Releasing your potential

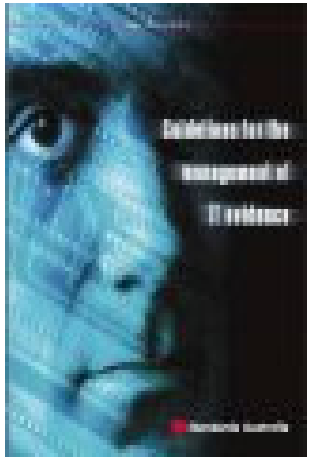
logica

Lessons from prosecutions of Child Pornography and other “prohibited” material

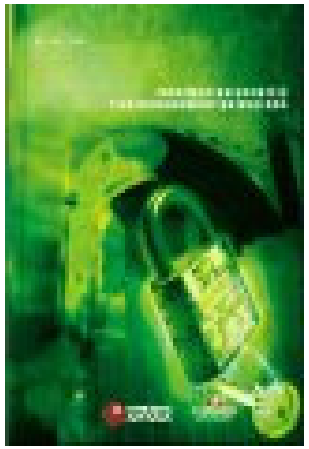
Ajoy Ghosh, Security Executive
ajoy.ghosh@logica.com

Why I'm up here

- Lecturer:
  - Australian Graduate Police College, Manly (CSU)
  - University of Technology, Sydney
  - Santa Clara Law School
  - Beijing Management College of Politics & Law
- Expert witness in court:
  - Civil: contract, evidence, reliability, authorship, times
  - Complex criminal: terrorism, identity theft, fraud, stalking, data leakage
  - Content: child pornography, terrorism, spam, harassment, vilification
  - Serious criminal: homicide, rape, corruption
- Litigation coach:
  - Lawyers, judges, prosecutors
  - International jurisdictions including alternative legal systems eg. ICC, China
  - Preparedness specialist
- 15+ years experience in information security, investigations and policy:
  - Police, Corporate & Consultant
  - Security Executive at Logica
  - National security clearance to TOP SECRET
- Best practice:
  - Author of HB171 – Guidelines for the Management of IT Evidence
  - Co-author HB 231 – Information Security Risk Assessment Guidelines
  - Currently working on ISO – Evidence Acquisition Procedure for Digital Forensics
  - CISSP and iRAP accreditations

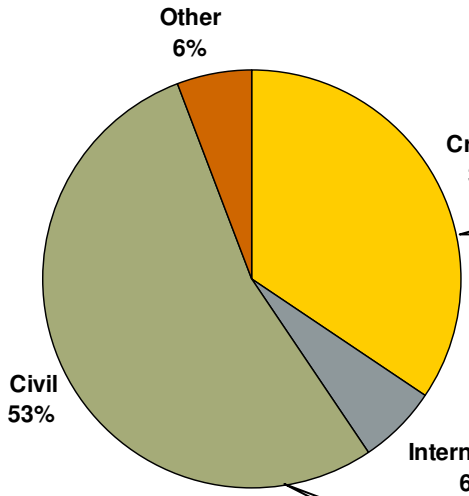


HB171: Guidelines for the Management of IT Evidence (above)
HB231: Guidelines for Information Security Risk Management (below)



Statistics from my expert-witness practice

Type by number

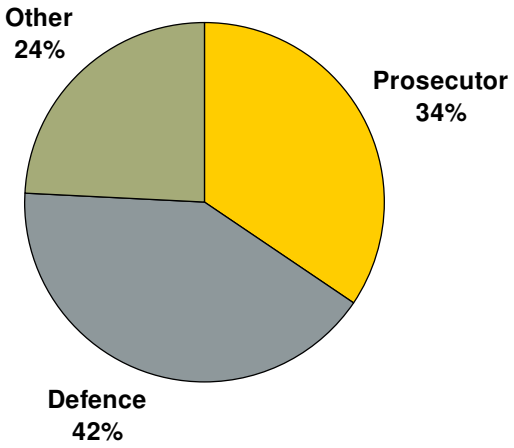


CRIMINAL CASES
- Cybercrime < 20% (incl. content if using Internet)
- Complex crimes: terrorism, identity theft, fraud, stalking, data leakage
- Content: child pornography, terrorism, spam, harassment, vilification
- Serious crimes: homicide, rape
- Conspiracy, corruption, pervert course of justice & contempt of Court, jury misconduct

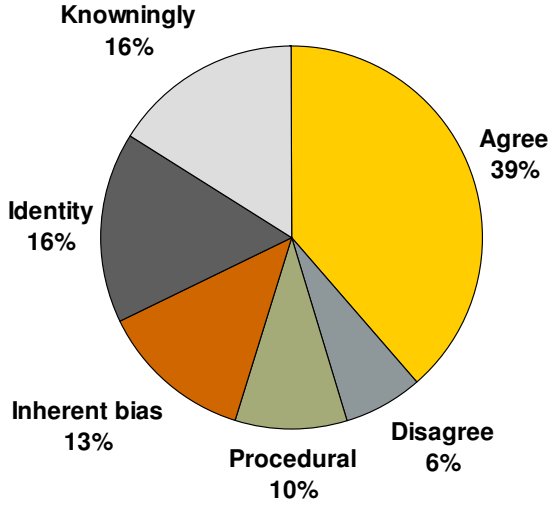
CIVIL CASES
- Searching documents, e-mails & faxes
- Data leakage
- Reliability of evidence
- Practice & procedure
- Conflicting experts

NOTE**: Electronic discovery has been removed from the number of civil cases**

Instructing party (criminal)



Opinion of Police examination (criminal)

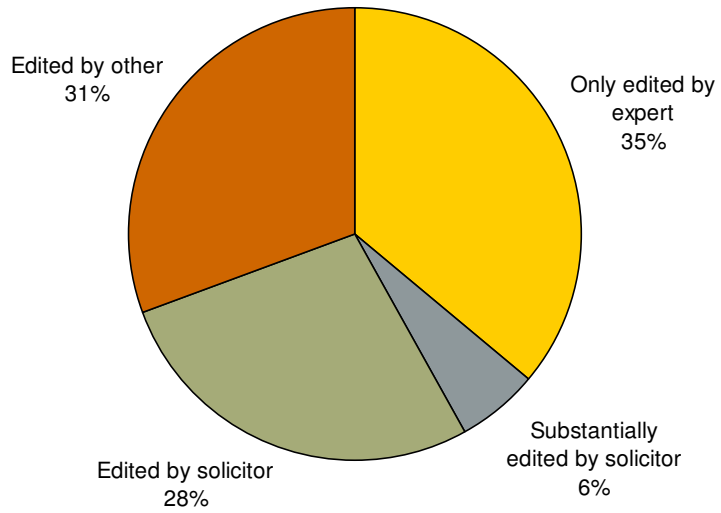


NOTE: Excludes current cases

- 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



What do you need to prove for an (electronic) document?

- Like Kipling, lets learn by simplification:

  "I keep six honest serving men, They taught me all I knew. Their names are **What** and **Why** and **When** And **How** and **Where** and **Who**." from Kipling's "Just So Stories"

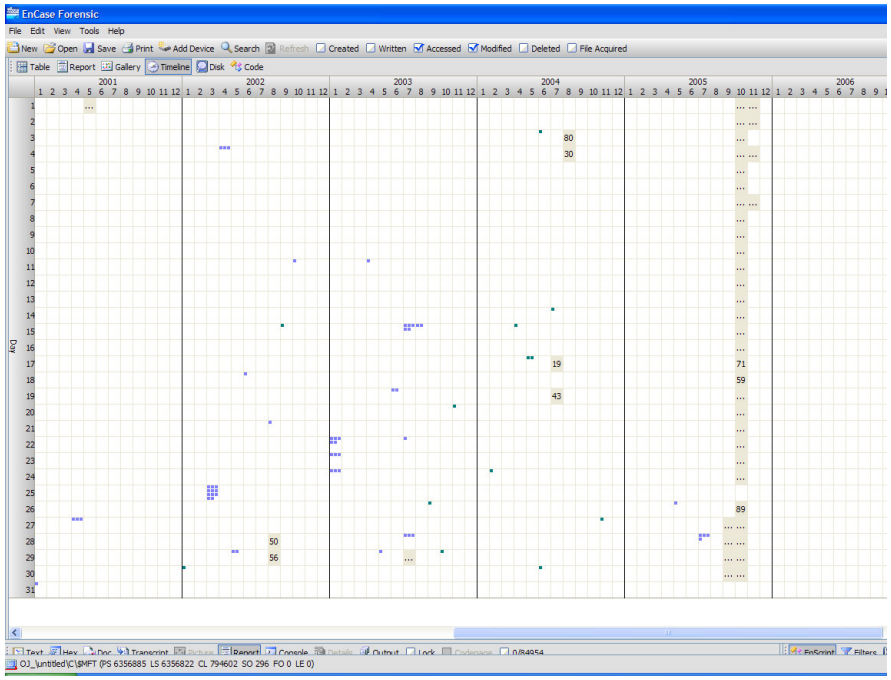
- Who
  - Who authored, edited, printed, read?
  - The person, not merely the computer or a username
  - Multiple digital personas may be same person
  - Identifying markings & document analysis

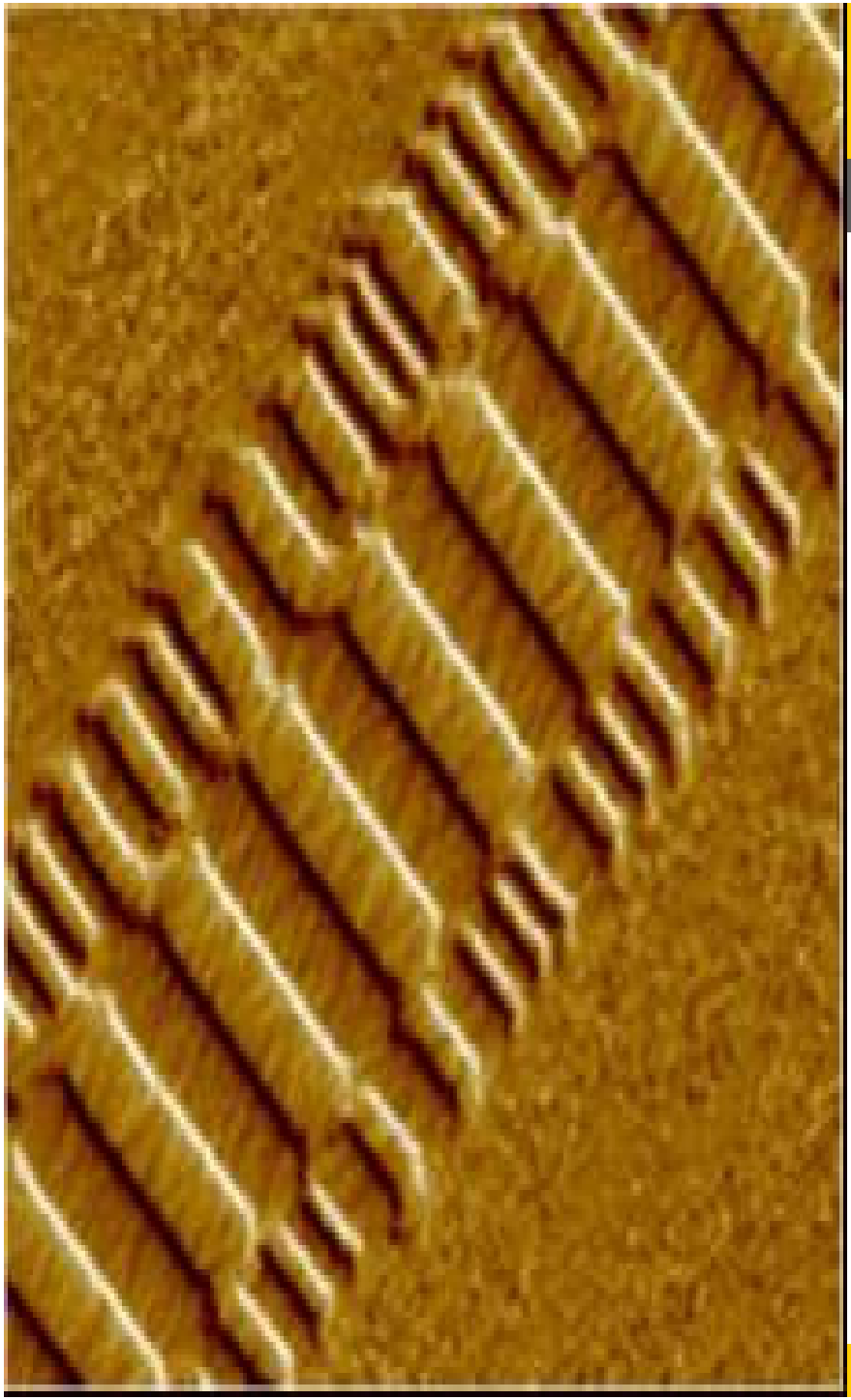
- What (and How)
  - Printed, faxed, e-mail, posted onto website, copied onto USB key, etc

- Where
  - Where was it authored, edited, sent?
  - A real address, not an IP Address (e.g. 203.109.23.2)

- When
  - Real time, not system time
  - Delayed action using time-bomb or salami i.e. pre-programmed
  - Timeline may provide indicator(s) for spoliation or tampering

- Why
  - Circumstantial evidence of Premeditation and indicators for State-of-mind





- Evidence needs to be:
  1. Relevant
  2. Reliable
  3. Sufficient

- Prosecution has an obligation to make reasonable effort to discover both incriminating and exculpatory evidence

- Is the forensic image complete? Are the missing bit(s) relevant?

  – `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. The256ick 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 quick512`

- Is the forensic allowed to have the forensic image?

Hash functions

- Digital Fingerprints
  - The chance of two different files generating the same MD5 hash or “digital fingerprint” is 2^{32}
  - The chance of two different files generating the same SHA1 hash or “digital fingerprint” is 2^{69}

- To put this in the context of “real” fingerprints:
  - the Galton study suggests that the chances of any two human beings having the same fingerprint is one in 6,400,000,000
  - or Osterburg study suggests that the chances of any two human beings having the same fingerprint is one in 100,000,000,000,000,000.

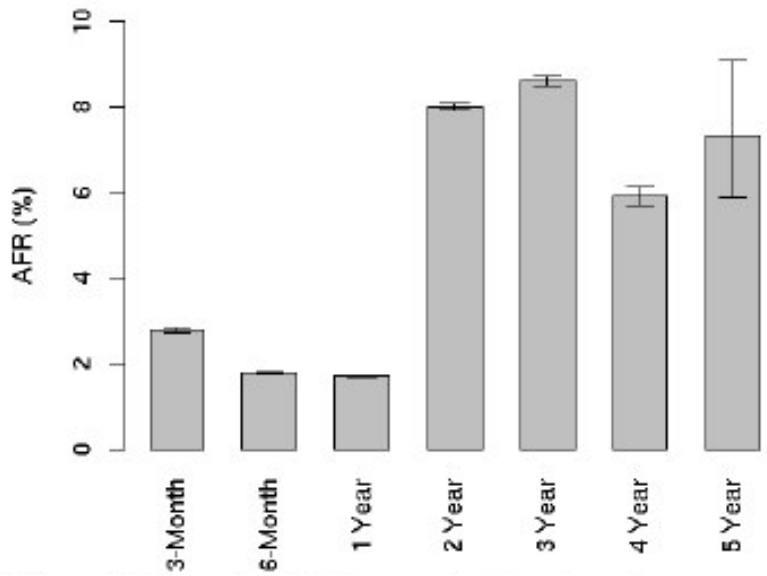
2^{32} = 4,294,967,296
2^{40} = 1,099,511,627,776
2^{69} = 590,295,810,358,705,651,712
6,400,000,000
100,000,000,000,000,000

SUCKOFF.JPG


Keep back from
the platform edge
or you may get sucked off
Penrith


Keep back from
the platform edge
or you may get sucked off
Penrith

Is the process reliable?



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

- 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:
  - 1.5% contained graphical versions of text
  - .5% of recognised formats were unable to be opened
  - 2% contained responsive text in metadata that was not searched
  - ~.05% of speech was responsive

THANK YOU