Course Outline

Contents

- Course Details
- Course Summary
- Assumed Knowledge
- Student Learning Outcomes
- Teaching Strategies
- Teaching Rationale
- Student Conduct
- Assessment
- Course Schedule
- Resources for Students
- Course Evaluation and Development

Course Details

Course Code	COMP6445/COMP6845
Course Title	Digital Forensics and Incident Response
LiC	Richard Buckland
Course Convener	Roland Wen
Lecturer	Timothy Boyce
Teaching Staff	Sketch Hely
Course Admin	Tek Huynh
Units of Credit	6
Course Website	https://webcms3.cse.unsw.edu.au/COMP6445/18s2/ (https://webcms3.cse.unsw.edu.au/COMP6445/18s2/)
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 is a specialist security course in Digital Forensics. Topics include principles of forensic analysis, forensics and the law, forensics on several types of infrastructure, management of forensic methodologies and various real life case studies of forensic analyses.

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.

Assumed Knowledge

Students should be familiar with core security concepts.

Students also need basic knowledge of operating system principles and digital device literacy (such as disk structures, machine memory structure, operating system structure caches logging and redundancy, device design authentication operation and weakness, boot and initialisation sequences, storage encryption and network logging).

If you have gaps in your assumed knowledge, you must carry out personal study on your own to rectify it if you find corresponding parts of the course material challenging. Ask your tutor for advice if in doubt.

Student Learning Outcomes

After completing this course, students will:

1. 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).
2. Understand how these elements can be used to extract and infer digital traces of activity, their characterising
3. Be able to conduct forensic analysis on common systems
4. Have an understanding of issues and key principles of professional digital forensic practice (including chain ofcustody and best practice procedures)
5. 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, Tutorials, Assignments
Professionals capable of ethical, self- directed practice and independent lifelong learning	Tutorials, Assignments
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	Lectures, Assignments

Teaching Rationale

Applied forensic are best mastered and reinforced by considerate practice so labs and programming assignments are critical component of the course. These forums allow students to practice design and implementation skills, and to develop teamwork skills. The portfolio will assist in developing students' ability to reflect on their own work. Tutorials will provide a forum for students to develop design skills and to practice presentations.

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 and which they report on in their portfolio. Students are also given assignments to explore topics in greater depth. Extended students will have an additional research project.

Students in both standard 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 ctf’s and private experiments and research. This may also include your something awesome project. Remember to blog about it so you get more evidence for your portfolio - remember we would like to see, not be told.

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 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 (mailto:ethics-officer@cse.unsw.edu.au) , Grievance Officer (mailto:grievance-officer@cse.unsw.edu.au) , or one of the student representatives.

Plagiarism at UNSW is defined as (https://student.unsw.edu.au/plagiarism) 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 (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.

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. 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 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.

Communication

For all course admin questions, email the class account: cs6445@cse.unsw.edu.au (mailto:cs6443@cse.unsw.edu.au) . Make sure to use your UNSW email and include your full name and student number.

For all course content questions, post in the course forum (https://webcms3.cse.unsw.edu.au/COMP6445/18s2/forums/) .

Assessment and Marking

COMP6445

Item	Topics	Due	Marks
Assignment1	Various	Week 7 (individual component) Week 9 (group component)	20%
Assignment2	Various	Week 10 (individual component) Week 12 (group component)	20%
Portfolio	Work journals for weekly exercises Reflections for core course activities Write-ups and reflections for self-directed learning activities	Week 13	10%
Final Exam	Prac exam and theory	Exam period	50%

COMP6845 (Extended)

Item	Topics	Due	Marks

Assignment1	Various	Week 7 (individual component) Week 9 (group component)	15%
Assignment2	Various	Week 10 (individual component) Week 12 (group component)	15%
Portfolio	Work journals for weekly exercises Reflections for core course activities Write-ups and reflections for self-directed learning activities	Week 13	10%
Research project	Choose from list of advanced topics	Week 11	10%
Final Exam	Prac exam and theory	Exam period	50%

Exam and overall course marks may be scaled to ensure a consistent standard from session to session.

If you do not pass the invigilated final exam your final mark for the course will be capped at your exam mark.

All in-semester marks must be finalised by the end of stuvac. If you think there is a problem with any of your marks then you need to advise us by emailing the course administrator within two weeks of the mark being released, and, in all cases before the end of stuvac. No in-semester marks will be changed after the end of stuvac.

Supplementary Exam

A supplementary examination will be held soon after the results have been released. If you think that you may be eligible for the Supplementary Examination, make sure you are available around that time. Be careful not to plan any overseas travel at that time. If you can't attend the sup exam you will not be offered a second chance. WE CAN ONLY RUN ONE SUP EXAM.

It is your responsibility to check your email, the CSE website, and to contact the CSE student office for details of Supplementary Examinations. If you think there is any chance you might be eligible for a Supplementary Exam then you should prepare for it. Requests such as "I didn't find out until the day before the sup exam that I could sit the sup exam, so I need more time to study" or "I have to go overseas at that time and I have already purchased the tickets so can you write and administer a special sup exam just for me" will not be granted.

Course Schedule

Week	Lectures	Assignments	Notes
1	-	-	-
2	Introduction to Forensics	-	-
3	The Forensic Method	-	-
4	Filesystems	-	-
5	Artefacts of User Behaviour	Assignment 1 Release	-
6	Guest Lecture	Project proposals due (extended)	-
7	Incidence Response 1 and Memory	-	-
8	Incidence Response 2	-	-
9	Mobile and Cloud Forensics	Assignment 2 Release	-
10	Guest Lecture	-	-
11	Guest Discussion Panel	-	-
12	E-discovery	Project presentations (extended)	-
13	Revision	Project presentations (extended)	-

Resources for Students

Reference Books

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

Course Evaluation and Development

This course is still relatively new, and we strongly encourage students to actively provide feedback about the course's progress and to make suggestions and give us your advice.

This course will be evaluated by UNSW's myExperience program. You'll receive an email to your student email address with instructions on completing this; we'll also (endeavour to) send out a notification.

This course will also be evaluated by the CSE Student Representatives' mid-session Course Survey.

Resource created 3 years ago (Monday 16 July 2018, 04:30:38 PM), last modified 3 years ago (Monday 10 September 2018, 10:09:26 PM).

Comments (/COMP6445/18s2/forums/search?forum_choice=resource/17392) (/COMP6445/18s2/forums/resource/17392)

There are no comments yet.