows:

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** • **Report Writing for High-Tech Investigations** • **Expert Testimony in High-Tech Investigation** • **Ethics and High-Tech Investigations**

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.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
- Grade Appeal Policy
- Complaint Management 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

Student Support

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

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- 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

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

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.