8 Years of Triage. A Case Study of State Electronic Evidence Branch (SEEB) of the NSW Police Force

Brian Jones
State Electronic Evidence Branch
New South Wales Police Force

Michael Wilkinson
Champlain College
(formerly New South Wales Police Force)
About Brian

IT Contractor
About Mike

IT Contractor
Today

- Background on LE & Law in Australia
- History of SEEB
- Challenges of CP investigations
- The SEEB Preview & ‘Discovery’ processes.
- EnScripts & applications created by SEEB.
Australian LE Agencies
About NSW

- Pop: 6.5 million
- Area: 309,432mi$^2$
  (area of Texas: 268,600mi$^2$)
- Police Force: ~20,000
  (~17,000 sworn)
State Electronic Evidence Branch (SEEB)

- Created in 2003
- Funded in response to terrorism threat presented by 9/11 & Bali bombings
- Provide a response to “serious major crime”

- NSW Police also have:
  - Computer Crime Unit
  - Internet Child Protection Unit
SEEB Structure 2003

Office Manager C5/6

SEEB Controller

SEEB Elect. Evidence Coordinator DPO6

SEEB Ops Coordinator Senior Sergeant

Analyst Team
- Electronic Evidence Specialist DPO5
- Electronic Evidence Specialist DPO4
- Electronic Evidence Specialist DPO2

Research and Development
- Senior E.E. R&D Officer DPO5

SEEB Team 1
- Sergeant
- Senior Constable
- Constable

SEEB Team 2
- Sergeant
- Senior Constable
- Constable
SEEB Capabilities

- Computers (duh)
- Mobile phones
- GPS
- CCTV
- Embedded devices (ECM etc)
- Hardware level recovery
- Covert activities
SEEB Business July 2010 – July 2011

- Child Pornography 19%
- Homicide 17%
- Sex Offence - Assault 12%
- Drug Detection 10%
- Robbery 8%
- Telecommunications 5%
- Fraud 6%
- Assault 3%
- Break and/or Enter 2%
- Fire - Breach 2%
- Miscellaneous 2%
- Judicial 2%
- Located Person 2%
- Other Offences Against Person 2%
- Firearm Offences 1%
- Other 7%
Operation Auxin - 2004

- Grew out of Operation avalanche in US
- Servers from Landslide productions seized
- Approx 300 targets in NSW
- 2 Stage response
  - High risk targeted in first 3 weeks
  - Low risk in following 3 months
NSW CP Laws (pre 2004 changes)

- Any media must be refused classification by Office of Film & Literature Classification Board
- Images refused classification if they depict children under 16 in sexual or sexualized posses. (includes created pictures)
- Stories describing sex involving children under 16 will also be refused classification
- Offences- Possession or Dissemination
Auxin on site preview

1. Identify CP files
   1. Pictures
   2. Video
   3. PPT
   4. Documents
2. Keyword search
3. Manual search

If material identified sample burnt to CD for classification
Auxin after 3 weeks (stage 1)

- 162 search warrants attended
- 782 computers examined
- 12,860 CD’s & Floppies examined
- 500,000+ Pictures & movies RC
- 24,850kms travelled
- $43,000 overtime for all NSW Police
- $40,000 overtime for SEEB staff 😊
Auxin Stage 2

- Investigators seize computers without preview
- Transported to SEEB for preview by SEEB staff
- Go on the backlog
- 6+ months by mid 2005.
- 3 officers transfer out due to stress induced by CP
Child Pornography – investigation issues

- Data volumes
- High plea rate
- ‘Criminality’ concepts – material quantity and severity.
- Investigation risks, OH&S, child at risk, prosecution time frames.
Change in the Law

- End of 2004 legislation changes. CP is identified by “reasonable person test”
- SEEB staff are no longer reasonable persons due to over exposure 😞
Client Assisted Preview (CAP)

- Commenced 2006

- Investigator:
  - ☐ attends SEEB with exhibit
  - ☐ Retains custody of exhibit
  - ☐ Spends day (or more) looking through system
  - ☐ Walks away with CD of material of interest
  - ☐ If further analysis required exhibit remains at SEEB
CAP resources

- Dedicated secure rooms
- Machines reghosted before each job
- Enscripts used to automate reporting e.g. Registry keys
- Keyword lists
- Hash sets
CAP Success

- Backlog reduced to < 3 months
- Significant reduction in staff exposure to CP
- Greater input/interaction with investigators
- SEEB staff spend more time on analysis 😊
CAP Challenges

- Backlog still too long
- SEEB staff over servicing
- Investigators getting distressed by over exposure to CP!
- With growing data sizes CAP can still take days
- SEEB and Police resources are finite and prioritising staff to work on other jobs i.e. homicides & other serious offences
About Research and Development

- Mission – “To provide enhanced computer forensic capability for SEEB and its clients”
- Possible name change to “Capability Development”
- Achieved through –
  - 50% Proactive
  - 40-45% Reactive
  - 5-10% Training
- History –
  - Between 1 – 2 staff since inception
Current limitations

- Exhibits can store large quantities of data.
- It is rapidly becoming impossible for a human reviewer to examine this data in a reasonable amount of time.
- This can take several days to process using Client Assisted Preview (CAP) method
- Previous average of almost 8 months between request and job completion.
- SEEB and Police resources are finite and prioritising staff to work on other jobs i.e. homicides & other serious offences
An Engineered Response

- The ‘Discovery’ Process - in use since September 2009.
- Task acceptance criteria
- Random sampling and limited examination
- ‘Deemed’ possession
- Paper based output
- Does not replace CAP’s – only for certain jobs
Legislative Amendment

From Crimes Amendment(Child Pornography & Abuse Material) Act 2010 No 9, Part 4A, Schedule 2, Page 8:

289B Use of random sample evidence in child abuse material cases

(1) An authorised analyst may, in connection with any proceedings for a child abuse material offence, conduct an examination of a random sample of the child abuse material or alleged child abuse material that is the subject of the proceedings concerned.

(2) In proceedings for the child abuse material offence concerned, evidence adduced by the prosecutor of any findings of the authorised analyst as to the nature and content of the random sample is admissible as evidence of the nature and content of the whole of the material from which the random sample was taken.
Discovery

- Uses random sampling to limit files viewed. No more than 10,000 images need to be sampled.
- Automated and assisted scaling, bookmarking, exporting and reporting.
- Job waiting period is now weeks instead of 8 months for CAPs. No backlog.
- One SEEB staff member can supervise up to 6 jobs at any one time.
- Multiple jobs completed in hours rather than days.
Discovery room
Discovery process overview

- SEEB R&D developed EnScripts controlling EnCase forensic software.
- The case officer only has to view a sample of the total data set.
- Results are extrapolated against the total population.
Create Discovery job dialogue

SEEB Job: Enter New Exhibit Details

Please enter the details of the exhibit below

Client Exhibit Reference (e.g. D12345)
X1234567890

Client Exhibit Location (e.g. Surry Hills Police Station)

SEEB Exhibit Reference (OPTIONAL)

☑️ Exhibit contains other items.

Description of Exhibit.

Exhibit model number

Exhibit serial number
Discovery Process

Exhibit “booted” into a controlled environment to facilitate forensic interrogation by room supervisor.

All valid allocated images, movies and documents are:
- Identified through signature analysis
- Counted
- Randomised

Registry files exported automatically and a system/registry report created for SEEB.

A statistically representative sample is isolated for examination.

Sample is then examined by case officer for prohibited material against the CETS scale.

Report and statement generated and printed at conclusion of examination.

The report given to the investigator contains:
- Basic job, device, OS and user account information.
- Selected files with file information.
- Statistical analysis for each file type.
Discovery Gallery / Bookmark view
Bookmark Image Dialogue

Quick CETS categorisation buttons

Category 1
Depictions of children with no sexual activity - Nudity, surreptitious images showing underwear/nakedness, sexually suggestive posing, explicit emphasis on genital areas, solo urination.

Non-penetrative sexual activity between children or solo masturbation by a child - Explicit sexual activity not involving an adult.

Non-penetrative sexual activity between child(ren) and adult(s) - Mutual masturbation and other non-penetrative sexual activity.

Penetrative sexual activity involving child(ren) or both child(ren) and adult(s) - Including, but not limited to, intercourse, cunnilingus and fellatio.

Sadism or bestiality - Sexual imagery involving pain, humiliation or animals.

ANIMATED or Virtual depicting CETS scales 1-5 - Anime, cartoons, comics, CGI and drawings depicting any of the CETS scales (1-5)

Statistics Information - "Must view at least the recommended sample unless 300 files selected"

*** When finished viewing images, record the INDEX NUMBER of the LAST file viewed ***

[Checkbox] Bookmark multiple selected files as the SAME CETS scale.

RECOMMENDED SAMPLE | VIEWED | SELECTED
---------------------|--------|--------
1796                 | 50     | 1      

ESTIMATE | RELIABILITY | RELATIVE STANDARD ERROR
1 - 126 | UNRELIABLE ESTIMATE | 25.21%

A lower Relative Standard Error indicates a more reliable estimate
Review & file export Dialogue

Picture files of interest selected: 227
- Level 1... (37%)
- Level 2... (17%)
- Level 3... (6%)
- Level 4... (14%)
- Level 5... (26%)

Multimedia files of interest selected: 2
- Level 1... (50%)
- Level 2... (0%)
- Level 3... (0%)
- Level 4... (0%)
- Level 5... (50%)

Documents of interest selected: 2
- Level 1... (0%)
- Level 2... (60%)
- Level 3... (0%)
- Level 4... (0%)
- Level 5... (60%)

Other files of interest selected: 4
- Level 1... (0%)
- Level 2... (0%)
- Level 3... (0%)
- Level 4... (0%)
- Level 5... (0%)

If you have finished your examination of files on this exhibit click the Next button.
Electronic Evidence Discovery Report
SEEB Task Number E01/0001

<table>
<thead>
<tr>
<th>Investigator Name</th>
<th>Detective Senior Constable John Smith</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accused Name</td>
<td>John DOE</td>
</tr>
<tr>
<td>Accused Date of Birth</td>
<td>12 March 1980</td>
</tr>
</tbody>
</table>

WARNING: This report contains offensive material. Disclosure is subject to the Sensitive Evidence Provisions under Chapter 6, Part 2A of the Criminal Procedure Act 1986.
2 Exhibit Item X1234567890

2.1 Description

<table>
<thead>
<tr>
<th>Exhibit Reference</th>
<th>X1234567890</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exhibit Location</td>
<td>Surry Hills</td>
</tr>
<tr>
<td>SEEB Exhibit Reference</td>
<td></td>
</tr>
<tr>
<td>Exhibit Description</td>
<td>A silver HP EliteBook laptop computer</td>
</tr>
<tr>
<td>Date/Time of examination</td>
<td>03/08/11 10:13:49</td>
</tr>
</tbody>
</table>

2.2 Device Summary

2.2.1 RS005

<table>
<thead>
<tr>
<th>Name</th>
<th>RS005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>88402656188E</td>
</tr>
<tr>
<td>Drive Type</td>
<td>DRIVE</td>
</tr>
<tr>
<td>Total Size</td>
<td>19.1GB</td>
</tr>
</tbody>
</table>

2.2.1 C

<table>
<thead>
<tr>
<th>Volume Label</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Name</td>
<td></td>
</tr>
<tr>
<td>File System</td>
<td>NTFS</td>
</tr>
<tr>
<td>Total Capacity</td>
<td>20538490380, 19.1GB</td>
</tr>
<tr>
<td>Unused Space</td>
<td>14GB</td>
</tr>
</tbody>
</table>

2.3 Operating System No 1

<table>
<thead>
<tr>
<th>Operating System Name</th>
<th>Microsoft Windows XP Service Pack 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>RS005C</td>
</tr>
<tr>
<td>Time Zone Information</td>
<td>GMT +10:00/Canberra, Melbourne, Sydney</td>
</tr>
<tr>
<td>Registered Owner</td>
<td>John Smith</td>
</tr>
<tr>
<td>Registered Organisation</td>
<td>John Smith</td>
</tr>
<tr>
<td>Installed Date</td>
<td>08/04/09 11:19:30</td>
</tr>
</tbody>
</table>

2.3.1 User Account 1

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td></td>
</tr>
<tr>
<td>Last Logon</td>
<td>21/05/09 09:34:00</td>
</tr>
<tr>
<td>Number of Logons</td>
<td>8</td>
</tr>
<tr>
<td>Password present</td>
<td>Yes</td>
</tr>
<tr>
<td>ScreensaverPassword</td>
<td>disabled</td>
</tr>
</tbody>
</table>

2.3.2 User Account 2

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td></td>
</tr>
<tr>
<td>Last Logon</td>
<td></td>
</tr>
<tr>
<td>Number of Logons</td>
<td>0</td>
</tr>
<tr>
<td>Password present</td>
<td>No</td>
</tr>
<tr>
<td>ScreensaverPassword</td>
<td>disabled</td>
</tr>
</tbody>
</table>
### 2.4.2 CETS Level 1: Depictions of children with no sexual activity

<table>
<thead>
<tr>
<th>File Index</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Bliss.bmp</td>
</tr>
<tr>
<td>File Path</td>
<td>X:\1234567890\RS0651\WINDOWS\Web\Wallpaper\Bliss.bmp</td>
</tr>
<tr>
<td>File Created</td>
<td>08/04/08 11:14:25</td>
</tr>
<tr>
<td>File Modified</td>
<td>08/04/08 11:14:25</td>
</tr>
<tr>
<td>MD5 Hash Value</td>
<td>218D23D52AF34D39089E0861D4B3AF</td>
</tr>
<tr>
<td>CETS Scale</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Index</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>F:\000338_WMF</td>
</tr>
<tr>
<td>File Path</td>
<td>X:\1234567890\RS0651\Program Files\Microsoft Office\CLIPART\PUB60\CORE\FD00338_WMF</td>
</tr>
<tr>
<td>File Created</td>
<td>08/03/08 16:57:04</td>
</tr>
<tr>
<td>File Modified</td>
<td>08/03/08 16:57:04</td>
</tr>
<tr>
<td>MD5 Hash Value</td>
<td>B0F4C80910EFC352BDF661D398681ADC0</td>
</tr>
<tr>
<td>CETS Scale</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Index</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>J:\0095167.jpg</td>
</tr>
<tr>
<td>File Path</td>
<td>X:\1234567890\RS0651\Program Files\Microsoft Office\CLIPART\PUB60\CORE\J0095167.jpg</td>
</tr>
<tr>
<td>File Created</td>
<td>08/02/08 02:03:03</td>
</tr>
<tr>
<td>File Modified</td>
<td>08/02/08 02:03:03</td>
</tr>
<tr>
<td>MD5 Hash Value</td>
<td>0C652AF8765E218F3CD5B6904E04FE2704</td>
</tr>
<tr>
<td>CETS Scale</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Index</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>J:\0239079.WMF</td>
</tr>
<tr>
<td>File Path</td>
<td>X:\1234567890\RS0651\Program Files\Microsoft Office\CLIPART\PUB60\CORE\J0239079.WMF</td>
</tr>
<tr>
<td>File Created</td>
<td>30/07/02 17:39:30</td>
</tr>
<tr>
<td>File Modified</td>
<td>30/07/02 17:39:30</td>
</tr>
<tr>
<td>MD5 Hash Value</td>
<td>0A2354D723ED2F85AE2571D4CAD2BEA1</td>
</tr>
<tr>
<td>CETS Scale</td>
<td>3</td>
</tr>
</tbody>
</table>
## 2.5.2 CETS Level 1 - Depictions of children with no sexual activity

<table>
<thead>
<tr>
<th>File Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>A description of a video viewed by the case officer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Name</th>
<th>Sample.mov</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>File Path</th>
<th>X1234567890\Program Files\QuickTime\Sample.mov</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>File Created</th>
<th>File Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/01/09 17:18:48</td>
<td>05/01/09 17:18:48</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MD5 Hash Value</th>
<th>CETS Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>0E242AB2D25193687BFFDF12813E667</td>
<td>1</td>
</tr>
</tbody>
</table>

Video Files with description
3 Statistical Analysis

The files of interest identified as child pornography in this report are the result of a randomised sampling of a filtered set of files found on each exhibit item.

The statistical breakdown of each exhibit item compares the number of files of interest for each CETS level with the total number of files examined for each file type.

3.1 Exhibit Item X1234567890

3.1.1 Picture files of interest

![Pie chart showing distribution of picture files of interest]

The percentage values in the above chart have been rounded to the nearest whole number. Refer to the following table for an accurate quantity value.

<table>
<thead>
<tr>
<th>Description</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Picture files on this exhibit</td>
<td>30788</td>
</tr>
<tr>
<td>Picture files in sample examined</td>
<td>7548</td>
</tr>
<tr>
<td>CETS Level 1 - Depictions of children with no sexual activity</td>
<td>35</td>
</tr>
<tr>
<td>CETS Level 2 - Non-penetrative sexual activity between children or solo masturbation by a child</td>
<td>33</td>
</tr>
<tr>
<td>CETS Level 3 - Non-penetrative sexual activity between child(ren) and adult(s)</td>
<td>14</td>
</tr>
<tr>
<td>CETS Level 4 - Penetrative sexual activity involving child(ren), or both child(ren) and adult(s)</td>
<td>31</td>
</tr>
<tr>
<td>CETS Level 5 - Sadism or bestiality</td>
<td>58</td>
</tr>
<tr>
<td>Picture files of interest selected from sample</td>
<td>227</td>
</tr>
<tr>
<td>Percentage of Picture files of interest in sample</td>
<td>3.01%</td>
</tr>
<tr>
<td>Estimated number of valid Picture files of interest on this exhibit</td>
<td>790 to 1061</td>
</tr>
</tbody>
</table>
SEEB EnScripts that are used to automate processes that were done manually or inefficiently – also used for full analysis jobs. They include:

- Initialise Case.
- Preview File Listing (Syd Pleno, AFP).
- Create Case (Syd Pleno, AFP).
- Web Page rebuilder.
- Email parsing / reporting.
- EXIF processing / reporting.
- Bookmark cache images.
- Google Chrome Internet history parser (Co-written with Oliver Hopli / Switzerland).
- Mounted / USB / Camera devices report.
- Bookmark data exporter (Syd Pleno, AFP).
- Internet & Windows Shortcut Parser (Syd Pleno, AFP).
- Date & Time Activity Parser.
- AVI/ASF/WMV/BMP File size carver.
- Duplicate files report
EnScripts – Initialise case

- Same as initialise case part of Discovery but customised for CAPS.
- Exports all registry files, maintaining folder structure
- Creates a formatted rtf report containing the following information:
  - Device & Volume information.
  - Connected USB / Mounted devices.
  - Operating system.
  - Time zone.
  - User accounts.
  - Network, IDE & processor info
  - Recents, MRU’s and User Assist entries for each user account.
- Creates a detailed excel report on mounted, usb and other devices. Based on Lance Mueller's script. Includes
Initialise case dialogue.
Initialise case report

Time Zone Information for: RS005/C

[ Registry base key path: System\Control\Set001\Control\TimeZoneInformation ]

SYSTEM: RS005/C

Standard Name: AUS Eastern Standard Time
Standard Time Start: Sunday the 1st week of April at 3:00
Daylight Savings Time Start: Sunday the 1st week of October at 2:00
Daylight Savings Name: AUS Eastern Daylight Time
Active Time Bias: 10 hours offset from UTC
Time Zone: (GMT+10.00) Canberra, Melbourne, Sydney

Standard time is set to change the standard bias by 0 minutes
Daylight savings time is set to change the standard bias by 60 minutes

Operating System Information for: RS005/C

Product Name: Microsoft Windows XP
Last Service Pack: Service Pack 3
Current Version: 5.1
Path Name: C:WINDOWS
Product Id: 55274-640-1478787-23070
Registered Owner: John Smith
Source Path: D:\i386
System Root: C:WINDOWS
Current Build No.: 2600
Install Date: 08/04/09 11:19:38
Last Shut Down Time: 21/05/09 10:13:12
Shut Down Count: 8
AutoAdminLogon: disabled
Default user name: Administrator
Default domain name: SOMEPC
Default Password: 

Account Information for: RS005/C

PROFILE: ********************** Administrator **********************

Full Name: 
Type of User: Local User
Account Description: Built-in account for administering the computer/domain
Primary Group: Domain_Users
Security Identifier: S-1-5-21-134012491-1644491937-682003330-500
Logon Script:
Profile Path: %SystemDrive%\Documents and Settings\Administrator
Last Logon: 21/05/09 09:33:54
Last Password Change: 08/04/09 21:07:33
Last Incorrect Password Logon: 21/05/09 09:33:54
Number of Logons: 8
Password present: Yes
Account active: Yes
NT password Hash: 0100001005b2641971e9febec7911b34fcee05
LM Password Hash: 01000100b23eefcbb77138b643a14c3ee27eb5d
Screen saver password: disabled
Last IE Download folder: C:Documents and Settings\Administrator\My Documents\ids

========================== RECENTS ==========================

Hilarious entertainment vid
.avi
BERNARD - Polar Bear (2007).avi

Vermont_Teddy_Bear_Commercial.flv
Preview File List

- Used in most preview jobs where files of interest have been selected.
- Written by Syd Pleno(AFP).
- Exports selected bookmarked files and creates folders based on bookmark names.
- Creates an excel spread sheet file listing.
- Many options allowing customisation of the file list.
- Helps maintain standardised output for all previews.
- May be updated to output to SQLite / XML format
Preview File List Dialogue

[Preview File List (version 2.2.2)] Step 3 - Configure output options

- Filelist Report Heading
  - TEST - *\BOOKMARK\FOLDER %*

- Organisation/Agency Name
  - State Electronic Evidence Branch, NSW Police Force

- Folder to export filelist and files
  - D:\TEST\Export

- Calculate MD5 hash values and add to case
  - [ ]

- Export entries to subfolder where filelist is saved
  - [ ]
  - Name of folder to export files to:
  - [ ] Customise export folder
  - [ ] Export physical file (logical file + file slack)

- Generate Excel filelist
  - [ ]
  - Excel filename
  - [ ] Customise filename
  - [ ] Include Glossary on the front page of the filelist

- Generate XML filelist
  - [ ]
  - XML filename
  - [ ] Customise filename

- Generate SQLite database
  - [ ]
  - SQLite filename
  - [ ] Customise filename

[ ] Finish
[ ] Cancel
[ ] < Back
# Preview File List Report

## ETEST - Pictures

Full Path - The location the file was found on the storage device.

File Created - In general, this should be the time the file was placed on the file system. This value may be changed by other actions such as unpacking a file from a zip archive or deleting data from an email.

File Contents Last Modified - In general, this should be the time the file was last saved. This value may be changed by other actions such as uploading files from a zip archive or downloading data from an email.

File Metadata Last Modified - By default, this is when the file system metadata for this file was last changed. This value may be changed by other actions such as virus scanning.

Deleted - This entry is a deleted file.

Export File Name - The files listed in this table have been exported to a CD or DVD. The directory structure has been preserved and in order to avoid identical filenames, numbers have been appended to the original file name. The original filenames are listed in the Full Path column.

Hash Value - The Message Digest 5 (MD5) hash value of the file’s contents.

Note: File system date and time values can be affected by a large number of different factors, without user interaction. If date and time values in this report are of any significance, further advice should be sought from a computer forensic expert.

<table>
<thead>
<tr>
<th>#</th>
<th>Full Path</th>
<th>File Created</th>
<th>File Contents Last Modified</th>
<th>File Metadata Last Modified</th>
<th>Deleted</th>
<th>Export File Name</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:41</td>
<td>07:39:41</td>
<td>07:39:41</td>
<td>No</td>
<td>Mike1[1].gif</td>
<td>5925742245241345415</td>
</tr>
<tr>
<td>2</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:40:05</td>
<td>07:40:05</td>
<td>07:40:05</td>
<td>No</td>
<td>Mike24[1].gif</td>
<td>662569726952528275</td>
</tr>
<tr>
<td>3</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:51</td>
<td>07:40:31</td>
<td>07:40:31</td>
<td>No</td>
<td>Mike3[1].gif</td>
<td>566397681364821465</td>
</tr>
<tr>
<td>4</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:48</td>
<td>07:40:48</td>
<td>07:40:48</td>
<td>No</td>
<td>Mike4[1].gif</td>
<td>5569723456345672345</td>
</tr>
<tr>
<td>5</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:49</td>
<td>07:40:39</td>
<td>07:40:39</td>
<td>No</td>
<td>Mike5[1].gif</td>
<td>565497681364821465</td>
</tr>
<tr>
<td>6</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:48</td>
<td>07:40:48</td>
<td>07:40:48</td>
<td>No</td>
<td>Mike6[1].gif</td>
<td>5569723456345672345</td>
</tr>
<tr>
<td>7</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:49</td>
<td>07:40:39</td>
<td>07:40:39</td>
<td>No</td>
<td>Mike7[1].gif</td>
<td>565497681364821465</td>
</tr>
<tr>
<td>8</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:48</td>
<td>07:40:48</td>
<td>07:40:48</td>
<td>No</td>
<td>Mike8[1].gif</td>
<td>5569723456345672345</td>
</tr>
<tr>
<td>9</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:49</td>
<td>07:40:39</td>
<td>07:40:39</td>
<td>No</td>
<td>Mike9[1].gif</td>
<td>565497681364821465</td>
</tr>
<tr>
<td>10</td>
<td>ETEST\Daimar\Documents and Settings\MikeLocal</td>
<td>07:39:48</td>
<td>07:40:48</td>
<td>07:40:48</td>
<td>No</td>
<td>Mike0[1].gif</td>
<td>5569723456345672345</td>
</tr>
</tbody>
</table>
SEEB Web Page Rebuilder

- Based on James Habbens (Guidance) Web Page Rebuilder script.
- Updated to allow for parsing, rebuilding and reporting of compound cache files i.e. Mozilla _CACHE files, safari and Google Chrome / desktop files.
- Can parse and search Gzipped files / compound files.
- Creates HTML reports containing, the rebuilt page, original page and the web page information. The web page information contains original entry info and contained objects etc.
- Examples next few slides...
## Object list for eo=3A8BE00_three-alleged-bikies-face-drugs-charges[1].htm

### Object folder link

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>logo_AAP[1].jpg</td>
<td>Image file</td>
<td>944</td>
</tr>
<tr>
<td>6D84_moldova_0b[1].jpg</td>
<td>Image file</td>
<td>6 KB</td>
</tr>
<tr>
<td>0804_koreasunch_a_145[1].jpg</td>
<td>Image file</td>
<td></td>
</tr>
<tr>
<td>0904_koreasunch_a_145[1].jpg</td>
<td>Image file</td>
<td></td>
</tr>
</tbody>
</table>

### Web Page Reports

- **Page Title:** Drug raids may help outlaw bikie group
  - Last Accessed: 08/04/09 16:53:45

- **Page Title:** News Headlines - Top Stories - NineMSN News
  - Last Accessed: 08/04/09 16:57:54

- **Page Title:** Fourth Knox school teacher charged
  - Last Accessed: 08/04/09 17:01:46

- **Page Title:** NineMSN.com.au
  - Last Accessed: 14/04/09 07:43:49
SEEB Web Page Rebuilder – rebuilt search page
SEEB Web Page Rebuilder cont.

- Has the ability to rebuild pages from selected cache images.
- Can create separate reports for “Search” pages i.e. Google, Yahoo.
- Keyword filtering available.
- Many other options.
- Internet History Spread sheets created. Run the Google Internet history search script 1st as EnCase does not support Chrome history.
- Example next slide...
<table>
<thead>
<tr>
<th>#</th>
<th>Browser Type</th>
<th>Profile Name</th>
<th>c1url</th>
<th>c1title</th>
<th>c2body</th>
<th>time</th>
<th>History File Full Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chrome (Windows/ Mac)</td>
<td>Brian</td>
<td><a href="http://www.google.com/chrome/int/en/welcomeback-new.html">http://www.google.com/chrome/int/en/welcomeback-new.html</a></td>
<td>Google Chrome: Welcome back</td>
<td>Welcome back! Check out the following improvements we’ve made since you visited us last. Faster Then Ever Starts up fast, loads pages fast, and searches fast. Themes to add delight to your browser Try Minimalist, Star Gazing, or Google Chrome Artist. Themes. Thousands of new features Add the functionality you need to Google Chrome by installing extensions from our gallery. Not sure what to do next? Type a website address or search query into the address bar, or visit google.com. ©2010 Google - Home - About Google - Privacy policy - Help</td>
<td>04/05/2010 06:30:19</td>
<td>D12345_1ainHIST0\E Hist SIEHIST 4\E Hat 4\Documents and Settings\Brian\Local Settings\Application</td>
</tr>
<tr>
<td>2</td>
<td>Chrome (Windows/ Mac)</td>
<td>Brian</td>
<td><a href="http://www.google.com/chrome?utf-8=en">http://www.google.com/chrome?utf-8=en</a></td>
<td>Google Chrome - Get a fast new browser. For PC, Mac, and Linux</td>
<td>Browses the web, Chrome Fast Google Chrome runs web pages and applications with lightning speed. Download Google Chrome it’s free and installs in seconds For Windows XP, Vista, and 7 Fast start-up Google Chrome Launches in a snap. Fast loading Google Chrome loads web pages quickly. Fast search Search the web right from the address bar. Learn about Google Chrome » Try the latest BETA version » ©2010 Google - Privacy Policy - Help - Google Chrome for Mac or Linux</td>
<td>04/05/2010 06:30:30</td>
<td>D12345_1ainHIST0\E Hist SIEHIST 4\E Hat 4\Documents and Settings\Brian\Local Settings\Application</td>
</tr>
<tr>
<td>3</td>
<td>Chrome (Windows/ Mac)</td>
<td>Brian</td>
<td><a href="http://www.google.com/search?q=hp&amp;src=hp&amp;hl=en&amp;sa=q&amp;ct=gaq&amp;q=hubblesqgalaxies=4ga_fal=">http://www.google.com/search?q=hp&amp;src=hp&amp;hl=en&amp;sa=q&amp;ct=gaq&amp;q=hubblesqgalaxies=4ga_fal=</a></td>
<td>Hubblesite - Search</td>
<td>Web Images Videos Maps News Books Email Search Results Hubblesite - Out of the ordinary...out of this world. News center, gallery, discoveries, sci-tech, fun and games, and reference desk. <a href="http://www.hubblesite.org/">www.hubblesite.org/</a> - Cochaubblesite - Gallery Explore the universe through Hubble’s eye and witness the most dangerous, spectacular and mysterious depths of the cosmos. hubblesite.org/gallery/ - Cochaubblesite - Gallery Explore the universe through Hubble’s eye and witness the most dangerous, spectacular and mysterious depths of the cosmos. - hubblesite.org/gallery/ - Cochaubblesite - Gallery Explore the universe through Hubble’s eye and witness the most dangerous, spectacular and mysterious depths of the cosmos. - hubblesite.org/gallery/ - Cochaubblesite - Gallery Explore the universe through Hubble’s eye and witness the most dangerous, spectacular and mysterious depths of the cosmos.</td>
<td>19/05/2010 09:57:02</td>
<td>D12345_1ainHIST0\E Hist SIEHIST 4\E Hat 4\Documents and Settings\Brian\Local Settings\Application</td>
</tr>
<tr>
<td>4</td>
<td>Chrome (Windows/ Mac)</td>
<td>Brian</td>
<td><a href="http://hubblesite.org/gallery/">http://hubblesite.org/gallery/</a></td>
<td>Hubblesite - Gallery</td>
<td>Search all of Hubblesite HOME NEWS CENTER GALLERY HUBBLE DISCOVERIES HUBBLE TELESCOPE EXPLORE ASTRONOMY EDUCATION &amp; MUSEUMS REFERENCE DESK THE FUTURE WEBB TELESCOPE Search Picture Album Capture the extraordinary Explore the universe through Hubble’s eye and witness the most dangerous, spectacular and mysterious depths of the cosmos. GALLERY PICTURE ALBUM WALLPAPER ASTRONOMY PRINTSHOP BEHIND THE PICTURES SPACECRAFT HUBBLE MOVIE THEATER IMAGE TOURS WALL MURALS Now Hubble images PICTURE ALBUM View an expansive collection of Hubble images. planets, stars, nebulae, galaxies and more. Picture Album spreads the universe out before you in all its dazzling complexity. WALLPAPER Fill your computer screen with a Hubble image. Your body may be trapped at your desk, but your imagination can roam the far reaches of the universe with our cosmic visuals. ASTRONOMY PRINTSHOP Take a piece of the universe home with you. Astronomy Printshop helps you print out your own, museum-quality Hubble images. BEHIND THE PICTURES A...</td>
<td>19/05/2010 09:57:00</td>
<td>D12345_1ainHIST0\E Hist SIEHIST 4\E Hat 4\Documents and Settings\Brian\Local Settings\Application</td>
</tr>
<tr>
<td>5</td>
<td>Chrome (Windows/ Mac)</td>
<td>Brian</td>
<td><a href="http://hubblesite.org/gallery/album/">http://hubblesite.org/gallery/album/</a></td>
<td>Hubblesite - Picture Album</td>
<td>Search all of Hubblesite HOME NEWS CENTER GALLERY HUBBLE DISCOVERIES HUBBLE TELESCOPE EXPLORE ASTRONOMY EDUCATION &amp; MUSEUMS REFERENCE DESK THE FUTURE WEBB TELESCOPE Search Picture Album SHARE GALLERY PICTURE ALBUM View an expansive collection of Hubble images. planets, stars, nebulae, galaxies and more. Picture Album spreads the universe out before you in all its dazzling complexity. WALLPAPER Fill your computer screen with a Hubble image. Your body may be trapped at your desk, but your imagination can roam the far reaches of the universe with our cosmic visuals. ASTRONOMY PRINTSHOP Take a piece of the universe home with you. Astronomy Printshop helps you print out your own, museum-quality Hubble images. BEHIND THE PICTURES A...</td>
<td>19/05/2010 09:57:30</td>
<td>D12345_1ainHIST0\E Hist SIEHIST 4\E Hat 4\Documents and Settings\Brian\Local Settings\Application</td>
</tr>
</tbody>
</table>
SEEB EXIF Viewer

- Processes EXIF data in allocated, deleted or unallocated jpg’s.
- Can filter on camera make and /or model.
- Bookmarks most EXIF, TIFF and Thumbnail tags with the data enumerated for meaningful values. (Used Phil Harvey's excellent “Exif tool” to verify and enumerate values)
- Bookmarks most GPS and XMP (Adobes eXstensible Metadata Platform) data. Provides metric GPS data for import into Google Maps / Earth.
- Reporting options include, Bookmarks, RTF, HTML and an excel file listing.
- Exports images.
- Other basic filtering available.
- Examples on next few slides...
SEEB EXIF Viewer dialogue
SEEB Email Parser

- Email parsing and reporting script using Aid4mail with the EnScript “Execute” class and the command line.
- Emails searched for and exported by EnCase.
- Control then given to Aid4Mail console version which parses emails and creates a HTML report.
- Control then given back to the EnScript which then re-formats HTML reports and creates the master reports.
- No need to mount emails in Encase – only exporting.
SEEB Email Parser

Options

Email export options | Email Reporting Options | Keyword / Filter Options

- Enable Keyword Search
- Enable date filtering

Filter emails by date

Use date format: "dd/mm/yyyy".

If "FROM DATE" is left blank then search will include all emails <= "TO DATE".
If "TO DATE" is left blank then search will include all emails >= "FROM DATE".

Email date type:
- [ ] received
- [ ] sent
- [ ] downloaded

FROM DATE: 04/08/2011

Search emails for keywords

Only email headers searched by default. Processing time will be increased if "Search full message text" is selected.

Put the most key keywords at the top of the list - this will cut down on processing time.

Only whole words are matched except for email addresses in email header search

- [ ] include
- [ ] exclude

- [ ] Search full message text

Enter key word list. Enter a new line for each search term/phrase.
SEEB Email Parser – Aid4Mail

This image displays the interface of Aid4Mail, a tool for parsing email. The window shows various mail source options, including MAPI, Outlook Express, Eudora, Windows Mail, and Pegasus Mail, among others. The user can select the mail source and specify additional options like including mail in the trash and searching for mail location. The interface also includes fields for profile name and an option to cancel or help with the process.
SEEB Email Parser – HTML Report
SEEB Bookmark Cache

- Parses Internet cache and allows for quick viewing of images from Internet Explorer, Mozilla, Google Chrome, Safari, Opera, Flock and Omni Web from Windows/MAC / Linux systems.
- Is part of Initialise case but can be used as a standalone script.
- Processes and bookmarks images contained within compound cache files, pdf, ppt, shockwave and Google desktop cache.
- All files can be exported and a file listing created – includes file offsets.
SEEB Bookmark Cache

Bookmark cache options

This script will parse and bookmark cache images form IE, Mozilla, Chrome, Safari and Opera from Windows / MAC systems.
It will also parse Mozilla/Chrome/MAC compound cache files and extract images from some pdf / powerpoint documents.
It will also extract images from google chrome web page screenshot thumbnails, shockwave flash files and Google Desktop indexed PNG thumbnails.

- ✔ Bookmark JPG Images
- ✔ Bookmark GIF Images
- ✔ Bookmark PNG Images
- ✔ Bookmark TIF Images
- ✔ Bookmark Bitmap Images

- Export cache image files - this will increase processing time.
  - Create exported files spreadsheet.
- Parse Google Desktop image cache databases. (Will include PNG thumbnails of ALL images indexed on the device)
- Parse deleted cache files.
- Extract images from video files.
- Extract images from documents.
- Extract images from shockwave flash.

OK  Cancel
SEEB Bookmark Cache
SEEB Mounted/USB/Portable Devices EnScript

- Based on Lance Mueller's Script with updates and customisations.
- Creates detailed spread sheets and bookmarks. Bookmarks allow filtering to be performed. Prints to the console.
- Works on offline registry files as well.
- Quick – uses the EnScript Registry class.
- Maps EnCase drive letter to the windows drive letter.
- System Hive – Contol\Set00#\...
  - Enum\USBSTOR
  - Enum\USB
  - Enum\WpdBusEnumRoot\UMB
  - Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  - Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  - Control\Class\{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}
  - Control\Class\{EEC5AD98-8080-425F-922A-DABF3DE3F69A}
- Software Hive
  - Microsoft\Windows NT\CurrentVersion\EMDMgmt
  - Microsoft\Windows Portable Devices\Devices
SEEB Mounted Devices - EnScript
SEEB Mounted Devices - EnScript
# Mounted devices

<table>
<thead>
<tr>
<th></th>
<th>Type</th>
<th>Vendor</th>
<th>Model</th>
<th>Serial</th>
<th>FriendlyName</th>
<th>Created</th>
<th>Revision</th>
<th>ParentFolder</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USB</td>
<td>STOR</td>
<td>SEAGATE</td>
<td>334545384735514780</td>
<td>SEAGATE5</td>
<td>22/01/2010 13:34:57</td>
<td>4.08</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_SEAGATE\PROD_STS6 52211USB8REV_4.08\324D45384735514780</td>
</tr>
<tr>
<td>2</td>
<td>USB</td>
<td>VERBATIM</td>
<td>STORE_N_GO</td>
<td>0791080162780</td>
<td>USB-DRIVE</td>
<td>31/07/2010 01:35:45</td>
<td>5.0</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_VERBATIM\PROD_STORE_N_GO\REV_5.09\0791080162780</td>
</tr>
<tr>
<td>3</td>
<td>USB</td>
<td>CORSAIR</td>
<td>FLASH_VOYAGER</td>
<td>A70680000002556680</td>
<td>ALAN 3GB</td>
<td>16/09/2010 10:17:29</td>
<td>1100</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_CORSAIR\PROD_FLASH_VOYAGER\REV_1100\A0000002556680</td>
</tr>
<tr>
<td>4</td>
<td>USB</td>
<td>APPLE</td>
<td>IPod</td>
<td>0604270014CA1F780</td>
<td>iPod</td>
<td>26/09/2010 16:19:15</td>
<td>1.02</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_APPLE\PROD_IPod\REV_1.02\604270014CA1F780</td>
</tr>
<tr>
<td>5</td>
<td>USB</td>
<td>LEXAR</td>
<td>USB فلاش</td>
<td>602FBW0001HUTN18IFL60</td>
<td>LEXAR</td>
<td>16/11/2010 12:16:45</td>
<td>3000</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_LEXAR\PROD_USB فلاش\REV_3000\602FBW0001HUTN18IFL60</td>
</tr>
<tr>
<td>6</td>
<td>USB</td>
<td>95AC</td>
<td>129A</td>
<td>13F7EA66B6ECCG93BEE1</td>
<td>Apple Fade</td>
<td>20/11/2010 16:14:41</td>
<td>1000</td>
<td>WSD\USB\05AC\PD_129A\13F7EA66B6ECCG93BEE1</td>
</tr>
<tr>
<td>7</td>
<td>USB</td>
<td>CORSAIR</td>
<td>VOYAGER</td>
<td>A30491270001927380</td>
<td>NEW VOLUME</td>
<td>06/31/2010 14:02:45</td>
<td>1100</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_CORSAIR\PROD_VOYAGER\REV_1100\A0041270001927380</td>
</tr>
<tr>
<td>8</td>
<td>USB</td>
<td>94AO</td>
<td>3140</td>
<td>0301875F3AEF4EDAA738E 62F57580826</td>
<td>Canon PowerShot S5</td>
<td>16/03/2014 13:49:83</td>
<td>1000</td>
<td>WSD\USB\04AO\PD_3140\0301875F3AEF4EDAA738E62F57580826</td>
</tr>
<tr>
<td>9</td>
<td>USB</td>
<td>NOKIA</td>
<td>560</td>
<td>35419992673259860</td>
<td>E1</td>
<td>10/03/2011 14:43:10</td>
<td>1</td>
<td>WPDUSENUMRFO\DR\U#33,37C186 B&amp;STOR\GAV\VOLUMEN_77_USBST ORMDISK\VEN_NOKIA\PROD_S5\REV_1.035419992673259860</td>
</tr>
<tr>
<td>10</td>
<td>USB</td>
<td>42I</td>
<td>601C</td>
<td>561067368A001</td>
<td>Portable Device</td>
<td>10/03/2011 14:43:49</td>
<td>1</td>
<td>WSD\USB\042I\PD_601C\561067368A001</td>
</tr>
</tbody>
</table>
Other R&D Projects

- Applications written by previous SEEB R&D staff
  - Forensic DIM SIM
  - Media Previewer
  - LAMA
  - Video Reconstruction / Recovery

- Current applications.
  - Behemoth – multiple & parallel DVD / Blu-Ray burning application in VB using threads.
  - Bulk Copier – C# program to copy and categorize data from optical media for previewing in EnCase.
  - SIRT
  - INFO2 Parser – Recycle bin files...
SEEB Image & Reporting Tool (SIRT)

- Word Macro written in Visual Basic that automates the process of taking screen shots of mobile phones and GPS units that have no standard connection method available i.e. XRY.
- Pictures taken and stored in a structured folder hierarchy.
- The macro is run and the user is shown a dialogue to input exhibit & case details
- Report automatically created. Case details and pictures inserted into document.
- Could be used for any reports using camera images.
- Used by police officers in the field.
- Used by The Australian Federal Police.
### SIRT - Dialogue

#### UserForm1

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event / Case Number</td>
<td>E12345678</td>
</tr>
<tr>
<td>Exhibit No.</td>
<td>D54321</td>
</tr>
<tr>
<td>Examiner</td>
<td>Senior constable Smith</td>
</tr>
<tr>
<td>OIC</td>
<td>Constable Jones</td>
</tr>
<tr>
<td>Branch / LAC</td>
<td>SEEB</td>
</tr>
<tr>
<td>Registered Number</td>
<td>87678</td>
</tr>
<tr>
<td>Registered Number</td>
<td>87879</td>
</tr>
</tbody>
</table>

A bold field name denotes a Mandatory field.

This Macro requires that all the photographs are downloaded into folders. The images are to be placed in relevant named folders or categories - i.e. "INBOX SMS" or "OUTBOX SMS" etc.

These folders are then placed into another main folder (the root or master folder) and given a relevant name that uniquely identifies the item - such as the exhibit number / job number / offender name or item name i.e. D12345/1 or Nokia 3200 etc.
Bulk Copier

- C# application used to improve the examination of optical media.
- Uses PC with 10 DVD/Blu-ray players to copy files, in parallel, from optical disks to a storage device - 40-240GB at a time.
- Many options to allow for categorisation of files and disks to allow for mapping original optical disks to copied files.
- Material from hundreds of DVD’s can be previewed in Encase in one session by the case officer.
Bulk Copier

Bulk Copier V 1.0 Beta

Drive 1
Source: E:\ Label: DVD1
Destination: F:\E11_0001\Disk_1\190811_1816
Progress: Copy
Status: Copying: Silverlight 1.exe to: F:\E11_0001\Disk_1\190811_1816\VBExpress\Silverlight

Drive 2
Source: G:\ Label:
Destination: ...
Progress:
Status: NO Disk in Drive

Drive 3
Source: H:\ Label: image1
Destination: F:\E11_0001\Disk_2\190811_1816
Progress: Copy
Status: Copying: KonicaMinolta.IMAGE_G530.jpg to: F:\E11_0001\Disk_2\190811_1816\VBox\Minolta\image1

Drive 4
Source: K:\ Label: image1
Destination: F:\E11_0001\Disk_3\190811_1816
Progress:
Status: NO Disk in Drive

Drive 5
Source: J:\ Label: image1
Destination: F:\E11_0001\Disk_4\190811_1816
Progress:
Status: Copying: Minolta.IMAGE_F200.jpg to: F:\E11_0001\Disk_4\190811_1816\VBox\Minolta\image1

Drive 6
Source: K:\ Label: image1
Destination: F:\E11_0001\Disk_5\190811_1816
Progress:
Status: Copying: KonicaMinolta.IMAGE_G600.jpg to: F:\E11_0001\Disk_5\190811_1816\VBox\Minolta\image1

Drive 7
Source: L:\ Label:
Destination: ...
Progress:
Status: NO Disk in Drive

Drive 8
Source: M:\ Label: image1
Destination: F:\Neo\Disk_2\Job1
Progress:
Status: NO Disk in Drive

Drive 9
Source: ...
Destination: ...
Progress:
Status:

Drive 10
Source: ...
Destination: ...
Progress:
Status:
Bulk Copier

- Machine Name: 
- User Name: 
- Operating System: Windows 7 Professional
- Source drive info: 
- Volume Label: image1
- Manufacturer: (standard CD-ROM drives)
- Name: ELBY CLONED-RIVE SCD Cfdrom Device
- Device ID: SCDI04R0MVEN_ELEY&PROD_CLONEDRIVE&REV_1A31%2F2D36181%3A000100
- Media Type: DVD-ROM
- Total Size: 250,479,564 bytes
- Format: UDF
- Serial Number: C32C424A
- Destination Path: \\E11\_0001\Disk1_190811_1816
- Directory Name: Disk2_190811_1816
- Number of files to copy: 1941
- Files Copied for drive H:\

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk1_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk2_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk3_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk4_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk5_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk6_190811_1816</td>
<td>19/08/2011</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Disk1_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>40 KB</td>
</tr>
<tr>
<td>Disk2_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>143 KB</td>
</tr>
<tr>
<td>Disk3_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>143 KB</td>
</tr>
<tr>
<td>Disk4_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>143 KB</td>
</tr>
<tr>
<td>Disk5_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>143 KB</td>
</tr>
<tr>
<td>Disk6_190811_1816_log.txt</td>
<td>19/08/2011</td>
<td>Text Document</td>
<td>143 KB</td>
</tr>
</tbody>
</table>
Outcomes

- SEEB has been successful in constantly refining business practices to produce outcomes in an environment of exponentially increasing data volumes and stable technical and human resources.
- Child Exploitation Material possession matters are processed by SEEB within days instead of months.
- Staff exposure to harmful material has been significantly reduced.
- High quality evidence is being presented to Australian Courts.
Future directions

- Pre-processing of data will increase as data volumes increase and automation tools improve.
- Sampling will be applied to other types of data i.e. emails and documents.
- The problem of data volumes for digital forensic triage & examination will most likely be solved using a number of solutions together or separately, such as:
  - Sampling.
  - Emerging image recognition & facial identification technologies.
  - Heuristic analysis.
  - Engineered automated tools / scripts.
References


