Autopsy 3.0

Brian Carrier
VP of Digital Forensics
Basis Technology
## Autopsy 2

### View Directory:

<table>
<thead>
<tr>
<th>Location</th>
<th>File Name</th>
<th>Size</th>
<th>Type</th>
<th>Date/Time</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>E:\</td>
<td>label.exe</td>
<td>32016</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:45 (EDT)</td>
</tr>
<tr>
<td>E:\</td>
<td>legacy.inf</td>
<td>4654</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:40 (EDT)</td>
</tr>
<tr>
<td>E:\</td>
<td>lights.exe</td>
<td>35600</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:40 (EDT)</td>
</tr>
<tr>
<td>E:\</td>
<td>LMREPL.EXE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>E:\</td>
<td>LMREPL.EXE</td>
<td>86800</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:45 (EDT)</td>
</tr>
<tr>
<td>E:\</td>
<td>loadfix.com</td>
<td>1131</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:40 (EDT)</td>
</tr>
<tr>
<td>E:\</td>
<td>loadfix.com</td>
<td>1131</td>
<td>48</td>
<td>2002.06.13</td>
<td>17:08:40 (EDT)</td>
</tr>
</tbody>
</table>

### ASCII (display - report) * Strings (display - report) * Export * Add Note

File Type: MS Windows PE 32-bit Intel 80386 GUI executable

String Contents Of File: E:\system32/inetins.exe

```plaintext
!This program cannot be run in DOS mode.
.text
..rdata
@.data
.rsdc
@.reloc
MSVCR71.dll
KERNEL32.dll
USER32.dll
SVW
```
Why it had to go

• Didn’t run natively on Windows
• Slow UI and analytics
• Old-school HTML
  – Couldn’t right click
• Didn’t allow much at the application level
Autopsy 3 Goals

- Open Source Graphical Platform / Framework
- Automation
- Fast Results / Triage
- Easy to use
- Appeal to large audience
• Started with the Netbeans Platform
  – Java.
  – Designed to build apps like this.
• Designed with lots of internal frameworks.
  – Places where modules can be dropped in.
• Writing lots of docs to help developers build modules.
Ingest Modules

- Run on each image as it is added.
  - In background
  - In parallel
  - Saves previous settings
Ingest Modules

- E01 File
- Web Browser Analysis
- Registry Analysis
- MBOX Thunderbird
- MD5/SHA1 Hash Calculation
- Hash Lookup
- EXIF Extraction
- Add Text to Keyword Index
- ...
Ingest Manager in Wizard

Configure Ingest Modules
Image has been committed. You can configure and run ingest modules on the new image.

- Recent Activity
- Hash Lookup
- Exif Image Parser
- Keyword Search
- Thunderbird Parser

NSRL Database: Enabled
Enable known bad databases for ingest:
- notable_hash_db.txt

- Process Unallocated Space

Calculate hashes even if no hash database is selected

Advanced
• Can configure ingest modules based on available time:
  – Process unallocated space?
  – Search for orphan files?
  – English-only strings extraction?
• Results from Ingest modules are shown as they are found.
  – Ingest Inbox gives updates.
Ingest Inbox Screen Shot
Scheduler focuses on user content:
1. User folders
2. Program Files folder
3. Windows folders

Scheduler will be modular to allow for different approaches.
• Wizards to create cases and import data.
• Single navigation tree to find ingest module results.
  – Modules post results to blackboard.
  – More details will be given in the framework talk.
• Common navigation concepts:
  – Back and Forward buttons
  – Search bar in upper right
Easy To Use
Appeal to Large Audience

• Focused first on Windows.
• Installer
• Auto-update
• Basic features
  – Keyword Search
  – Hash Databases
  – File System Browsing
  – Registry Analysis
  – E-mail Analysis
Keyword Search Module

• Index-based search
• Extracts text from documents:
  – Better for non-English PDF and HTML files
• Uses Lucene SOLR (open source)
• Can support more advanced text analytics.
• Searches are done as image is indexed.
• Can save and export keyword lists.
Configure Ingest Modules

Image has been committed. You can configure and run ingest modules on the new image.

- Recent Activity
- Hash Lookup
- Exif Image Parser
- Keyword Search
- Thunderbird Parser

Select keyword lists to enable during ingest:

- Phone Numbers
- IP Addresses
- Email Addresses
- URLs
- Drug Terms
- Bank Terms

Scripts enabled for string extraction from unknown file types:
- Latin - Basic

Encodings: UTF8, UTF16

Process Unallocated Space

Advanced
Hash Database Module

• Can calculate MD5 and SHA-1 hashes of all files.
• Looks up hashes in:
  – NSRL (known files)
  – EnCase hashsets (notable / known bad)
  – Md5 hashsets (notable / known bad)
• Identifies known bad files as they are found.
Recent Activity Module

• Focuses on user activity
• Browser artifacts:
  – History, cookies, downloads, bookmarks
  – Firefox, Chrome, Safari, IE
• Recent user docs
• Recent devices
• Uses:
  – RegRipper
  – Pasco2
Recent Activity Results

- **Images**
- **Views**
- **Results**
  - **Extracted Content**
    - Bookmarks (97)
    - Cookies (412)
    - Web History (888)
    - Downloads (1)
    - Recent Documents (8)
    - Installed Programs (41)
    - Devices Attached (14)
    - Web Search Engine Queries (230)
    - EXIF Metadata (3)
  - **Keyword Hits**
    - Single Literal Keyword Search (0)
Other Ingest Modules

- MBOX / Thunderbird
  - Parses into individual messages
- Exif
  - Extracts dates, GPS, and device information
- More to come
• Allows for different file types to be viewed differently.

• Standard modules:
  – Hex
  – Strings extraction (4 or more printable characters)
  – Extracted Text from index
  – Media (pictures / video)
    • gstreamer
### Content Viewer: Hex

<table>
<thead>
<tr>
<th>Hex View</th>
<th>String View</th>
<th>Result View</th>
<th>Text View</th>
<th>Media View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page: 1 of 1</td>
<td>Page</td>
<td>Go to Page:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Offset</th>
<th>Hex</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000000</td>
<td>FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 48</td>
<td>......JFIF......H</td>
</tr>
<tr>
<td>0x000010</td>
<td>00 48 00 00 FF DB 00 43 00 0A 07 07 08 07 06 0A</td>
<td>.H.......C.......</td>
</tr>
<tr>
<td>0x000020</td>
<td>08 08 08 0B 0A 0A 0B 0E 18 10 0E 0D 0D 0E 1D 15</td>
<td></td>
</tr>
<tr>
<td>0x000030</td>
<td>16 11 18 23 1F 25 24 22 1F 22 21 26 2B 37 2F 26</td>
<td>......#.!&quot;&quot;!&amp;7/ &amp;</td>
</tr>
<tr>
<td>0x000040</td>
<td>29 34 29 21 22 30 41 31 34 39 3B 3E 3E 3E 25 2E</td>
<td>}4)!&quot;0A149;++&gt;%</td>
</tr>
<tr>
<td>0x000050</td>
<td>44 49 43 3C 48 37 3D 3E 3B FF DB 00 43 01 0A 0B</td>
<td>DIC&lt;?7=&gt;;...C...</td>
</tr>
<tr>
<td>0x000060</td>
<td>0B 0E 0D 0E 1C 10 10 1C 3B 28 22 28 3B 3B 3B 3B</td>
<td>...........{&quot;;</td>
</tr>
<tr>
<td>0x000070</td>
<td>3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B</td>
<td></td>
</tr>
<tr>
<td>0x000080</td>
<td>3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B</td>
<td></td>
</tr>
<tr>
<td>0x000090</td>
<td>3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B</td>
<td></td>
</tr>
<tr>
<td>0x0000a0</td>
<td>00 11 08 00 64 00 CO 03 01 11 00 02 11 01 03 11</td>
<td>....d................</td>
</tr>
<tr>
<td>0x0000b0</td>
<td>01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00</td>
<td></td>
</tr>
<tr>
<td>0x0000c0</td>
<td>00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09</td>
<td></td>
</tr>
<tr>
<td>0x0000d0</td>
<td>0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05</td>
<td></td>
</tr>
<tr>
<td>0x0000e0</td>
<td>05 04 04 00 00 00 01 7D 01 02 03 00 04 11 05 12 21</td>
<td></td>
</tr>
<tr>
<td>0x0000f0</td>
<td>31 41 06 13 51 61 07 22 71 14 22 FD 18 A1 08 23 1A. Qa.&quot;q.2...#</td>
<td></td>
</tr>
<tr>
<td>0x000100</td>
<td>42 B1 C1 15 52 D1 F0 24 33 62 72 1A 09 0A 16 17 B...R...$3br........</td>
<td></td>
</tr>
</tbody>
</table>
Other Content Viewer Uses

• Finds names of people and places.
• Translates from Arabic to Latin Characters
• Looks names up in watch lists.
• Results can be saved to HTML or XML.
• Other modules can be created in the future.
How do you get it?

- Available from sleuthkit.org:

  http://www.sleuthkit.org/autopsy
For Developers

- Writing modules will make your life easier:
  - We deal with file access.
  - We deal with displaying results
  - ...
- We’re polishing up the module writer’s guide:
  [www.sleuthkit.org/autopsy/docs/api-docs](www.sleuthkit.org/autopsy/docs/api-docs)
For Users

• Give us feedback.
• Bug the developers of your favorite tools to write them as modules.
• Partly funded by US Army Intelligence Center of Excellence (USAICoE).
  – Partnered with 42Six Solutions
Next Steps

- Framework Enhancements
- Linux / OS X support
- More modules
- Tighter integration with TSK Framework.
Thank you!

For more information:
Visit [www.basistech.com](http://www.basistech.com)
Write to [conference@basistech.com](mailto:conference@basistech.com)
Call 617-386-2090 or 800-697-2062