Faculty of Science, Engineering and Built Environment

# SIT282 Computer Crime and Digital Forensics

## Deakin University Unit Guide

Trimester 2, 2019

## CONTENTS

**WELCOME** .......... 2

**WHO IS THE UNIT TEAM?** .......... 2

Unit chair: leads the teaching team and is responsible for overall delivery of this unit .......... 2

Unit chair details .......... 2

Other members of the team and how to contact them .......... 2

Administrative queries .......... 2

**ABOUT THIS UNIT** .......... 3

Unit development in response to student feedback .......... 3

Your course and Deakin's Graduate Learning Outcomes .......... 3

Your Unit Learning Outcomes .......... 4

**ASSESSING YOUR ACHIEVEMENT OF THE UNIT LEARNING OUTCOMES** .......... 4

Overview .......... 4

Summative assessments .......... 4

- Summative assessment task 1 .......... 4

- Summative assessment task 2 .......... 5

- Summative assessment task 3 .......... 6

Your learning experiences in this Unit - and your expected commitment .......... 7

Scheduled learning activities - campus .......... 7

Scheduled learning activities - cloud .......... 7

Note .......... 7

**UNIT LEARNING RESOURCES** .......... 8

Prescribed text .......... 8

Essential learning resources .......... 8

Recommended learning resources .......... 8

**KEY DATES FOR THIS TRIMESTER** .......... 8

**UNIT WEEKLY ACTIVITIES** .......... 9

## WELCOME

Greetings from the teaching team and welcome to this engaging and interactive Computer Crime and Digital Forensics unit which forms an integral part of the Bachelor of Cyber Security Course. We hope you will enjoy the learning experience as we take you on a journey to explore computer crime and apply computer forensics techniques and the associated laws and ethical issues to real world scenarios.

As digital forensics is a continuously developing subject, we will be experimenting with new ideas in terms of presentation of the material and what we do in the pracs. Your responses to these experiments are welcomed. Please let us know where we can improve as well as what works well.

If you are encountering any problems coping with the workload, feel free to approach any of the staff members in person, by telephone or e-mail to ask for assistance.

This Unit Guide provides you with the key information about this Unit. For the best chance of success, you should read it very carefully and refer to it frequently throughout the trimester. Your Unit site (accessed in **DeakinSync**) also provides information about your **rights and responsibilities.** We will assume you have read this before the Unit commences, and we expect you to refer to it throughout the trimester.

## WHO IS THE UNIT TEAM?

### Unit chair: leads the teaching team and is responsible for overall delivery of this unit

Damien Hutchinson

### Unit chair details

| | |
|---|---|
| Campus: | Geelong, Waurn Ponds |
| Email: | d.hutchinson@deakin.edu.au |
| Phone: | +61 3 522 71343 |

Contact the campus leader for assistance at your campus.
* Cloud students please contact the Unit Chair

### Other members of the team and how to contact them

Melbourne Burwood Campus Leader: contact the campus leader for assistance at your campus
Name: Dr. Lei Pan, Burwood Campus Leader
Email: l.pan@deakin.edu.au
Phone: +61 3 925 17483

### Administrative queries

- Contact your Unit Chair or Campus Leader
- Drop in or contact Student Central to speak with a Student Adviser

For additional support information, please see the Rights and Responsibilities section under 'Resources' in your unit site

**ABOUT THIS UNIT**

In SIT282 students will learn how crime is manifested in the IT world, the laws that govern the IT domain, and approaches to investigating cyber-crime and cyber-terrorism using digital forensic techniques. Students will examine both criminal and terrorist activities, the nature of these activities and the people that initiate them. The unit enables students to develop knowledge of laws that have been recently enacted to counter computer crime and terrorism as well as the institutions responsible for implementing those laws. Students will investigate techniques such as acquisition, verification, extraction, reconstruction and reporting. The key focus of SIT282 is on introducing students to computer crime, forensic techniques, digital evidence and retrieval of information. In addition, students will explore ethical implications of crime and terrorism.

**Unit development in response to student feedback**

Every trimester, we ask students to tell us, through eVALUate, what helped and hindered their learning in each Unit. You are strongly encouraged to provide constructive feedback for this Unit when eVALUate opens (you will be emailed a link).

In previous versions of this unit, students have told us that these aspects of the Unit have helped them to achieve the learning outcomes:

- The unit learning outcomes are clearly specified.
- The course materials are closely aligned to the learning outcomes.
- The hands-on nature of the unit helps student understand and master the computer forensic techniques quickly.

They have also made suggestions for improvement, and so this is what we have done:

- The practical materials are expanded and updated so that the information related to more tools will be provided.
- The virtual machine image containing software tools essential for learning will be available for each and every student to download to avoid the VM server issues prior to assignment due dates.

If you have any concerns about the Unit during the trimester, please contact the unit teaching team - preferably early in the trimester - so we can discuss your concerns, and make adjustments, if appropriate.

**Your course and Deakin's Graduate Learning Outcomes**

| | | |
|---|---|---|
| GLO1 | Discipline knowledge and capabilities: | appropriate to the level of study related to a discipline or profession |
| GLO2 | Communication: | using oral, written and interpersonal communication to inform, motivate and effect change |
| GLO3 | Digital literacy: | using technologies to find, use and disseminate information |
| GLO4 | Critical thinking: | evaluating information using critical and analytical thinking and judgment |
| GLO5 | Problem solving: | creating solutions to authentic (real world and ill-defined) problems |
| GLO6 | Self-management: | working and learning independently, and taking responsibility for personal actions |
| GLO7 | Teamwork: | working and learning with others from different disciplines and backgrounds |

| | |
|---|---|
| GLO8 Global citizenship: | engaging ethically and productively in the professional context and with diverse communities and cultures in a global context |

Each Deakin course has **course learning outcomes** which explain what the Deakin Learning Outcomes mean in your discipline. Learning in each unit builds towards the course learning outcomes.

**Your Unit Learning Outcomes**

Each Unit in your course is a building block towards these Graduate Learning Outcomes - not all Units develop and assess every Graduate Learning Outcome (GLO).

| | These are the Learning Outcomes (ULO) for this Unit<br>**At the completion of this unit successful** students can: | Deakin Graduate Learning Outcomes |
|---|---|---|
| ULO1 | Apply knowledge of legal processes and follow standard procedure to investigate different types of cyber-crime and cyber-terrorism; | GLO1 |
| ULO2 | Investigate the usefulness of various forensic techniques and apply relevant methods to gain access and recover computer crime data; | GLO3, GLO4, GLO5 |
| ULO3 | Analyse forensic data and review findings to further probe and investigate serious computer crimes; and | GLO3, GLO4, GLO5 |
| ULO4 | Reflect on findings and prepare reports for target audience that justifies findings and recommends potential action. | GLO2, GLO4, GLO5 |

**ASSESSING YOUR ACHIEVEMENT OF THE UNIT LEARNING OUTCOMES**

**Overview**

In brief, these are the assessment tasks for this Unit (details below):

Investigation report 20%, case investigation and recommendation report 20%, examination 60%

**Summative assessments**

**(tasks that will be graded or marked)**
**NOTE: It is <u>your responsibility</u> to keep a backup copy of every assignment where it is possible (eg written/digital reports, essays, videos, images).** In the unusual event that one of your assignments is misplaced, you will need to submit the backup copy. Any work you submit may be checked by electronic or other means for the purposes of detecting collusion and/or plagiarism.

When you are required to submit an assignment through your unit site (accessed in DeakinSync), you should receive an email to your Deakin email address confirming that it has been submitted. You should check that you can see your assignment in the Submissions view of the Assignment folder after upload, and check for, and keep, the email receipt for the submission.

**- Summative assessment task 1**

| | **Investigation report** |
|---|---|
| **Brief description of assessment task** | This assessment is for students to demonstrate their ability to investigate a computer crime case. Students will be required to follow standard forensic procedure and apply their knowledge of specific legal processes in order to investigate a case. Students will be tested on their ability to follow procedures, use of forensic software tools and justify their findings of the case in a lawful manner. |
| **Detail of student output** | This is an individual assessment task. Students are required to submit an investigation report of approximately 2000 words as well as exhibits to support findings and a list of bibliography. This report should consist of:<br>• an overview of the case<br>• description of the nature of the case<br>• list of necessary resources for forensic investigation<br>• analysis and presentation of findings |
| **Grading and weighting** (% total mark for unit) | Marked; 20% |
| **This task assesses your achievement of these Unit Learning Outcome(s)** | ULO1 Apply knowledge of legal processes and follow standard procedure to investigate different types of cyber-crime and cyber-terrorism<br>ULO2 Investigate the usefulness of various forensic techniques and apply relevant methods to gain access and recover computer crime data. |
| **This task assesses your achievement of these Graduate Learning Outcome(s)** | GLO1 through the assessment of student knowledge of standard procedures and legal processes to be followed in crime investigation<br>GLO3 through the assessment of student ability and competence in using appropriate forensic software to investigate serious computer crimes<br>GLO4 through the assessment of student ability to reflect and critically analyse evidence to further probe information<br>GLO5 through the assessment of student ability to use IT techniques such as encryption, steganography, data recovery and system authentication methods to gain access to information. |
| **How and when you will receive feedback on your work** | Students will be provided with regular feedback in the practical sessions to improve their skills in using forensic software tools, interpreting legal issues and applying laws to case analysis. |
| **When and how to submit your work** | Investigation report submission should be made electronically via the unit site (accessed in DeakinSync) and is due by Sunday 11 August 2019 (week 5) at 11.59pm AEST. |

**- Summative assessment task 2**

| | **Case investigation and recommendation report** |
|---|---|
| **Brief description of assessment task** | This assessment is for students to demonstrate their ability to investigate a serious computer crime case. Students will be required to apply standard forensic procedure as well as encryption techniques, steganography, data recovery and system authentication methods to gain access. They will be required to prepare a forensic report using knowledge of specific legal processes in the case investigation. Students will be tested on their ability to review the case and reflect on their findings in a lawful manner. |

| | |
|---|---|
| **Detail of student output** | This is an individual assessment task. Students are required to submit a case investigation report of approximately 2000 words along with exhibits to support findings and a list of bibliography. This report should consist of:<br>• an overview of the computer crime case<br>• list of necessary resources for forensic investigation<br>• analysis of initial findings, and clues for further investigation<br>• review and reflection on the findings<br>• discussion on potential actions based on justification of findings. |
| **Grading and weighting** (% total mark for unit) | Marked; 20% |
| **This task assesses your achievement of these Unit Learning Outcome(s)** | ULO1 Apply knowledge of legal processes and follow standard procedure to investigate different types of cyber-crime and cyber-terrorism;<br>ULO3 Analyse forensic data and review findings to further probe and investigate serious computer crimes; and<br>ULO4 Reflect on findings and prepare reports for target audience that justifies findings and recommends potential action. |
| **This task assesses your achievement of these Graduate Learning Outcome(s)** | GLO1 through the assessment of student knowledge of standard procedures and legal processes to be followed in crime investigation<br>GLO2 through the assessment of student ability to justify findings of investigation and preparation of a report for target audience<br>GLO3 through the assessment of student ability and competence in using appropriate forensic software to investigate serious computer crimes<br>GLO4 through the assessment of student ability to reflect and critically analyse evidence to further probe information<br>GLO5 through the assessment of student competence in using IT techniques such as encryption, steganography, data recovery and system authentication methods to gain access to information. |
| **How and when you will receive feedback on your work** | Individual feedback from the assessment task 1 will be useful for students to use appropriate investigation procedures and forensic software. Ongoing feedback will be provided during practical sessions to aid case analysis, documentation and justification of findings. |
| **When and how to submit your work** | Case investigation and recommendation report submission should be made electronically via the unit site (accessed in DeakinSync) and is due by Sunday 16 September 2019 (week 9) at 11.59pm AEST. |

**- Summative assessment task 3**

| | **Examination** |
|---|---|
| **Brief description of assessment task** | This closed book examination will assess student's knowledge of computer crimes, investigation procedure and broad Information Technology knowledge related to computer systems. Students must demonstrate an ability to relate, analyse and respond to questions around computer crime and digital forensics under examination conditions. |
| **Detail of student output** | Written closed-book exam paper which needs at least 300 words to answer. |
| **Grading and weighting** (% total mark for unit) | 60% |
| **This task assesses your achievement of these Unit Learning Outcome(s)** | ULO1 through assessment of knowledge of legal processes and ability to follow standard procedure in investigating different types of cyber-crime and cyber-terrorism;<br>ULO2 through assessment of ability to apply forensic techniques and relevant IT methods in crime case analysis<br>ULO3 through assessment of student ability to analyse forensic data; |

| | |
|---|---|
| **This task assesses your achievement of these Graduate Learning Outcome(s)** | GLO1 through assessment of student knowledge of computer crimes, investigation procedure and broad Information Technology knowledge related to computer systems. |
| **How and when you will receive feedback on your work** | Ongoing feedback is provided to students following weekly in class quiz and case study discussions. Feedback provided to students in practical sessions focuses on appropriate use of forensic software techniques. Students are also required to undertake a guided research case studies underpinning modern high-tech crime. Feedback and student reflection on these activities will be relevant for enhanced student performance in the examination. |
| **When and how to submit your work** | Students will be required to attend a two hour supervised written examination during the end of trimester examination period.<br>Please check the date, time and location for the examination from DeakinSync |

**Your learning experiences in this Unit - and your expected commitment**

To be successful in this unit, you must:

- Read all materials in preparation for your classes or seminars, and follow up each with further study and research on the topic;
- Start your assessment tasks well ahead of the due date;
- Read or listen to all feedback carefully, and use it in your future work;
- Attend and engage in all timetabled learning experiences as follows:

**Scheduled learning activities - campus**

2 x 1 hour classes per week, 1 x 2 hour practical per week.

**Scheduled learning activities - cloud**

1 x 1 hour scheduled online workshop per week.

Students will on average spend 150 hours over the trimester undertaking learning and assessment activities for this unit. For campus students this includes class time as described, designated activities in the practical sessions, assessment tasks, readings and study time. For cloud students the time should be divided between online learning activities, discussion boards, designated activities in the practical sessions, assessment tasks, readings and study time.

The unit site will host most of the studying materials including class slides, practical instructions and solutions. Assignment instructions will be posted on the unit site approximately two weeks before the due dates. Most of the practical sessions will be conducted in virtual machine environment which is hosted by the school of IT's vm clusters; the instructions of using VM will be introduced during practical sessions in week 1.

**Note**

At Deakin,

- *Lectures* are referred to as *classes* (definition: a general meeting for all students, for which students do not need to register and where students are engaged through presentations and learning activities)

- *Tutorials, workshops and seminars* are referred to as seminars (definition: more interactive meetings for smaller groups of students).
- For the complete list of agreed definitions for learning experiences, see the Course Design and Delivery Procedure.

## UNIT LEARNING RESOURCES

Your unit learning resources are available in your unit site accessed in DeakinSync.

### Prescribed text

Nelson et al, 2018, Guide to Computer Forensics and Investigations, 6th Ed, Course Technologies, USA.

### Essential learning resources

There is a prescribed textbook for this unit. Please see above.

Please refer to the table in the 'Weekly Activities' section below for the weekly reading schedule; you should read the relevant chapters before the class in which it is covered.

Textbooks, reference books, general books and software may be ordered from the bookshop:
phone 1800 686 681 (freecall);
email to DUSA-Bookshop@deakin.edu.au; or
order online from the University bookshop web site at http://www.dusabookshop.com.au/

### Recommended learning resources

Suitable reference books for this unit include:

- M. T. Britz, “Computer Forensics and Cyber Crime: An Introduction”, Prentice Hall, 2004.
- B. Carrier, “File System Forensic Analysis”, Addison Wesley, 2005.
- C. Davis, A. Phillipp, and D. Cowen, “Hacking Exposed: Computer Forensics”, McGraw Hill, 2005.
- D. Farmer, and W. Venema, “Forensic Discovery”, Addison Wesley Professional, 2005.
- B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, “Guide to Computer Forensics and Investigations”, Third Edition, Course Technology, 2008. (Most of the contents are usable. If you can't afford the new book, this edition is OK to use.)
- B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, “Guide to Computer Forensics and Investigations”, Second Edition, Course Technology, 2005. (Please note that some contents of this reference are based on Windows 98 and are out of date and no longer taught this year. Not highly recommended.)
- Prosise, and K. Mandia, “Incident Response”, Second Edition, McGraw Hill, 2003.

## KEY DATES FOR THIS TRIMESTER

| | |
|---|---|
| **Trimester begins (classes begin)** | Monday 8 July 2019 |
| **Intra-trimester break (a short break during trimester)** | Monday 12 August - Sunday 18 August 2019 |
| **Trimester ends (classes cease)** | Thursday 26 September 2019 |
| **Study period (examination preparation period)** | Monday 30 September - Friday 4 October 2019 |
| **Examinations begin** | Monday 7 October 2019 |

| | |
|---|---|
| **Examinations end** | Friday 18 October 2019 |
| **Inter-trimester break (the period between trimesters)** | Monday 21 October - Friday 8 November 2019 |
| **Unit results released** | Thursday 7 November 2019 (6pm) |

**UNIT WEEKLY ACTIVITIES**

| Week | Commencing | Topic | Weekly Reading Chapter(s) | Assessment activity |
|---|---|---|---|---|
| 1 | 8 July 2019 | Understanding the Digital Forensics Profession and Investigations | 1 pp. 1-22; 5 pp. 248-256 | |
| 2 | 15 July | Preparing a Digital Forensics Investigation | 1 pp. 20-52 | |
| 3 | 22 July | Current Digital Forensics Tools and Data Acquisition | 3 pp. 93-124; 6; and 12 pp. 500-506 | |
| 4 | 29 July | Processing Crime and Incident Scenes | 4 | |
| 5 | 5 August | Digital Forensics Analysis and Validation | 9 | Assignment 1 |
| 6 | 19 August | The Investigator's Office and Lab and Report Writing for Investigations | 2 and 14 | |
| 7 | 26 August | Working with Windows and CLI Systems | 5 | |
| 8 | 2 September | Recovering Graphics Files | 8 | |
| 9 | 9 September | Email and Social Media Investigations | 11; and 12 pp. 494-495, 510-512 | Assignment 2 |
| 10 | 16 September | The Expert Witness and Ethics | 15 and 16 pp. 631-637; and 639-642 | |
| 11* | 23 September | Revision | | |

Intra-trimester break: **Monday 12 August - Sunday 18 August 2019** (between weeks 5 and 6)
***Friday 27 September:** AFL Grand Final Eve public holiday - University closed