Automated Forensics with the Sleuth Kit Framework

Eamonn Saunders
Principal Software Engineer, Digital Forensics
Basis Technology
What is the framework?

- Infrastructure distributed with The Sleuth Kit
- Supports development of pluggable modules
- Benefits
  - End to end solution
  - Automation
  - Simplifies module and tool development
Framework Phases

2- File Analysis Phase
Each file is analyzed with the File Analysis Pipeline

<table>
<thead>
<tr>
<th>MD5/SHA1 Hash Calculation</th>
<th>Hash Lookup</th>
<th>File Type ID</th>
<th>Open ZIP Files</th>
<th>EXIF Extraction</th>
<th>Add Text to Keyword Index</th>
<th>...</th>
</tr>
</thead>
</table>

1- File Extraction Phase

- Enumerate Files (Sleuth Kit)
- Carve Unallocated Space (Scalpel)

- E01 File

Database (SQLite, MySQL, PostgreSQL, etc.)

3- Post Processing Phase

Post Processing Pipeline is run after all files have been analyzed.

- RegRipper
- Web Browser Analysis
- Search Keyword Index
- Check for Known File / Path Names
- ... Summary Report Generation

Results (HTML, XML, etc.)
• Blackboard
  – Supports inter-module communication
  – Stores results generically
  – Modules can post their own results
  – Modules can read previously posted results
  – e.g. Hash calculation, lookup
### Blackboard Artifacts and Attributes

<table>
<thead>
<tr>
<th>TSK_WEB_BOOKMARK</th>
<th>TSK_HASH_HIT</th>
<th>TSKDEVICE_ATTACHED</th>
<th>TSK_KEYWORD_HIT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FILE_ID</strong>: 441</td>
<td><strong>FILE_ID</strong>: 345</td>
<td><strong>FILE_ID</strong>: 59</td>
<td><strong>FILE_ID</strong>: 1033</td>
</tr>
<tr>
<td><strong>TSK_URL</strong>: <a href="http://www.google.com">http://www.google.com</a></td>
<td><strong>TSK_SET_NAME</strong>: Bad Pictures</td>
<td><strong>TSKDEVICE_ID</strong>: 1234</td>
<td><strong>TSK_KEYWORD</strong>: bomb</td>
</tr>
<tr>
<td><strong>TSK_TITLE</strong>: Google</td>
<td><strong>TSK_PATH</strong>: E:\</td>
<td><strong>TSK_DATE_TIME</strong>: April 1, 2012</td>
<td><strong>TSK_KEYWORD_PREVIEW</strong>: The bomb was under the seat.</td>
</tr>
<tr>
<td><strong>TSK_PROGNAME</strong>: Firefox</td>
<td><strong>TSK_SET_NAME</strong>: Bad Pictures</td>
<td><strong>TSK_PATH</strong>:</td>
<td><strong>TSK_SET_NAME</strong>: Explosives</td>
</tr>
<tr>
<td><strong>FILE_ID</strong>: 871</td>
<td><strong>FILE_ID</strong>: 339</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TSK_URL</strong>: <a href="http://www.ebay.com">http://www.ebay.com</a></td>
<td><strong>TSK_SET_NAME</strong>: Bad Pictures</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TSK_TITLE</strong>: &quot;Electronics, Cars, ...&quot;</td>
<td><strong>TSK_PATH</strong>:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TSK_PROGNAME</strong>: Chrome</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TSK_RECENT_OBJECT**

| **FILE_ID**: 811  | **TSK_PATH**: C:\Users\Jdoe\My Documents\Bad Stuff.doc  | **TSK_DATE_TIME**: April 5, 2012 | **TSK_PROG_NAME**: Windows |
| **TSK_KEYWORD**: bomb |
| **TSK_KEYWORD_PREVIEW**: The bomb was under the seat. | **TSK_SET_NAME**: Explosives | | |
### Available Modules

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Example Use Case(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Calculation/Hash Lookup</td>
<td>Find all known (e.g. NSRL) or notable files.</td>
</tr>
<tr>
<td>Entropy</td>
<td>Find potentially encrypted files.</td>
</tr>
<tr>
<td>File Type Identification</td>
<td>Find files of a particular type or identify files whose extension does not match type.</td>
</tr>
<tr>
<td>Exif Extraction</td>
<td>Identify location, device make/model, author information for JPEG images.</td>
</tr>
<tr>
<td>Zip Extraction</td>
<td>Circumvent attempts to hide data in zip files.</td>
</tr>
<tr>
<td>Interesting Files</td>
<td>Find Skype database files (main.db, <em>.dbb) or all multimedia content (</em>.mpg/wmv/avi etc.)</td>
</tr>
<tr>
<td>SaveInterestingFiles</td>
<td>Extract all multimedia content for further analysis.</td>
</tr>
<tr>
<td>RegRipper</td>
<td>Analyze system registry files.</td>
</tr>
<tr>
<td>SummaryReport</td>
<td>Present results of analysis modules.</td>
</tr>
</tbody>
</table>
Using the framework

- Framework is a foundation
- Incorporate framework into other tools
- `tsk_analyzeimg`
  - Sample implementation for testing
  - Extracts files from disk image into SQLite
  - Runs file analysis and post processing pipelines
    
    `tsk_analyzeimg.exe C:\Images\testimage.E01`
• Configure modules in pipeline_config.xml

```xml
<?xml version="1.0" encoding="utf-8"?>
<PIPELINE_CONFIG>
  <PIPELINE type="FileAnalysis">
    <MODULE order="1" type="plugin" location="HashCalcModule.dll"/>
    <MODULE order="2" type="plugin" location="HashLookup.dll"/>
  </PIPELINE>
  <PIPELINE type="PostProcessing">
    <MODULE order="1" type="plugin" location="SummaryReport.dll" arguments="#OUT_DIR#\Summary.htm"/>
  </PIPELINE>
</PIPELINE_CONFIG>
```
What does a module look like?

- **TskModule::Status initialize(const char * args)**
  - Called when the framework loads the module

- **TskModule::Status run(TskFile * pFile)**
  - Called by file analysis pipeline for each file

- **TskModule::Status report()**
  - Called by post processing pipeline

- **TskModule::Status finalize()**
  - Called when the framework unloads the module

What’s next?

• We will continue to support TSK framework
• Call for developer participation
  – https://github.com/sleuthkit/sleuthkit/issues
  – Add new modules to Wiki page
  – More platforms: (Linux, Mac)
  – ...
• Ideas and contributions are always welcome.
Thank you!

For more information:
Visit www.basistech.com
Write to conference@basistech.com
Call 617-386-2090 or 800-697-2062