Course Outline Student

Edit Resource (/COMP6445/19T3/resources/31851/edit)

Course Details

Course Code	COMP6445
Course Title	Digital Forensics
Convenor	Richard Buckland (/users/z9700463)
Lecturer	Ajoy Ghosh (/users/z3528125)
Admin	Hayden Smith (https://webcms3.cse.unsw.edu.au/users/z3418003) , Annie Liu (https://webcms3.cse.unsw.edu.au/users/z5161603)
Classes	**Lectures** : • Tuesday 6pm-9pm **Laboratories:** • Wed 9am - 11am • Wed 11am - 1pm • Wed 1pm - 3pm • Wed 5pm - 7pm Timetable for all classes (/COMP6445/19T3/timetable)
Consultations	TBD
Units of Credit	6
Course Website	http://cse.unsw.edu.au/~cs6445/19T3/ (http://cse.unsw.edu.au/~cs6445/19T3/)
Handbook Entry	http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP6445.html (http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP6445.html)

Course Summary

This course is an exploration of the behaviours, knowledge and competencies needed by an entry-level digital forensic examiner wanting to practice in an Australian jurisdiction, supporting criminal prosecutions and civil litigations.

This course introduces both professional practices and technical competencies, looking at the discipline of forensic examination and the underlying engineering of collecting, discovering, analysing and interpreting digital evidence. Students will use a blend of open source and commercial tools to extract and analyse data. By the end of the course students should be able to conduct a simple forensic examination and write a basic forensic examiner’s report.

The course explores the professional and legal framework, Windows forensics, Mac forensics, memory forensics, network forensics, mobile forensics and emerging technologies e.g. cloud and artificial intelligence.

This course focuses on the practice of digital forensic examination as an expert witness, rather than focusing on the practice of digital forensic examination as an incident responder.

Course Features

Assumed Knowledge

Before commencing this course, students should:

Have completed both of:

- COMP3441 or COMP6441 or COMP6841
- COMP3231 or COMP3891

Student Learning Outcomes

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	Lectures and activities
Entrepreneurial leaders capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change	Lectures and activities
Professionals capable of ethical, self-directed practice and independent lifelong learning	Lectures and activities
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	Lectures and activities

Teaching Strategies

- Lectures: Where the bulk of your learning will take place through engaging exposition and conversation from an industry expert.
- Laboratories: Self-guided activities with facilitators to assist your learning
- Assignments: Opportunities to develop in-depth knowledge on particular practical and theoretical items.

Student Conduct

The **Student Code of Conduct** (Information (https://student.unsw.edu.au/conduct) , Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)) 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 enrollment 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 (mailto:ethics-officer@cse.unsw.edu.au) , Grievance Officer (mailto:grievance-officer@cse.unsw.edu.au) , or one of the student representatives.

Plagiarism is defined as (https://student.unsw.edu.au/plagiarism) using the ideas or words 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 (https://student.unsw.edu.au/plagiarism)
- UNSW Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

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. Plagiarism at UNSW means using the ideas or words of others and passing them off as your own.

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 (https://student.unsw.edu.au/plagiarism)

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

- Student Code Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)
- Student Misconduct Procedure (https://www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf)
- Plagiarism Policy Statement (https://www.gs.unsw.edu.au/policy/documents/plagiarismpolicy.pdf)
- Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

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

- Essential Advice for CSE Students (https://www.engineering.unsw.edu.au/computer-science-engineering/about-us/organisational-structure/student-services/policies/essential-advice-for-cse-students)

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. Don't be a bad person.

Assessment

Item	Due	Marks
First activity • Short essay / report	End of week 2	10%
Weekly activities • 8 weeks each worth 2.5%	End of weeks 3-10	20%
Mid-term Quiz • Multiple choice and short answer	Week 5 (Tuesday 15th October 2pm-4pm)	10%
Major Assignment • Hands on examination • Preparation of report • Released in week 2	End of week 8	30%
Final Exam • Multiple choice, short answer, and short essay	Exam Period	30%

Final exam marks and final course marks are scaled to ensure results are consistent from year to year. That is, an HD this year should mean the same as an HD in previous years, that you would have received the same grades in any year for the same quality of work/demonstrated ability.

Course Schedule

Week	Lectures (part 1)	Lectures (part 2)	Activities	Major Assessments
1	**Course Introduction** Introduction to careers in digital forensics (Guest lecturer - Tabitha Bauer, CBA) The digital forensic expert • Forensics versus incident response • Types of witnesses • The investigator and the expert	**Forensic copying** Windows forensics #1 • Windows file system • Software data recovery (also for Mac/Linux) – hands on exercise NOTE: some of these overlap with Mac forensics	Lab familiarization (i) Making a forensic copy, manipulating it and explaining the steps (ii) Short reflection activity	-

2	**The digital forensic expert #2** • Expert evidence in the Australian jurisdiction	**Windows forensics #2** • Useful artefacts • Anti-forensics	Data carving scenario-based activity	First activity due
3	**Digital Forensic concepts**	**Windows memory forensics + hands on instructor-led exercise**	Memory forensics activity, students using exercise VM	
4	(Guest lecturer - Tabitha Bauer & Tim Boyce, CBA) • Careers in digital forensics • Days in the life of a digital forensic practitioner	(Guest lecturer - Tabitha Bauer & Tim Boyce, CBA) • Pathways to develop your career • War stories	Using Forensic Explorer for Windows artefacts	-
5	**Disturbing cases and self-care** • Recognising distress and PTSD	**Mac forensics** • Mac file system • Useful artefacts • Anti-forensics Note: focus on what is different from windows	Using Forensic Explorer for Mac artefacts	Quiz
6	**Basic network forensics** • Network capture and analysis • Malware analysis - hands on exercise	Same as left	Students continue with in-class exercise	-
7	(Guest lecturer - Shane Bell, McGrath Nicol) **The expert's report and giving testimony**	Same as left	Getting familiar with qGIS	

8	**Telecommunications data and metadata** • Gathering telecommunications data/metadata • Hands on exercise - locating the accused from telco data	Same as left	Students continue with in-class exercise	Major Assignment Due
9	**Basic mobile forensics** • Mobile phone data extractions - instructor led • iPhone artifacts • Android artifacts	Same as left	Students do mobile phone extraction and analysis	
10	**Emerging technologies** • Examining emerging technologies • Using emerging technologies for forensic examinations Exam brief	(Guest lecturer - Tabitha Bauer, CBA) • You've done this course - what's next? • Getting yourself job-ready	Presentations of Week 9 activity	-

- Unless otherwise stated, weekly activities are to be commenced during the tutorial/lab on the Wednesday following the lecture.
    - Students can continue at home and hand in the weekly activity during following week at the beginning of the tutorial.

Resources for Students

Texts and resources will be provided by course staff throughout the duration of this course.

Students will be loaned an external HDD containing VMWare-compatible virtual machines needed for the course. Students will be expected to run the VMs on their own laptop using VMWare Player (for Windows) or VMWare Fusion (for Mac and Linux) in order to complete the hands-on activities, laboratories and the major assignment. Loan HDD must be returned as a condition of successful course completion.

Software licenses can be acquired for free by all current UNSW CSE students.

Course Evaluation and Development

This course will be evaluated at the end of session using the myExperience system.

Resource created 8 months ago (Wednesday 28 August 2019, 09:57:19 PM), last modified 8 months ago (Saturday 14 September 2019, 05:10:12 PM).

Comments

(/COMP6445/19T3/forums/search?forum_choice=resource/31851)

(/COMP6445/19T3/forums/resource/31851)



Daniel Power-Smerdely (/users/z5084557) 6 months ago (Tue Nov 12 2019 19:13:31 GMT+1100 (Australian Eastern Daylight Time))

Hello, when is the final exam? I have another exam on the same day starting at 12:20,will the digital forensics exam end too close to that?

Edit Delete



Ash Liu (/users/z5161603) 6 months ago (Tue Nov 12 2019 19:49:41 GMT+1100 (Australian Eastern Daylight Time))

Hi Daniel,

I believe there are few students in the same situation as you, with COMP2511 (and other exams) being on the same day.

We'll liaise with the COMP2511 staff to make sure that you can make it to your exam okay :)

Edit Delete



Daniel Power-Smerdely (/users/z5084557) 6 months ago (Tue Nov 12 2019 20:29:14 GMT+1100 (Australian Eastern Daylight Time)), last modified 6 months ago (Tue Nov 12 2019 20:33:50 GMT+1100 (Australian Eastern Daylight Time))

Thanks for the quick reply, you're a cool admin. I'll hold on for now until 2511 gets back to you!

Edit Delete



Laura Chambers (/users/z5059509) 7 months ago (Mon Oct 14 2019 22:44:07 GMT+1100 (Australian Eastern Daylight Time)), last modified 7 months ago (Mon Oct 14 2019 22:49:26 GMT+1100 (Australian Eastern Daylight Time))

What is the "assumed knowledge for entry-level digital forensics practitioners" referencing? It was mentioned in the post about the midsem. Does this mean that there is assumed knowledge for the course beyond the listed prerequisites (6441 and 3231)? If so, where can we find what this added assumed knowledge is because I'm not sure if I have it.

Edit Delete



Ho Chau (/users/z5205954) 7 months ago (Tue Sep 17 2019 08:47:32 GMT+1000 (Australian Eastern Standard Time))

Hi, will lectures be recorded for this course?

Edit Delete



Chaitrali Nandedkar (/users/z5019858) 7 months ago (Mon Sep 16 2019 23:08:13 GMT+1000 (Australian Eastern Standard Time))

Hello,

Just wanted to double check - we don't need to turn up to the Tuesday classes unless there's a pre-planned consultation/activity taking place, right? Or, is it recommended that we come into this class every week, anyway?

Thanks!

Edit Delete



Joseph Schirato (/users/z5115412) 7 months ago (Mon Sep 16 2019 15:43:26 GMT+1000 (Australian Eastern Standard Time))

What is recommended to be completed before each lecture and tutorial each week?

The weekly readings are recommended to have been read before each lecture, is there anything else that is also advisable to have completed before lectures?

Edit Delete



Burny Lu (/users/z5116054) 8 months ago (Tue Sep 10 2019 22:41:22 GMT+1000 (Australian Eastern Standard Time))

Can more details for each of the assessment be provided such as done in groups or pair? Also, can first activity be provided in greater details? Based off the course outline, the final exam is compeltely a written exam?

Edit Delete



Hayden Smith (/users/z3418003) 8 months ago (Fri Sep 13 2019 09:55:41 GMT+1000 (Australian Eastern Standard Time))

The weekly activity will be a mix of individual and group work, clearly stated in the Activity Instruction. All other assessments will be individual.

The final exam is a written exam (multiple choice, short answer and written). Some of the questions will be based on the hands-on activities across the Term, so students will need to have completed those to have a better chance of answering these questions.

Edit Delete



Burny Lu (/users/z5116054) 8 months ago (Fri Sep 13 2019 10:24:15 GMT+1000 (Australian Eastern Standard Time)), last modified 8 months ago (Fri Sep 13 2019 10:24:30 GMT+1000 (Australian Eastern Standard Time))

What is the reason behind the final exam to be all written exam compared to a mix of practical and theory last year

Edit Delete



Hayden Smith (/users/z3418003) 8 months ago (Fri Sep 13 2019 11:10:36 GMT+1000 (Australian Eastern Standard Time))

Hey Burny - it's a new lecturer so general comparisons to last year won't be too useful :(What exactly are you hoping to see out of a practical exam? What about the practical component would you like to see more heavily integrated into the assessment? Specifics help

Edit Delete



Burny Lu (/users/z5116054) 8 months ago (Fri Sep 13 2019 11:47:09 GMT+1000 (Australian Eastern Standard Time)), last modified 8 months ago (Fri Sep 13 2019 19:12:55 GMT+1000 (Australian Eastern Standard Time))

Like getting tested on the tools and skills that we learnt throughout the course and applying them to files we haven't seen in the exam. Similar to how COMP6447 testing knowledge and utilizing tools taught in the course.

Edit Delete



Hayden Smith (/users/z3418003) 8 months ago (Sat Sep 14 2019 00:16:45 GMT+1000 (Australian Eastern Standard Time))

Hey Burny,

Likely comes down to just different teaching staff looking after the course - will look for a more concise exlpanation for you

Edit Delete



Burny Lu (/users/z5116054) 8 months ago (Sat Sep 14 2019 06:14:06 GMT+1000 (Australian Eastern Standard Time))

Thanks

Edit Delete



Hayden Smith (/users/z3418003) 8 months ago (Fri Sep 13 2019 09:47:56 GMT+1000 (Australian Eastern Standard Time))

Hi Burny,

I'll get these details back to you ASAP

Edit Delete