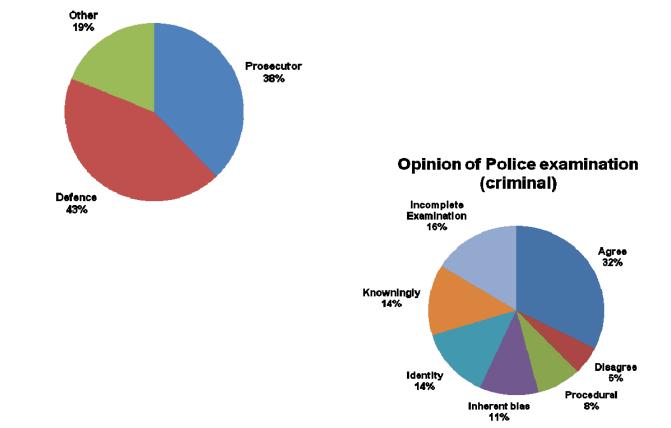
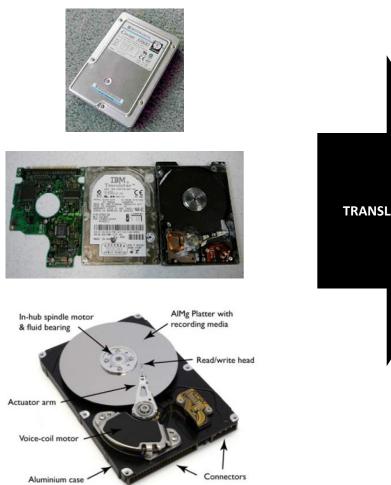
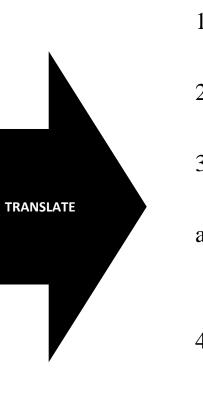
Statistics from my expert-witness practice

Instructing party (criminal)







1. RELIABLE

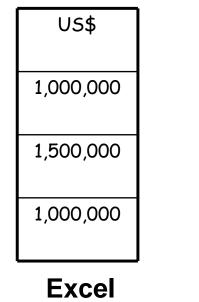
2. RELEVANT

3. SUFFICIENT

and

4. UNDERSTOOD by lawyers, judges and other lay people

Example from a fraud matter





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				

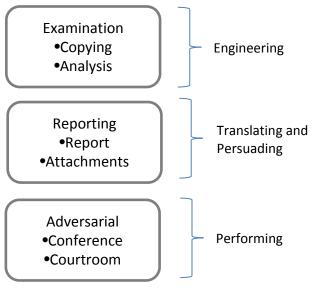
US\$		
1		
1	500	
1		

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?



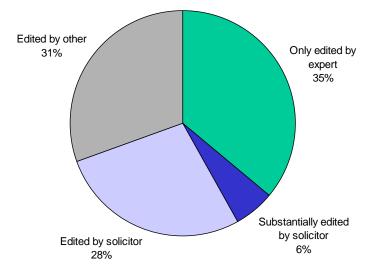
Barrister: So Mr X, are you in the habit of lying? Mr X: No.

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

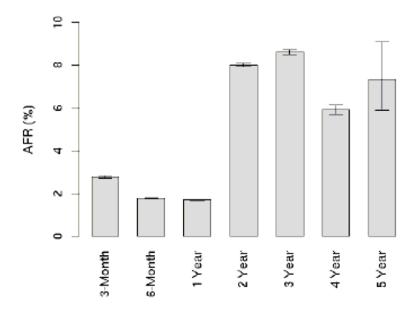
Sequential search of file system fails to read 1 in 6 million files (typically)

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:

- \Box ~5% of attachments to e-mail were encrypted
- □ 1.5% contained graphical versions of responsive text
- \Box 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
- \Box ~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 <u>could</u> 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



Con-Access Sca	an Messages									
File View Opt	ions Help						_	_		
h h. 9 %	A 8 4									
Name	In Folder	Source	Detected As	Detector Type	Status	Date and Time	Application	u	Clent D	
DEH_Thes	Hierconelespot Ann Purched Filiaden 2		Allana	(Marca	Overed	23/01/2011	C Windows	-6	10	
DEH_TSb pg	H Vencase/export/tem7/untitled/IP/Eudora 2		JPG/raner	Virus	Ceaned	23/01/2011_	C:\Windows	G	10	
C#20 pg	H'encase/expot/item/?untitled/P/Eudors 2		JPG/ramer	Mean	Oeaned	23/01/2011	C:\Windows	G	10	
C814 pg	H /encase/export/arm?untitled/F/Eudora 2		3PG/ramer	Mr.n	Cleaned	23/01/2011	C:\Windows	G	10	
Patch eve	H 'encase'export / tem 38' C' New folder (3) crack		Generic dvitme	Tisjan	Deleted	23/01/2011	C1Windows	G.,	10	
d op101 mu.	H 'encase'export'sem36'/C'/New folder (7)/QUXPRES 8.01.MLXFORCE KSN		Generic Down	Trajan	Deleted	23/01/2011	C\Windows	G.,	10	
AnyDVD.v65	H tencase'export ten 381C New folder (7)		Generic dx	Trajan.	Deleted	23/01/2011	C1Windows	G	10	
Patch eve	H1encase1export1tem381C1New folder (10)1WinRAR crack		Generic driftme	Trojan	Deleted	23/01/2011	C1Windows_	G	10	
Anna and	H Januara annot Jan 30 C Aire folder (10) Custo 8 2 Kennen		Genetic Down	Treas	Californi	23/01/2011	CiWindows	6	1.6	

Anti-forensics

- In layman's terms: "Cleaning up after yourself" •
- Internet is replete with instructional material ٠
 - 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 ٠
 - Glaries Utilities
- The tools are not reliable...in my experience, • even when the above software has been used, useful data is commonly recoverable

Google	hiding your tracks on the internet	Search
0	About 795,000 results (0.06 seconds)	Advanced searc
Everything	Anonymous Proxy - Hide your tracks!	
Images	You can hide your tracks during your internet travels using tools like an anonymous	
Videos	proxy, and here is how. It's a fact, websites are tacking you right now	
	www.auditmypc.com/anonymous-proxy.asp - Similar	
News	The Truth About Hiding Your Tracks on the Internet	
More	11 Jul 2005 Ok, ok, I know you've seen them. All those pop up windows claiming that	
	"You're being watched!" or banner ads saying "Your computer is under ezinearticles.com > Internet and Businesses Online > Security - Cached - Similar	
dney New South	ezineartoes.com / internet and businesses on me / becunty - bached - on mar	
ange location	How to Delete your Usage History Tracks in Windows - wikiHow Q	
ange location	7 Feb 2011 Attempting to hide your computer usage at work is likely to bring Clean	
e web	your internet tracks with Ad-Aware 2007 · Use the history brush www.wikihow.com/Delete-your-Usage-History-Tracks-in-Windows - Cached - Similar	
e web ges from Australia	www.mixinow.com/bereteryour-bage-instory-fracks-in-windows - Cabled - Similar	
	How to hide your tracks on the Internet without software?	
re search tools	9 Mar 2003 I owed you with the Gallery so here is my contributionHow to hide your	
	tracks on the Internet without softwareCookies are small bits of code www.ex-designz.net/articleread.asp?aid=249 - Cached - Similar	
	www.ex-designz.nevarticleread.asp?aid=249 - Cached - Similar	
	Covering Your Tracks if you're concerned about someone knowing Q	
	21 Mar 2003 The Internet can be a great place to get information and to make or "	
	Hiding Your Tracks On-line", the Domestic Violence site of the dawn.thot.net/workshops/concerns.html - Cached - Similar	
	dawn.triot.networkshops.concerns.ntmi - dadred - Sinnar	
	HPP SurfSawy: hide your tracks	
	5 Oct 2010 searchable list of abuse hotlines, shelters, refuges, crisis centres and	
	women's organizations, by country, plus index of domestic violence www.hotpeachpages.net/a/surfsavvy.html - Cached - Similar	
	The Truth About Hiding Your Tracks on the Internet What's My IP 🤉	
	The Truth About Hiding Your Tracks on the Internet. Posted on September 1, 2010 by	
	admin. Ok, ok, I know you've seen them. All those pop up windows claiming www.ipbee.com//the-truth-about-hiding-your-tracks-on-the-internet/ - Cached	
	www.pbee.com//ine-addraboa/maing-your-aacks-on-aie-menter - cached	
	Hide your internet activities - Shelternet	
	www.shelternet.ca/en/women/internet-safety/ - Similar	
	Hiding your tracks online - City of Fremantle Q	
	Hiding your tracks online. If you are concerned that your partner will check where you	
	have been online - email, internet chat or just searching the web	
	www.fremantle.wa.gov.au/services//Hiding_your_tracks_online - Cached	
	How to hide your tracks at work Webware - CNET Q	
	21 posts - 19 authors - Last post: 18 Apr 2009	
	We all know that you play when you should be working. But at least we're here to help	
	you hide what you shouldn't be doing. news.cnet.com/8301-17939_109-10222031-2.html - Cached - Similar	
	G00000000gle >	
	1 2 3 4 5 6 7 8 9 10 <u>Next</u>	
	hiding your tracks on the internet	Carach
		Search

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 brown fox jumps over the lazy grey dog. The quick



qANQR1DBwEwDrcTYAONuPR8BB/9x01NppIyoXme0iA0tmDlP3eNgfDI9q2RMorZa RbnDZIcqPPfUYISrb4w1V003Gwb2jLdmW9CZHuADKJzNC9QzwaIPyp6pysV17ZvG B6OrlsyBvHYCglcKzPcYQLmy1E2udg8Nix6bDOs19vzq+L/TX6nRPh3Lgun8EJ/s FVyGQ59/HLKwFYBQah7p2TyvOKq4A/MTaVjXoDLV6RS2wRJDRFi07QC03k6depbD o8raGEtzkejx5PK90ze6veKjcXM9bIUxjTTor6Fr3eFBG/Y9t8VpKkgCCVjrviC4 IGvrDeU7ym29myiNy9TBDnhNCSaV9eZxf0/oPrGNjbSlpUic0sFxAZKFFHWiWV2y EKYz20x82f7KgvnbdymjMLQA7Fc1UWwELNg8ChKBDu12107Jsday8XHIXJ9vY42S g4Wjggs8IrtWIsDAuWOeWmFDEeBLmP7XOT7qvnAmMpAbxj8gQlIHvdGx9ADBtmPd 831SmBReENhE9pjVQ+pg1AEYs6fszLh8ExaxNOv9Bmy0gZsNdLzaddERpcJLSDy+ MCn2Asvn8DvxrrVXWM2BOvrlq6sqZLAMDCEL0JuR3fANNJXbqwUuKdZ14Ch0W8eM /nrnwdaMmOaTcpWDvqTsJGdEOfLnvIb0wkC7BqYEtsoxW9WDlUtcP4c5zmxFVszJ LnqU/ef4AOTbWMJ1Ra9CU4b49PgrrvCv88oa69oIdhwkOP2v2PJHOtg2L61ZGiQe tZox7IjWe7WE4KbjAoohHNTy1ND5jMGmliT2FLfp1FoAo19wN11RzHiuN0wb6GAq tFWXOvcDwVGHMBx/bAnlvC84h/NaF0k1RrZ9pnzNhW4TH2j3xxdWcCHAS6XeN4Hr Zzbc0VwBeaortskzTzluJdAUPLCVrXw6jX7bWoz/hkx1L9Lh3vedY4/JfAq/ZeZn 7HeuYoKIyu9t7au6TozlZTfSeyapDxBkgJQnjmp/4MOlv1M62AfZswuRdAIi/h1P IWjqOBZ+1A5VS73jwPqfQmTm1U1KS2gx09WgetWM/0MLAf3xowJ2tT2QXMtHeKvJ mgnY+4nHkPO9ePXhBeLYFbUvT8vQL15B

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)

