USC

Course Outline

Code: SEC704
Title: Digital Crime Scene Management

School:	Science & Engineering
Teaching Session:	Semester 2
Year:	2019
Course Coordinator:	Dr Graeme Edwards
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

In this online course, you will learn the legal and organisational requirements of managing a digital crime scene including evidence identification, preservation and seizure, as well as the general management and preservation of the digital crime scene. You will learn about the volatility of digital evidence and how to manage it to preserve its integrity and prove its authenticity. You will also learn the way digital evidence is used to progress an investigation into a cyber breach and how the digital investigator contributes in a multi-disciplinary investigation team. The course will analyse the forms of digital evidence you will find in your investigations and introduce evolving technology of specific relevance to the digital investigator including cloud computing and the Internet of Things.

1.2 Field trips, WIL placements or activities required by professional accreditation

Activity	Details
Nil	Nil

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:
Identify the different forms of cybercriminal, their motivations and skillsets.	1	Knowledgeable *Weekly content 1 and 2*
Analyse and discuss the methodologies used in managing a digital crime scene including preparation of an investigation plan.	2,3	Creative and Critical Thinkers *Weekly content week 3*
Analyse and discuss the many forms of digital evidence available and their relevance to a digital investigation.	1,2,3	Ethical *Weekly content 4,5, and 6*
Demonstrate the requirements of competently handling digital evidence.	2,3	Empowered *Weekly content 7*
Interrogate digital evidence to identify its value to an investigation	3	*Weekly content 8 and 9*
Understand and apply legal options available to the civil investigator	3	Engaged *Weekly content 10*
Identify and explain the different legal considerations an investigator must understand when planning and commencing a digital crime scene examination including evidence preservation and capture as well as preserving the chain of custody.	3	Ethical *Weekly content 10*
Demonstrate an understanding of evolving technology and its implementation into a digital investigation.	3	Empowered *Weekly content 11 and 12*
Communicate the outcomes of your inquiries to non-technical audiences such as senior managers.	1,2,3	Engaged *Content included in each week*

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

Enrolled in program SC510 or SC704

5.2 Pre-requisites

SEC701

5.3 Co-requisites

Nil

5.4 Anti-requisites

Nil

5.5 Specific assumed prior knowledge and skills (where applicable)

Students will be assumed to have an understanding of technology and its role in society. They will be expected to have 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

Students will participate in continuous peer and self-assessment during tutorials. Students will also receive feedback during the case study working groups.

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	Case Study	Individual	25%	2000 words	Week 5	Online Assignment Submission with Plagiarism check
2	Report	Group	25%	2000 words	Week 9	Online Assignment Submission with Plagiarism check
3	Case Study	Individual	50%	3000 words equivalent	Week 13	Online Assignment Submission with Plagiarism check
			100%			

Assessment 1: Digital evidence case study

Goal:	From a given case study, identify the different forms of physical and technical evidence that may be expected to be located in a cybercrime scene. Analyse the evidence and discuss how each may be used to advance your investigation and provide evidence as to the identity of the cybercriminal and their motivations.
Product:	Written report based on a provided case study
Format:	The product to be presented is a 2,000-word analysis of the identified digital crime scenes and an explanation of the value of the physical and digital evidence that may be located within it. You will - • Research and discuss what constitutes a digital crime scene. • Identify and discuss the forms of digital evidence located within and from the digital crime scene. • Explain the potential for identifying a suspect from the evidence collected. • Communication of research using academic writing conventions. • Identify a potential motivation for the crime from the evidence provided and your analysis.
Criteria:	• Discussion of a crime scene • Identification and discussion on forms of evidence • Explanation of suspect identification • Professional communication

Assessment Task 2: Investigation plan

Goal:	Identify and describe the logistical requirements for attending to a digital crime scene including the necessity to ensure evidence preservation. You will also discuss the volatility of evidence you may locate and demonstrate the professional relationship between yourself as an investigator and the digital forensic officer. You will present a report explaining your reasoning including safety provisions.
Product:	Group Written report
Format:	2,500-word group report – details on Blackboard.
Criteria:	• Demonstration of leadership qualities (in an online environment) • Demonstration of collaboration skills • Analysis of digital crime scene • Analysis of physical crime scene • Application of ‘chain of evidence protection’ • Communication of research

Assessment Task 3: Digital crime scene presentation

Goal:	Show an ability to prepare and provide a presentation to a legal practitioner and senior executive reporting on a digital crime scene examination where the content shows the scene examination, legality of actions, preservation of evidence and the correlation of evidence located. You will explain the evidence seized and the relevance to the investigation, as well as identifying new lines of inquiry. You will produce the investigation plan you have prepared to show your actions, and these will relate to your examination and plans for future inquiries.
Product:	Video presentation
Format:	The product to be presented is a video recorded presentation to a legal practitioner detailing the circumstances and activity within a digital crime scene using material from a provided case study.
Criteria:	• Application of methodology • Application of the rules of evidence • Explanation of case study • Conclusions supported by evidence • Professional communication of research

7. What are the course activities?

7.1 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 study hours (including online if required), 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.

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

7.2 Course content (Proposed)

Week # / Module #	What key concepts/content will I learn?
1	Introducing the cybercriminal and their motivations
2	The cybercriminals methodologies, skillsets and networks
3	Digital evidence 1
4	Digital evidence 2
5	Digital evidence 3
6	Introduction to the scene and exhibit management
7	Evidence management
8	Investigating cybercrime types 1
9	Investigating cybercrime types 2
10	Civil legislation
11	Investigating in a cloud computing environment 1
12	Investigating in a cloud computing environment 2
13	Case studies incorporating an investigation framework

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

8.2 Specific requirements

This is an online course therefore access to a computer and the internet for 10-12 hours per week is essential.

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 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

10.6 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 Fraser Coast -** Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au