Autopsy: Wait, there are still more features?

Brian Carrier
Basis Technology
What is Autopsy?

• Open source digital forensics platform.
• Has been designed for:
  • Ease of use
  • Fast results
  • Extensibility (many plug-in frameworks)
Main Interface
Why Should You Care?

• Has the features you need (and more).
• Will reduce your licensing costs.
• Will reduce errors because:
  • It is easy to use
  • Can automate your investigations
• Has commercial support and development backing.
Summary of Past Year

• 3 Releases.
  • Version 4.0 released next week.

• New Features:
  • Multi-user cases
  • New modules
  • Lots of improvements to existing features.
Autopsy Tour

With Highlights of New Features
New Case Wizard

Enter New Case Information:

Case Name:
Base Directory: R:\
Case Type: Multi-user
Case data will be stored in the following directory:
New Case Wizard: What’s New

Enter New Case Information:

Case Name:  

Base Directory:  R:\  

Case Type:  Single-user  Multi-user  

Case data will be stored in the following directory:
Multi-User Cases

• Analyze large cases faster by enabling collaboration.
  • Multiple users can work on the same case at the same time.
  • Real-time updates from each user.

• All infrastructure software is free and open source:
  • Database server: PostgreSQL
  • Text index server: Apache Solr
  • Messaging server: ActiveMQ

• See Richard’s talk after lunch for more details.
Add Data Source Wizard

Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add: Image File
Browse for an image file: [Browse]
Z:\vmware-share\imgs\auto [Local Disk]
Logical Files

Please select the input timezone: [GMT-5:00] America/New_York

Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
Data Source Support

• The Sleuth Kit is used to support all common file systems:
  • NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, etc.
  • Covers common computers and smart phones

• Can also analyze:
  • Local drives (USB attached)
  • Local files

• What’s New: Bug fixes to underlying code in The Sleuth Kit
Configure Ingest Modules

Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- C4P Hash Lookup
- Bin and Round File Finder

Select known hash databases to use:

- NSRLFile.txt-md5

Select known BAD hash databases to use:

- notable_hash_db

- Calculate MD5 even if no hash database is selected

Identifies known and notable files using... [Advanced]
Recent Activity

- Web artifacts from Firefox, Chrome, and IE.
- Registry analysis using regripper.
Hash Lookup

- Flags known and known bad files
- Supports:
  - NIST NSRL
  - EnCase format
  - Autopsy SQLite
  - Project Vic (with add-on)
File Type Identification

- Detects files based on signatures.
- New: Supports user specified signatures.
  - Can raise alerts when they are found.
Standard Features

Embedded File Extractor

- Opens ZIP, RAR, and many other archive files.
- New: Extracts images from office documents.
Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- C4P Hash Lookup
- Big and Round File Finder

Exif Parser

- Finds JPEG images with Exif.
- Extracts device information, dates, and Geo-location.
Keyword Search

- Indexed search using Solr.
- Performs periodic searches.
- Supports terms and regular expressions.
Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- C4P Hash Lookup
- Big and Round File Finder

Email Parser
- Supports MBOX and PST.

Extension Mismatch
- Users can specify rules

E01 Verifier
Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- F01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- C4P Hash Lookup
- Big and Round File Finder

Android Analyzer

- SMS, Call logs, Contacts
- Tango
- Words With Friends
- ...
### Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- C4P Hash Lookup
- Big and Round File Finder

### Interesting Files Module

- Flags files based on name.
- Allows you to automate your investigation checklist.
- Always look for:
  - iPhone Backup files
  - True Crypt
  - Virtual machines
  - ...
### Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- **PhotoRec Carver**
- C4P Hash Lookup
- Big and Round File Finder

**PhotoRec Carver**

- Uses PhotoRec tool to carve unallocated space.
- Files are fed back through.

#OSDFCon
Standard Features

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer
- Interesting Files Identifier
- PhotoRec Carver
- G4B Hash Lookup
- Big and Round File Finder

Big and Round File Finder

- ????
- We did a lot of work on Python support.
- You’ll learn more about this later.
Review the Results
The Tree

- The tree has all of the results.
- Updated in real-time.
- Find:
  - Files of a given type
  - Web artifacts
  - Registry results
  - ....
- New: Refreshes better when ZIP files are expanded behind the scenes.
Workflow
File Viewers

• View a file in the most relevant way.
• Images and video playback.
File Viewers

• View a file in the most relevant way.

• Text:

To The Zombie apocalypse
It’s Z-Day. Virus, toxic gas, or re-animation experiment gone wrong? “How”
doesn’t matter now. What matters is you and what you’re going to do to keep
from becoming one of them. Lucky for you, open source adapts to fill needs.
And that’s exactly what you need to do right now—adapt to survive. You’re facing
the quest of a lifetime: Find energy. Find your friends. Rebuild all of civilization.
You can do it. Here’s how.

Facebook or new episodes of Warehouse 13.
File Viewers

- View a file in the most relevant way.
- Long video as sequence of frames:
### Timeline

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Description</th>
<th>Base Type</th>
<th>Sub Type</th>
<th>Known Ext.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-02-08 07:50:30</td>
<td>NIKON CORPORATION : NIKON D700 : B0137801</td>
<td>Misc Types</td>
<td>Exif</td>
<td>UNKN</td>
</tr>
<tr>
<td>2011-10-13 10:00:20</td>
<td>Phase One : H 25 : 0</td>
<td>Misc Types</td>
<td>Exif</td>
<td>UNKN</td>
</tr>
<tr>
<td>2011-10-13 10:00:20</td>
<td>Phase One : H 25 : 0</td>
<td>Misc Types</td>
<td>Exif</td>
<td>UNKN</td>
</tr>
</tbody>
</table>
Image Gallery

New!
Generate A Report

- Standard reports:
  - HTML
  - Excel
  - CSV
  - KML
- STIX module looks for indicators of compromise.

New!
Impact

- Download Statistics:
  - One release during each time period.
  - 2014: 45,232 total downloads (253 per day)
  - 2015: 59,718 total downloads (334 per day)
  - Increase of 32%.

- Does not include Linux users on Sumuri Paladin.
We continue to build our Cyber Triage application on it.

Enables incident responders to:
- Collect data from live system (or dead) by pushing agents as needed.
- Applies heuristics to collected data
- Guides responder through other data that requires manual review

Stop by the table outside for more information.
- Get a free “Cyber First Responder” T-shirt.
What’s Next This Year?

- More work on collaboration features.
- More support for Python.
- More timeline and image gallery work.
- New feature to help search for account numbers and more easily review false positives.
- ....
What Can You Do?

• If you are using it:
  • Spread the word to your friends.
  • Provide us some quotes and stories for www.sleuthkit.org.
  • Let us know what else you want.

• If you aren’t using it:
  • Try it out.
  • Especially if your existing software is up for renewal.

• Send me an e-mail: brianc@basistech.com
Support

- Community:
  - E-mail list and web forum

- Basis Technology:
  - Commercial support
  - Access to engineers who can fix any issues.
• Basis offers public training courses.
• Next one will be next March.
  • Besides the one tomorrow.
• We also offer private training courses.
Contact

Brian Carrier
brianc@basistech.com

Download It Today
http://www.sleuthkit.org/autopsy/