

SIT282/SIT703 Computer Forensics and Investigations

Workshop Session 6

It is vital for forensic professionals to understand different types of computer crime that can be committed and the types of crimes that would warrant the use of a digital forensic lab. Analyzing the types of crimes helps ensure the lab is equipped with the required equipment and devices to process the evidence for a particular geographical area.

In this session, we learn about the Australian Groups/Agencies involved in the reporting of computer crime. We then analyze recent reports to understand the types of digital crimes that are being committed. Finally we review some cases where digital evidence has played a role in the conviction of the defendant.

Learning Objectives

1. Describe the Australian Groups/Agencies involved in the reporting of computer crime.
2. Analyze relevant reports to understand the types of digital crimes that are being committed.
3. Review cases where digital evidence has played a role in the conviction of the defendant.

1. Cybercrime reporting in Australia

There are a number of agencies involved with reporting of cybercrime in Australia. For each of the following organisations describe their purpose in digital forensics or role in reporting cybercrime. Use the table provided to record your findings.

- ACORN: <https://www.acorn.gov.au/>
- Scam watch: <https://www.scamwatch.gov.au/>
- Australian Federal Police: <https://www.afp.gov.au/rats>
- AusCERT: <https://www.auscert.org.au/>
- Australian Criminal Intelligence Commission: <https://www.acic.gov.au/>
- Australian Cyber Security Centre: <https://www.cyber.gov.au/>

Task:

Organisation	Description
ACORN	
Scam Watch	
AFP	
AusCERT	
ACIC	
ACSC	

2. Analysis of Threat Report

Read the 2020-21 ACSC Annual Cyber Threat Report and answer the questions.

<https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2020-june-2021>

Tasks:

- a. Provide definitions to distinguish between:

COVID-19 themed malicious activity:

Ransomware:

Exploitation of security vulnerabilities:

Software supply chain compromises:

Business email compromise:

- b. The report suggests approaches to protecting networks from the above 5 threats. Create a table to compare these approaches, listing which approaches are generic and can be applied to all and which are specific to the threat only.

Threats	Protection approaches	Generic/Specific
COVID-19 themed malicious activity	(1)	
	(2)	
	...	
Ransomware	(1) ...	
...		

- c. List the top 3 cybercrime types (& their percentage) reported via ReportCyber and the cyber security incidents by the top 5 reporting sectors (& their percentage) for financial year 2020-21.

3. Analysis of Crime Statistics

The Crime Statistics Agency (CSA) is responsible for processing, analyzing and publishing Victorian crime statistics, independent of Victoria Police. Navigate their website and find crime statistics for your geographical area. There are many types of offences reported.

Task:

Identify any crimes that would be related to digital forensics. Can you identify any trends over the past decade? Produce a one-page summary to present your findings.

NOTE: If you are NOT located in Victoria, perform the research based on your campus location.

<https://www.crimestatistics.vic.gov.au/>

<https://www.crimestatistics.vic.gov.au/crime-statistics/latest-victorian-crime-data/recorded-criminal-incidents-2>

4. Evaluation of Case Studies

Mark Lundy, a New Zealand man, was convicted for murdering his family. Do a Google search and discover how he was convicted. Find out how the NZ police explained why his family was murdered at about 7pm but the family PC was shutdown at 11pm while Mark Lundy was witnessed at a different city at 5:30pm and 8:30pm. Discuss with your tutor or classmates on CloudDeakin discussion forum about possible scenarios how the police made conclusions.

<https://www.stuff.co.nz/national/crime/107699306/mark-lundy-appeal-rejected> <http://www.stuff.co.nz/national/crime/9253570/Mark-Lundy-murder-convictions-quashed>

<https://www.stuff.co.nz/dominion-post/comment/67586684/>

Search for the American homicide case of Bobbie Jo Stinnett and Lisa Montgomery. Discuss how and why Lisa Montgomery was sentenced to death penalty. What type of digital evidence did FBI use? Did they get any help from overseas forensic experts? If so, who helped FBI?

<https://ecf.ca8.uscourts.gov/opndir/11/04/081780P.pdf>