Understanding Computer Forensics

also known as:

How to do a computer forensic investigation
... and not get burned

Nick Klein

SANS Canberra Community Night
11 February 2013

Klein&Co.
experts in computer forensics.

The scenario ...

- Your boss tells you a senior executive has just resigned and is going to work for an aggressive competitor
- He has a strong suspicion that the (former) employee has taken confidential information; a very serious allegation
- The boss asks you to investigate what the former employee was doing before he left
- What a great opportunity for you to do some really interesting work, help your company and impress your boss

So ... *what do you do?*

What is *forensics?*

Forensic:

1. Relating to, connected with, or used in courts of law or public discussion and debate
2. Adapted or suited to argumentation; argumentative
3. Applied to the **process** of collecting evidence for a legal case: *forensic accounting; forensic archaeology; forensic linguistics*

[Latin *forens(is)* of the forum]

- Macquarie Dictionary Online (2010)

What is *computer forensics?*

*"A digital forensic investigation is a **process** that uses science and technology to analyze digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred."*

- Brian Carrier

File System Forensic Analysis (2005)

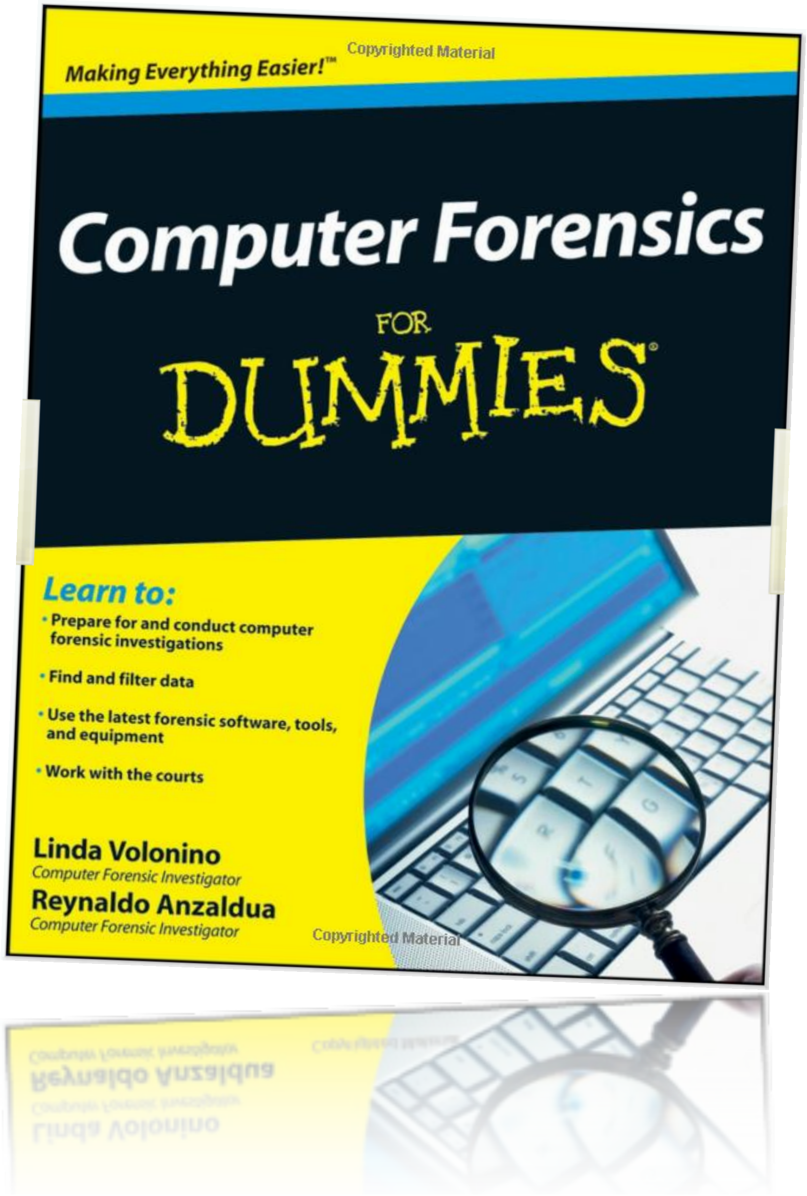
... there is no *Forensicator Pro*

How can computer forensics be used?

- Financial and other fraud
- Employee misconduct and corporate policy breach
- Incident response, computer hacking and system intrusion
- Theft of confidential information and intellectual property
- Issues surrounding termination of employment
- Internal organisational investigations
- Litigation and commercial disputes
- Electronic discovery
- Independent collection and analysis of electronic evidence
- Search and retrieval of responsive documents from computer systems and backup media
- Criminal investigations, both prosecution and defense
- Independent review of work performed by other experts
- Regulatory investigations
- Expert testimony for civil and criminal proceedings
- Search warrants and seizure orders

Phases of an investigation

1. Understand the case
2. Identify and collect evidence
3. Analyse the evidence
4. Present findings



Making Everything Easier!™

Copyrighted Material

Computer Forensics

FOR DUMMIES®

Learn to:

- Prepare for and conduct computer forensic investigations
- Find and filter data
- Use the latest forensic software, tools, and equipment
- Work with the courts

Linda Volonino
Computer Forensic Investigator

Reynaldo Anzaldua
Computer Forensic Investigator

Copyrighted Material

Phase 1: Understand the case

- Initial instructions are often incomplete
- Ask specific questions - *who, what, why, where, when, how?*
- Assist with technical knowledge and practical experience
- Need to be specific in defining forensic objectives
- Start to identify relevant sources of evidence

Forensic or IT?

- Most companies naturally turn to their IT staff for help; this can be damaging to an investigation and risky for the staff involved

- Digital evidence is volatile in nature and can be altered or destroyed, accidentally or deliberately, by a user or automated process

- Simply *copying* or *backing up* a computer will not capture all potentially relevant data

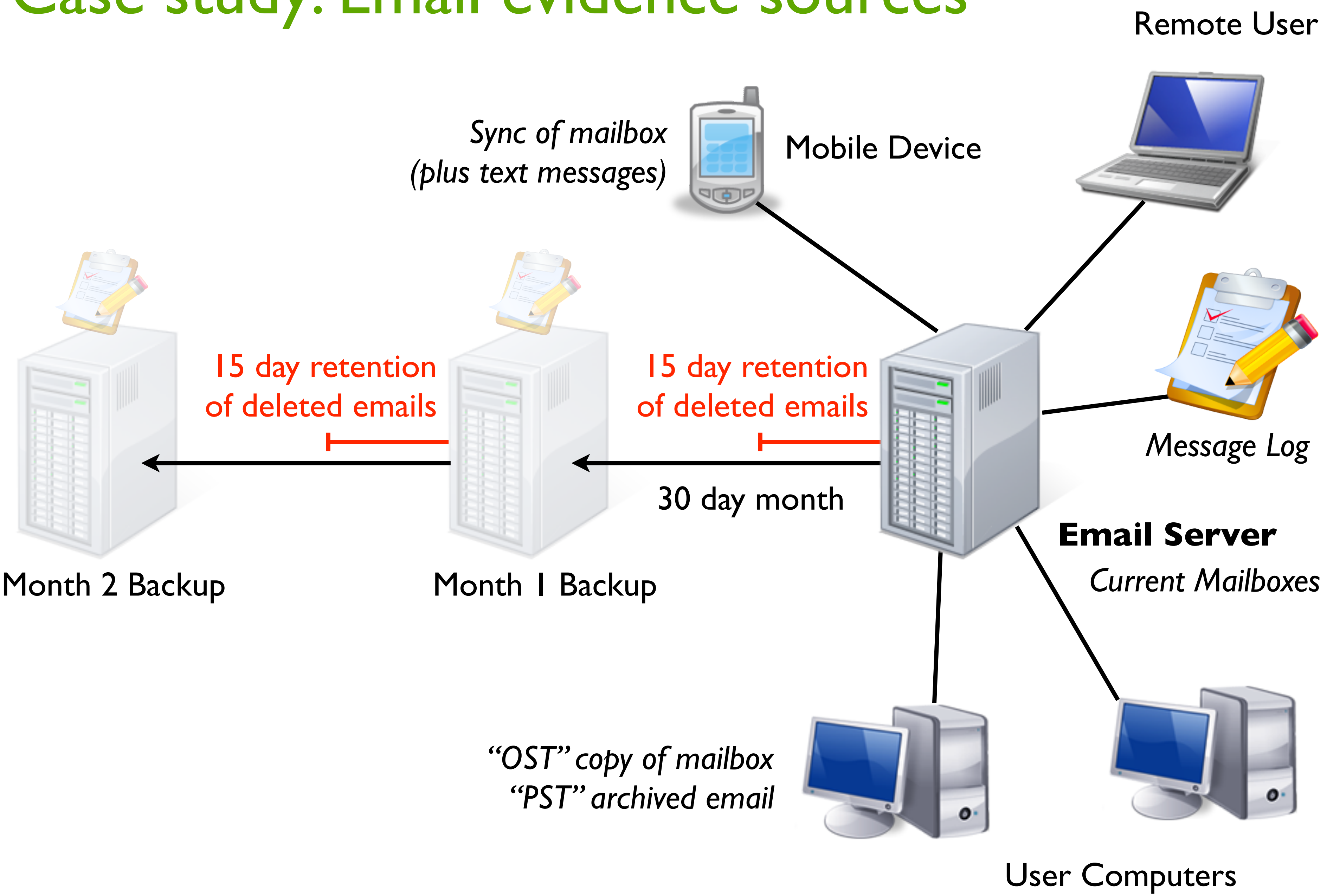
- Most IT *experts* aren’t conscious of the difference between fact and opinion

- The effectiveness of a computer forensic analysis is underpinned by the quality of the data acquired

Phase 2: Identify and collect evidence

- Evidence usually exists in multiple places
- Preservation is key; should avoid analysing live data *
- Think outside immediate and obvious data sources
- Collection methods *should* use ‘forensic’ processes
- *Forensic* collection doesn’t necessitate ‘forensic’ tools
- Aim to minimise changes to evidence during collection
- Opt to collect more rather than less
- We can then do as much, or as little analysis as needed

Case study: Email evidence sources



Klein & Co.
experts in computer forensics.

Potential sources of evidence

- **Local computers:** live memory, active state information, file system, Internet cache, email archives, system logs, recycle bin, info2 records, link files, MRU lists, Internet cache, index.dat, browser artefacts, document metadata, unallocated disk space, system restore points, volume shadow copies, shellbags, jump lists, registry, registry, registry ...
- **Servers:** network drives, application systems, databases, email servers, document management systems, email archiving, proxy logs, extended logging ...
- **Backups:** of servers, executive computers, clean configurations ...
- **Removable devices:** serial number, file system, unallocated space ...
- **Mobile devices:** phones, PDAs, Blackberrys, iPhones, iPads, sat nav ...
- **Facilities:** electronic doors, CCTV, photocopiers, carpark systems, telephones, voicemail ...

Phase 3: Analyse the evidence

☑ Follow an analysis plan

☑ Identify every potential source of artifacts

☑ Observe the facts of the evidence; *know the tools!*

☑ Identify typical provenance of factual findings; ask *why is it so?*

☑ Consider variables which influence the factual finding

☑ See what other findings corroborate observations

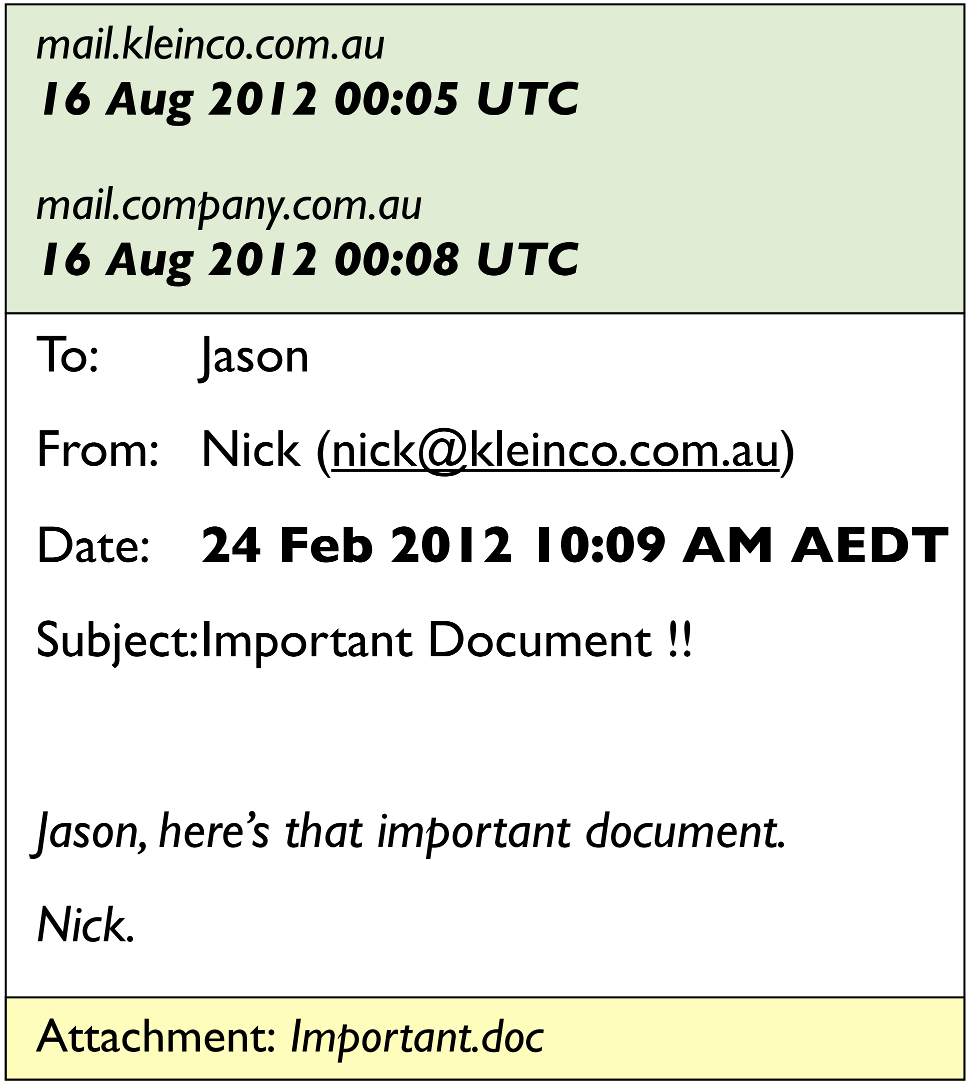
☑ Analyse any discrepancies - test scenarios if required

☑ Be specific in describing what the findings prove

☑ Understand what the finding does not prove

"If all you have is a hammer, everything looks like a nail"

Case study: Email timestamps



mail.kleinco.com.au
16 Aug 2012 00:05 UTC

mail.company.com.au
16 Aug 2012 00:08 UTC

To: Jason

From: Nick (nick@kleinco.com.au)

Date: **24 Feb 2012 10:09 AM AEDT**

Subject:Important Document !!

Jason, here's that important document.

Nick.

Attachment: *Important.doc*

Email headers contain timestamps added by mail servers and relays

Emails contain multiple timestamps:

- Creation in sender's email program
- Submission to outgoing server
- Delivery by outgoing server
- Receipt by incoming server
- Delivery to recipient's mailbox
- Filing into an email folder
- Deletion

- ***Plus** attachment timestamps*

Case study: “Super” timeline analysis

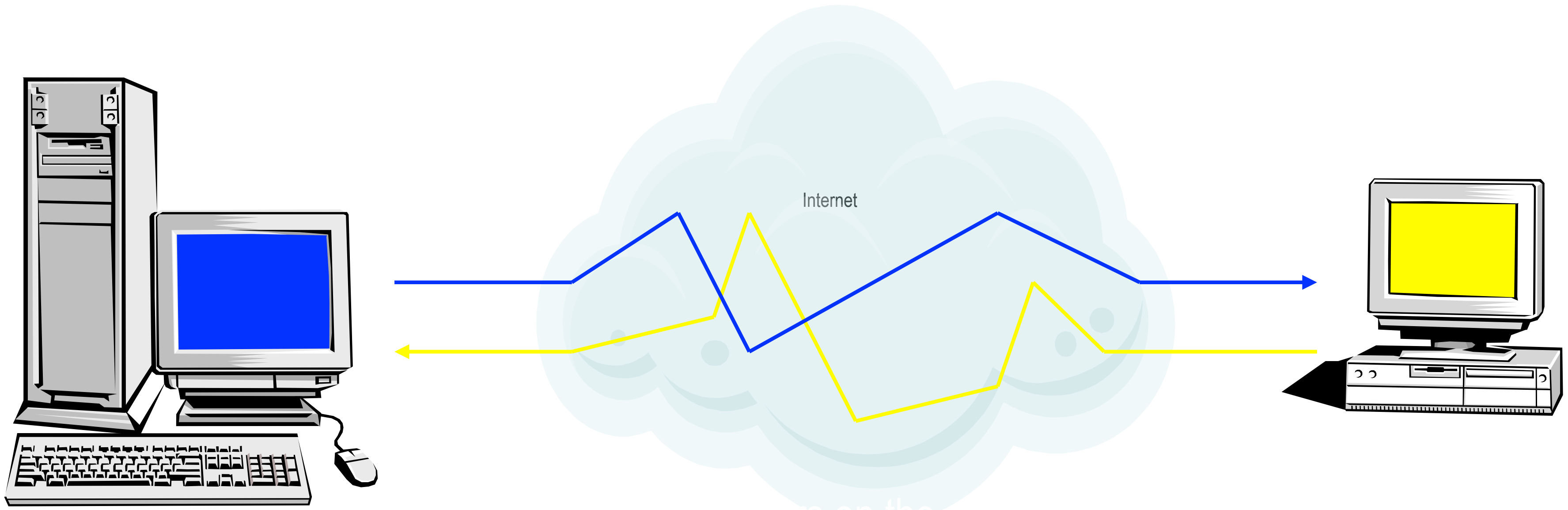
Date	Time	Time Source	Timeline Entry
13 Nov 2011	09:47.19	Document Metadata	Document **Secret File.docx** first created by user **John**
16 Nov 2011	15:39.44	Recycle Bin	Document **Secret File.docx** last modified
17 Nov 2011	11:14.50	Internet History	**Secret File.docx** accessed by user **Bob** from network drive **P://Projects/Secret Project/**
17 Nov 2011	11:24.45	Recycle Bin	Document **Secret File.docx** first created on this computer
17 Nov 2011	11:25.14	Registry	**Microsoft Word** executed by user **Bob**
17 Nov 2011	11:25.14	Link Files	**Secret File.docx** accessed by user **Bob** from local path **C:\...\Bob\Desktop**
17 Nov 2011	11:47.00	Recycle Bin	**Secret File.docx** deleted in Recycle Bin of user **Bob**

Phase 4: Present findings

- Evidence can be provided in a variety of forms:
  - informal findings
  - formal reports
  - statements / affidavits
  - expert reports

- Always be conscious that your work may be used as evidence in court

Case study: Explaining network data traffic



The recipient computer receives the data, sending replies as required

Computers on the Internet route the data as required, so it reaches the intended recipient

One computer sends data to another computer across the Internet

Case study: The “CSI effect”

Time	C-IP	URL	Status	Data
16:35	10.0.1.5	www.illegalsite.com.au	502	0 KB
16:35	10.0.1.5	www.illegalsite.com.au	502	0 KB
16:36	10.0.1.5	www.illegalsite.org	502	0 KB
16:36	10.0.1.5	www.illegalsite.com.au	502	0 KB
16:38	10.0.1.5	www.anotherillegalsite.com.au	502	0 KB
16:38	10.0.1.5	www.yetanotherillegalsite.com.au	502	0 KB
16:40	10.0.1.5	www.kinkysite.com.au	200	5 KB
16:40	10.0.1.5	www.kinkysite.com.au	200	6 KB
16:40	10.0.1.5	www.kinkysite.com.au	200	8 KB

Contracts and engagement

- Consider engagement through legal counsel for legal privilege
- Clearly define the scope, objectives and analysis phases
- Be clear on critical decisions during the investigation and ensure they're made by the appropriate person and documented
- Set realistic expectations and keep the client updated, manage the investigation professionally
- Involve the client's staff (especially IT) in the investigation process as required by your investigation plan
- Remain impartial, maintain independence between your process and your findings (and any fees)
- Define important assumptions and limitations

Other legal considerations

- *Expert Witness Code of Conduct* defines how experts should present their findings
- *NSW Workplace Surveillance Act 2005* requires notification to employees before surveilling *input or output* to a computer system
- *Telecommunications (Interception and Access Act) 1979* limits access to stored communications on a carrier network
- *Criminal Code Act 1995* defines unauthorised access to computer system
- Some other countries have much stricter privacy laws