USC

Course Outline

Code: SEC706
Title: Network Forensics

School: Science & Engineering
Teaching Session: Semester 2
Year: 2020
Course Coordinator: Stephen Best
Course Moderator: Professor David Lacey

Please go to the USC website 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 Field trips, WIL placements or activities required by professional accreditation

Activity	Details
N/A	N/A

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?

Specific Learning Outcomes On successful completion of this course, you should be able to:	**Assessment tasks** You will be assessed on the learning outcomes in task/s:	**Graduate Qualities or Professional Standards mapping** Completing these tasks successfully will contribute to:
Demonstrate knowledge of network forensics evidence acquisition processes and techniques.	1, 3	Knowledgeable

Specific Learning Outcomes On successful completion of this course, you should be able to:	**Assessment tasks** You will be assessed on the learning outcomes in task/s:	**Graduate Qualities or Professional Standards mapping** Completing these tasks successfully will contribute to:
Identify and explain current cyber attacks, relevant network controls, infrastructure interception points, standard and advanced security intelligence platforms and develop the practical skills to detect, extract and analyse all relevant forensic artefacts.	1, 2	Empowered
Develop and produce reports suitable for admission as case evidence, that describe identification, search and seizure requirements and examine and analyse provided evidence.	3	Engaged

5. Am I eligible to enrol in this course?

Refer to the USC Glossary of terms for definitions of "pre-requisites, co-requisites and anti-requisites".

5.1 Enrolment restrictions

Nil

5.2 Pre-requisites

Prerequisites: SEC705

5.3 Co-requisites

Nil

5.4 Anti-requisites

Nil

5.5 Specific assumed prior knowledge and skills (where applicable)

Students will be expected to have a sound knowledge of device forensics and a working knowledge of computer systems and networks.

6. How am I going to be assessed?

6.1 Grading scale

Standard – 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

Task No.	Assessment Product	Individual or Group	Weighting %	What is the duration / length?	When should I submit?	Where should I submit it?
1	Portfolio	Individual	20%	Weekly Entry (300 Words / Week)	Weekly from Week 2 to 11	Blog, Wiki or Journal
2	Practical / Laboratory Skills	Individual	40%	1 Hour	Week 8	In Class
3	Report	Individual	40%	4000 Words	Week 15	Online Assignment Submission with Plagiarism check
			100%			

Assessment Task 1: Competency Portfolio

Goal:	To demonstrate knowledge of network forensics evidence acquisition processes and techniques.
Product:	Portfolio
Format:	The portfoloio should form reference material for students of the course to be able to refer to and contain succinct summaries of each concept with one or two examples of techniques and resulting output for a given concept. A reference manual containing: • Reference notes of topics covered in semester • Playbook Template • Application and usage reference list including role of tool and process documentation for essential -to-know tasks.
Criteria:	• Identification and explanation of common network level attacks, infrastructure interception points and common network forensics tools • Development of the practical skills to detect, capture and analyse all relevant forensic artefacts.

Assessment Task 2: Practical Scenario

Goal:	To sit a practical involving two scenarios requiring students to utilise tools and techniques taught throughout semester to capture Indicators of Compromise, attacker identification, packet capture and log artefacts.
Product:	Practical/Laboratory Skills
Format:	Online interactive practical lab consisting of equally weighted challenges.
Criteria:	• Identification and explanation of traffic anomaly and conversation information utilising monitoring platforms. • Selection of the appropriate network infrastructure device on which to acquire traffic of interest. • Detection and extraction of relevant information from Firewall / IPS platforms. • Analysis of log aggregation platform / SIEM to report relevant events and alerts.

Assessment Task 3: Network Forensics Report

Goal:	To prepare a report
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:	• Description of identification, search and seizure requirements. • Examination and analysis of provided evidence.

7. Directed study hours

The directed study hours listed here are a portion of the workload for this course. A 12 unit course will have total of 150 learning hours which will include directed online study hours, self-directed learning and completion of assessable tasks. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

This course will be delivered via technology-enabled learning and teaching. All lectures will remain in this mode for Semester 2 2020. When government guidelines allow, students that elected on-campus study via the class selection process will be advised when on campus tutorials and practical sessions will resume.

Location	Directed study hours for location
Online	This online course will take between 10-12 hours per week and may include a combination of: webinar, peer to peer collaboration, asynchronous online materials, and synchronous lecturer and peer to peer zoom meetings.

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

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

8.1 Prescribed text(s) or course reader

Please note that you need to have regular access to the resource(s) listed below as they are required:

Author	Year	Title	Publisher
Nil			

8.2 Specific requirements

This is an online course and will require access to a computer and the internet for at least 12 hours per week.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low.
It is your responsibility as a student 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. It is also your responsibility to familiarise yourself with the University's general health and safety principles by reviewing the online Health Safety and Wellbeing training module 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 Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

10.2 Assessment: Additional requirements

Eligibility for Supplementary Assessment

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

a) The final mark is in the percentage range 47% to 49.4%
b) The course is graded using the Standard Grading scale
c) You have not failed an assessment task in the course due to academic misconduct

10.3 Assessment: Submission penalties

Late submission of assessment tasks will 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 and supply the required documentation to negotiate an outcome.

10.4 Study help

In the first instance, you should contact your tutor, then the Course Coordinator. Additional assistance is provided to all students through Academic Skills Advisers. To book an appointment or find a drop-in session go to Student Hub.

Contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au

10.5 Wellbeing Services

Student Wellbeing Support Staff are available to assist on a wide range of personal, academic, social and psychological matters to foster positive mental health and wellbeing for your success. Student Wellbeing is comprised of professionally qualified staff in counselling, health and disability Services.

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, mental health issue, learning disorder, injury or illness, or you are a primary carer for someone with a disability, AccessAbility Services can provide assistance, advocacy and reasonable academic adjustments.

To book an appointment with either service go to Student Hub, email studentwellbeing@usc.edu.au or accessability@usc.edu.au or call 07 5430 1226

10.6 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
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website:
http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.7 General Enquiries

In person:

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

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au

For new course approvals only

Appendix 1 Course content

Concepts	What key concepts/content will I learn?
1 Network evidence types and acquisition and packet capture and analysis techniques.	Network evidence acquisition, types of evidence and technical requirements to ensure validity of forensic data. Learn how to perform manual packet captures using industry standard open source tools. Develop a detailed understanding of the IPv4 header format and wireshark techniques. Learn how to carve files from packet captures.
2 SNMP and Netflow	Develop knowledge of current industry standard network management and monitoring tools in the area of network forensics relating to SNMP based and Netflow / sFlow Layer 3 and 4 Netflow Conversation Capture and Analytic.
3 Proxy Servers	Understand the role of proxy servers in network forensics including proxy types, authentication methods, cache flags, attribution and artefact recovery.
4 Common Attack Techniques and Protocol Analysis	Develop a technical understanding of common cyber attacks including common protocols and applications are exploited during an attack, how these protocols (HTTP, DHCP, DNS, SMB) and applications operate and how attacks are performed (applications, scripts and frameworks).
5 Logging Techniques and Platforms	Explore log sources and formats, correct log export configuration, collection methods, analysis techniques, high performance log platforms and SIEM platforms.
6 Continuous Packet Capture Platforms, Orchestration and automation	Expanding on logging techniques and platforms explores automation techniques through the use of continuous full packet capture platforms. Learn how to link tools together through threshold-based alerts from monitoring platforms and automate reporting using orchestration software.
7 Wireless LAN interception and detection techniques.	Learn common WLAN attacks and techniq••ues to detect and capture evidence of attacker activity using corporate WLAN platforms utilising security log analysis and Wireless IPS (WIPS) services.
8 Other NFAT Tools	Learn how to use industry standard applications Zeek NSM, Xplico and NetworkMiner.
9 Network Forensic Report Writing	Learn how to build a 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.