COMP2310
Digital Forensics
Session 1, In person-scheduled-weekday, North Ryde 2024
School of Computing

Contents

General Information 2
Learning Outcomes 3
General Assessment Information 3
Assessment Tasks 7
Delivery and Resources 11
Unit Schedule 12
Policies and Procedures 12
Changes from Previous Offering 14
Changes since First Published 14

Disclaimer
Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.
Unit convenor and teaching staff
Lecturer and Convenor
Muhammad Ikram
muhammad.ikram@mq.edu.au
Contact via +61 2 9850 8439
Room 214, Level 2, School of Computing, 4RPD, Macquarie University
(4:00pm to 5:00pm) or requested via email.

Lecturer
John Kim
j.kim@mq.edu.au
Contact via j.kim@mq.edu.au

Teaching Assistant
Izabella Lloyd-White
izabella.lloyd-white@mq.edu.au

Teaching Assistant
Rafiullah Khan
rafiullah.khan@mq.edu.au

Teaching Assistant
Muhammad Salman
muhammad.salman2@hdr.mq.edu.au

Teaching Assistant
Mohib Ullah
mohib.ullah@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:

UL01: Adhere to highest ethical standards, obey the laws and follow procedures at all times when collecting and dealing with digital evidence.
UL02: Develop and follow suitable processes when performing incident response and conducting digital forensics investigations.
UL03: Use appropriate tools and techniques to collect and recover data from a variety of digital sources.
UL04: Communicate effectively the results of an investigation following professional standards.

General Assessment Information
Weekly submissions, assignments, or module exams must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure, students may apply for Special Consideration.

Requirements to Pass this Unit
To pass this unit you must:

• Attempt all assignments and module exams,
• 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.

Hurdle Assessments
Development of knowledge and skills requires continual practice at authentic problems in a laboratory-based setting. This unit has weekly laboratory classes and you must demonstrate your progress in developing and communicating knowledge and skills in a minimum of 8 of the
10 classes. This is a hurdle assessment meaning that failure to meet this requirement may result in a fail grade for the unit. Students are permitted up to two absences: additional absences will require approval of Special Consideration.

**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 Tasks -- 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 **two** of the weekly *practical* classes.

**Weekly Tasks**

Assessment Type¹: **Quiz/Test**

Indicative Time on Task²: **15 hours**

---

¹ For the purposes of this course, a Quiz/Test is defined as any assessment that is completed online and submitted electronically.

² For the purposes of this course, the Indicative Time on Task is defined as the time required to complete the assessment to a satisfactory standard, excluding any additional time required for research, preparation, or submission.
Due: Weekly  
Weighting: 10%

This is a hurdle assessment task (see Assessment Policy, mentioned 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 the 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 Type¹: Project  
Indicative Time on Task²: 15 hours  
Due: 23:55 Friday Ending 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 the 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 Type¹: Project  
Indicative Time on Task²: 15 hours  
Due: 23:55 Friday Ending 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 the 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 Type¹: Examination
Indicative Time on Task²: 10 hours
Due: 09:00–21:00 Friday Ending Week 5
Weighting: 20%

A 50-minute long written examination worth 20% that will be held in week 5, Friday anytime from 9:00 am to 9:00 pm. This will test your understanding of material covered in weeks 1 to 4.

On successful completion you will be able to:

- Adhere to the 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 Type¹: Examination
Indicative Time on Task²: 10 hours
Due: 09:00–21:00 Friday Ending Week 9
Weighting: 20%

A 50-minute long written examination worth 20% will be held in week 9, Friday anytime from 9:00 am to 9:00 pm. This will test your understanding of the material covered in weeks 5 to 8.

On successful completion you will be able to:

- Adhere to the 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: **09:00–21:00 Friday Ending Week 13**

Weighting: **20%**

A 50-minute long written examination worth 20% will be held in week 13, Friday anytime from 9:00 am to 9:00 pm. This will test your understanding of the material covered in weeks 9 to 12.

On successful completion you will be able to:

• Adhere to the 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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Weighting</th>
<th>Hurdle</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Exam #3</td>
<td>20%</td>
<td>No</td>
<td><strong>09:00–21:00 Friday Ending Week 13</strong></td>
</tr>
<tr>
<td>Assignment 2</td>
<td>15%</td>
<td>No</td>
<td><strong>23:55 Friday Ending Week 12</strong></td>
</tr>
<tr>
<td>Weekly Tasks</td>
<td>10%</td>
<td>Yes</td>
<td><strong>23:55 Wednesday Week 2 to 13</strong></td>
</tr>
<tr>
<td>Module Exam #1</td>
<td>20%</td>
<td>No</td>
<td><strong>09:00–21:00 Friday Ending Week 5</strong></td>
</tr>
<tr>
<td>Module Exam #2</td>
<td>20%</td>
<td>No</td>
<td><strong>09:00–21:00 Friday Ending Week 9</strong></td>
</tr>
</tbody>
</table>
## Module Exam #3

Assessment Type: Examination  
Indicative Time on Task: 10 hours  
Due: **09:00–21:00 Friday Ending 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.

## Assignment 2

Assessment Type: Project  
Indicative Time on Task: 15 hours  
Due: **23:55 Friday Ending 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.

Weekly Tasks
Assessment Type 1: Quiz/Test
Indicative Time on Task 2: 15 hours
Due: 23:55 Wednesday Week 2 to 13
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 #1
Assessment Type 1: Examination
Indicative Time on Task 2: 10 hours
Due: 09:00–21:00 Friday Ending 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**: Examination  
**Indicative Time on Task**: 10 hours  
**Due**: 09:00–21:00 Friday Ending 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.

### Assignment 1

**Assessment Type**: Project  
**Indicative Time on Task**: 15 hours  
**Due**: 23:55 Friday Ending 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.

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 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 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.

Week 1 classes will introduce the lecture activities as well as the administration information. 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 and through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to the unit convenor via the contact email on iLearn.

RECOMMENDED TEXTS


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

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

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
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
Unit guide COMP2310 Digital Forensics

- **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/](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](http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/). The policy applies to all who connect to the MQ network including students.

**Changes from Previous Offering**

Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff. As such, no change to the delivery of the unit is planned, however we will continue to strive to improve the level of support and the level of student engagement.

**Changes since First Published**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/03/2024</td>
<td>Minor edits to the timing description of module exams.</td>
</tr>
</tbody>
</table>

https://unitguides.mq.edu.au/unit_offerings/163015/unit_guide/print
Due to the public holiday on Friday of Week 6, kindly approve the rescheduling of Assignment 1 submission to Friday of Week 7.

As per Gaurav suggestion, I changed "Tutor" to "Teaching assistant" in the list of teaching staff.

Updated teaching staff (co-lecturer and tutors) info.

Unit information based on version 2024.01R of the [Handbook](https://unitguides.mq.edu.au/unit_offerings/163015/unit_guide/print)