UNSW Course Outline

ZEIT8028 Digital Forensics - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8028
Year : 2024
Term : Semester 2
Teaching Period : Z2
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course will introduce participants to digital forensic analysis and investigation first principles. Students will be introduced to theoretical concepts including the digital forensic method, intent and its application. The course will also cover introductory Microsoft Windows centric technical topics such as file system, memory and operating system artefact analysis

using contemporary open source tools, techniques and procedures. Students will be expected to demonstrate both their theoretical and technical understanding through the completion of practical exercises in a contemporary simulated operational environment.

This is an introductory course covering:

- Forensic analysis theory
- Disk forensic theory and practical exercises targeting common Windows centric filesystems
- Configuration forensic theory and practical exercises targeting the Microsoft Windows Registry
- Network forensic theory and practical exercises
- Memory forensic theory and practical exercises targeting the Microsoft Windows operating platform

Digital Forensics comprises five separate modules of intensive theory and practical sessions delivered remotely in conjunction with the UNSW ADFA campus. Theory, taught during lectures, is reinforced with practical hands-on laboratories.

The intended audience for this course are students that have no previous experience or exposure to the field of digital forensics. As a result, students should expect the course material to be introductory and all inclusive, with no digital forensic pre-reading required. However, students are expected to be comfortable working in a Linux command line environment and must have some experience with the Python programming language.

Course Aims

Upon completion of this course students will have gained the required theoretical and practical knowledge to:

- Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.
- Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.
- Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.
- Perform a cyber centric forensic investigation producing an intelligence product that is succinct, accurate, and actionable.

Relationship to Other Courses

N/A

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.
CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.
CLO3 : Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.
CLO4 : Perform a cyber centric forensic investigation producing an intelligence product that is succinct, accurate, and actionable.

Course Learning Outcomes	Assessment Item
CLO1 : Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.	• Forensic Method Essay • Minor Forensic Report • Major Forensic Report
CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.	• Artefact Research Report • Forensic Method Essay • Minor Forensic Report • Major Forensic Report
CLO3 : Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.	• Artefact Research Report • Minor Forensic Report • Major Forensic Report
CLO4 : Perform a cyber centric forensic investigation producing an intelligence product that is succinct, accurate, and actionable.	• Minor Forensic Report • Major Forensic Report

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

The concepts presented in this course require students' demonstration of skill including structured thinking and decision-making in dealing with complex problems. Teaching strategies employed in this course aim to provide an engaging and rewarding educational experience though the development and application of expertise in digital forensic concepts and processes.

The lecture notes provided in the course are synthesised from multiple sources – including

computer forensic courses taught at Universities and to government agencies across the world.

An introductory activity is designed to guide student's self-reflection and stimulate their thinking around their achievement of course outcomes.

During the semester, students will get a chance to work on a number of activities designed to give an opportunity to think about and prepare for the major assignment.

Other Professional Outcomes

N/A

Additional Course Information

N/A

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Forensic Method Essay	20%	Start Date: Not Applicable Due Date: Week 3: 29 July - 02 August Post Date: 15/07/2024 12:00 AM
Minor Forensic Report	15%	Start Date: Not Applicable Due Date: Week 6: 19 August - 23 August Post Date: 15/07/2024 12:00 AM
Artefact Research Report	25%	Start Date: Not Applicable Due Date: Week 9: 23 September - 27 September Post Date: 15/07/2024 12:00 AM
Major Forensic Report	40%	Start Date: Not Applicable Due Date: Week 13: 21 October - 25 October Post Date: 15/07/2024 12:00 AM

Assessment Details

Forensic Method Essay

Course Learning Outcomes

- CLO1 : Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.
- CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.

Detailed Assessment Description

This is the first assessment and is worth 20% of the total course grade. You're required to select one (1) discussion topic from the three options provided before critically evaluating its merit and relevance to forensic investigations. As this is the first assessment, you're not expected to conduct isolated research. Instead, leverage existing research regarding the selected discussion topic. However, you may still leverage any existing experience you have. Once complete, you are to compile your evaluation as a critical discussion essay, presenting both your argument and explanation. This essay should be five (5) to six (6) pages long.

Assessment Length

3,000 words

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Minor Forensic Report

Course Learning Outcomes

- CLO1 : Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.
- CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.
- CLO3 : Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.
- CLO4 : Perform a cyber centric forensic investigation producing an intelligence product that is succinct, accurate, and actionable.

Detailed Assessment Description

This is the second assessment, and it's worth 15% of the total course grade. It'll require you to apply the relevant disk, registry, network, and memory theory you've learned during lectures to achieve the desired outcomes. Furthermore, you're also expected to apply all the forensic analysis techniques you've learned during the technical labs to find and follow investigation leads. If required, you may utilise additional tools and techniques that are beyond the scope of this course to complete this assessment, however doing so is not considered a requirement for completing this assessment.

Assessment Length

3,000 words

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Artefact Research Report

Course Learning Outcomes

- CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.
- CLO3 : Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.

Detailed Assessment Description

This is the third assessment, and it's worth 25% of the total course grade. It'll require you to select one (1) Microsoft Windows artefact from the list provided above and then conduct your own research about how the selected artefact can be exploited for information during a digital forensic investigation. As this assessment is post your first investigation, you're expected to conduct some of your own independent technical research to demonstrate your understanding of the artefact. This should complement any existing research you find regarding the artefact. Don't forget to detail the internals of the artefact.

Assessment Length

3,000 words

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Major Forensic Report

Course Learning Outcomes

- CLO1 : Understand how to professionally approach and conduct a digital forensic investigation, regardless of its size and complexity.
- CLO2 : Demonstrate how to utilise contemporary open source tools, techniques and procedures to conduct forensic analysis.
- CLO3 : Demonstrate their ability to derive and exploit the forensic value of atomic operating system artefacts using first principles.
- CLO4 : Perform a cyber centric forensic investigation producing an intelligence product that is succinct, accurate, and actionable.

Detailed Assessment Description

This is the fourth assessment, and it's worth 40% of the total course grade. It'll require you to apply the relevant disk, registry, network, and memory theory you've learned during lectures, to

achieve the desired outcomes. Furthermore, you're also expected to apply all forensic analysis techniques you've learned during the technical labs to find and follow investigation leads. If required, you may utilise additional tools and techniques that are beyond the scope of this course to complete this assessment, however doing so is not required for completing this assessment.

Assessment Length

4,000 words

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

General Assessment Information

Turnitin

What does Turnitin do?

This assessment will be submitted through Turnitin, an online service used to check non-original language and citation practices in students' work. When you submit your assessment, Turnitin will use pattern-matching technology to look for similarities against internet pages, books, journals and previously submitted student papers. Any matching text will be highlighted however, Turnitin is unable to differentiate between correctly cited references and unacknowledged copying. Do not be alarmed if you see matches. A good piece of academic work should have matches as it should draw on the work of other scholars.

Protect your privacy

Your assessment will be stored in the Turnitin database and may be used to determine whether other individuals have engaged in academic misconduct. Therefore, it is important for your privacy that you don't put any personally identifying information except for your student number on your assessment, including in the file name.

AI

For these assessment tasks, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work
or not. Please note that your submission will be passed through an AI-generated text detection

tool. If your marker has concerns that your answer contains passages of AI-generated text you may be asked to explain your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Grading Basis

Standard

Requirements to pass course

Students require an aggregate grade of 50% or greater to pass the course.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Module 0: Course Overview Module 1: The Forensic Method
	Laboratory	Lab 1: The Virtual Analysis Environment
Week 2 : 22 July - 26 July	Lecture	Module 2: Disk Forensics
	Laboratory	Lab 2: Disk Forensics
Week 3 : 29 July - 2 August	Lecture	Module 3: Registry Forensics
	Laboratory	Lab 3: Registry Forensics
	Assessment	Assessment 1 due: Forensic Method Essay
Week 4 : 5 August - 9 August	Lecture	Module 4: Network Forensics
	Laboratory	Lab 4: Network Forensics
Week 5 : 12 August - 16 August	Lecture	Module 5: Memory Forensics
	Laboratory	Lab 5: Memory Forensics
Week 6 : 19 August - 23 August	Assessment	Assessment 2 due: Minor Forensic Report
	Lecture	Discussion, Q&A
Week 8 : 16 September - 20 September	Lecture	Discussion, Q&A
Week 9 : 23 September - 27 September	Assessment	Assessment 3 due: Artefact Research Report
Week 10 : 30 September - 4 October	Lecture	Discussion, Q&A
Week 12 : 14 October - 18 October	Lecture	Discussion, Q&A
Week 13 : 21 October - 25 October	Assessment	Assessment 4 due: Major Forensic Report

Attendance Requirements

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

General Schedule Information

The first six weeks of semester there will be a lecture, followed by a lab on the lecture material. From week 7 onwards, lectures will occur every other week in the form of a lab demonstration and general discussion/Q&A related to the material and the assessments.

Course Resources

Prescribed Resources

There are no prescribed resources for this course other than the lectures and other materials provided throughout semester.

Recommended Resources

There are no recommended resources for this course other than the lectures and other materials provided throughout semester.

Additional Costs

There are no additional costs for this course.

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the "On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct Policy

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Seth Enoka		Remote		Please email to make an appointment for consultation.	No	Yes
Lecturer	Matt O'Kane				Please email to make an appointment for consultation.	No	No

Other Useful Information

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
• Google Chrome 50+
• Safari 10+
Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
• Windows 10,
• Mac OSX Sierra,
• iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support
Email: externalteltsupport@unsw.edu.au
Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

• Where to get help

• Administrative matters

• Getting your passwords set up

• How to log on to Moodle

• Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 4pm, Mon to Fri)