School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Week 12 - Digital forensics

Material based upon Chapter 2, Digital Forensics, Digital Forensics and Incident Response, Gerard Johansen, Pakt Publishing (2017)

DIGITAL FORENSICS

Digital forensics

- Digital forensics is a **branch** of forensics science.
- ***Forensics science*** is the application of science to criminal and civil laws.
- Recovery and investigation of material found in digital devices.
- Often related to *cyber crime* but could be for other purposes such as incident response.
- Big difference is the timeframe.
  - **Cyber crime** – the evidence is old and the work could last years.
  - **Incident response** – the evidence might be very recent and work could last hours to weeks.

Digital forensics

- Relates to any criminal or civil law issue involving:
  - Internet
  - computer
  - any electronic device

- Encompasses wide range of devices:
  - PCs
  - Mobile devices
  - CCTV cameras
  - Fitness trackers
  - Cloud services
  - …

Forms of crime

- Some crime is specific to computers but also:
  - Fraud
  - Harassment
  - Copyright breaches
  - Making, possessing or distributing objectionable material such as child pornography.

- Some relevant New Zealand legislation:
  - Unsolicited Electronic Messages Act 2007
  - Harmful Digital Communications Act 2015
  - Copyright (Infringing File Sharing) Amendment Act 2011

Legal aspects

- What the person might guilty of isn't the only important legal aspect.
- How do you collect evidence **lawfully**?
- **What represents evidence?**
- How do you avoid evidence being somehow tainted and unsuable?
- Governed by Acts, for example the Evidence Act 2006 (extends the original Act from 1908)
- Each type of evidence has **guidelines** and best practice that try to capture the answers to these questions ...

Example: CCTV

- ANZPAA, 2012, Australia and New Zealand Police Recommendations for CCTV Systems
- ANZPAA, 2012, Australasian Guidelines for Digital Imaging Processes
- Home Office Scientific Development Branch, 2005, Scan Converters & Retrieving Digital CCTV Images
- Home Office Scientific Development Branch, 2007, Video Processing & Analysis
- Home Office Scientific Development Branch, 2008, Retrieval of Video Evidence & Production of Working Copies from Digital CCTV Systems v2.0
- ISO/IEC 17025
- LEVA Guidelines for the Best Practice in the Forensic Analysis of Video Evidence
- LEVA Best Practices for the Acquisition of Digital Multimedia Evidence
- National Policing Improvement Agency, 2007, Police Use of Digital Images
- SMANZFL, 2006, Recommended Practice for Forensic Processing – Management of Recordings
- SWGIT Best Practices for Forensic Video Analysis
- SWGIT Best Practices for Forensic Image Analysis
- SWGIT 2007 Best Practices for Maintaining the Integrity of Digital Images & Digital eo
- SWGIT Best Practices for the Analysis of Digital Video Recorders (Draft version 1.0 2012)
- SWGIT Digital Imaging Technology Issues for the Courts

WHAT IS EVIDENCE?

Main Types of Evidence

- **Primary:** the best, or “first hand” evidence
- **Secondary:** where primary evidence is not available a copy will be accepted.
- **Similar fact:** previous methods of operating (modus operandi of an offender).
- **Documentary:** Any documentary evidence and includes *Photographic Evidence.*
- **Character:** Evidence as to the character of one of the “players”.
- **Oral:** Evidence given verbally.
- **Direct**: Any evidence being given by a first party (usually oral).
- **Real:** Inanimate object – such as the weapon used.
- **Opinion:** Expert is the only opinion a court usually accepts (after proving expertise)
- **Circumstantial:** Various evidence points to one logical conclusion
- **Hearsay:** Something overheard and relayed by a third party.

Main Types of Evidence

NOT ADMISSABLE UNLESS "BY LEAVE OF THE COURT"

- **Primary:** the best, or "first hand" evidence
- **Secondary:** where primary evidence is not available a copy will be accepted.
- **Similar fact:** previous methods of operating (modus operandi of an offender).
- **Documentary:** Any documentary evidence and includes *Photographic Evidence.*
- **Character:** Evidence as to the character of one of the "players".
- **Oral:** Evidence given verbally.
- **Direct**: Any evidence being given by a first party (usually oral).
- **Real:** Inanimate object – such as the weapon used.
- **Opinion:** Expert is the only opinion a court usually accepts (after proving expertise)
- **Circumstantial:** Various evidence points to one logical conclusion
- **Hearsay:** Something overheard and relayed by a third party.

Example: CCTV

- CCTV recordings are primary, secondary, and direct evidence.
- Does a copy of the CCTV recording count?
  - Downloaded from the system – **secondary**.
  - Secondary allowed if no other option.
- What if the primary or secondary recording weren't kept securely?
  - Could have been changed.
  - Might still be admissible but could be argued out of court pre-trial.
- What if needs **processing** to make it viewable?
  - No longer the original evidence!
  - But generally accepted that first usable manifestation of the data is the original and primary evidence.
  - Have to show though that transformation doesn't change nature of the evidence.

DIGITAL FORENSICS PROCESS

Digital forensics process

- Investigators follow a process so that they avoid tainting the evidence and make unusable in court.
- A well-known process was defined by the **Digitial Forensics Research Workshop (DFRWS)** Digital Investigation Process
  - Indentification
  - Preservation
  - Collection
  - Examination
  - Presentation

Identification

- We first need to identify our evidence, this is usually not the event but related to the event.
- “When two objects come into contact, they leave a trace on each other” **Locard’s exchange principle**.
- Consider someone entering a house with carpeting.
- What are some examples of potential traces?

Identification (cont.)

- “When two objects come into contact, they leave a trace on each other” Locard’s exchange principle.
- Consider someone entering a house with carpeting.
- What are some examples of potential traces?
  - ***Soil on your shoes.***
  - ***Fibres from your soles of the shoes.***
  - ***…***

- ***Trace evidence used to show you were present.***

Identification (cont.)

- “When two objects come into contact, they leave a trace on each other” Locard’s exchange principle.
- Consider someone browsing a website?
- What are some examples of potential traces?
  - Browser history.
  - Web server logs.
  - Web proxy logs.
  - Cookies left on laptop.
  - DNS lookups.

Identification (cont.)

- *Trace evidence in the digital world is relatively easy to manipulate.*
- Would not rely upon a single source of trace evidence.
- Look for evidence that correlates with each other.
- Use this to verify the evidence.

Preservation

- Safeguard from:
  - Deletion
  - Modification
- Isolate the system from the network (logical or physical).
- Do not allow users access to suspect system.
- Snapshot virtual machines.
- Use of encryption or digital signatures to ensure that any tampering is noticed.

Collection

Process of acquiring digital evidence.
Volatile evidence = evidence lost when switch off the system.
Most volatile to least volatile (see RFC 3227):

- Registers, cache
- Routing Table, ARP Cache, process table, kernel statistics, Memory (RAM)
- Temporary filesystems
- Disk
- Remote logging and monitoring data
- Physical configuration, network topology
- Archival media

Collection (cont.)

- **MUST NOT CHANGE THE VOLATILE EVIDENCE AS RESULT OF COLLECTION.**
- Example:
  - Windows system (if you boot up the system do you change evidence on the system, what if automatics updates run etc.)
  - Mount a USB drive (what if it gets corrupted?)
- Often why might image a machine using special software and load in a virtual environment or use tools like USB blockers that prevent writing to the drive.
- This moves it from volatile to non-volatile state.

Proper evidence handling

- Mistakes in how you collect evidence can make it **useless**:
  - Tainted
  - Not forensically sound
  - Excluded from being admitted in criminal or civil proceeding

- Actions taken should not alter original evidence.
  - Do not access running systems.
  - Some processing inevitably modifies evidence (consider old fashioned photographic film).
  - Document any processing and have justifiable reason to avoid tainting the evidence.

Documentation

- “if you didn’t write it down, it didn’t happen”
- Evey action must be documented.
- Detailed notes and diagrams.
- Can include photographs.
- Construct chain of events if integrity is challenged.
- Use standard approaches.
  - *http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf*
  - *https://www.ncjrs.gov/pdffiles1/nij/219941.pdf*
  - *http://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf*

Chain of custody

- Documents the lifecyle of evidence.
  - Starts with taking custody of evidence.
  - Ends with incident ending and evidence either returned or destroyed.
- Any **break** in the chain means the evidence could be prevented from being admitted.
- Recorded either:
  - Electronicallly, unique bar code stickers and scanner to create a trail.
  - Pen and paper, paper forms.
- Choice based on cost and convenience.

Example form

ELECTRONIC EVIDENCE
CHAIN OF CUSTODY FORM

Case No: Page: of:

ELECTRONIC MEDIA/COMPUTER DETAILS

IMAGE DETAILS

CHAIN OF CUSTODY

Details

- Details:
  - Uniquely identies item
  - Item number, description, make, model, serial number

ELECTRONIC MEDIA/COMPUTER DETAILS

Item No:	Description:		
1	Western Digital WDØ1EURS Hard drive		
Manufacturer:	Model No:	Serial No:	
Western Digital	WDØ1EURS	WMAV1234567	

Details (cont.)

- Steps taken within life cycle
  - Tracking number, date and time, to and from (people or storage place, people sign it), reason (must always have a reason).

CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:
1	Date: 1-21-07 Time: 12:07 pm	Name/Org: Acme Comp Data Center Signature: N/A	Name/Org: John Smith /ACME Signature: John Smith	Seizure
2	Date: 1-21-07 Time: 12:33 pm	Name/Org: John Smith /ACME Signature: John Smith	Name/Org: Evidence Locker /ACME Signature: n/a	Secure Storage

Examination

- Use tools.
- Standard tools that have been approved within legal jurisdictions exist (for example, enCase).
- Might be tools to extract from:
  - Memory
  - Network traces
  - Log files on servers
  - Mobile phones

- Again need to prevent damage to the evidence when examining it.

Analysis

- Examination phase extracted potentially relevant pieces of data.
- Analyse data in light of other relevant data.
- Example:
  - Host as open connection to external IP address
  - Examine a packet capture
  - Use IP address as starting point and isolate that traffic
  - Perhaps determine if host is contacting a Control and Command server.
  - This might lead to an understanding of the type of attack.

Presentation

- Present the findings:
  - Clear
  - Concise
  - Capture every action taken and reports on critical data.
  - Without opinion or bias.
  - Aids in determining the root cause.

- Might have to appear in court and state the **facts**.

- Might have to be an expert witness who is allowed to give an opinion.

DIGITAL FORENSIC LAB

Need for a lab

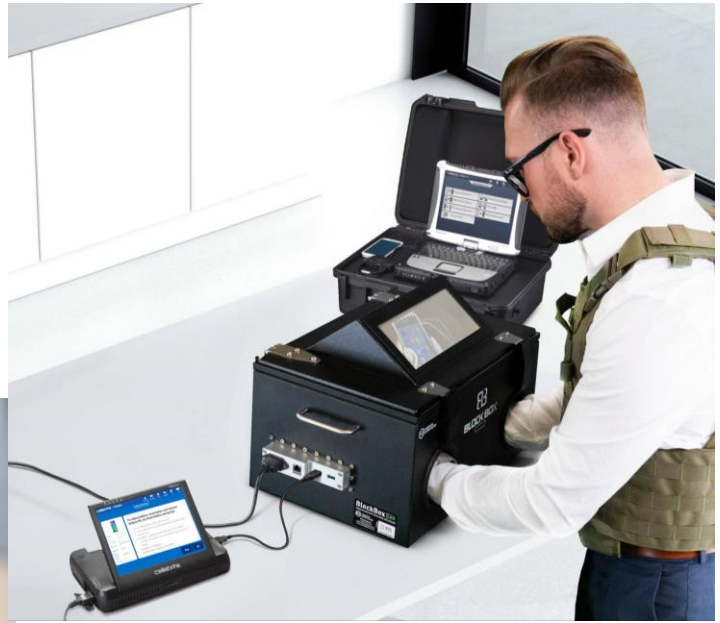
- Requires special tools, techniques and knowledge.
- Use a separate location from rest of organisation.
- Aim is to avoid damage to the evidence.
- Also **privacy**.

Physical security

- Access to lab must be controlled for chain of custody purposes.
- Remove chance of tampering or destruction of evidence.
- Locked always with access via access cards etc.
- Keep a log of entry and exit.
- Evidence lockers as well.
- Ideally keep evidence related to different incidents separate.
- Climate controlled environment.

Tools

- Literally have hand tools.
- Boxes for securing evidence.
- Faraday bags for smart phones or tablets to isolate them from network.



Hardware

- Forensic workstations with plenty of storage.
- Workstation is **not connected** to Internet for protection against corruption of evidence.
- Internet connected machine in same room.
- Physical write blocker:
  - Connects hard drive and forensic imaging machines.
  - Prevents writing of data to a drive.

Going offsite with hardware

- Durable case to transport necessary hardware.
- Support offsite examination.
- Should be capable of being checked in on a plane and arriving undamaged.

Software

- Forensic applications
  - Carry out variety of tasks
  - Documentation as well as collection etc.
- Three most common:
  - EnCase – works with hard drive and storage media.
  - FTK Forensic Tool Kit – similar to EnCase.
  - X-Ways – low cost linux based.
- Platforms for RAM captures and network evidence:
  - SANS SIFT – imaging, memory analsys, timeline creation etc. (free)
  - CAISE Computer Adied Investigative Environment - multiple tools

Jump Kit

- Equipment for forensics analysis on the move,
- Suggested components:
  - Forensic laptop.
  - Networking cables.
  - Physical write blocker.
  - External USB hard drives and USB devices.
  - Bootable USB or CD/DVD
  - Evidence bags or boxes
  - Anti-static bags.
  - Chain of custody forms.
  - Tool kit
  - Notepad and writing instrument

Summary

- Brief overview of digital forensics.
- What’s it for ...
- Legal aspects ...
- Phases ...
- What you need to do it.