UNSW Course Outline

COMP6845 Extended Digital Forensics and Incident Response - 2024

Published on the 22 May 2024

General Course Information

Course Code : COMP6845
Year : 2024
Term : Term 2
Teaching Period : T2
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

The subject of Digital Forensics is a blend of technical expertise, legal procedures for an expert

witness, persuasive report writing and your performance in the theatre of court. This course covers both forensic theory / professional practice, and looking at the underlying engineering of hiding, finding, interpreting and responding to traces. Students will use of standard forensic tools to extract, carve and analyse data as well as learning the low-level technical skills and knowledge underlying them. Students will also be introduced to advanced topics such as Cloud Forensics and latest anti-forensics techniques.

COMP6445 and COMP6845 run in an overlapping mode. Both share a set of common activities and assessments; however COMP6845 students have additional extension activities and assessments related to digital forensics. These activities offer more advanced and in-depth study of the topic.

The information below applies to both courses except where otherwise indicated. The main differences between COMP6445 and COMP6845 derive from the motivations behind them, unlike other SECedu courses, the extended course (COMP6845) is not only exclusively a more technical deep dive into core (COMP6445) concepts but also exposes students to advanced topics in Digital Forensics such as Splunk Logging, iOS and Android Forensics. Hence, COMP6845 includes a deeper dive into more technical aspects of digital forensics. This is achieved through additional weekly workshop/lecture during the term.

COMP6445 students are welcome to attend the extended lectures.

By the end of the course students should be able to write and analyse simple forensic tools as well as being able to use them. The course covers Memory Forensics, Disc Forensics Network, Device Forensics, Stealth Techniques, Anti-forensics, Professional Forensic Practice, (chain of custody, records etc), Logging, and Mobile Forensics. Students of this course will apply forensic methods in controlled environments and gain an understanding of the technical process of uncovering hidden data and other metadata which may reveal user behaviour. Students will also develop skills in reporting their findings and evaluate the ethical consequences of their findings. Digital Forensics students are invited to participate in a mock courtroom experience involving testimony and cross-examination of digital forensics expert witnesses. We plan to run a mock civil trial of company vs rogue employee with a presiding Judge, and lecturers acting as advocates and students as expert witnesses.

Course Aims

The course aims to:

1. Provide students with a solid foundation in the principles and techniques used to hide, discover, interpret, and respond to digital traces effectively.
2. Enable students to gain proficiency in extracting, carving, and analyzing data using a wide range of digital forensics tools.
3. Introduce students to advanced areas of digital forensics, such as anti-forensics techniques designed to hinder investigation, as well as the unique challenges posed by cloud-based environments.
4. Develop students' skills in presenting their forensic findings in a manner that meets the requirements for admissibility in court trials.

The course can be used as a core component of the Cybersecurity major.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Have an applied working knowledge of the principle elements of digital forensic literacy (such as Windows, Linux and OSX disk structures, machine memory structure, operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption, network logging, stealth techniques and anti forensic strategies).
CLO2 : Extract and infer digital traces of activity.
CLO3 : Apply forensic analysis on common systems.
CLO4 : Explain issues and key principles of professional digital forensic practice (including chain of custody and best practice procedures).
CLO5 : Illustrate an understanding of digital forensics to design, conduct, and report on effective forensic investigations.

Course Learning Outcomes	Assessment Item
CLO1 : Have an applied working knowledge of the principle elements of digital forensic literacy (such as Windows, Linux and OSX disk structures, machine memory structure, operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption, network logging, stealth techniques and anti forensic strategies).	• Weekly Investigations / Challenges • Investigation Reports • Exam
CLO2 : Extract and infer digital traces of activity.	• Weekly Investigations / Challenges • Investigation Reports • Exam
CLO3 : Apply forensic analysis on common systems.	• Weekly Investigations / Challenges • Investigation Reports
CLO4 : Explain issues and key principles of professional digital forensic practice (including chain of custody and best practice procedures).	• Exam • Weekly Investigations / Challenges
CLO5 : Illustrate an understanding of digital forensics to design, conduct, and report on effective forensic investigations.	• Investigation Reports • Weekly Investigations / Challenges

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

This course is hosted on WebCMS3 and that's where we'll share information and build the course community. You access the course site on WebCMS3 for the first time via the link in Moodle.

Find the *Digital Forensics* course page on Moodle (it's just a stub page); then

1. Click on the link to WebCMS3.

Subsequently you can access the course directly via: https://webcms3.cse.unsw.edu.au/COMP6445/24T2/

Additional Course Information

How to Contact Us

- Speak/chat with the lecturers at and after lectures
- Speak with your tutor at/after tutorials
- Chat with us and your classmates on the EdForum
- Confidential questions about course: cs6445@cse.unsw.edu.au

Enquiries about Security Engineering major: SECedu@unsw.edu.au

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Weekly Investigations / Challenges Assessment Format: Individual	20%	Start Date: Each Week or Biweekly Due Date: Not Applicable
Investigation Reports Assessment Format: Individual	40%	Start Date: Week 2, Week 4 Due Date: Week 4 and Week 7/8
Exam Assessment Format: Individual	40%	Start Date: Week 11

Assessment Details

Weekly Investigations / Challenges

Assessment Overview

Students are expected to spend 5-7 hrs each week on completing weekly challenges (This will be 10-15 hrs if challenges are biweekly). Challenges or weekly investigations cover various topics such as memory forensics, network forensics, mobile forensics, malware analysis, splunk, and

OS forensics. CTF challenges are hosted on a dedicated CSE AWS server, and all relevant information related to weekly investigations can be accessed through the Web CMS. CTF responses are stored on our server for automated grading. The course administrator reviews the automated grading results and makes manual adjustments if necessary. Grades are then posted on Moodle and accessible to students. If any issues arise, students can reach out to their respective tutor or course convenor directly for assistance.

Course Learning Outcomes

- CLO1 : Have an applied working knowledge of the principle elements of digital forensic literacy (such as Windows, Linux and OSX disk structures, machine memory structure, operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption, network logging, stealth techniques and anti forensic strategies).
- CLO2 : Extract and infer digital traces of activity.
- CLO3 : Apply forensic analysis on common systems.
- CLO4 : Explain issues and key principles of professional digital forensic practice (including chain of custody and best practice procedures).
- CLO5 : Illustrate an understanding of digital forensics to design, conduct, and report on effective forensic investigations.

Detailed Assessment Description

Students are expected to spend 5-7 hrs each week on completing weekly challenges (This will be 10-15 hrs if challenges are biweekly). Challenges or weekly investigations cover various topics such as memory forensics, network forensics, mobile forensics, malware analysis, splunk, and OS forensics.)

CTF challenges are hosted on a dedicated CSE AWS server, and all relevant information related to weekly investigations can be accessed through the Web CMS. CTF responses are stored on our server for automated grading. The course administrator reviews the automated grading results and makes manual adjustments if necessary. Grades are then posted on Moodle and accessible to students. If any issues arise, students can reach out to their respective tutor or course convenor directly for assistance.

Investigation Reports

Assessment Overview

There will be 2 reports throughout trimester.

Students are expected to spend 15-30 hours per report. Students need to investigate network pcap files, hard drive images, mobile image, and find the suspect by analysing their emails, document, network traces, and images in the hard drives.

A marking rubric is created and shared with students and markers so that reports are submitted and marked as per the marking rubric.

Feedback and grades are uploaded on Moodle and viewable to students. In case of any issues, students can contact the respective tutor or convenor directly.

The report is expected to be done in more depth than a COMP6445 report.

Course Learning Outcomes

- CLO1 : Have an applied working knowledge of the principle elements of digital forensic literacy (such as Windows, Linux and OSX disk structures, machine memory structure, operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption, network logging, stealth techniques and anti forensic strategies).
- CLO2 : Extract and infer digital traces of activity.
- CLO3 : Apply forensic analysis on common systems.
- CLO5 : Illustrate an understanding of digital forensics to design, conduct, and report on effective forensic investigations.

Detailed Assessment Description

There will be 2 reports throughout the trimester. Students are expected to spend 15-30 hours per report. Students need to investigate network pcap files, hard drive images, mobile image, and find the suspect by analysing their emails, document, network traces, and images in the hard drives.
A marking rubric is created and shared with students and markers so that reports are submitted and marked as per the marking rubric.
Feedback and grades are uploaded on Moodle and viewable to students. In case of any issues, students can contact the respective tutor or convenor directly.

Exam

Assessment Overview

This is the final exam of 2 hours, in the UNSW exam period, that includes MCQs, short question and answers on Professionalism, and then applied questions on Technical part of Digital Forensics. It is hand-marked by course staff.

The exam will be conducted online via content delivery platform.

Course Learning Outcomes

- CLO1 : Have an applied working knowledge of the principle elements of digital forensic literacy (such as Windows, Linux and OSX disk structures, machine memory structure,

operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption, network logging, stealth techniques and anti forensic strategies).
- CLO2 : Extract and infer digital traces of activity.
- CLO4 : Explain issues and key principles of professional digital forensic practice (including chain of custody and best practice procedures).

Detailed Assessment Description

This is the final exam of 2 hours, in the UNSW exam period, that includes MCQs, short question and answers on Professionalism, and then applied questions on Technical part of Digital Forensics. It is hand-marked by course staff.

The exam will be conducted online via content delivery platform.

Assignment submission Turnitin type

This is not a Turnitin assignment

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 27 May - 2 June	Lecture	Introduction to Forensics Case-study Two stories that highlight where the forensics professionalism went well, and one that went bad. The impact of forensics Why is forensics important? why you should take it seriously? History Where forensics came from, the history of it? prominent cases
	Lecture	Lecture Course Overview Brief high-level of all the technical concepts of forensics in the coming weeks Forensics Methodology Chain of Custody Forensic Soundness Physical Evidence handling Acquisition Logical and Physical Capture
	Lecture	Introduction to Extended Course The Forensic Mindset Background on project/scenario 20 mins logging 15 mins on mobile 15 mins on tutorials 10 mins Questions
	Tutorial	Forensic Soundness Verifying Disk Images
	Assessment	Week 1 Challenges Released: 27th May, 2024 (Monday) Due: 2nd June, 2024 (Sunday, 11:59pm)
Week 2 : 3 June - 9 June	Lecture	Forensics Method What is it? Why does it matter? why is important? How it relates to scientific method (repeatable etc.), being provable. Observer principles (e.g., Write blockers) Ethics in Forensics When you need an investigation license? Cases when you might decline to investigate. Case studies / war stories
	Lecture	File Systems What their purpose? How they work? Deleted files, Recycle bin vs soft delete, hard, unallocated space, Recovering files FAT NTFS Disk Forensics File Signatures, USB Drives
	Lecture	File System Deep Dive Hiding files in slack space Disk Deep Dive Hidden Regions, RAID Configuration
	Tutorial	Introduction to Forensics Tooling The Sleuth Kit Autopsy Disk Forensics Demo – USB Capacity Spoofing Demo – USB Recovery
	Assessment	Week 2-3 Challenges Released: 3rd June, 2024 (Monday) Report 1 Released: 3rd June, 2024 (Monday)
Week 3 : 10 June - 16 June	Lecture	Putting it all together – the investigative process. • Telling the story Making a persuasive argument / piece of writing
	Lecture	Timeline Analysis Representation of time in filesystems, MACB, Correlating evidence Windows Artefacts History, Events, Registry, Caches

	Lecture	Modern Windows Artefacts
	Tutorial	Exporting Artefacts
	Assessment	Week 2-3 Challenges Due: 16th June, 2024 (Sunday, 11:59pm)
Week 4 : 17 June - 23 June	Lecture	Presenting your work Go over example of report ABC Pharmaceuticals v Marcus
	Lecture	Gathering Memory Volatile Memory Hibernation Files Memory Forensics Process Information Process Memory
	Lecture	Memory Traces Page File Crash Dump Analysis
	Tutorial	Introduction to Volatility Password Cracking
	Assessment	Report 1 Due: 23rd June, 2024 (Sunday, 11:59pm) Week 4-5 Challenges Released: 17th June, 2024 (Monday) Report 2 Released: 17th June, 2024 (Monday)
Week 5 : 24 June - 30 June	Lecture	Self Care Porn, Terrorism, managing emotions
	Lecture	Networking Packets, Network Stack, Ports Network Forensics Packet Capture, Flows, Encryption & MITM
	Lecture	Cloud Network Forensics
	Tutorial	Analysing network artifacts Hostname examination, IP address examination, Port examination, Analysis and extraction with Wireshark
	Assessment	Week 4-5 Challenges Due: 30th June, 2024 (Sunday, 11:59pm)
Week 6 : 1 July - 7 July	Other	Quiet Week
Week 7 : 8 July - 14 July	Lecture	Deductive and Inductive Reasoning Forensics Best Practices
	Lecture	Gathering mobile data Acquisition challenges Mobile Forensics Text messages, Emails, File synchronisation
	Lecture	Extended Mobile Forensics
	Tutorial	Android and iOS Forensics iLeapp, aLeapp, Celebrite
	Assessment	Report 2 Due: 14th July, 2024 (Sunday, 11:59pm) Week 7-8 Challenges Released: 8th July, 2024 (Monday) Week 9-10 Challenges Released: 8th July, 2024 (Monday)
Week 8 : 15 July - 21 July	Lecture	Court Preparation Preparing Expert Witness Statements How to write in a format that is admissible in court War stories Admissibility of Evidence
	Lecture	Guest Lecture on Incident Response & Malware Analysis
	Tutorial	Tabletop Discussion
	Assessment	Week 7-8 Challenges Due: 21st July, 2024 (Sunday)

Week 9 : 22 July - 28 July	Lecture	Court Preparation Expert Witnessing
	Lecture	Guest Lecture on Detection Engineering
	Tutorial	Splunk & SIEMs
Week 10 : 29 July - 4 August	Lecture	Court Case (Mock Trial on 31st July 2024)
	Lecture	Revision
	Tutorial	Revision
	Assessment	Week 9-10 Challenges Due: 4th August, 2024 (Sunday)
Week 11 : 5 August - 11 August	Assessment	Exam

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Prescribed Resources

- Attend Lectures and Tutorials
- Real Digital Forensics: Computer Security and Incident Response
- Incident Response & Computer Forensics, Third Edition

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Rahat Masood					Yes	Yes

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism
- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. *Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be

awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the courses convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum queries, cannot understand the lecturer)

You should **never** contact any of the following people directly:

- Vice Chancellor

- Pro-vice Chancellor Education (PVCE)

- Head of School

- CSE administrative staff

- CSE teaching support staff

They will simply bounce the email to one of the above, thereby creating an unnecessary level of indirection and a delay in the response.