Electronic Evidence
(Fact - NOT Fiction)

COMP 4027 Forensic & Analytical Computing Presentation
University of South Australia
April 2009

Robert Taylor
Senior Electronic Evidence Specialist
Electronic Crime Section
South Australia Police

Overview

• About Me
• Definitions
• Background of the Electronic Crime Section
  – Staffing, equipment and forensic tools
• Forensic tools - software and hardware
• Examples of 'Fact, not Fiction'
• Analysis process
• Current and future issues
• Expert evidence

About Me

• Interest in computing started in 1983
  – First ‘home’ computer
• Learnt to type on electric typewriter
• No computers at school until year 10
• No Internet
  – Books, encyclopaedias or newspapers
• ‘cutting and pasting’ involved glue and scissors

Commodore Vic-20
Primary Storage: Cassette tape
Optional: 5¼" disk drive
Cartridge
Microbee 'Computer in a Book'
Primary Storage: 3.5" 400KB disk drive

Amstrad CPC6128
Primary Storage: 3" 180KB (per side) disk drive
Optional: Cassette tape

Commodore Amiga 500
Primary Storage: 3.5" 880KB Disk drive
Optional: 20MB Hard disk drive

IBM 3380
1 Gb hard disk circa 1980
$100,000 USD
About Me

- Worked in Electronic Crime for six years
- Started in retail
- Obtained TAFE Diploma of IT in 1998
  - Lectured at TAFE
  - Help desk
  - Desktop support
  - IT project work
- Hope to complete Bachelor of Information & Communications Technology this semester

Background

- Started in 1998
  - With one member
- Formal ECS established six years ago
  - Part of Commercial and Electronic Crime Branch
- Mixed model
  - Sworn conduct investigations
  - Unsworn conduct Analysis
- Service provided across SAPOL
  - Post seizure & on-site analysis, expert witness

Staffing – 2003

- Officer In Charge (OIC)
- Analysts
  - Technical Skills
    - Prior Expertise
- Investigators
- Intelligence

Staffing - 2009

- Officer In Charge (OIC)
- Specialists
  - Technical Skills
    - Qualifications
    - Prior Training
    - Prior Expertise
- Investigators
- Intelligence
- Support officers
**Forensic Tools**

**2003**
- EnCase version 3
- Dr. Sim

**2009**
- EnCase version 6
- FTK version 2
- Mac Forensics Lab
- X-Ways Forensics
  - Infinadyne CD/DVD Inspector
  - Mount Image Pro
  - Virtual Forensic Computing
  - XRY
  - Cellebrite UFED

**Hardware**

**2003**
- 8 Laboratory Bays, 7 PCs
- SAPOL Computer
- Analysis Computer
- Laptop
- Single Monitor (CRT)
- Removable HDDs for storage
- IDE write blockers
- Rimage (CD-ROM only)
- 2 Image Masster Solo-II

**2009**
- 8 bays, 3 PCs & and 3 Apple Macs
- SAPOL Computer
- Analysis Computer
- Laptop
- One 22” & 19” Screen (LCD)
- 30TB of central storage
- IDE, SATA & USB write blockers
- Rimage (CD/DVD/Blu-ray)
- 2 Image Masster Solo-II + Solo-III
Forensic
“pertaining to, connected with, or used in courts of law or public discussion and debate.”
Random House Dictionary
“Relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law.”
American Heritage Dictionary

Forensic Computing
“the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable”
McKemmish, Rodney (1999). ‘What is forensic computing’

Electronic Evidence
“any records generated by, or stored on a computer system that may be used in evidence in court”
Standards Australia, HB171-2003 Guidelines for the management of IT evidence

Why?
- Where electronic evidence is the subject forensic computing is the process
- Developed as a response to demand by law enforcement
- Civil litigation – intellectual property infringement
- Disciplinary issues - employee misuse
- E-discovery
**Reasons for Analysis**

- Identify the presence of electronic evidence
- Absolve the innocent
- Locate an offender
- Pattern of behaviour
- Identify an owner
- Identify method of offending

**Principles**

- No action taken should change electronic data
- Original data should only be accessed by a qualified person.
- An audit trail of processes undertaken must be kept (chain-of-custody).

**Write Blockers**

[Source: http://www.ics-iq.com/images/product/DriveLockIDEPic1.gif]

**Forensic Duplicators**

[Source: http://www.tableau.com/images/products/t3u_front_view_hi_res.gif]

[Source: http://www.tableau.com/images/products/td1_front_elevated_hi_res.jpg]
**Forensic Duplicators**

- Physical examination of the exhibit(s)
- Creation of a forensic copy (image)
- Examination/Review
  - File comparison – hash values
  - Keyword searching
  - Time lines
  - Recovery of deleted folders / files
  - History of Internet usage, emails & chats
  - Extraction to other media
- Analysis/Extraction of identified data
- Declaration and Report

**Hardware Accelerator**

- View encrypted volumes/protected content
- Use software on the exhibit to parse data
  - CCTV
  - File sharing
- Malware/virus behaviour analysis
- Demonstration in court
- VMware disk (.vmdk) can be loaded into forensic analysis software for analysis
**Fact or Fiction?**

Electronic Evidence is only related to fraud.
Fact or Fiction?
Electronic Evidence is only about computers.

Electronic devices
- Organisers / Pocket Computers
- Mobile Phones
- Fax Machines
- Digital Cameras
- MP3 Players
- GPS units

Other devices
Have become increasingly complex in the range of functions:

- Audio/Voice Recorder
- Digital Still Camera
- USB Data Storage
- Video Camera
- Video Player

Data storage has exceeded the capacity of the SIM card.

Mobiles now store most data on built-in memory, and other types of removable media.

Mobile Telephones

- Data storage has exceeded the capacity of the SIM card.
- Mobiles now store most data on built-in memory, and other types of removable media.

Closed Circuit Television

- CCTV Everywhere!
- Proprietary hardware/recording standards
- Large amount of data
- Time-consuming

CCTV Everywhere!

To: Officer in Charge, Electronic Crime Subject: Electronic Analysis

I am investigating ... and as a result have 4 computer servers, as well as laptops and USB drives I need analysed.

I was wondering if I could arrange a time with you later this week to bring these items in as I will need to bring them in a Ute.
Fact or Fiction?
Having a quick look through a computer doesn’t hurt!

• Example - Laptop powered on (Windows XP):
  – 2,522 accessed, 169 Files/Folders created,
  – 318 written, 405 modified

• Evidence may be overwritten and lost.
• File date / time stamps will be modified.
Fact or Fiction?
Anyone can find electronic evidence.

Fact or Fiction?

Electronic Evidence is always complex

Fiction

- You will not see everything:
  - Deleted files
  - Hidden files
  - Unallocated space
    - Text fragments
    - Printer output
  - File slack
  - Registry information and settings
  - Instant Messenger conversations
Issues

- Increasing workload
  - Storage levels increase, get smaller & cheaper
  - Increasing amount of data
- Accreditation & Training
- Encryption
- Online Applications & Storage
- Triage considerations
- CCTV
- Time for research & development

Certification

IACIS
The International Association of Computer Investigative Specialists
Conferences

01100101
11001011
0010100110

e-Forensics 2009

<table>
<thead>
<tr>
<th>THE 2009 TECHNO SECURITY CONFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>C$$IC 2009</td>
</tr>
<tr>
<td>May 17th - 20th</td>
</tr>
<tr>
<td>Crown Metropalece Resort</td>
</tr>
<tr>
<td>at Universal Orlando</td>
</tr>
<tr>
<td>Reaching New Heights</td>
</tr>
<tr>
<td>Digital Investigations</td>
</tr>
</tbody>
</table>

QUESTIONS?

Robert Taylor
Senior Electronic Evidence Specialist
Electronic Crime Section
South Australia Police

FILE SYSTEM FORENSIC ANALYSIS

BRIAN CARRICK

4/26/2009