

# *computer forensic investigations*



Allan Watt BBS, BSc,  
PGDip Forensic, CFCE

# What is Computer Forensics?

- Collection, preservation, analysis and presentation of computer-based evidence
- In litigation, often requires expert testimony

# Extended Definition

Computer-based offending covers:

- criminal offences
- breaches of civil obligations
- procedural offences against organisations' internal policies.

## (a) Computer Crimes

Activity related to the use of computers which amounts to committing an offence as defined by New Zealand's statutory criminal law.

## (b) Civil Offences

Activity related to the use of computers which amounts to breach of a New Zealand Statutory civil obligation or the breach of some form of commercial contractual, tortuous or equitable obligation.

## (c) Procedural Offences

Activity related to the use of computers which amounts to an unauthorised act not covered by (a) or (b) above, such as, for example, a breach of a company's acceptable use policy.

# Some Statistics

- 80% offences committed internally
- Very low percentage prosecuted
- Many cases lost due to the mishandling of evidence.



# Types Of Cases

- Corporate Litigation
- Employment Litigation
- Family Matters
- Criminal Matters

# Corporate Litigation

- Every piece of paper/document originated from a computer.
- Word docs, spreadsheets, memos, faxes, emails, forms, reports, labels, database data.
- Passing off, trademarks, trespass.
- “Every contact leaves a trace” (Edmund Locard)

# Employment Litigation

- Intellectual property theft
- Sales & marketing documents, client lists, patents, operational and technical information.
- Unauthorised access and use.

# Family/Domestic Matters

- Matrimonial
- Cyber sex, web cams
- Chat rooms, emails, harassment, domestic violence, intimidation
- Stalking

# Criminal Matters

- Fraud
- Insolvency, liquidations, bankruptcy
- Indecent publications
- Corroborative evidence

# Value of the Information

- Corroborative evidence
  - Emails
  - Parts of documents
  - Parts of financial information

# Value cont

- Deleted file and formatted hard disk drive.
  - Has it really gone?
  - Can we fix it?
  - Yes we can
  - Temp files, autosave, print spooling
  - Emails the same
  - Swap files

# Value cont

- Intellectual property theft
  - Zip up those marketing/sales plans and send them home on the hotmail account and take them off to the new job or set up in opposition across the road.



# Value cont

- Patent and other legal document theft
  - Let's get those patents and file them before the company does; it was my invention anyway.

# Value

- Anton Piller Orders
  - The key to real and complete discovery.

# Types of Electronic Devices

- Computers
- Palms
- Cell phones
- Faxes

# Tools Used

- Encase principle tool
- Many others fill the box
- Many others on the horizon

# Case Studies

- Florist
- Husband Wife
- Patent
- Passing off
- Sales manager

# Contact Details

Computer Forensic Investigations

Phone (09) 476 7410

[allan.watt@computer-investigations.co.nz](mailto:allan.watt@computer-investigations.co.nz)