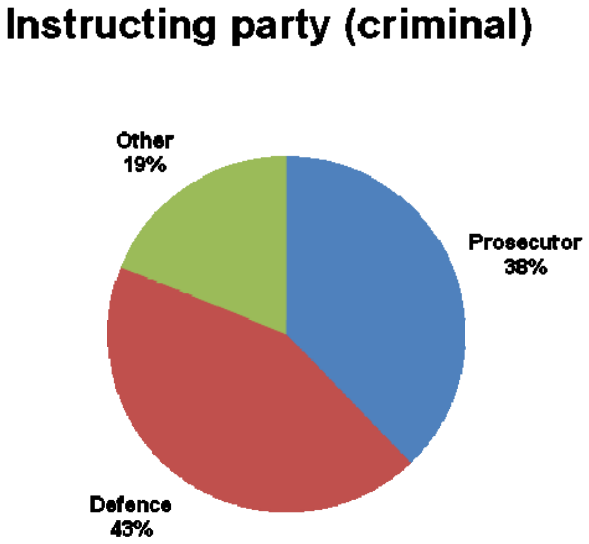
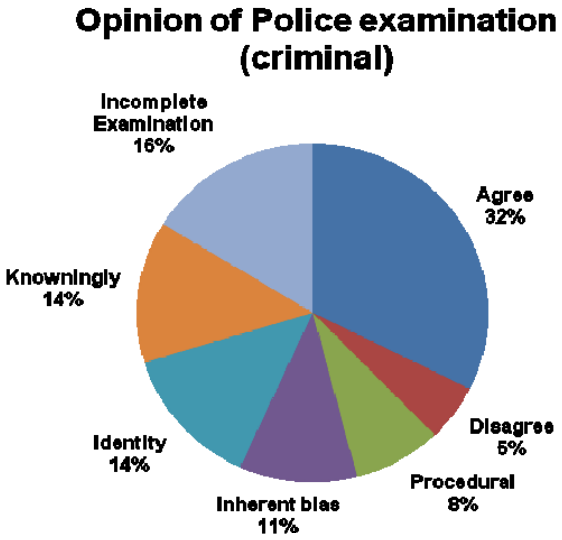
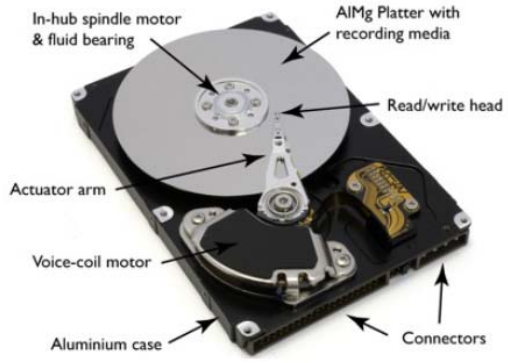
Statistics from my expert-witness practice





NOTE: Excludes current cases



TRANSLATE

1. RELIABLE
2. RELEVANT
3. SUFFICIENT

and

4. UNDERSTOOD by lawyers, judges and other lay people

Example from a fraud matter

US$
1,000,000
1,500,000
1,000,000

Excel

US$		
1		
1	500	
1		

Lotus123

US$
1,000,000
1,500,000
1,000,000

Excel

US$		
1	000	000
1	500	000
1	000	000

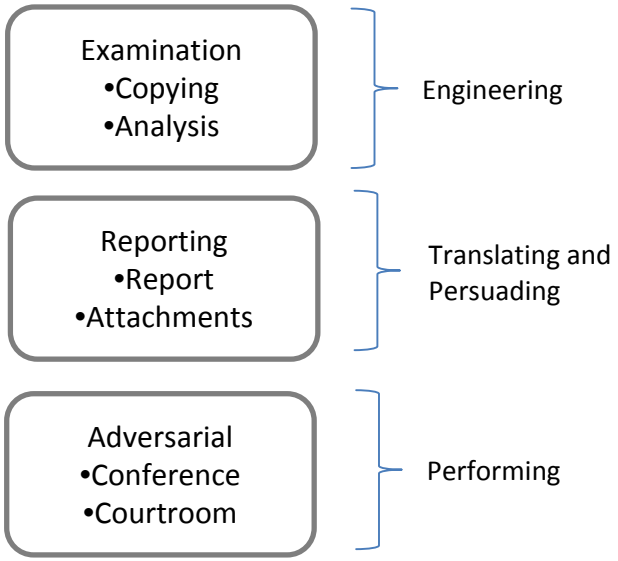
OpenOffice

US$		
1		
1	500	
1		

Lotus123

Choosing an Expert

- Qualifications
  - Academic qualifications
  - Match area of expertise
    - Will the Expert let themselves be taken outside of their expertise?
  - Credibility
    - Can the Expert be more than a “technician”?
    - Has the Expert got Courtroom experience?
  - Access to sensitive material
- Suitable facilities and tools
  - Have the tools been properly licensed?
  - Is the evidence properly stored?
- Cost
  - $200-$550/hr
  - Copying a computer ~2hrs
  - Analysing a computer ~2 days
  - Writing a report ~1 day per computer
  - Allow time for arranging to get the evidence



Reliability

- Reliable people
  - The accused and other witnesses
  - The computer forensic expert him or herself
  - The jury
- Reliable process
  - Tools
  - Methods
- Reliable evidence
  - Has the computer produced reliable records?
  - Mitigating factors (e.g. The “unknown hacker defence”

An increasingly common scenario?

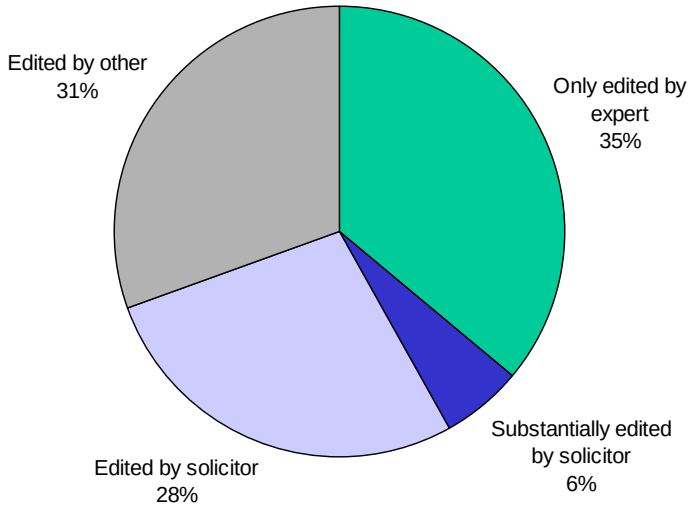
Barrister: So Mr X, are you in the habit of lying?
Mr X: No.

Barrister: Then how do you explain these....
PRODUCES POSTINGS FROM INTERNET (evidence regarding the credibility of a witness in relevant)

Although remember, just because someone publishes something it does not always mean it is so (including pictures and video)

Expert Witnesses

- A survey of 244 Australian judges in 2005 by the Institute of Judicial Administration found the judges believed that the most important problem with expert evidence is that it is partisan:
  - 27% said that expert witnesses were often biased
  - 65% said they were occasionally biased
  - One judge commented: "Bias is almost inevitable given that the expert is paid for by one party and only called if his/her evidence helps the party's case. Experts frequently slant evidence in favour of the litigant on whose behalf evidence is given.“
- "I have little faith in experts' reports which are really the work of solicitors/counsel….I cannot imagine any other reality in an adversarial system“
- Sample of 200 experts reports in civil registry
  - Electronic submission
  - Check of document properties and metadata
  - Imaged reports ignored



Reliable tools don’t have to be expensive

	My cheap kit	My mid-range kit	Enterprise Kit
Size of Job	Up to 10 computers	20+ computers 1million documents	Large corporate So far ~370m documents
Web 2.0 Capture	n/a	$20 per-seat	$5 per-seat
Computer forensic	$400	$5,000	$8,000
OCR	$300	$500	$5,000
Text searching	$0	$6,000	$20,000
Voice-to-text	$300	$5,000	$60,000
Face Recognition	Free		$150,000
Voice Identification	Free		$200,000
Video processing	$400	$1000	n/a
Visualisation	Free		
Productions	$4-5 per page	$10,000	$50,000 4c per page

Is the copying/searching process reliable?

Tapes fails to write/read/restore ~20% of the time

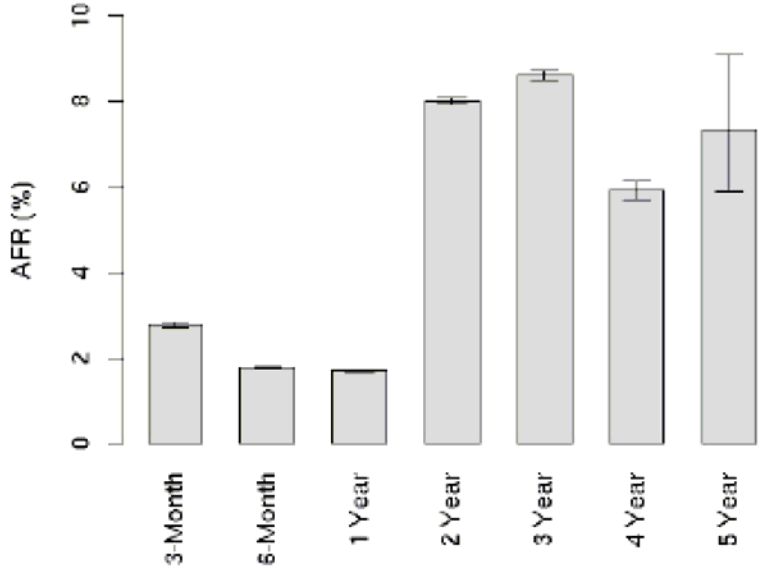
Sequential search of file system fails to read 1 in 6 million files (typically)

OCR 98% reliable in better implementations

Permutations and representations of common words rely on corporate lexicon

Of a sample of 1.2m and another of 150m+ documents:

- ~5% of attachments to e-mail were encrypted
- 1.5% contained graphical versions of responsive text
- 0.5% of recognised formats were unable to be opened
- 2% contained responsive text in metadata that would not have been searched by a human
- ~0.05% of speech was responsive



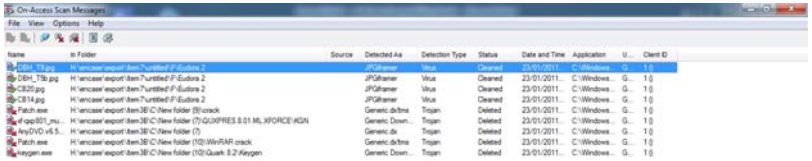
** Pinheiro et al (2007) Failure Trends in a Large Disk Drive Population

The “unknown hacker defence”

- Not good enough to merely assert: “an unknown hacker could have done it”

- Need to find indicator that it is a reasonable assertion:
  - Malware
  - Peer-to-peer network (e.g. Torrents)

- Legal insertion of malware:
  - When was interception authorised? (e.g. ASIO warrant)
  - Becoming commonly used amongst teenagers and private investigators (I’m not so sure that’s legal?)



- Capability:
  - Insert/extract files
  - Use programs
  - Capture keystrokes (e.g. Passwords)
  - Turn ON/OFF camera
  - Turn ON/OFF microphone

Anti-forensics

- In layman's terms: "Cleaning up after yourself"
- Internet is replete with instructional material
  - Having the tools on the computer is a good indicator
  - Having the instructions on the computer is a good indicator of behaviour
- Popular software includes:
  - CC-cleaner (most common one I see)
  - Web-washer/E-mail washer
  - Evidence Eliminator
  - Glaries Utilities
- The tools are not reliable...in my experience, even when the above software has been used, useful data is commonly recoverable

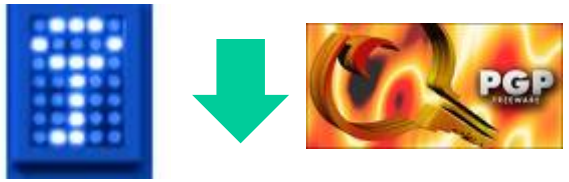
Encryption

- In layman's terms: "Hiding your data"

- Most popular tools:
  - Truecrypt
  - PGP (pretty good privacy)
  - Bitlocker (part of Microsoft)
  - There are many others

- Overcoming encryption:
  - Can often "find" the password
  - Can often "guess" a password
  - Can sometimes break encryption
  - The clear-text is sometimes left in remnant data

```
The quick brown fox jumps over the lazy grey
dog. The quick brown fox jumps over the lazy
grey dog. The quick brown fox jumps over the
lazy grey dog. The quick brown fox jumps over
the lazy grey dog. The quick brown fox jumps
over the lazy grey dog. The quick brown fox
jumps over the lazy grey dog. The quick brown
fox jumps over the lazy grey dog. The quick
brown fox jumps over the lazy grey dog. The
quick brown fox jumps over the lazy grey dog.
The quick brown fox jumps over the lazy grey
dog. The quick
```




```
qANQR1DBwEwDrcTYAONuPR8BB/9x01NppIyoXme0iA0tmDlP3eNgfDI9q2RMorZa
RbnDZIcqPPfUYISrb4wlVOO3Gwb2jLdmW9CZHuADKJzNC9QzwaIPyp6pysVl7ZvG
B6Or1syBvHYCglcKzPcYQLmy1E2udg8Nix6bDOs19vzq+L/TX6nRPh3Lgun8EJ/s
FVyGQ59/HLKwFYBQah7p2TyvOKq4A/MTaVjXoDLV6RS2wRJDRFiO7QC03k6depbD
o8raGEtzkejx5PK90ze6veKjcXM9bIUxjTTor6Fr3eFBG/Y9t8VpKkgCCVjrviC4
IGvrDeU7ym29myiNy9TBDnhNCSaV9eZxfO/oPrGNjbSlpUic0sFxAZKFFHWiWV2y
EKYz2Ox82f7KgvnbdymjMLQA7FclUWwELNg8ChKBDu12l07Jsday8XHIXJ9vY42S
g4Wjggs8IrtWIsDAuWOeWmFDEeBLmP7XOT7qvnAmMpAbxj8gQlIHvdGx9ADBtmPd
83lSmBReENhE9pjVQ+pg1AEYs6fszLh8ExaxNOv9Bmy0gZsNdLzaddERpcJLSDy+
MCn2Asvn8DvxrrVXWM2BOvrlq6sgZLAMDCEL0JuR3fANNJXbgwUuKdZ14Ch0W8eM
/nrnwdaMmQaTcpWDvgTsJGdEQfLnvIb0wkC7BqYEtsoxW9WDlUtcP4c5zmxFVszJ
LnqU/ef4AOTbWMJ1Ra9CU4b49PgrrvCv88oa69oIdhwkOP2v2PJHOtg2L6lZGiQe
tZox7IjWe7WE4KbjAoohHNTy1ND5jMGm1iT2FLfp1FoAo19wN11RzHiuN0wb6GAq
tFWXOvcDwVGHMBx/bAnlvC84h/NaF0k1RrZ9pnzNhW4TH2j3xxdWcCHAS6XeN4Hr
Zzbc0VwBeaortskzTzluJdAUPLCVrXw6jX7bWoz/hkx1L9Lh3vedY4/JfAg/ZeZn
7HeuYoKIyu9t7au6TozlZTfSeyapDxBkgJQnjmp/4MOlv1M62AfZswuRdAIi/h1P
IWjqOBZ+lA5VS73jwPqfQmTm1UlKS2gx09WgetWM/0MLAf3xowJ2tT2QXMtHeKvJ
mgnY+4nHkPO9ePXhBeLYFbUvT8vQLl5B
```

Is the metadata consistent?

- Metadata is data about data. It can be stored:
  - internally (i.e. Within a file); or
  - externally

- Many computer forensic examiners rely on metadata stored in the File Allocation Table
  - Created date
  - Last modified date
  - Last accessed date

- Common sources of metadata:
  - Email
  - Microsoft documents
  - Photographs (EXIF)

- Hidden Information (PowerPoint)
- Your name (All)
- Your initials (All)
- Your company or organization name (All)
- The name of your computer (All)
- The name of the network server or hard disk where you saved the document (All)
- Other file properties and summary information (All)
- Non-visible portions of embedded OLE objects (All)
- The names of previous authors (All)
- Document revisions (Word, Excel)
- Document versions (Word)
- Template information (Word, PowerPoint)
- Hidden text (Word, Excel)
- Hidden Cells (Excel)
- Personalized views (Excel)
- Comments (All)
- Globally Unique Identifiers (GUIDs) (All)

- Generator (All)
- Title (All)
- Description (All)
- Subject (All)
- Keywords (All)
- Initial Creator (All)
- Creator (All)
- Printed By (All)
- Creation Date and Time (All)
- Modification Date and Time (All)
- Print Date and Time (All)
- Document Template (All)
- Language (All)
- Editing Duration (All)
- User-defined Metadata (All)
- Document Statistics (All)