UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

# COMP6445 – Digital Forensics

Term 3 2019 - Week 8

5 November 2019

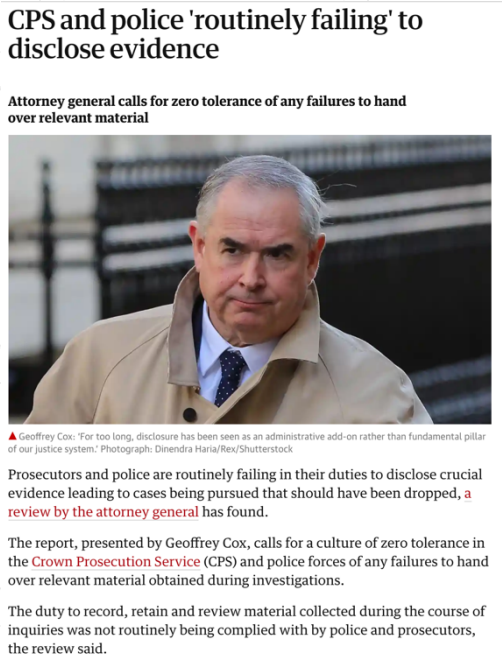
# Agenda

1. iPhone (and iPad)
2. Android

3. Demos
    1. Andriller demo
    2. Cellebrite UFED (tomorrow's tutorial)

We will not be exploring physical data extraction e.g. JTAG, chip tapping, chip-off, etc (computer engineering activity)

- Data on/from/about phone is part of what needs to be “fused”
- An investigator is expected, to make reasonable efforts to discover incriminating and exculpatory evidence
  - Courts have come to have an expectation that common digital forensic capabilities are reasonable, especially for Police and agencies
- Most jurisdictions have rules regarding disclosure for both criminal and civil cases
- An expert is expected to be able to explain mobile phone evidence and persuade a decision-maker



CPS and police 'routinely failing' to disclose evidence

**Attorney general calls for zero tolerance of any failures to hand over relevant material**

▲ Geoffrey Cox: 'For too long, disclosure has been seen as an administrative add-on rather than fundamental pillar of our justice system.' Photograph: Dinendra Haria/Rex/Shutterstock

Prosecutors and police are routinely failing in their duties to disclose crucial evidence leading to cases being pursued that should have been dropped, a review by the attorney general has found.

The report, presented by Geoffrey Cox, calls for a culture of zero tolerance in the Crown Prosecution Service (CPS) and police forces of any failures to hand over relevant material obtained during investigations.

The duty to record, retain and review material collected during the course of inquiries was not routinely being complied with by police and prosecutors, the review said.

news.com.au The news in colour news.com.au

National | World | Lifestyle | Travel | Entertainment | Technology | Finance | Sport

real life news life

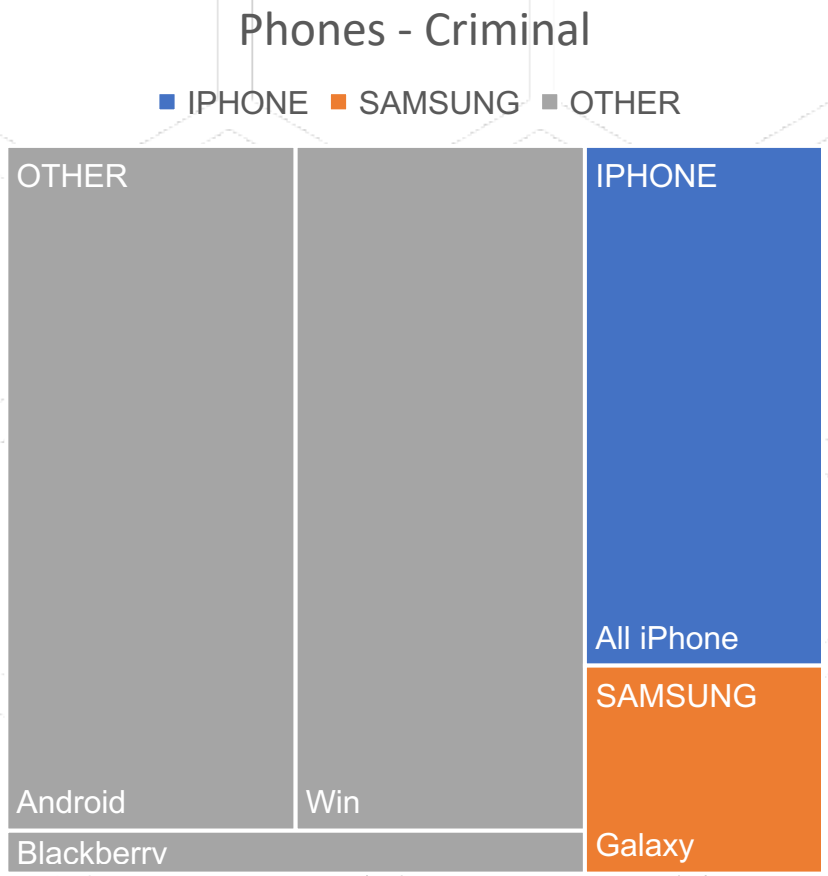
**British detectives in hot water after second rape trial in one week collapses**

ANOTHER young man accused of rape has been freed after it was revealed police withheld texts that proved his accuser was “a liar”.

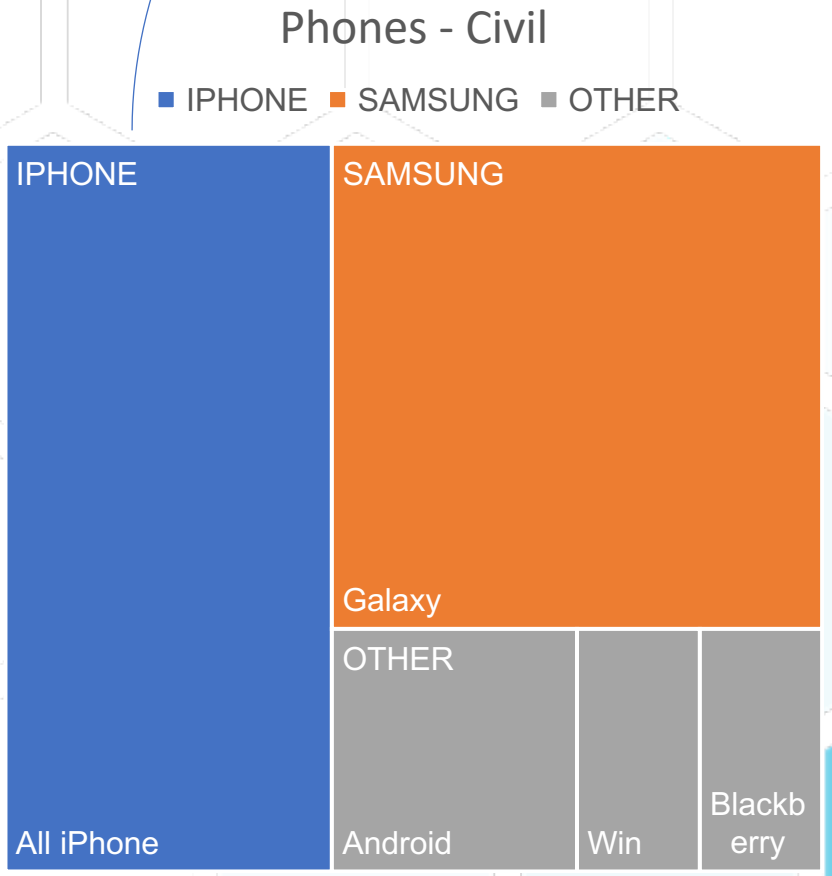
Marnie O'Neill @marnieoneill7 news.com.au DECEMBER 21, 2017 7:35AM

See https://www.theguardian.com/law/2018/nov/15/cps-and-police-routinely-failing-to-disclose-evidence and https://www.news.com.au/lifestyle/real-life/news-life/british-detectives-in-hot-water-after-second-rape-trial-in-one-week-collapses/news-story/c6ead61baca83a02e954964513ff6b0a

# Types of phones



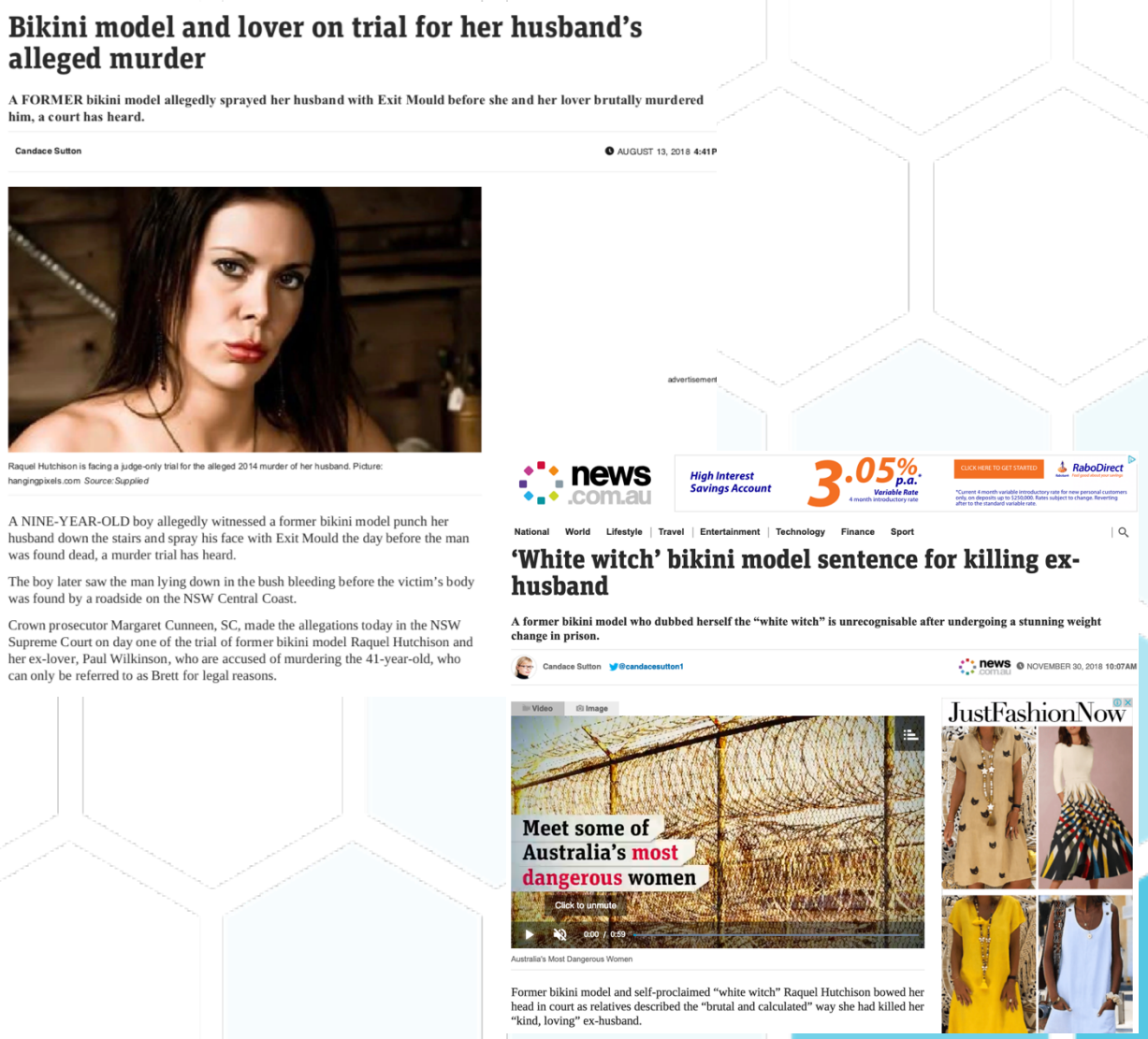

Only 2x iPhoneX and many iPhone 4 and 5 which reflects 2+ year lag for civil litigation and lawyers putting phones away for later




Data from my practice across 2018, rounded to nearest 5%. Matters finished in the year. Excludes 1x corporate eDiscovery in which all phones were iPhone and another where they were all Nokia Lumia (WinCE)

# iPhone (and iPads)

- iTunes Backup
  - And then extract artefacts
- Logical extraction
  - PhoneView, iPhone Explorer, etc
- Physical extraction
  - Jailbreak, connect to shell, dd copy
  - Haven't seen it work properly on iOS 12
    - Tools such as Elcommsoft claim to do it[1]
  - Still not uncommon to have to forensically examine phones where this does work[2]



**Bikini model and lover on trial for her husband's alleged murder**

A FORMER bikini model allegedly sprayed her husband with Exit Mould before she and her lover brutally murdered him, a court has heard.

Candace Sutton — AUGUST 13, 2018 4:41P

Raquel Hutchison is facing a judge-only trial for the alleged 2014 murder of her husband. Picture: hangingpixels.com Source:Supplied

A NINE-YEAR-OLD boy allegedly witnessed a former bikini model punch her husband down the stairs and spray his face with Exit Mould the day before the man was found dead, a murder trial has heard.

The boy later saw the man lying down in the bush bleeding before the victim's body was found by a roadside on the NSW Central Coast.

Crown prosecutor Margaret Cunneen, SC, made the allegations today in the NSW Supreme Court on day one of the trial of former bikini model Raquel Hutchison and her ex-lover, Paul Wilkinson, who are accused of murdering the 41-year-old, who can only be referred to as Brett for legal reasons.

advertisement

news.com.au — High Interest Savings Account 3.05% p.a. Variable Rate 4 month introductory rate — CLICK HERE TO GET STARTED — RaboDirect

National World Lifestyle | Travel | Entertainment | Technology Finance Sport

**'White witch' bikini model sentence for killing ex-husband**

A former bikini model who dubbed herself the "white witch" is unrecognisable after undergoing a stunning weight change in prison.

Candace Sutton @candacesutton1 — news.com.au NOVEMBER 30, 2018 10:07AM

Video Image

Meet some of Australia's most dangerous women

Click to unmute

0:00 / 0:59

Australia's Most Dangerous Women

Former bikini model and self-proclaimed "white witch" Raquel Hutchison bowed her head in court as relatives described the "brutal and calculated" way she had killed her "kind, loving" ex-husband.

JustFashionNow

1. See https://blog.elcomsoft.com/2019/02/physical-extraction-and-file-system-imaging-of-ios-12-devices/
2. For example, see appeal trial of Raquel Hutchinson in 2019 - iPhone was seized in 2014
3. https://www.news.com.au/national/courts-law/white-witch-bikini-model-sentence-for-killing-exhusband/news-story/a5776d16277e3c91269408b9e14e6103

# iPhone Backup

- Discover iPhone backup on computer, storage or iCloud (subpoena Apple)
- Create iPhone backup onto a pre-prepared forensic workstation
- Many tools to view and save artefacts
  - My tools of choice are Reincubate iPhone Backup Extractor on Windows and Phoneview on Mac
  - iExplorer is also popular
  - Also built in to Forensic Explorer
  - Ensure they allow extraction and copy of source SQLite databases
  - Nice to explore/recover deleted data
  - Nice to export as CSV


Being able to show that others are using the same software can assist in persuading the Court that the process was reliable

Be able to explain how it does this and why the recovered data is reliable

See https://reincubate.com/iphone-backup-extractor/

# Key artefacts

- .sqlite, .sqlitedb or .db

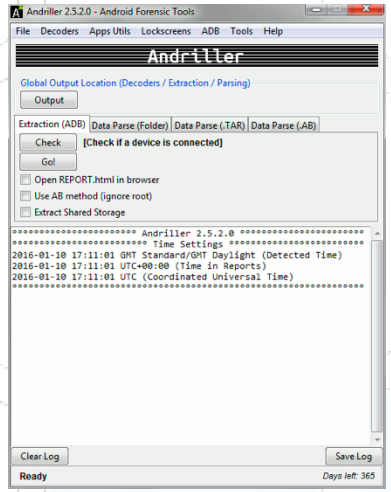
- accounts3, truststore
- addressbook and addressbookimages
- calendar, extras and notifications
- callhistorydb – a set of data
- notes
- bookmarks (safari), mobilesafari history
- sms – sms,mms, facetime
- voicemail
- photos – photos/videos themselves in DCIM folder
- locationd – a set of data
- cellularusage, datausage
- + applications specific databases

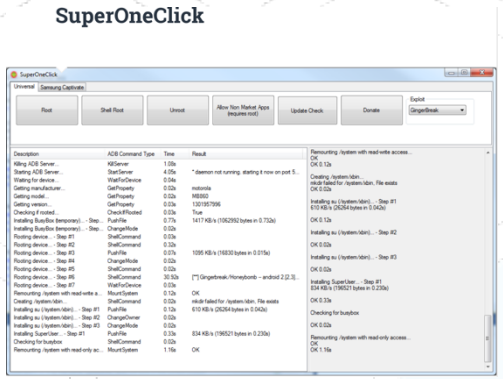
- Forensic software have tools to parse iOS artefacts
  - Mobile phone specific
  - Encase, FTK, Forensic explorer, etc

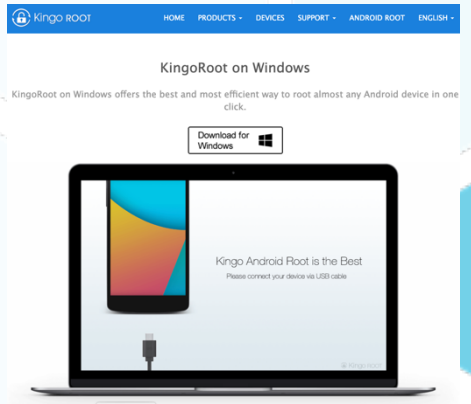
- Cheap and open-source tools
  - Tools for viewing/extracting backups, typically in $50-300 range (noting correct license i.e. not personal use)
  - Open source e.g. Santuko Linux

# Android Phones

- Connect to the phone
  - Android developer/debug bridge (ADB)
  - Toolkits
- Root the phone
  - Give access to data
  - Framaroot, TowelRoot, ActiveRoot, KingoRoot, or SuperOneClick
- Copy the data thru shell
  - Partition (e.g. dd)
  - Selected artefacts
  - Use tool such as Andriller



# Key artefacts

- Usually .db
- Brand and sometimes model specific

- Common ones:
  - mmssms
  - Telephony
  - Contacts, contacts2
  - Photos, pictures
  - + application specific
    - E.g. /data/data/com.android.chrome
  - + in cache

- Remember that many are Google apps and data may be stored there

- Root android phone and use root explorer

- Backup to cloud
  - Most manufacturers have backup using their own “account”
    - E.g. Samsung, HTC

- Backup software
  - Samsung Kies or Smartswitch
  - 3rd party Easy backup and Titanium are popular

# Phone forensic software

- Allows extraction and analysis
- Popular commercial
  - Cellebrite UFED
  - MSAB XRY
  - Encase mobile investigator
  - Oxygen Detective
  - Axiom Magnet
  - Elcommsoft
  - Blackbag Blacklight

Police tools of choice

- The manufacturer worries about data consistency, reliability and providing up-to-date jailbreak or root

- Need to decide whether you are going to rely on output of a process, machine or device
  - Even so, can you withstand a challenge by an expert engaged by the adversary?
- I make a habit of using two tools:
  1. The same as used by the other expert;
  2. A different one

⇩

Arrive at the same result (reliable) or explain the differences (reliable) or use as evidence of unreliable evidence

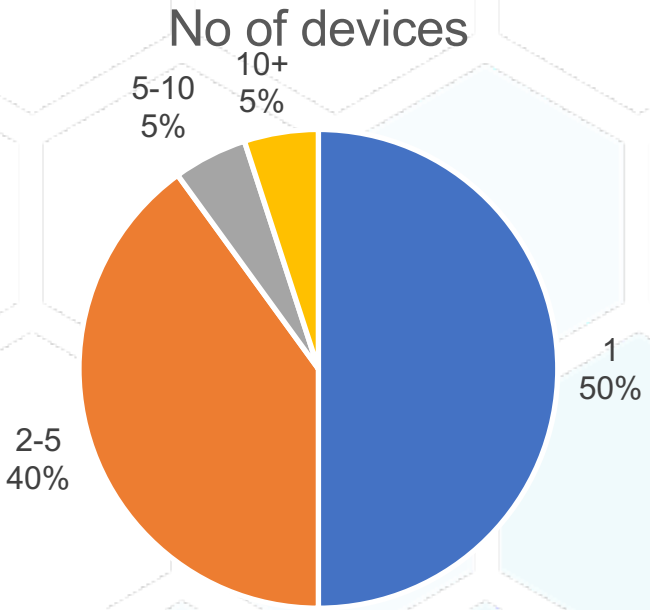
# The challenge is many phones

- Typical investigation has multiple phones – and multiple phone types
  - Corporate ediscovery may have the same type

- Challenge is data consistency
  - Data elements
  - Meaning e.g. message
  - Format e.g. time

⇩

Spend a lot of time working out why something is missing or doesn't match




Data from my practice across 2018, rounded to nearest 5%. Matters finished in the year. Excludes 2x corporate eDiscovery each with 100+ devices of the same type

# Establishing your credibility

- How do you establish your credibility as an expert to be able to give testimony regarding the contents of a mobile phone?
- How do you demonstrate that your process was appropriate and produced a reliable outcome?
- Some use pro-forma statements or copy a previous report
  - Most Police and consultants e.g. KPMG, PwC, Delloitte, etc

Example from NSW Police (same in many of their statements):

1. ….
2. I am certified by the NSW Police Force to operate the Cellebrite Mobile Forensic Extraction Device. This device enables the operator to identify, copy and present data stored on mobile devices.
3. Prior to commencing the examination, I checked the Cellebrite UFED Logical Analyser software version and Cellebrite UFED Touch Logical Device firmware version. I observed them both to be the most up to date versions. I checked and adjusted the UFED Logical Device time and date settings against a known accurate time source being the World Clock website www.timeanddate.com
4. ….
5. On completion of the extraction of the reports I verified a representative sample of the reports contents against the directly observable contents of the handset. I am satisfied the machine generated report is an accurate representation of the handset contents in relation to contacts, call legs, instant messages, SMS messages, MMS messages amongst other collected data

The examiner was unable to say what "the most up to date" version of firmware was

The examiner was unable to say how many items were sampled and how he selected the sample

"Legs" instead of "Logs" has been in several statements from different people

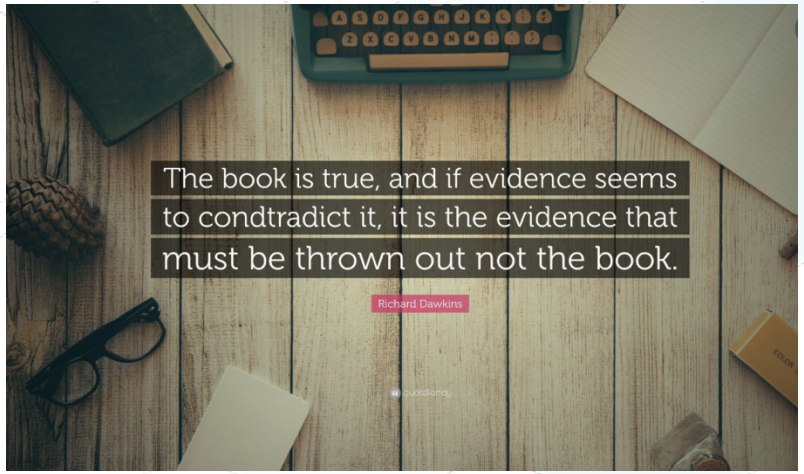
# Spoiling or tampering with phone evidence

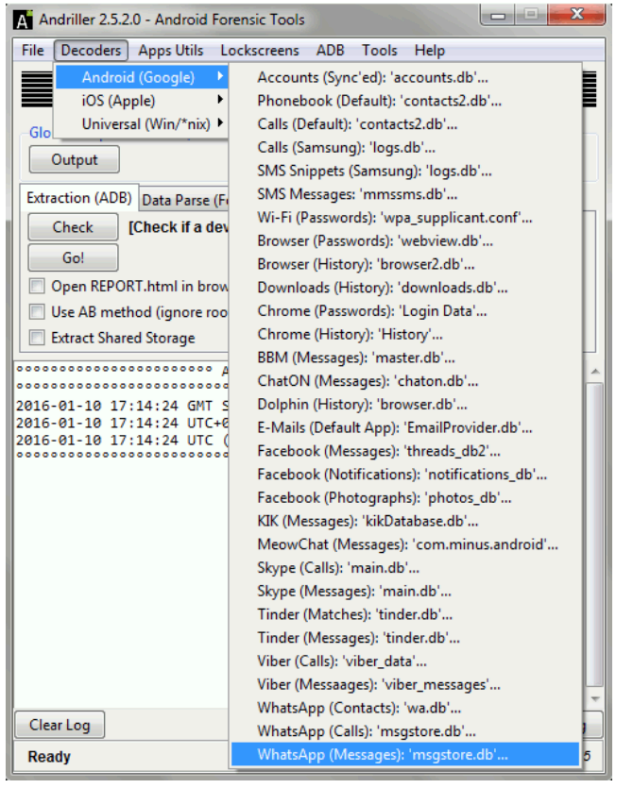
- Deletion is common
- Editing photos is common
- Use of VPN is becoming increasingly common
- Fake messages
- Fake sender/recipients
  - Commonly be editing contacts
- Asserting location is common (someone else has the phone)

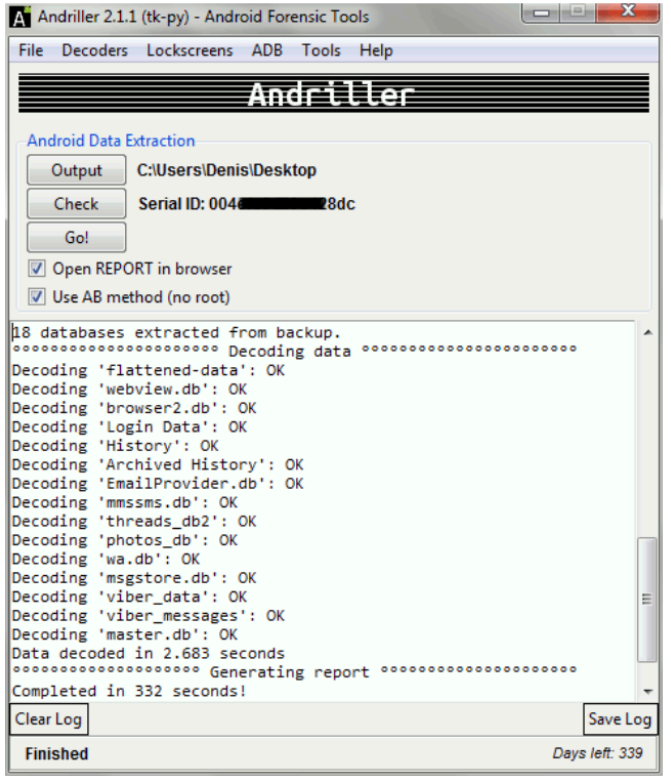
- Once by editing a backup and then restoring

- Spoiling at time of seizure or during storage is by far the most common
  - Fumble fingers
  - Don’t realise they are overwriting key data

- Spoiling by an examiner is also common




# Instructor-led activity

Use Andriller to extract and analyse an Android phone

# Your tutorial/lab tomorrow

Use UFED to perform an extraction and view results