

SEC706 Network Forensics

School: School of Science, Technology and Engineering

2024 | Trimester 2

UniSC Sunshine Coast

**BLENDED
LEARNING**

Most of your course is on campus but you may be able to do some components of this course online.

Online

ONLINE

You can do this course without coming onto campus.

Please go to usc.edu.au for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

This online course teaches you how to monitor the network for traffic anomalies and identify attacks and instructions across points of interest within the network infrastructure environment. Through practical applications and real world investigations You will develop the skills required to monitor and analyse network traffic to assist in incident response and forensic investigation. This includes performing activities such as packet capture and protocol analysis as well as data collection, aggregation and intelligence analysis.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – On campus workshop	2hrs	Week 1	12 times
Seminar – On campus seminar	1hr	Week 1	2 times
ONLINE			
Learning materials – Asynchronous learning material.	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous online workshop	2hrs	Week 1	12 times
Seminar – Online seminar	1hr	Week 1	2 times

1.3. Course Topics

Topics will include:

Types of evidence, acquisition & packet analysis

Proxies

Protocol analysis

Logging & log collectors

Forensic log management & log reporting

Netflow

Firewall and IPS

SOAR & continuous packet capture platforms

Acquisition architecture investigation techniques

Introduction to forensic report-writing

2. What level is this course?

700 Level (Specialised)

Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES	GRADUATE QUALITIES
On successful completion of this course, you should be able to...	Completing these tasks successfully will contribute to you becoming...
1 Demonstrate knowledge of network forensics evidence acquisition processes and techniques.	Knowledgeable
2 Identify and explain current cyber attacks, relevant network controls, infrastructure interception points, standard and advanced security intelligence platforms	Creative and critical thinker
3 Develop practical skills to detect, extract and analyse all relevant forensic artefacts.	Empowered Engaged
4 Develop and produce reports suitable for admission as case evidence, that describe identification, search and seizure requirements and examine and analyse provided evidence.	Empowered Engaged

5. Am I eligible to enrol in this course?

Refer to the [UniSC Glossary of terms](#) for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

SEC705

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment tasks. Opportunities will be provided during tutorials for peer-review of responses to online tutorial questions.

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Portfolio	Individual	20%	Weekly Entry (250 Words / Week)	Refer to Format	Online Assignment Submission with plagiarism check
All	2	Practical / Laboratory Skills	Individual	40%	1 Hour	Week 8	Online Assignment Submission with plagiarism check
All	3	Report	Individual	40%	3000 Words	Exam Period	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Competency Portfolio

GOAL:	To demonstrate knowledge of network forensics evidence acquisition processes and techniques.										
PRODUCT:	Portfolio										
FORMAT:	Submit: Weekly from Week 2 to 11										
	The response format for assessment item 1 may utilise a number of formats (e.g. Q/A Style short answer, technical Wiki Article or Blog Entry), all written from the perspective of a Cyber Security professional to address weekly questions.										
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Identification and explanation of current cyber attacks, relevant network controls, infrastructure interception points, standard and advanced security intelligence platforms</td> <td>2</td> </tr> <tr> <td>2</td> <td>Development of the practical skills to detect, capture and analyse all relevant forensic artefacts.</td> <td>3</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Identification and explanation of current cyber attacks, relevant network controls, infrastructure interception points, standard and advanced security intelligence platforms	2	2	Development of the practical skills to detect, capture and analyse all relevant forensic artefacts.	3	
No.		Learning Outcome assessed									
1	Identification and explanation of current cyber attacks, relevant network controls, infrastructure interception points, standard and advanced security intelligence platforms	2									
2	Development of the practical skills to detect, capture and analyse all relevant forensic artefacts.	3									
GENERIC SKILLS:											

All - Assessment Task 2: Network Attack Practical

GOAL:	To sit a practical involving an ongoing attack and will be required to utilise tools taught throughout semester to capture Indicators of Compromise, attacker identification and packet capture and log artefacts.	
PRODUCT:	Practical / Laboratory Skills	
FORMAT:	Online interactive practical lab consisting of equally weighted challenges.	
CRITERIA:	No.	Learning Outcome assessed
	1	Identification and explanation of traffic anomaly and conversation information utilising monitoring platforms. 2 4
	2	Selection of the appropriate network infrastructure device on which to acquire traffic of interest. 2
	3	Detection and extraction of relevant information from Firewall / IPS platforms. 3
	4	Analysis of log aggregation platform / SIEM to report relevant events and alerts. 4
GENERIC SKILLS:		

All - Assessment Task 3: Network Forensics Report

GOAL:	To prepare a report appropriate for submission as legal evidence in line with Australian federal law.	
PRODUCT:	Report	
FORMAT:	A written network forensics report providing a high-level summary suitable for executive level communication articulating the chronological order of events as well as a high level and deep-dive explanations of events within a case.	
CRITERIA:	No.	Learning Outcome assessed
	1	Description of identification, search and seizure requirements. 1
	2	Examination and analysis of provided evidence. 4
GENERIC SKILLS:		

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

There are no required/recommended resources for this course.

8.2. Specific requirements

Not applicable

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the [online induction training for students](#), and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

10.2. Assessment: Additional Requirements

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:

The final mark is in the percentage range 47% to 49.4%

The course is graded using the Standard Grading scale

You have not failed an assessment task in the course due to academic misconduct

10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate:

- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.

- 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.

- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

10.4. SafeUniSC

UniSC is committed to a culture of respect and providing a safe and supportive environment for all members of our community. For immediate assistance on campus contact SafeUniSC by phone: [07 5430 1168](tel:0754301168) or using the [SafeZone](#) app. For general enquires contact the SafeUniSC team by phone [07 5456 3864](tel:0754563864) or email safe@usc.edu.au.

The SafeUniSC Specialist Service is a Student Wellbeing service that provides free and confidential support to students who may have experienced or observed behaviour that could cause fear, offence or trauma. To contact the service call [07 5430 1226](tel:0754301226) or email studentwellbeing@usc.edu.au.

10.5. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the [Learning Advisers](#) web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

10.6. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to [Student Hub](#), email studentwellbeing@usc.edu.au or call 07 5430 1226.

10.7. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, [AccessAbility Services](#) can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to [Student Hub](#), email AccessAbility@usc.edu.au or call 07 5430 2890.

10.8. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit <https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching>

10.9. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The [Student Charter](#) sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.10. General Enquiries

In person:

- **UniSC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **UniSC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **UniSC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **UniSC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **UniSC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **UniSC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au