Lectures

Week 1

Pt1 - into

- Things to look for
    - Look for search history, communications
    - Private documents
    - When things were accessed
- Incidence Response is immediate (protect the victim) where as Computer Forensic is post event (find the truth) vs electronic discovery (discover and produce material to the other side)
    - E.g incident response: getting ddosed, trying to prevent it from happening
    - E.g computer forensics: analyse, see how attackers got through
- Computer Forensics do not figure out the WHY → stay within your scope of expertise (not psychology. Should not provide an opinion on human behaviour)

Pt2 - COMMBANK TALKS

- Always document acquisition of data

P3 - THEORY

Brief Intro to Evidence

1. Testimony → given by a witness
2. Documentary → See dictionary at end of evidence act; part 4.3 of evidence act relates to documents, including: evidence produced by processes, machines and other devices
3. Physical → a real thing that is able to be produced in court. Often documents are used in place of physical evidence

Witnesses

- Lay witness, investigator, expert, independent expert

Evaluation of evidence

- Look at source acts instead of compilations. Useful graphics may be left out.

Standards of Proof

- Civil
    - Balance of probability
- Criminal
    - Prosecution - beyond reasonable doubt
    - Defendant - on the balance of probabilities
- In both civil and criminal
    - Admissibility of evidence is always on the balance of probability

Exerts need to do four things. Is it:

- Relevant
    - Fact
    - Opinion
- Reliable
    - Evidence
    - Witness

- Sufficient
    - Standard of proof
    - Prove the right thing(s)
- Persuasive
    - Understood by the decision maker(s)
    - Know the audience

P4 - practical

- Forensic Copying
- Windows file system, software data recovery

Why is forensic copying so important? Aka acquisition, imaging, duplication
Allow us to freely damage e.g make 1000 copies of iphone and brute force password
Team can work at the same time
Maintain original for verification

A three part process

1. Make a copy (duplicate data; reliable + sufficient)
2. Make verification metadata (create metadata i.e data about the data that can be used later to verify that the data has not changed)
3. Demonstrate the copy is a reliable copy

There are many different ways to create a forensic copy -- so long as there is a duplicate and verification metadata.
TODO: IMAGE
Can use dd instead of eo1
Dcfldd → defense computer forensic labs dd
→ an extended version of dd. Adds features useful for forensics: Hashing on the fly; progress indicator
Write blocking → used to ensure that original cannot be written onto i.e cannot be changes; Hardware or software (hardware tested by NIST)

What happens when verification fails?

- It sometimes happens that the copy is changed
- How can a copy change?
    - Spoilage = accidental
    - Tampering = purposeful
    - Was the examiner reckless or negligent? Was it wear and tear?
- A single bad sector will cause the hash to be different

Common file systems

- FAT -- FAT12, FAT16, FAT32
- NTFS -- Microsoft
- exFAT - for flash drives
- Ext2, ext3, ext4 - genesis in Unix now linux. Still popular on devices

- HPFS - high performance file system IBM
- HFS and HFS+ Apple’s early file systems
- APFS - Apple file system
- ISO 9660 and Joliet - CD/DVD
- + emerging file systems for cloud

Data recovery

- Also called data carving
- Common data carving tools which you will use in the tutorial/lab include scalpel/foremost, recoverjpg, photorec
- NIST provides standardises methods and test cases for data carving

Codocile = precursor to de facto relationship

Week 2

Recap

- Standards of Proof
    - Criminal
        - Prosecution -- beyond reasonable doubt
        - Defendant - on the balance of probabilities
    - Civil
        - Balance of probability
        - Some matter require higher e.g. forgery
    - Criminal and civil
        - Admissibility is always on the balance of probability
- Types of evidence
    - Testimony
        - Given by a witness
    - Documentary
        - Relates to documents, including: evidence produced by processes, machines and other devices
    - Physical
        - A real thing that is able to be produced in court
        - Often, documents are used in place of physical evidence e.g picture, video, etc.
- Types of witnesses
    - Lay witness
        - Merely to recall facts based on their own sensual experience and strictly adhering to the rules of evidence. Not expected to understand the rules of evidence and evidentiary process relies on objection of opposing counsel.
    - Investigator

        - Discover facts. In evidence may also merely recall fact however courts have come to expect that the investigator has attempted to discover as much **incriminating** and **exculpatory** evidence as reasonable.
    - Expert
        - Answer a particular question, or questions as instructed by legal counsel. In doing so, the expert is allowed to provide an opinion based on their particular expertise.
        - Loosely defined as a person who has specialised knowledge based on the person's training, study or experience.
    - Independent Expert
        - Not formally distinguished, but in practice weighs heavily when assessing credibility.
        - As well as demonstrating his or her expertise, an independent expert must demonstrate that, apart from their instructions, they have no other interest in matter of hand

PART 1 OF LECTURE

- Evidence
    - Pre-trial
        - Generally where you do your examination, write your report and generally have a conference/meeting or interview with solicitor/barrister instructing you. May be required to have a conference with solicitor/barristers on the other side.
        - Special conference called a conclave, a conference between two or more experts with rules.
        - Any party may engage you with written questions. Questions from parties in the trial that aren't the solicitors or barristers must be ignored.
        - Barristers make up 1-1.5% of legal practitioners and are considered "cream of the crop" and is sworn to the higher courts and appear as an advocate for one or more parties in the higher courts.
            - Usually a solicitor is used to do the day to day running of the case (e.g interview witnesses, create affidavits, filings/paperwork) and the barrister will take an advisory role pre-trial and when it comes to trial it will be the barrister that will stand at the bar table and makes the submissions.
        - Agreed Fact will be create → all parties and barristers submitted to court in writing otherwise not contested in rest of court process
        - Fact in Issue → parties don't come to an agreement. Prefer agreed fact since as an expert you care about the cost of case.
    - Evidence in Chief
        - Crown gets to run the case first, call witnesses then call you to give "evidence in chief"

        - In trial you get 3 goes, first is trial in chief. First you will be led by the advocate generally your employer/client’s barrister.
    - Cross examination (usually in the court room, otherwise by video or telephone)
        - Led by other side’s barrister. Just prior to cross examination, if there is more than one advocate they will work out amongst themselves who can go first (usually the smartest, meanest barrister).
        - They can raise a number of points of evidence. First includes evidence of your credibility, are you a credible witness/person to be in the witness box to be giving the evidence you just gave.
        - They can also ask you questions that relate to clarifying the evidence that you gave as evidence in chief.
        - They can’t ask you questions about new things.
        - Can refer to report and your notes. Not allowed to communicate with the advocate who engaged you.
        - If you do not want to answer a question, Any advocate has to object (usually the one who engaged you).
        - Do not answer for a few seconds. **Wait 4 seconds** so that your barrister has a chance to object. Also tricks the barrister questioning you to think that you are thinking about an answer. Do this even for simple questions such as “what is your name?” etc.
    - Re-examination
        - The advocate that engage you can ask anything that was brought up in cross-examination. Can’t introduce new evidence. A good barrister will ask “is there anything else you think is relevant?”
    - GENERAL
        - Courts always take lunch break from 12-2 so the advocate will try and take this time to waste time in court. You cannot talk to your advocate til the next time.
        - Advocacy 101 (barristers are school don’t this in law school). Attack the evidence, otherwise attack the process otherwise attack the witness. If they are attacking your credibility, what do you do? You go great, i’ve done well in my cross examination and writing the report. DON’T take it personally, it’s a sign you are doing your job really well. The other thing is that many experts will fail in cross-examination because they are not familiar enough with their own evidence. You need to know your evidence back-to-front as the questions you will get will cause your head to be jumbled up. Don’t let your ego trap you! → This will make you answer questions out of your league.
- Factual and opinion evidence
    - Fact
        - Something the person saw, hear or otherwise perceived (sense with own senses)
        - Something that is self-evidence or common knowledge

        - Opinion
            - Hearsay → saying what someone else told you aka testimony given in court that is not allowed to be given by anyone else but by an expert e.g “she told me this happened”
            - Specialised knowledge based on the person’s training, study or experience
        - There is a grey area that relates to business records, tags and labels and electronic communications. These happen to be what we are often asked to ive evidence on.
        - Admissibility: Will the evidence be allowed?
            - This is the first hurdle 1. Fact in issue (during trial, only admissible) 2. Agreed Fact (before trial, only admissible)
        - Weighting: How persuasive is the evidence? If there are opposing views, which one will the decision-maker rely on?
            - Weighting depends on written report + testimony in court → often referred to as “the theatre of court”
    - Hearsay
        - Hearsay generally excluded.
            - Referred to as an asserted fact
            - A person has personal knowledge of the asserted fact if his or her knowledge of the fact was, or might reasonably be supposed to have been based on something that the person saw, heard or otherwise perceived, other an a previous representation made by another person
        - Relevant exceptions: business records, tags and labels, electronic communications
    - Opinion
        - Not admissible to prove the existence of a fact about the existence of which the opinion was expressed
        - Expert opinion is an exception
    - Evidence produced by processes machines and other devices
        - Is a fact unless otherwise proven. I.e unless evidence sufficient to raise doubt that the presumptions is adduced
    - Meaning of document → any record of information

PART2

- Relevant
    - Could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding.
    - Depends on the case and its circumstances. Includes
        - Credibility of a witness
        - Admissibility of other evidence
        - Failure to adduce evidence
        - Decision maker has broad discretion in deciding to admit evidence (or not), including provisionally admitting evidence.

- Reliable
    - The witness
        - Appropriately qualified for the evidence they want to give?
        - Truthful and unbiased
        - Compromised
    - The process
        - The administrative process
            - Lawfully acquired
            - Opportunity for spoilage or tampering → chain of custody
        - The scientific process
            - Appropriate training and experience
            - Equipment calibrated and operating correctly
            - Predictable
            - Repeatable
            - Can quantify errors
            - Broad practice base i.e used by peers, standardised
            - Supported by published research -- avoid vendor “research”
    - Sufficient
        - Is subjective and depends on the fact you are trying to prove and the particular circumstances, bearing in midn the standard of proof
        - Courts generally react badly who cast doubt through “mere speculation” e.g A hacker could have done it, The machine mightn’t have been working
        - Often limited by time/budget
            - Say so in the limitations section or your report
        - Consider having more than what is sufficiente.g
            - If you are relying on a record that is an ordinarily produced outcome, are you able to demonstrate the machine was operating properly and behind properly operated?
            - Can you produce the same outcome in a different way?
            - Is your thesis supported by your peers -- present the supporting research
            - SOMETIMES YOU JUST HAVE TO RELY ON THE SNIPPET YOU HAVE, HOPE YOU ARE PERSUASIVE AND LET THE CIRCUMSTANCES FALL INTO PLACE
    - Persuasive
        - Experts have to overcome somewhat sceptical decision-makers
        - Barristers and judge can be demanding, time-poort and somewhat direct and have limited understanding of technology.
    - Export Report Useful Format
        - Table of contents
        - Preliminaries
        - Instructions and Scope

        - Summary
        - Main Body
        - Declaration
        - Signature
        - List of Attachments

Some tips on style and writing

DO	DON'T
Be clear about what is fact and what is opinon	Use jargon or complicated explanations - If you can't explain it simply, you haven't mastered the subject well enough
Write clearly, simply and in the first person - If you are supervising or working in a team, be clear about who did what	Skip over steps and arrive at a conclusion - Someone in a jury may know more about something that you expect
Write step-by-step and chronologically - Consistently with contemporaneous note	Be argumentative or attack the other expert(s) - Lay out your argument on its merits
Write using logic and critical reasoning - Decompose, answer each bit, synthesise your thesis - Lead the reader on a journey of understanding	Insist that you are right - "I don't know" should be used more often - "I was wrong and now I believe … because…" can be used to re-state a position → at the particular time that is what I believed, but now I have had the opportunity to do more examination and now I think something else
justify , justify, justify - Why did I choose that method, tool, etc.	

- Expert's given some privileges
    - Not expected to know the rules
        - Advised by instructing Counsel
        - Knowing the rules adds to your credibility
    - Allowed to stay in Court and listen to other evidence
    - Allowed to advise Counsel
        - Except when under examination
    - Allowed to address the Court (through judge)
        - Includes pre-trial and access to documents
    - Some of Court's privileges are extended e.g copyright exemption

        - Use with discretion and ONLY for the Court purposes (may not include your own pre-trial examinations)
- Expert's responsibility
    - Confidentiality
    - Responsibility to the court
    - Respect privileges
    - Limited to instructions

PART 2 - TECHNICAL

- Time Synch issues
    - Ask for a full months of data to determine whther format is in dd-mm-yyyy and mm-dd-yyyy
- Daylight savings!!!
- Windows versus unix/Mac time

- What things would you want to prove for?
    - Human generated document i.e a recording foo human input
    - Computer generated - generated without the intervention of a human
- The registry
    - Is a fancy name for a set of configuration files
    - SEE SLIDES FOR MORE DETAILS (WEEK2 PT2)
    - VOLATILE REGISTRY (IN MEMORY)
- Reference the source. Try and reference the software e.g Microsoft for Windows
- Log files need to be interpreted. Key logs include:
    - Application
    - Security
    - Ssmte
    - Application and service logs
- DETAIL IS IMPORTANT
    - Should take on face value. Small changes in detail indicate further enquiry
        - A missing event indicates something odd is happening
        - A mismatch between sequence (EventRecordID) and Time indicates change to a system clock
- Anti Forensics
    - Four common categories
        - 1. Avoid recording i.e recording the wrong things; using services knowing recordings aren't made or are to be hard to get;
        - 2. Hide recordings
        - 3. Expunging (deleting) or destroying the recording
        - 4. Changing the recording
- Avoid Recordings
    - Use of public computers and public wireless
    - Steep increase in use of secure email

    - Change identifiers (use of VPNs, change MAC); being built-in to consumer products in the name of privacy e.g Apple now scramble browser signature
    - Use of these services might indicate something to hide. Might also indicate the person values their privacy. A give-away might be when they start using a service or selectively use a service.
- Hide recordings
    - Use code sand encryption. Low tech is favoured by drug dealers, jihadists, etc.
    - Use encryption to hide in plain sight e.g steganography, multiple containers, etc
    - Hide in play sight e.g draft of email but don't send
    - Physically hide e.g use of detection dogs

PART 3 ASSIGNMENT

- Single pdf!!!
- Not going to be assessed on preliminaries → but write something relevant to you
- 6-10 pages mark. Be clear.
- 3-4 hours to do the examination the sample examination
- 3-4 days working full time to write the report.
- Wireshark, network miner and solarwinds
- E.g An MD5 hash is the result of a standardised cryptographic algorithm i.e mathematical forumalue etc.
- Part 2 → take one of the two positions put forward an eloquently argue your position
    - → max 4 pages
    - → appropriate referencing e.g Harvard Style Referencing
- When writing an experts report, use AGC citation is recommended but not forced.

Week 3

General Forensic Concepts

Forensics comes from the Latin word forensis meaning "in open court" or "public"
Forensic science is the application of a broad spectrum of sciences to answer questions of interest to the legal system. The study and application of science matters of law.

Locard's Principle

- Developed one of the earliest systems of documenting personal evidence on criminals
- First time police started using scientifically rigorous methods to solve crimes

Computers turn this on its head

- A "trace" is only created if a computer is designed to record and store it
- The trace is the observing computer's interpretation of the interaction
    - Some things that are interpreted (sometimes wrongly):
        - Number Format
        - Character set and language
        - Time
        - Etc.

    - It is the computer's interpretation of the interaction

Principles for dealing with digital evidence

International Organisation for Computer Evidence (IOCE)

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. Where changes occur during any of the phases of digital forensic process, the nature, extent and reason for such changes shall be properly documented
4. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose
5. All activity relation to the seizure, access, storage or transfer of digital evidence must be fully documented, reserved and available for review
    a. E.g recording yourself doing the examination with commentary
6. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession/ custody.

- IF CHANGES ARE ABSOLUTE NECESSARY, MAKE SURE YO JUSTIFY THE CHANGE AND EXPLAIN HOW IRRELEVANT THE CHANGES ARE TO THE CASE OF HAND.

Definition of Digital Forensics and Network Forensics

LOOK AT SLIDES TO FINISH

Network Forensics

- The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned
    - Related to unauthorised activities but not directly related to criminal

DFRWS - Network Forensic Challenges

- Time
- Performance
- Complexity
    - Tools across multiple environments
    - Correlation
- Collection
    - Who when and what
- Paradigms
    - Intelligence, network operations, law enforcement
- Collaboration
- Legal Hurdle
- Emerging Technologies

Guidelines for Evidence Collection and Archiving

- Order of volatility → directs urgency of work when taking evidence. Direct efforts at getting most volatile evidence first. Rest you can take your time with.
    - Registers, Cache
    - Routing Table, arp cache, process table, kernel statistics
    - Memory
    - Temporary file systems
    - Disk
    - Remote logging and monitoring data that is relevant to the
    - System in question
    - Physical configuration, network topology
    - Archival media
- Legal Considerations
    - Admissible
    - Authentic
    - Complete
    - Reliable
    - Believable → should be more than believable, should be persuasive

HB171 - Guideline for Management of IT Evidence

- Six Stages
    - 1. Design for evidence
        - Important as it will only sense and store the interaction if you design for it.
    - 2. Produce records
    - 3. Collect evidence
    - 4. Analyse evidence
    - 5. Reporting and presentation
    - 6. Determine evidentiary weight

Forensic Examination of Digital Evidence

- Process:
    - 1. Policy and Procedure Development
    - 2. Evidence Assessment
    - 3. Evidence Acquisition
    - 4. Evidence Examination
    - 5. TODO

PART2 - WINDOWS MEMORY FORENSICS

- Windows memory forensics
- Instructor-led exercise

- Is typically practiced as part of incident response and usually relating to malware
- Is also used for extracting credentials

- Extract secrets from pagefile.sys and hibefil.sys
    - Windows passwords
    - Truecrypt and Veracrypt
    - Password managers
        - KeePass
        - OnePassword
        - LastPass
    - Grab TOR browsing i.e DarkWeb

- T

Week 4

DID NOT DO NOTES LOL

Week 5

.PLIST files are equivalent to windows registry.
They contain settings, parameters associated with applications. They can be application specific.
Can have web browser history or safari.
Usually in XML or Binary but can be found in JSON.
Can include passwords, password hashes and binary data.
Passware is commercial password cracker ($2000)

APPLE FILE SYSTEMS
HFS → hierarchical file system
HFS+ → hierarchical file system plus; can be used with FileVault2
APFS → Apple file system; native support for full-disk encryption and single or multi-key file encryption;

HOW AFPS differs from HFS/HFS+

- Adds support for single or multi-key file based encryption
- Supports point-in-time snapshots
- No support for fusion drives (hybrid magnetic disk and SSD)
- No support for NVRAM (RAM disks)
- Limited or no support by some DF tools

T
Controlled operation, warrant → cannot lawfully access cloud. Can access device with free reign. Can apply to a court.
Section 3la of SOME ACT. Can sometimes under commonwealth can get password. (ASSIGNMENT).

Forensic Explorer

Week 6

PART 1

In the assignment, refer to Johnny as Johnny Coach or the accused. Never refer to them by full name unless you know it is that person. Never refer to a suspect using words like suspect. Can refer to victim using victim. Use the descriptor in the charge-sheet. Can be called person of interest, sometimes called accused. Use the label on the formal paper work (on police side). If you are an independent expert, shy away from this, Ajoy thinks it gives you more credibility to call it as you see it e.g Johnny Coach first time with Coach in brackets, then shorten it down to Coach.

In the assignment, refer to the computer as Coach's computer. If you don't know who used the computer, refer to it as "the computer I am examining".

PART 2

Network forensics

DFRWS -- Network Forensic Challenges

- Time, performance, complexity (tools across multiple environments and correlation), collection (who, when and what), paradigms (intelligence, network operations, law enforcement), collaboration, legal hurdle, emerging technologies.

Common interactions to be analysed

- Ip packets
- Email
- Telephone and sms
- Non ip protocols e.g zigbee, modbus
- "Old" protocol e.g SNA, X.25, etc
- Sneaker and other "dark nets"

A word of warning. When using cloud-based tools, understand their terms of service and how they affect your responsibilities as an expert:

- Must keep any materials provided to you confidential;
- The court's copyright exemption does not apply to your own pre-trial investigations.

Use graphiz

DONT WORRY ABOUT PART B ON IS $10000 AN APPROPRIATE PRICE.

DON'T FORGOT BASIC PROCEDURES SUCH AS HASHING THE EVIDENCE WHEN YOU GET IT.

PART 3

Lab explanation

Week 7

Supreme Court vs Federal court

Federal Court → become an expert by being qualified in their area of expertise, training and specialised knowledge. Need to be qualified, not just explanation. Because you studied

something, doesn't mean that you are an expert by default. Need study, experience (work in an area of field) and specialised knowledge (Certifications, industry recognition). Passionate, qualified, time.
Experts can NOT be bias.
A single draft may be appropriate to your party, but subsequent are not → afraid of lawyers grabbing informal drafts than firing you and pretending they never got a final report

Greater than 10 pages, write executive summary at top of report

Assumptions of reliability on dates and times
I am an independent of the parties in these proceedings
My opinion is based solely on the information set out in this report. I reserve the right to amend any conclusion if necessary, should any further information become available

In the box, usually not allowed to take anything other than the report. No notes, sometimes no pen, etc.

Let the barrister ask to full question, don't preempt!!!

Hotubbing → two people in the box

Week 8

Without a warrant - cannot authorise illegal access —> The court does not have discretion to admit evidence on the basis of natural justice of public interest

The person or entity that legally owns the phone is the only person who can authorise access to the phone, except if access it illegal

The entity that owns the device on which the data is stored can access the data e.g apple OR police when they are conducting a search warrant

Owner of phone cannot authorise illegal access COURT CAN ADMIT ILLEGALLY OBTAINED EVIDENCE although everyone would rather avoid this

Stored communication is an email stored in an email box and has yet to be read.Once it has been read it stops being a communication and can be dealt with as any other piece of data.

Onus of proof —> it is on the party seeking to establish that outcome produced by a process, machine or device is unreliable.
Once they object and demonstrate one or any problem, the onus flips.

CCRs are considered particularly sensitive documents —> Ajoy usually gets them because he is advising one side or the other on a court case —> based on billing data not calling data

Week 9

Phones from victims were mostly jailbroken in domestic cases things because their abusive partner/spouse/etc was installing commercially bought spyware on the phone which would essentially jailbreak the phone.

Ids can't be used to validate a particular entry should be before or after an event. Cellebrite just adds it in, it's not actually on the phone.

Week 10

Just, fair and timely is the most important

First section windows vm 1.5-2hrs
Second section kali vm
gi

Tutorials

Week 1

NOTES FOR USING DD

- If = input file
- Of = output file
- count =N copy only N input blocks
- E.g sudo if=/dev/n count=33
    - Sudo dd if=/dev/sdb of=adam
- convs=CONVS
- Gzip -k
    - -k maintains the original file
- Split -b 50M whatever.img.gz USBkey.o -d

- Mount whateveriwant

Lsblk → to look at files on linux
Made a forensic copy

- We split the copy into smaller parts so that we can burn them to smaller hardware e.g a 1TB drive can be burnt into multiple smaller discs and sent to the lawyers.
- The hash computed on each individual split is to verify any copies of these splits to check they have not changed, however, you can not verify the integrity of the whole thing until you piece it back together.

Week 2

Umount to unmount

Scalpel 32 → land rover
recoverjpeg 34 → land rover
Photorec nope

Tool	Photos on test image	Photos successfully recovered		Unusable files recovered (false positives)	
-		Number	%	Number	%
Scalpel (for each tool, note down the switches used)	57	60	100	0	0
Photorec	35	30	85.71	5	14.28
Recoverjpeg	60	60	100	0	0
Foremost (-T)	65	65	100	0	0
PhotoRescue	65	65	100	0	0
Magicrescue (USBkey.img -d output_2 -r jpeg-jfif)	64	64	100	0	0

Assignment
Pcap = packet capture
Https → body/text part would be encrypted.
Right click packet, follow, HTTP Stream → to see stuff
Analyzing a pcap file

Lab
To mount NEDE TO HAVE AN EMPTY FOLDER
Lsblk
→ sdc (standard drive c)
Sudo mount /dev/sdc1 adamt
Sudo unmount adamt

Can mount in readonly
Sudo mount -o ro /dev/sdc1 adamt

IN KALI VM
Ext
~~File command~~
Config file → magic number

Ext3 → usually linux file system. Doesn't have concept of file system.
Linux doesn't care about file extensions, they only care about magic bytes (usually first few bytes and sometimes last file bytes)

Scalpel
Search through data file and look for magic bytes or ending/trailing bytes and try to carve the file.

Week 3
Goal is to extract the malware and do analysis using volatility.
Look for url to banking app or things like this using "strings".
Imageinfo is equivalent to the "file" command e.g volatility -f cridex.vmem imageinfo
Service package → different version of windows → suggested profile(s)
KDBG → kernel debugging block → will have the version somewhere inside

Pslist looks for process structure in kernel memory and trust that list → faster
Pscan will scan all of memory for things that look like processes. Using this you can find dead process, excited but still in memory or hidden → more intrusive
E.g volatility -f cridex.vmem --profile=WINXPSP2x86 pslist
Note svchost is a default windows process. The parent should be services.exe

E.g volatility -f cridex.vmem --profile=WINXPSP2x86 psscan

E.g volatility -f cridex.vmem --profile=WINXPSP2x86 pstree

E.g psxview, sockets (shows open sockets -- what process opened it), connscan,

Dodgy as explorer.exe pid has open connections. Equivalent to notepad connecting to russian. Explorer should not open a port. Another process should open a port and communicate with explorer. Analogy is like a sea port, boats connect to the ports to exchange goods, not directly to the harbour.

E.g cmdline

Csrss.exe has a log of stuff. CMDLINE looks at this to determine what commands have been run.

Dodgy, opening adobe reader from commandline. Who the f does that. Need to extract this.

KRIS' TUTORIAL

Volatile

Processes

- Metadata
- Stack
- Heap
- File Handlers

Data

- Credentials
- Keys e.g api keys, encryption keys

Kernel

Structures

Pslist list

psscan

psxview

Ports should be one to one.

1037 port doesn't have socket. Suspicious. Connection but no socket?...

FINAL COMMAND

```
Mkdir temp
Cd temp
Volatility -f c../ridex.vmem --profile WinXPSP2x86 procdump -p 1640 --dump-dir .
```

Looks at the process, memory location and dumps the memory

```
Ls
```

```
Volatility -f c../ridex.vmem --profile WinXPSP2x86 memdump -p 1640 --dump-dir .
```

Pulls out executable and memory for executable

```
Strings <the mem file>
```

Strings <executable>

bulk_exctractor

Week 4

Usb
Cloud
Email
Virus
Windows, system32, config, system → mounted devices
Look at dates
E drive is most dodge because C is usually a hard drive and anything else plugged in goes alphabetically up. Last accessed means around 21st was the last access time (anything before this is unknown, USB could be plugged in multiple times before as well). E drive say removable media.

Figure out what app was used e.g thunderbird, mail (mac), outlook (windows)
Local settings → Application Data → Microsoft → outlook → outlook.pst and outlook.pst-slacl

→ right click outlook.pst and extract
→ can see webchat was used (AOL)

mv outlook.pst pst

File outlook.pst
Readpst outlook.pst

KRIS' TUT
Large unpartitioned space
Slack Space
Logs
Registry → config for the system stuff e.g kernel
Email history
USBs
Credential related
Browser History
Starbucks public wifi

Web history → in extracted content
Email-messages in default
View emails

Programmers → into search history excel spreadsheet m57biz.xls
0'd out change time → suspicious (or it could be corrupted)

“Yes I got this email” created same day 2 hours earlier than file was created but no record of the actual email was sent.

SOLUTION
vol2-->document and settings → jean → desktop
Jean → local settings → application data → microsoft → outlook.pst
(one of these has an md5 in it?)

Use encase forensics
“Thanks for the file, I’ll handle
Once again, please don’t tell anyone about this”
2008-07-21 11:17:54 AEST modified time → someone passed it on and then on from someone else again. Tuckgeorge 253???

224 → tuckgorge aliases himself as Alison’

WHEN DID JEAN CREATE THE SPREADSHEET?
Desktop → 11-28
EMAIL → 2008-07-20 11:28 AEST

HOW did it get to ao competitors account?
Email to tuckgorge

I’m sorry to bother you, but I really need the information now

Alison, 18th July speafishing 6:05-6:13

Someone’s posing as Alison, Alison asked Jean to send to her, forwarded to Tuck Gorge
QQbubbles installed at around the same time that the email was sent

Analysis of the users internet explorer and firefox does not reveal anything
Files installed, usbs, etc.
System devices → usb

Week 5
/private/var = mac system files e.g system keychain, user info in plist
/private/var/db = will have plist files
Ds local, nodes, default
Shadowfile = hashed password?

Users/Michael/keychains/login.keychain
FSEvents = file system events

Home was mounted → computer turned on
Accounts email

Exif metadata → you have a photo, metadata on location or time taken
System.keychain
Systemkey → unlocks keychain file above
Login.keychain → logins /users/username/library/keychain/???
8ae8 → afb9

Python2 chainbreaker.py -f _____ -k 8ae8_______

1. user s/michael/safari/history.db
2.
3.
4.
5.
6.
7.
8.

KRIS' STUFF
Users michael library application support
Tools → timeline
private/var
ASSIGNMENT SAMPLE

Week 6

ADAM' STUFF

Pcap is like a really in-depth packet capture that captures everything. Takes up a lot of disk as a result (big). Netflow stores very minute amount of data instead of all data to get an overview of network. PCAP is really little breadth because can't store a lot but has a lot of depth since it stores really details info. Netflow is like the opposite.

Dabber → honeypot to jebait malware. All network can be assumed to be malicious.
Sasser → Dabber would find machines exploited by sasser and exploit this malware and then exploit sasser to download itself.

Open dabber file in wireshark.

How many computers were infected? Search for that here we will find something: scan for specific port in the filter “tcp.port == 5554 and data” → right click and follow stream
“tcp.len == 1” → gives all the “D”s
“ip.src == 70.237.254.204 and tcp.flags.ack == 1 and data and tcp.flags.push == 0” → gets all the acks → one of them looks like a noop sled so probz shellcode → copy as raw escaped string to see.
WRITE DOWN THE DESTINATION IPS.
Will start listening on 8967 so filter “”

Trying to get rid of all the noise.

Promiscuous mode = mode where they just listen instead of connecting to something.

KRIS’ STUFF
APACHE

```
ls /var/log/apache2/access.log
tail -1 /var/log/apache2/access.log
Ls /var/www/html/nfsen

cat commands.txt
```

4 infected computers.

ASSIGNMENT
Definition of 146 what does it do how does it shift the burden
Accuracy of tools 2? E.g autopsy, scientific evidence e.g these are the files that were never discovered. Data leaving chain of trust. Jailbreaking phone can be an issue. Lawyers are also law enforcement as well as police. Protect and serve - fed police? Police are out to get you, expert is bias - independent expert. In the best interest for police to be on the prosecution side than the innocent side. E.g speed cameras, out to find bad guys and KPIs
Cases 2-3 cases before and after - some findings

Week 7

GIS = geographical information system
QGIS → instruction to setup is on docs
Xyz tile, openstreetmap (to download, go to plugins and download open street maps)
layers→ add layer → delimited text (put in csv file dwlded from mymaps) → geometry crs WGS 64 → user spatial index → press add
Vector → gemoetry tools → distance matrix → input unique id field = NAME, target unique id filed = NAME

Earth’s round → can’t measure straight line distance so QGIS gives you distance in degrees. Multiple by 110 to convert to metres.

Not use google maps for a real case → not as accurate e.g China → not accurate as satellite random offsets

KRIS’ TUTORIAL
720m
880m

Week 8

VOLATILITY
NETWORK FORENSICS
Probs not disk forensics
Bill date, mobile number, time, origin, number dial, total
Number, convert all to plain text

LachlanJ
Qwerty1234

```
Graph {
0418782572 -- 0418174231 [penwidth=1.5];
}
```

Replace origin town with lat and long —> MAP OUT LOCATIONS OVER TIME
QGIS —> layer, add layer, add delimited text layer, select csbv file, set point coordinated LAT, LONG

SIGNAL = END TO END ENCRYPTION

Week 9

T

Week 10

T

5114062 → tutor Kris

2:30pm, IP is 129.94.8.71, Google Chrome
Where does James Bond live?
What is Moneypenny’s first name?
are ms moneypenny and mr bond married

is ms moneypenny well off
what cars does mr bond own