Digital Forensics - COMP6445

Extended Digital Forensics - COMP6845

Course Outline 2021T3

These two courses 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 and professional security engineering. 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 exclusively a more technical deep dive into core (COMP6445) concepts. COMP6845 exposes students to the discipline of being an expert witness.

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. Hence COMP6845 includes a deeper dive into more technical aspects of digital forensics AND the realm of the expert witness. This is achieved through a term-long project culminating in a mock trial and an additional weekly workshop/lecture during the term. COMP6445 students are welcome to attend the extended lectures.

Course Website

This course is hosted on OpenLearning and that's where we'll share information and build the course community.

You access the course site on OpenLearning for the first time via the link in Moodle. That way your OpenLearning account will be correctly linked to your zID:

1. Find the *Digital Forensics* course page on Moodle (it's just a stub page); then
2. Click on the link to OpenLearning.

Subsequently you can access the course directly via: https://www.openlearning.com/unswcourses/courses/digital-forensics

Course Staff

Lecturers:

- Tabitha Bauer
- Timothy Boyce
- Wes Lacy
- Ajoy Ghosh

Convenor and Lecturer in Charge: Professor Richard Buckland Course Admin: Brendan Nyholm Industry Lead and Advisor: Adam Smallhorn

How to contact us

- Speak/chat with the lecturers at and after zoom lectures
- Speak with your tutor at/after zoom tutorials
- Chat with us and your classmates on the OpenLearning course website
- Confidential questions about course: cs6445@cse.unsw.edu.au
- Enquiries about Security Engineering major: SECedu@unsw.edu.au

Summary of the course

Here is the handbook entry. 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. 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.

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.

Conditions for Enrolment

Prerequisite: (COMP6441 or COMP6841 or COMP9441), and (COMP9201 or COMP9283)

Course weekly schedule

Week	Core Lecture	Extended Lecture	Assessment
1	**Forensics Professionalism** [Tabitha Bauer]- The impact & history of digital forensics**Applied Digital Forensics** [Wes Lacy and Timothy Boyce]- Course overview- Physical evidence handling	**Extended Workshop** [Ajoy Ghosh]- Intro to the extended course- Background on project/scenario	**Tutorials** - Investigation quiz due Week 2 Monday**External Investigation-** Artifact drop 1: HDD image
2	**Forensics Professionalism** [Tabitha Bauer]- The forensic method- Ethics in forensics**Applied Digital Forensics** [Timothy Boyce]- Physical layer- Data Carving- Acquisition- Cloud	**Extended Workshop** [Ajoy Ghosh]	**Tutorials** - Investigation quiz due Week 3 Monday- Review Artifact drop
3	**Forensics Professionalism** [Tabitha Bauer]- The investigative process - Putting it all together**Applied Digital Forensics** [Timothy Boyce]- File systems	**Extended Workshop** [Ajoy Ghosh]	**Tutorials** - Written report released
4	**Forensics Professionalism** [Tabitha Bauer]- Case studies- Presenting your work**Applied Digital Forensics** [Wes Lacy]- Network forensics/Logs investigation	**Extended Workshop**[Ajoy Ghosh]	**Tutorials** - Review Artifact drop**External Investigation-** Artifact drop 2: network

Week	Core Lecture	Extended Lecture	Assessment
5	**Forensics Professionalism** [Tabitha Bauer]- Self-care**Applied Digital Forensics** [Timothy Boyce]- Timeline analysis- Windows artifacts- Linux/Mac	**Extended Workshop** [Ajoy Ghosh]	**Tutorials** - Investigation quiz due Week 7 Monday- Report due
6	*Quiet Week*		
7	**Forensics Professionalism** [Ajoy Ghosh]- Forensics documenting- Ethics & the Legal Process- The Law & Witness Statements**Applied Digital Forensics** [Wes Lacy]- Memory forensics	**Extended Workshop** [Ajoy Ghosh]	**Tutorials** - Investigation report due- Investigation quiz due Week 8 Monday**Extended Course**- Artifact drop 3: mobile
8	**Forensics Professionalism** [Ajoy Ghosh]- Expert witnessing- Forensics & Metadata**Applied Digital Forensics** [Timothy Boyce]- Mobile Forensics- Antiforensics- Logs & Cloud	**Extended Workshop** [Ajoy Ghosh]	**Tutorials** - Investigation quiz due Week 9 Monday
9	**Forensics Professionalism** [Tabitha Bauer]- What forensics means as a career**Applied Digital Forensics** - Revision/Guest Lecture	**Extended Court case**	**Tutorials** - Investigation quiz due Week 10 Monday**Extended Course**- Expert Witness Report due
10	**Revision**	**Review & Feedback**	**Tutorials**- Revision
11	*No class*	*No class*	**Final exam** (date TBC)

Class	Course	Time	Location
Lecture	COMP6445 & COMP6845	Tuesday 5-8pm	Zoom
Extended Lecture/Workshop	COMP6845	Wednesday 4-5pm	Zoom
Laboratory H18A	COMP6445	Thursday 6-8pm	Zoom
Laboratory W11A	COMP6445	Wednesday 11am-1pm	Zoom
Laboratory H16A	COMP6845	Thursday 4-6pm	Zoom
Laboratory W18A	COMP6845	Wednesday 6-8pm	Zoom

Assessment

COMP6445 - Core

- 40% - Exam
- 40% - Course work
  - 18% - Weekly investigation - case report - Week 3
  - 12% - Weekly investigation - quiz - 6 quizzes x 2% each
  - 10% - Weekly forensic professionalism reflections - participation each week
- 20% - External Report
  - 20% - Written report - Week 7 - based on external project

COMP6845 - Extension

- 20% Exam
- 20% Core Course Work
  - 9% - Weekly investigation - written case report – Week 3
  - 6% - Weekly investigations - quizzes - other weeks
  - 5% - Weekly forensic professionalism reflections - participation each week
- 40% External Report
  - 40% - written report - Week 7 - based on external project
- 20% - Extended course only assessments
  - 20% Evidence drop 3 - based on supplementary instructions
  - 0% court case appearance (no marks allocated, but attendance expected)

Reference Books

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

Requirements

This course requires you to Bring Your Own Device. Any laptop capable of running the software in the pre-course preparation activities (Week 0 Activity) should be sufficient, you do not need a super-fancy machine. Note that even if we return to campus during Term 3 you will still need to bring your own device as the CSE lab computers won't have the required software to perform exercises or assignments.

This course makes use of VMs which can be slow on low powered devices, however tools can be installed separately to improve performance.

Due to COVID-19 all of the tutorial content will be distributed online requiring you to download some large files. In some instances it will also be necessary to store and process the same large files.

Equity of access

If you have difficulties in arranging any of the above discuss this with the course staff as soon as possible and ensure you have been able to arrange satisfactory workable solutions before the census date. Flexibility can be provided to ensure no student is disadvantaged but it is your responsibility to let the course staff know as early as possible.

Solutions are available to assist those with low internet bandwidth who are unable to download the large files, those with low powered devices who are unable to process the required files or those without the necessary storage capacity to store the required files. Email cs6445@cse.unsw.edu.au as soon as possible to discuss your options with course admin, Brendan.

Learning Outcomes

After completing COMP6445, students will:

- 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).
- Understand how these elements can be used to extract and infer digital traces of activity, their characterising
- Be able to conduct forensic analysis on common systems
- Have an understanding of issues and key principles of professional digital forensic practice (including chain of custody and best practice procedures)
- Apply an understanding of digital forensics to design, conduct, and report on effective forensic investigations.

This course contributes to the development of the following graduate capabilities:

Graduate Capability	Acquired in
Scholars capable of independent and collaborative enquiry, rigorous in their analysis, critique and reflection, and able to innovate by applying their knowledge and skills to the solution of novel as well as routine problems	Tutorials, Assignments
Entrepreneurial leaders capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change	Lectures, Tutorial-Labs, team learning activities
Professionals capable of ethical, self-directed practice and independent lifelong learning	Lectures, Written and practical activities
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	Lectures, team learning activities

Teaching Rationale

Applied forensic skills are best mastered and reinforced by considerable practice, so labs and programming assignments are critical component of the course. These will help you to practice design and implementation skills, and to further develop your professional teamwork skills. The reports and weekly reflections will help you develop your ability to reflect on your own work which is an essential professional skill. Weekly tutorials provide a forum for you to develop design skills and to practice presentation.

Lectures will be split between discussion of concepts, discussion of practical work (and practical demonstrations), revision work, and extension lectures.

Students are given weekly formative activities to work on in tutorials/labs. Students are also given exercises to explore topics in greater depth. Extended students will have an additional professional project based on a mock trial.

Students in both core and extended courses are expected to spend 150 hours on the course. We expect students to spend a significant time each week on self-directed studies related to forensics. This ranges from reviewing lecture materials, learning related content, to going to security meetups, playing CTFs and private experiments and research.

Student Conduct

The Student Code of Conduct (Information, Policy) sets out what the University expects from students as members of the UNSW community. As well as the learning, teaching and research environment, the University aims to provide an environment that enables students to achieve their full potential and to provide an experience consistent with the University's values and guiding principles. A condition of enrolment is that students *inform themselves* of the University's rules and policies affecting them, and conduct themselves accordingly.

In particular, students have the responsibility to observe standards of equity and respect in dealing with every member of the University community. This applies to all activities on UNSW premises and all external activities related to study and research. This includes behaviour in person as well as behaviour on social media, for example Facebook groups set up for the purpose of discussing UNSW courses or course work. Behaviour that is considered in breach of the Student Code Policy as discriminatory, sexually inappropriate, bullying, harassing, invading another's privacy or causing any person to fear for their personal safety is serious misconduct and can lead to severe penalties, including suspension or exclusion from UNSW.

If you have any concerns, you may raise them with your lecturer, or approach the School Ethics Officer, Grievance Officer, or one of the student representatives.

Plagiarism at UNSW is defined as using the words or ideas of others and presenting them as your own. UNSW and CSE treat plagiarism as academic misconduct, which means that it carries penalties as severe as being excluded from further study at UNSW. There are several on-line sources to help you understand what plagiarism is and how it is dealt with at UNSW:

- Plagiarism and Academic Integrity
- UNSW Plagiarism Procedure

Make sure that you read and understand these. Ignorance is not accepted as an excuse for plagiarism. In particular, you are also responsible that your assignment files are not accessible by anyone but you by setting the correct permissions in your CSE directory and code repository, if using. Note also that plagiarism includes paying or asking another person to do a piece of work for you and then submitting it as your own work.

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW.

If you haven't done so yet, please take the time to read the full text of

- UNSW's policy regarding academic honesty and plagiarism

The pages below describe the policies and procedures in more detail:

- Student Code Policy
- Student Misconduct Procedure
- Plagiarism Policy Statement
- Plagiarism Procedure

You should also read the following page which describes your rights and responsibilities in the CSE context:

- Essential Advice for CSE Students

Special Consideration

Students whose performance is affected by serious and un-foreseeable events outside their control can apply at the student centre for special consideration. If special consideration is granted you will be able to sit the supplementary exam.

Special consideration does not mean we adjust your marks, it means that we permit you to sit the supplementary examination. If you apply for special consideration after the cut-off date set by the university or after the supplementary exam has been held then it will not be granted. Special consideration will only be granted when every other component of the course has been attempted and satisfactorily completed/passed.

Good Faith Policy

This course has a "Good Faith Policy". This means we expect you to act in good faith at all times. We expect you to be a good citizen. To not invade, alter or damage the property of others including the university, invade the privacy of others, break any laws or regulations, annoy other people, deprive others of access to resources, breach or weaken the security of any system, or do or omit to do anything else which you know or suspect we would not be happy about. Furthermore you are not to do anything which appears OK by a loophole or a strict interpretation of "the letter of the law" but which is not consistent with the spirit. Basically you must not act in any way so as to bring disrepute to the reputation of the course, the course staff, fellow students, the school, the university, or the ICT profession. Also, don't be a dick.

If you are unsure, ask!

If, in our sole discretion, we feel you have violated the Good Faith Policy or cheated in any assessment you will be awarded 0 Fail for the course. Further penalties may apply also depending on the nature and severity of the violation. Students who have violated the Good Faith Policy may not be permitted to re-enrol in future offerings of the course.

Students who are found (or who have previously been found and have not disclosed this) guilty of academic or computer related misconduct or any other activity in a way which which casts doubt on their ability or willingness to comply with the Good Faith Policy will be dis-enrolled and will be not permitted to re-enroll in future offerings of the course. If you have ever been found guilty of such an activity you must disclose it to the lecturer in writing immediately.

Supplementary Exams

Supplementary exams will only be awarded in well-justified cases. They will not be awarded if your reason for not sitting the final exam was for holiday travel (!) Read the School policy for Special Consideration.

There will only be one supplementary exam held. If you miss it you will not be awarded another. So do not plan overseas travel at the end of the exam period if there is any chance you may wish to sit a supplementary exam. It is up to you to contact the school office and/or website and find the date of the supplementary exam and keep it free (the date is usually set centrally by the school not by the course staff) If you think you might be eligible for the supplementary exam hold yourself ready to sit it – sometimes people are awarded entry to the supplementary exam at the last minute and saying "I didn't know if I would be awarded it so I didn't study for it" is not a valid reason for special treatment.

Marks

Exam marks and your overall course result will be scaled if necessary, to keep the standard of the different grade levels consistent from year to year and between the security engineering courses. In particular we strive to ensure that the pass/fail boundary and the D/HD boundary are roughly equivalent from year to year. This means your final course mark will not just be the sum of the raw marks for each of the individual items. In cases where the overall result for the teamwork assessment items significantly exceeds the individual (non-team) assessment items the teamwork results will be capped at the level of the individual results and you may be called in for an interview to explain the difference. In significant cases you may be offered further practical individual assessment activity to replace your team results and you will not be awarded a pass in the course unless you clearly demonstrate pass level ability in that work.

Identified Work

We use assessment feedback as a way of your facilitator getting to know you and the areas in which you need help. Hence assignment work is not marked anonymously. Contact the course administrator or lecturers if you have any individual concerns with this approach. Wherever possible we share student work as a way of developing the entire cohort, if you do not wish to be identified in any of your work which is shared contact the course administrator or lecturers and discuss it with them BEFORE submitting the work.

Course Evaluation and Development from MyExperience and related surveys

These courses are still relatively new, and we strongly encourage students to actively provide feedback about the course's progress. Each tutorial-lab class will elect a student representative – give your feedback to them and they will pass it onto the course staff anonymously. We'll also run a debrief session before the conclusion of the course where you can give feedback and suggestions. Many of the good things in the course now have come from students giving great suggestions in the past so do pass on your thoughts as we take them seriously and it will make a difference.

These courses will also be evaluated by UNSW's myExperience survey and feedback program at the end of the trimester. It's not a brilliant survey but it actually helps us a lot if you fill it in as it's pretty much the main feedback that the rest of the university administration looks at and good feedback helps us survive and grow.

Feedback from the recent course offering suggested covering report writing in lectures and releasing feedback on reports earlier in the term. As a result, lecture schedules have be adjusted to introduce report writing earlier in the term and the timing for Report 1 has been adjusted to allow feedback to be provided to students before Report 2 is due. Some feedback also mentioned that solutions to past investigations would be beneficial to students and as a result, tutors will give solutions to investigations and provide walkthroughs to students in tutorials.

You, The Future

We are proud of our former students: they are awesome, and go on to do good things and be good people. Indeed some of the industry guest lecturers in UNSW SECedu courses are often former UNSW security students. So please stay in touch after you have graduated and let us know your achievements and what you are doing. It makes us happy and we are proud to brag about you.

Please do thank the returning and new guest lecturers and let them know how much you appreciate their effort and care in giving up so much time to help you. They go to considerable trouble to do this and they do it because they think it is the right thing to do to grow the profession and help those coming after them.

After you graduate please consider giving back (well, paying forward really) and coming back to help future students once you are an industry practitioner. The help former students give future students is quite moving and changes lives.

Also, even sooner than that, after you have finished this course, if you enjoyed it, then let your tutor know and we will consider you as a staff member for the next offering of the course. Teaching others is very rewarding, gives you great professional skills, makes you more connected in the profession and, weirdly enough, helps you master the material of the course to a level far beyond the level you attained when you did it as a student. We don't just look for results when selecting tutors and course staff. The lecturers are the domain experts, not the tutors. In selecting tutors we mainly look for communication ability, kindness, an interest in developing leadership skills, a sense of fun, and a love for the course material.