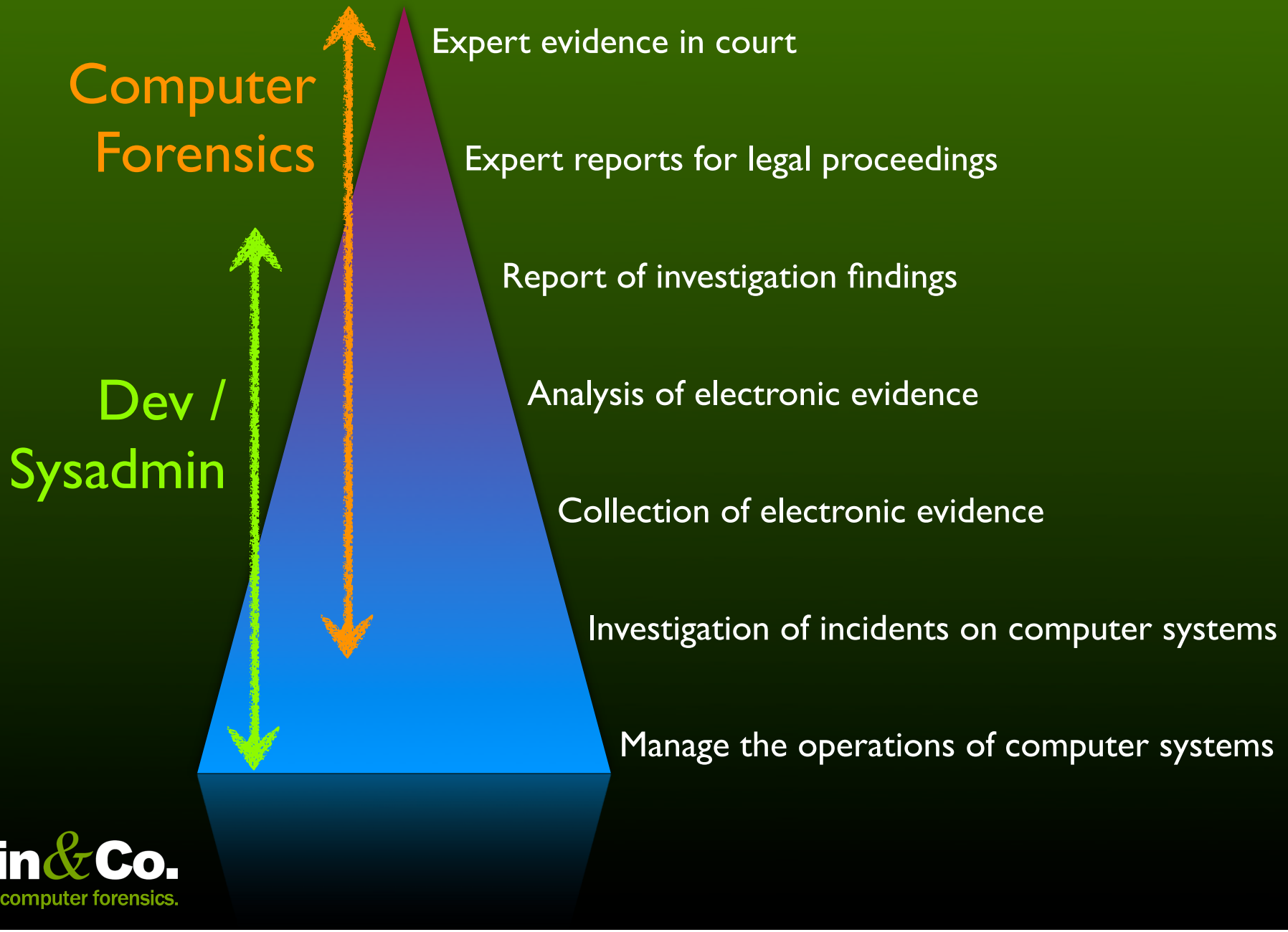
How to do real world computer forensics

... and not get burned

Klein&Co.

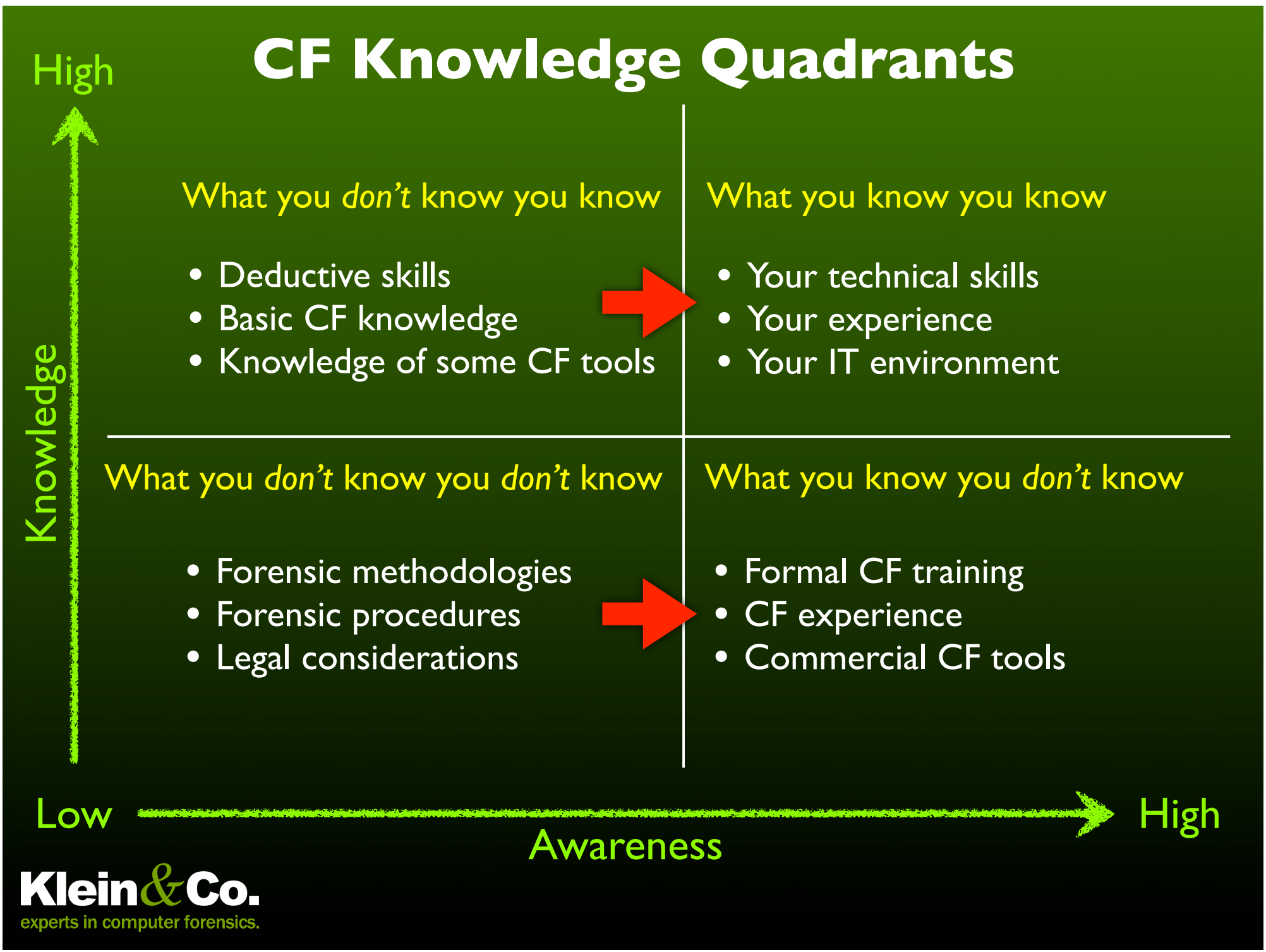
experts in computer forensics.

Dev / Sysadmin & Computer Forensics



Klein&Co.
experts in computer forensics.

CF Knowledge Quadrants



Klein & Co.
experts in computer forensics.

What this presentation is *not*

- Legal advice
- A definitive guide for undertaking a computer forensic investigation

Klein&Co.
experts in computer forensics.

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)

Klein & Co.
experts in computer forensics.

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)

Klein&Co.
experts in computer forensics.

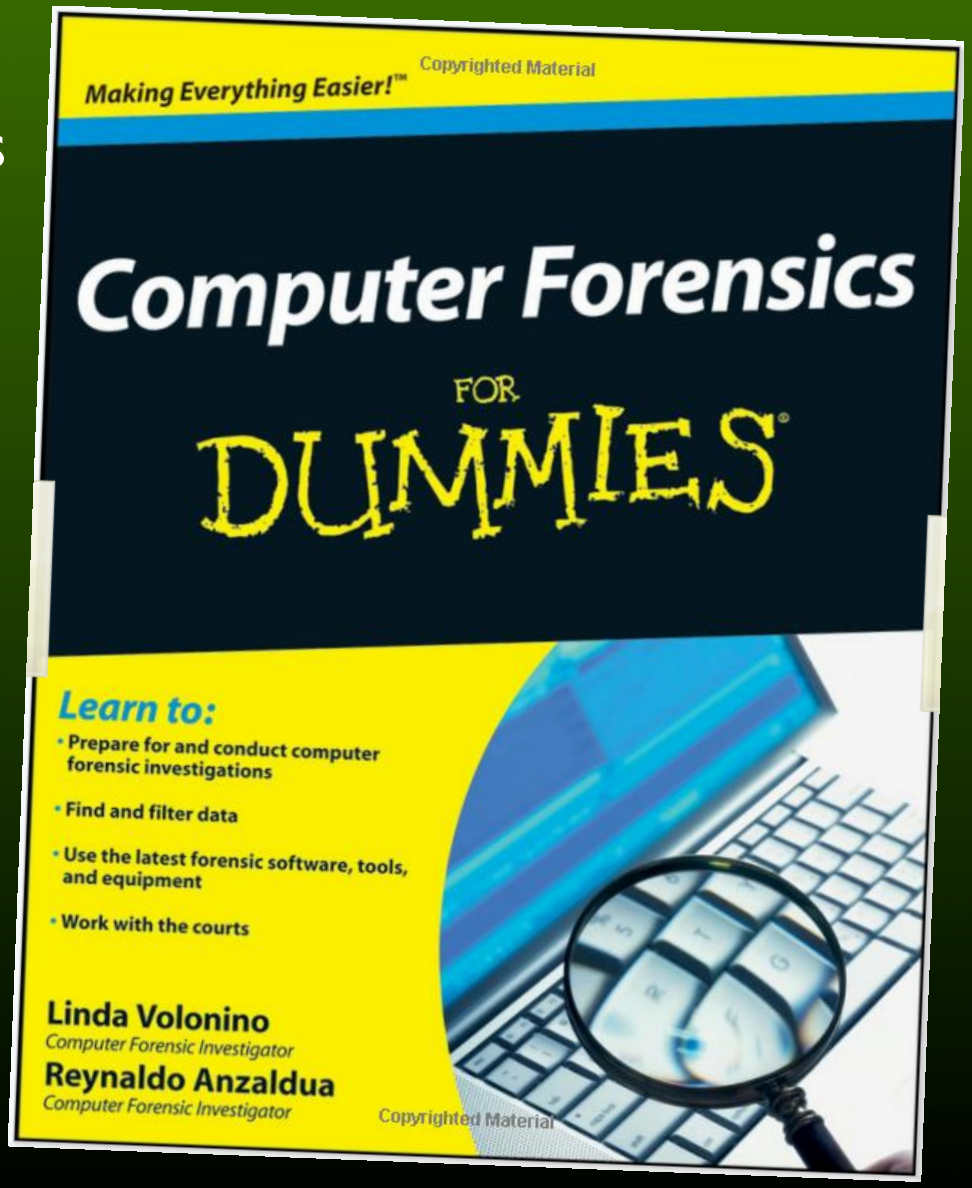
Where can Computer Forensics be used?

- Financial and other fraud
- Employee misconduct and corporate policy breach
- Computer hacking and system intrusion
- Theft of confidential information and intellectual property
- Issues surrounding termination of employment
- Internal organisational investigations
- Litigation and commercial disputes
- 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 and Anton Pillar orders

Klein&Co.
experts in computer forensics.

Some Useful CF References

- SANS Computer Forensics
- Forensic 4cast
- Cyberspeak Podcast
- www.forensicblog.org
- www.forensicswiki.org



Klein&Co.
experts in computer forensics.

Phase I - Understand the Case

- Ask questions - who, what, why, where, when, how?
- Assist with your technical knowledge
- Don't run the case
- You're not a lawyer (or maybe you are?)
- Be specific in defining the objectives and identifying what evidence might assist in determining the facts

Klein&Co.
experts in computer forensics.

Phase 2 - Identify and Collect Evidence

- Evidence might exist in multiple places
- Preservation is key – don't use live data
- Think outside the data sources where you're directed
- Collection methods *should* be forensically sound
- Forensic collection doesn't require proprietary tools
- One golden rule: **Minimise changes to evidence during collection and analysis**

Klein&Co.
experts in computer forensics.

Your first Computer Forensic tool

... also known as *How to take good notes*

- Record the steps you've taken or observed
- Note direct observations of the evidence
- Then note any potential findings and ideas
- Record the time
- Be factual

Klein&Co.
experts in computer forensics.

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, 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, carpark systems, telephones ...

Klein&Co.
experts in computer forensics.

Phase 3 - Analyse the Evidence

- Reviewing the general nature of information stored on computer systems
- Reconstructing user and system activities at relevant dates and times
- Identifying the use of mobile or removable storage devices
- Reviewing email communications and the interactions of people involved
- Performing advanced content searches using file signature analysis, date filters, keywords, phrases and data patterns
- Analysing document metadata to help determine provenance
- Recovering files which have been deleted or partially overwritten
- Determining the authenticity of documents and email messages
- Extracting records of application usage and Internet activity
- Determining the nature and extent of suspected system compromise
- Reviewing, analysing, testing or providing an opinion on the analysis of other forensic practitioners

Klein & Co.
experts in computer forensics.

Analysis Questions

- Where did this piece of evidence come from?
- How is it relevant?
- What does it mean?
- Who created it?
- How has it changed over time?
- Who knows about it?
- How does it relate to other evidence?
- Can it be trusted?
- What can it prove, or not prove?
- How can it be extracted and presented?

Klein&Co.
experts in computer forensics.

Analysis Planning

- Follow an analysis plan
- Know where to look
- Observe the facts of the evidence - know your tools!
- Identify typical provenance of factual findings - why is it so?
- Consider variables which influence the factual finding
- See if other findings corroborate your observations
- Analyse any discrepancies - test scenarios if required
- Be specific in describing what your findings prove
- Be conscious of what the finding does *not* prove

Klein&Co.
experts in computer forensics.

Case Study - Proxy Log Analysis

Date	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

Klein & Co.
experts in computer forensics.

Klein & Co.
experts in computer forensics.

Phase 4 - Present Findings

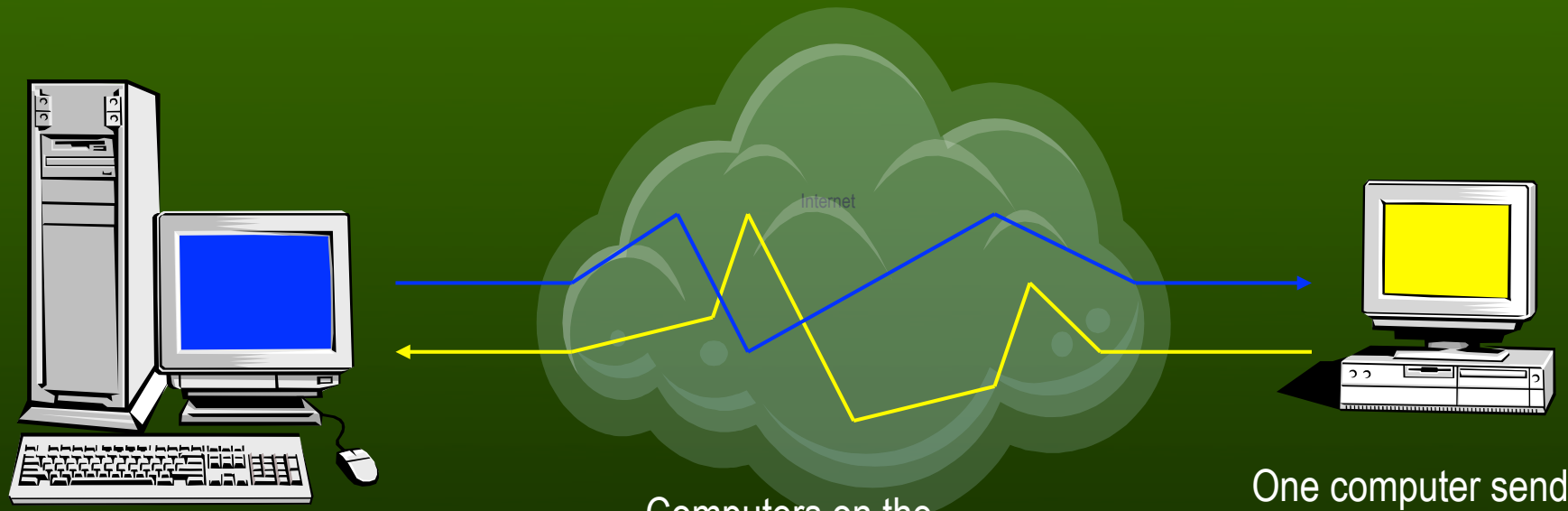
Evidence can be provided in different forms

- informal
- a formal report
- a statement or affidavit
- an expert report

- Always consider your reports might be used in evidence

Klein&Co.
experts in computer forensics.

Aids to Understanding



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

Klein&Co.
experts in computer forensics.

Giving Expert Evidence

- Expertise is determined by the court
- There are only two kinds of witnesses – a witness of fact and an expert
- Expert evidence is by definition opinion evidence

Expert Witness Code of Conduct

1.1 An expert witness has an overriding duty to assist the Court on matters relevant to the expert's area of expertise.

1.2 An expert witness is not an advocate for a party …

1.3 An expert witness's paramount duty is to the Court and not to the person retaining the expert.

Federal Court of Australia, Practice Note CM7
Expert Witnesses in Proceedings in the Federal Court of Australia

Klein & Co.
experts in computer forensics.

Other Legal Considerations

- Your work could be the subject of a subpoena
- *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 a computer system
- Your own company's policies and procedures
- Conducting an investigation does not provide automatic exemption from illegal activity

Klein & Co.
experts in computer forensics.

FYI ...

UNSW Continuing Legal Education Seminar

24 Nov 2010 - Sydney

www.cle.unsw.edu.au

eCrime Symposium 2010

25 Nov 2010 - Sydney

www.internetevents.com.au/upcoming-events

Klein&Co.
experts in computer forensics.

Thank You

Nick Klein

nick@kleinco.com.au

www.kleinco.com.au

Skype: nicholas.klein

Klein & Co.

experts in computer forensics.