The Forensic Process
Cybercrime
Australian Law
Legal Issues

Sammons: Ch4 & Ch7
Casey: Digital Evidence and Computer Crime: Ch 6
Urbas: Cybercrime
Readings

Objectives

- To understand the Forensic Process
- To understand Cybercrime
- To be aware of Australian Law regarding DF
- To understand common legal issues in DF
- To be aware of our ethical responsibilities

Identification

- On being notified of a possible Security Breach, the investigator must decide:
- Is it a Civil or Criminal case?
- Who has jurisdiction of the case?
  - is it in the workplace?
  - is it on public property?
  - has a crime been committed?

Criminal Law

- Criminal Law
  - deals with acts of intentional harm
  - such acts are offences against us all
  - the offences are listed as crimes in a criminal code
  - to be convicted it must be proved that the person committed the crime (authentication)
  - it must also be proved the person meant to commit the crime

Civil Law

- Civil Law
  - deals with disputes between private parties
  - Breaking agreements such as contracts
  - or negligent acts that cause harm to others
- negligence is the failure to exercise the degree of caution that an ordinarily prudent person would take in the situation
- the usual outcome is to pay damages

Civil Law #2

- Civil Cases may not involve Law Enforcement
- Civil Cases may involve a Court Order
  - Child custody for example
- The Court Order may impact on what the Investigator can do
  - There may be time limits on the evidence
- Forensics procedures and techniques can vary significantly from case to case

Standards of proof

- To convict in a criminal case there must be proof beyond a reasonable doubt
- The judge or jury must be almost certain
- To convict in a civil case requires proof on the balance of probabilities
- It is more likely than not that the defendant causes harm or loss

Crime Scene Preparation

- Notify Decision Makers and Acquire Authorization
- Risk Assessment
  - privacy issues
- Obtain Search Warrant
- Issue Subpoenas
- Document the procedure to be followed

Search and Seizure

- A police officer may apply for a warrant to search if:
- she has reasonable grounds for believing that there is or will be on the premises:
  - A thing connected with a particular crime
  - A thing stolen or otherwise unlawfully obtained.

- A warrant authorises a police officer to enter premises, and Search only for those things listed
- A warrant is not required to search a person or package for a dangerous article or a thing used in a crime

Subpoenas

- If a person refuses to produce documents or give evidence, a party may request the Court to issue:
- a subpoena for production;
- a subpoena to give evidence;
- a subpoena for production and to give evidence

Evaluate and Secure the Scene

- Gather the Preliminary Information at the Scene
- First Responder duties
  - ensure the safety of all persons
  - protect the integrity of all evidence
  - If it is off, leave it off. If it is on, leave it on
  - remove all persons from the scene
  - conduct preliminary interviews

Collect the Evidence

- Search and Seizure
- Photograph the scene
  - include all peripherals
- Collect Physical Evidence
  - books, notes, passwords
- Collect Electronic Evidence
  - look for a backdoor Trojan

Examples of things that become evidence

- Documents detailing a crime
- Financial documents detaining of a crime
  - Orders, Invoices and Receipts
- Illegal images
- Web History of visits to a website relating to a crime
- Web Searches relating to performing a crime

Digital Evidence

- Acquisition methods depend on the type of digital evidence.
- It can be Transient
  - reside in memory
  - such as open network ports
- It can be Fragile
  - easily altered
  - date/time stamps

Digital Evidence #2

- Access can be Temporary
  - encrypted file system
  - requires access to the private key/password
- It can be Active
  - current open files
  - current TCP session
- It can be Archived
  - backup copy

Digital Evidence #3

- It can be Residual
  - fragments left after file deletion
- It can be Meta Data
  - data about the data
  - date/time stamps, owner, printer used

Acquiring a Forensic Duplication

- We need to examine the non volatile evidence stored on a hard disk
- To ensure that we do not alter the evidence

- We need to analyse a copy of the disk
- The original disk is now evidence so is sealed
- A second copy may be necessary to return the device to service

Legal Issues in taking a copy

- Cybercrime Act 2001 Section 3K

- Use of equipment (laptop) to examine or process things (make a copy of the suspect's disk)
- Equipment may be brought to the warrant premises
- Things may be moved for examination (take the device away)
- Time limit on moving a thing – 14 days

Testifying as an Expert Witness

- An expert is a person who, by virtue of education, training, skill, or experience, is believed to have expertise and specialised knowledge in a particular subject
- An “Expert” is considered so by her peers
  - There is no exam to be an expert
- Only an expert witness can give an opinion in court
  - Give some opinions and conclusions

A summary of the Forensic Process

- A suspicious item is found

- What is the item?
- How did it get there?
- When was it placed there?
- Who put it there?
- Why was it placed there?

- Is it forensic evidence?

A summary of the Forensic Process #2

- Identification
  - Criminal or Civil?
- Preparation
  - warrants and subpoenas
- Evaluate and Secure the Scene
- Collect the Evidence
- Secure the Evidence
  - make hashed copies
- Acquire the Data
  - disk images, decryption, unhiding
- Analyse the Data
  - keyword searches
- Prepare the Final Report

Objectives

- To understand the Forensic Process
- To understand Cybercrime
- To be aware of Australian Law regarding DF
- To understand common legal issues in DF
- To be aware of our ethical responsibilities

Cybercrime

- Three options:
- 1) involves digital devices in the commission of a crime
  - online fraud
  - cyberstalking
  - cyber terrorism
- 2) is directed at digital devices themselves
  - hacking
  - malware
  - botnets
- 3) is incidental to the commission of other crimes
  - communications about a crime
  - purchasing stolen credit cards

Cybercrime laws

- Older Commonwealth laws refer to a communication service
- Any new form of communication is a like service
- OECD countries approved the Convention on Cybercrime in 2004
- Australia signed the convention in 2012 and the law came into force in March 2013

Legal View of Cybercrime

- Council of Europe Convention on Cybercrime
- Australia signed the convention in 2012 and the law came into force in March 2013

Three parts:

- access to a computer system or interception of data transmission
- committed intentionally
- illegal or without right (not permitted by the owner)

Cybercrime motivation

- Scale: The internet can access 3 billion people
- Accessibility: Smart phones are everywhere
- Anonymity: Proxy servers, VPNs and TOR
- Data Portability: A Smart phone can hold GB of data

- The availability of large numbers of victims
- The supply of large numbers of offenders
- The absence of capable guardians
  - no surveillance of data, networks and activities online

Objectives

- To understand the Forensic Process
- To understand Cybercrime
- To be aware of Australian Law regarding DF
- To understand common legal issues in DF
- To be aware of our ethical responsibilities

Right of Privacy

- the right of natural persons to protect their personal life from invasion and to control the flow of their personal information

- Privacy is not an absolute
- is balanced against other competing rights and duties

Privacy concepts

- Information privacy
  - the handling of personal data such as credit information, and medical and government records.
  - Also called data protection.

- Bodily privacy
  - protection against invasive procedures such as genetic tests, drug testing and cavity searches

Privacy concepts #2

- Privacy of communications
  - the security of mail, telephones and e-mail

- Territorial privacy
  - limits intrusion into the workplace or public space.
  - This includes searches, video surveillance and ID checks.

Australian Privacy Principles (APPs)

- Became law on 12 March 2014
- Contain 13 principles
  - See Reading
- Companies must comply with these principles
- Once approved, the company is given an APP code

APP 11 – Security example

- Company xyz store their customer data with Amazon Web Services (AWS)
- The data gets hacked and damaging personal information is made public
- Who is to blame?

Data Retention

- Telecommunications (Interception and Access) amendment (Data Retention) Bill March 2015
- requires telecommunications service providers to retain telecommunications metadata for two years
- Conflicts with the right of privacy Act 1988

Data Retention phone call example

- Phone call – data not retained
  - the conversation
- Phone call – data retained
  - the caller number and the called number
  - the duration of the call
  - the location of the caller
  - this can be the exchange line for fixed lines
  - or the mobile cell tower for mobile calls
  - or GPS data

Data Retention email example

- email – data not retained
  - the content
- email– data retained
  - the sender and the recipients
  - the size of the message
  - the location of the sender
  - Receipt acknowledgement
  - this can be the ISP line for fixed lines
  - or the mobile cell tower for mobile calls
  - or GPS data

Objectives

- To understand the Forensic Process
- To understand Cybercrime
- To be aware of Australian Law regarding DF
- To understand common legal issues in DF
- To be aware of our ethical responsibilities

A Legal Case Study

- A person was charged with assaulting police after heavily armed officers ordered her out of bed in the early hours of September 18 2014 during the largest counter terrorism raids in Australia's history.
- It emerged that the woman was not named on the search warrant and was not shown paperwork accompanying the warrant as required by law.
- While police had the authority to enter the premises, they did not have the authority to arrest, detain or search the woman without reasonable suspicion.
- On Monday, the Magistrate found that searching the woman was unlawful and that the officers were not acting in the execution of their duties.
- So the charges against her must be dismissed.
- The woman is likely to seek an order that NSW Police pay her legal costs.

Search Warrants

- The warrant is very specific
- What if the investigator discovers something outside the warrant?
- What if it is evidence of a reportable offence?

Adverse Inference

- a legal inference, adverse to the concerned party, drawn from silence or absence of requested evidence.
- the jury can infer that the evidence would have been adverse to (the defendant), and adopt the plaintiff's reasonable interpretation of what the document would have said
- Examples include encrypted emails and incognito browsers

Exclusionary Evidence

- There are some legal principles that prevent certain evidence being used in a court

- Contamination
  - the evidence may have come from another user or even the investigator
- An illegal (not done properly) step in an investigation may void all following evidence

Privacy

- The investigator may be restricted in searching due to the privacy laws

Objectives

- To understand the Forensic Process
- To understand Cybercrime
- To be aware of Australian Law regarding DF
- To understand common legal issues in DF
- To be aware of our ethical responsibilities

Ethics

- Concepts of Ethics
- Rules you internalise and use to measure your performance.

- Standards that others apply to you.
- Standards your profession applies to you.
  - Also called rules of conduct
- The International Society of Forensic Computer Examiners
- https://www.isfce.com/ethics2.htm

Purpose of Ethics

- To maintain your balance in a difficult situation
- To maintain your self respect
- To maintain the respect of others
- Forensic examiners have no formal code of conduct
- To protect yourself against legal challenge
- To identify and control your bias when presenting evidence

Ethical principles

- To have nothing to hide
- To present unbiased evidence
- To comply with the rules of evidence
- To preserve confidentiality
- To disclose all fees and charges
- To disclose any conflict of interest.

FIN

- All done and Goodbye