Happy Holidays From Renzik

What Happened in Autopsy in the Past Year

Brian Carrier
It’s That Time Of Year.....

• We get to tell you about all of the great things that happened in the past year!
Side Note: Our Dogs.....

Renzik

Hash
What is Autopsy?

• Open source digital forensics platform.
• Designed to be:
  o Easy to use
  o Extensible with open plug-in frameworks
• Supports hard drives, media cards, and smart phone formats.
• Has all of the standard features, plus some unique features.

• Let’s go through a typical workflow and point out the new features.
• “Intro to Autopsy” talk this afternoon will cover more of the basics.
Make A Case

New Case Information

Steps
1. Case Information
2. Optional Information

Case Information

Case Name: case123
Base Directory: c:\cases

Case Type:
- Single-user
- Multi-user

Case data will be stored in the following directory:

c:\cases\case123
Multi-user Case Documentation

- People were having trouble setting up multi-user clusters.
  - Usually because of user permissions and the Solr service.
- We updated the docs to help diagnose issues and added a test button to the “Auto Ingest” panel (i.e. running 24x7 and scanning for new images)
Add A Data Source

Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Ingest Profile Selection
4. Configure Ingest Modules
5. Add Data Source

Select Type of Data Source To Add
- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
Add A Data Source

Steps:
1. Select Type of Data Source To Add
2. Select Data Source
3. Ingest Profile Selection
4. Configure Ingest Modules
5. Add Data Source

Select Type of Data Source To Add:
- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
Logical Imager

• Command line program that runs on target computer and collects:
  • Files (based on a set of rules)
  • System information (such as users)

• Parses raw drive data and the registry using The Sleuth Kit

• Unique Benefits:
  o Can access locked files and bypass rootkits that hide files
  o Does not update time stamps during search
  o Can access dual boot volumes (Linux for example)
  o Can create a full image if you keep it plugged in long enough.

• See Ann’s talk later today for more details.
Configure Ingest Modules to Analyze Data

- Run ingest modules on:
  - All Files, Directories, and Unallocated Space

Selected Modules:
- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Correlation Engine
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Plaso
- Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently used applications, and more.
Configure Ingest Modules

Run ingest modules on:
- All Files, Directories, and Unallocated Space
- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Correlation Engine
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- Plaso
- Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently used applications, or text messages.
Recent Activity Module

- Lots of features added from our DHS S&T contract.
- All of them came from “What’s Needed” and surveys from past OSDFCons.
- Web: Added Safari and Edge. Added form fill data to Firefox and Chrome. Added cache parsing to Chrome.
- Parse Zone.Identifiers to show source of downloaded files.
- Ported existing 3rd Party Modules (all from Mark McKinnon):
  - Recycle Bin: Make artifact and create file at original location.
  - ShellBag: Make artifacts (using RegRipper output)
  - Users: Parse more RegRipper output to simulate "Parse SAM" module
Plaso & Email Modules

- Also from DHS S&T contract
- New Plaso module:
  - Creates events to be displayed in the timeline
- Updated Email module:
  - Added support for EML files. Based on Mark McKinnon’s module.
  - Added support to make Contact Book Entries based on vCards
Correlation Engine Module

- This module:
  - Saves artifacts to a central database for future correlation
  - Flags artifacts that were previously seen and marked as notable

- Updates:
  - More artifacts: SSID, MAC address, IMEI, IMSI, and ICCID
Android Analyzer Module

• Added support for many more apps:
  o Browsers: Android browser, Opera, Samsung SBrowser
  o Messaging: Facebook Messenger, IMO, LINE, Skype, TextNow, Viber, WhatsApp
  o File Transfer: ShareIt, Xender, Zapya
  o …

• Made it even easier to make 3rd party apps. 3 steps:
  o Find and open SQLite and associated WAL files with one call.
  o Query correct tables
  o Add artifacts for contacts, messages, etc. (one call each instead of 8 or 10).

• See talk later today for more details
Case Opens Up
Basic UI Flow
Performance

- Several things were done to improve performance with large datasets
- Improved some backend queries
- Added paging everywhere
Content Viewer: Added Willi’s Registry Viewer
Content Viewer: Image Tags Can Have Boxes
Setting up a high speed connection

Enter the following settings to set up your DSL or cable modem Internet account. You can get these settings from your Internet services provider: Enter the following settings to set up your LAN connection. You can get these settings from your network administrator.

Please enter a valid setting.

- Obtain IP automatically:
- Static IP address:
- Obtain DNS automatically:
- Preferred DNS:
- Alternate DNS:
Content Viewer: Other Occurrences

- Shows past cases where a file or other artifact was seen
- Changed layout to make it easier to see unique case names
**Content Viewer: Added Translation Viewer**

- **Uses Google or Microsoft API (requires credentials)**

<table>
<thead>
<tr>
<th>Hex</th>
<th>Text</th>
<th>Application</th>
<th>Message</th>
<th>File Metadata</th>
<th>Results</th>
<th>Annotations</th>
<th>Other Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strings</th>
<th>Indexed Text</th>
<th>Translation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Matches on page:</th>
<th>of</th>
<th>Match</th>
<th>Page:</th>
<th>of</th>
<th>21</th>
<th>Page</th>
<th>Text Source:</th>
</tr>
</thead>
</table>

**General [Edit]** The jurisdiction of Tokyo is comprised of the Tokyo metropolitan area (23 wards of Tokyo), the Tama area (26 Subbranch offices of the Tokyo Islands (Oshima, Miyake, Hachijo, Ogasawara) (2 towns, 7 villages). Tokyo-ku (Tokyo 23 were located at the southernmost and most eastern end Japan to include the Ogasawara Islands, including the Okinoshima Island.  

There are other Tokyo Prefecture and Tokyo Metropolitan Prefecture. The population is 13,843,403 people (as of October 1.

This is the largest population in Japan prefectures, accounting for more than 10% of the Japan population. The population is the largest metropolitan area in the world with more than 37 million population. 34 percent of the Japan population is the official population, Poland, Algeria and Canada, each of which rivals the entire country's population. The second-largest Mum million [note 4].

October 16, 2019 - Herndon, VA - Hosted by Basis Technology
## Translation: File Names Too

<table>
<thead>
<tr>
<th>Name</th>
<th>Original Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spain</td>
<td>España</td>
<td>/LogicalFileSet5/Test files/Translation Testing/España</td>
</tr>
<tr>
<td>test</td>
<td></td>
<td>/LogicalFileSet5/Test files/Translation Testing/test</td>
</tr>
<tr>
<td>Greece</td>
<td>Ελλάδα</td>
<td>/LogicalFileSet5/Test files/Translation Testing/Ελλάδα</td>
</tr>
<tr>
<td>Russia's Federation</td>
<td></td>
<td>/LogicalFileSet5/Test files/Translation Testing/Российска...</td>
</tr>
<tr>
<td>Russia</td>
<td>Россия</td>
<td>/LogicalFileSet5/Test files/Translation Testing/Россия</td>
</tr>
<tr>
<td>Bahrain</td>
<td>البحرين</td>
<td>/LogicalFileSet5/Test files/Translation Testing/البحرين</td>
</tr>
<tr>
<td>Japan</td>
<td>日本</td>
<td>/LogicalFileSet5/Test files/Translation Testing/日本</td>
</tr>
<tr>
<td>Korean</td>
<td>한국어</td>
<td>/LogicalFileSet5/Test files/Translation Testing/한국어</td>
</tr>
<tr>
<td>Four.txt</td>
<td>أبسة.txt</td>
<td>/LogicalFileSet5/Test files/Translation Testing/أبسة.txt</td>
</tr>
</tbody>
</table>
Other Viewers

• Some data types need an interface more specific than the generic tree and table.

• All of those viewers received updates too:
  o Timeline
  o Image Gallery
  o Communications
Timeline

- [Image of a timeline graph with data points and filters for view options like 'Counts' and 'Details'].

- [Table showing date/time, event ID, file ID, result type, base type, sub type, and know status with hex values and strings].
Timeline Enhancements

• No longer need to create timeline databases the first time it is opened.
  o It is now maintained as files and artifacts are created
• 3rd Party modules can now add events to the timeline.
• Users can manually create their own events.

• Nothing changed in the UI. Just backend changes.
• Timeline has been funded by DHS S&T
Communications UI

<table>
<thead>
<tr>
<th>Account</th>
<th>Device</th>
<th>Type</th>
<th>Msgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>+12025551234</td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>78</td>
</tr>
<tr>
<td>456</td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>28</td>
</tr>
<tr>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>17</td>
</tr>
<tr>
<td>12025551234</td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>11</td>
</tr>
<tr>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>6</td>
</tr>
<tr>
<td>+1410553456</td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>5</td>
</tr>
<tr>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>target_phone.bin</td>
<td>Email</td>
<td>4</td>
</tr>
<tr>
<td>+14435590987</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>4</td>
</tr>
<tr>
<td>32665</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>3</td>
</tr>
<tr>
<td>130155555555</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td><a href="mailto:example444@test.com">example444@test.com</a></td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>12345609</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>123456006</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>123456004</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>123456003</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>180</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>+15715556543</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>2</td>
</tr>
<tr>
<td>1511</td>
<td>target_phone.bin</td>
<td>Email</td>
<td>1</td>
</tr>
<tr>
<td>12765552468</td>
<td>target_phone.bin</td>
<td>Phone</td>
<td>1</td>
</tr>
</tbody>
</table>

**Messages**

<table>
<thead>
<tr>
<th>Type</th>
<th>From</th>
<th>To</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail</td>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>2012-06-06 17:06:19</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>2012-06-06 17:06:22</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>2012-06-06 17:06:22</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>2012-06-06 17:12:19</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:07:16</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:09:04</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:09:39</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:12:39</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:16:45</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:17:16</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:19:19</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td><a href="mailto:example2@test.com">example2@test.com</a></td>
<td>2012-06-06 17:22:02</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:mail-noreply@google.com">mail-noreply@google.com</a></td>
<td><a href="mailto:example111@test.com">example111@test.com</a></td>
<td>2012-06-06 17:22:02</td>
</tr>
</tbody>
</table>

**Example Message**

From: example111@test.com
To: example2@test.com
CC: 
Subject: Hi

Headers: Text

this is a test
Communications Updates

- Organize emails into threads and display messages by thread
- Added “Account Summary” tab to provide basics of an account (# of messages, other devices it was seen on, etc.)
- Added tab to show contact book entries
- Added tab to show image and video attachments
- Added filter to more easily focus on most recent messages

- Communications UI has been funded by DHS S&T
## Contacts

### Summary

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forrest Gump</td>
<td><a href="mailto:forrestdump@example.com">forrestdump@example.com</a></td>
<td>(404) 555-1212</td>
</tr>
</tbody>
</table>

### Properties

- **Source File**: Forrest Gump
- **Name**: Forrest Gump
- **Phone (Work)**: (111) 555-1212
- **Phone (Voice)**: (404) 555-1212
- **Phone Number (Home)**: (404) 555-1212
- **Email (Pref)**: forrestdump@example.com
- **Email (Internet)**: forrestdump@example.com
- **Organization**: Bubba Gump Shrimp Co.
- **Data Source**: LogicaFileSet1
- **Name**: Forrest Gump
- **Phone (Voice)**: (404) 555-1212
- **Phone (Voice)**: (111) 555-1212
Common Property Search

- This feature matches files and other artifacts within a case or with past cases.
  - Finds patterns between devices and cases.
- Updates:
  - Updated the ways the results are shown
  - Can focus on certain file types when matching past cases
  - Can search past cases for specific artifact values (email, SSID, etc.)
New Past Case Matching Grouping

<table>
<thead>
<tr>
<th>Name</th>
<th>Local Parent Path</th>
<th>MIME Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cr_test4.vhd1</td>
<td>/0002/</td>
<td>text/plain</td>
<td>007c81e906d4d0b582bf56406e967f</td>
</tr>
<tr>
<td>logs.db</td>
<td>/Android Folders/data/9333-com.sec....</td>
<td>application/x-sqlite3</td>
<td>031b467ac8306ececf08a493b80fd4b8</td>
</tr>
<tr>
<td>index.dat</td>
<td>RL testing/2/</td>
<td>application/octet-stream</td>
<td>0b0239d86b5fb7e47fe00cf148fb45a</td>
</tr>
<tr>
<td>0002_s.txt</td>
<td>/0002/</td>
<td>text/plain</td>
<td>0cbf0ceab2335e54c8e4bb5e6b9ba30d</td>
</tr>
<tr>
<td>0004_e.txt</td>
<td>/0004/</td>
<td>text/plain</td>
<td>057d25172c2f54485ccb86e3f1883589</td>
</tr>
<tr>
<td>9223372034707292161</td>
<td>/Android Folders/data/12193-com.and....</td>
<td>text/xml</td>
<td>15d725172c2f54485ccb86e3f1883589</td>
</tr>
<tr>
<td>mmsms.db-shm</td>
<td>/Android Folders/data/12765-com.and....</td>
<td>application/octet-stream</td>
<td>16b4a62100ff96cd4d0408610958233</td>
</tr>
<tr>
<td>$TxLogContainer000000000000000000000001</td>
<td>$Extend/$RmMetadata/$TxLog/</td>
<td>application/octet-stream</td>
<td>1a2183c96878c974b4693c15ebc2626</td>
</tr>
<tr>
<td>0000_x.txt</td>
<td>/0000/</td>
<td>text/plain</td>
<td>1a487c7525d23007763a22c50a8d0031</td>
</tr>
</tbody>
</table>

OCTOBER 16, 2019 • HERNDON, VA • HOSTED BY
Reporting

• At the end of the case, it’s time to generate a report.
Reporting

- At the end of the case, it’s time to generate a report.
CASE/UCO Report

• Is a manifest that contains information on all files in the case.
• CASE/UCO is a JSON format.
• Makes it easier to import into other tools.
• See the talk later today for more details.

• More CASE/UCO integrations coming this year.
Portable Case

• Contains a subset of data from the original case.
  o Tagged files or others marked as “Interesting”
• Self contained folder with a SQLite case database and all relevant files.
• Resulting case can run ingest modules, tag files, etc.
• Can be compressed and split for easy transmission.
• Makes it easier to send data for review.
Command Line

• You can now run Autopsy from the command line:
  o Make Cases and Add Data Sources
  o Run Ingest Modules
  o Generate Reports
• Example:

```bash
> autopsy64.exe

- createCase -caseName="case123" -caseBaseDir="C:\Cases"
- addDataSource -dataSourcePath="C:\images\disk.bin"
- runIngest -generateReports
```

• Requires you to preconfigure what modules to run.
Linux / OS X

• Linux support stopped working this year because of Oracle’s change to Java licensing.
• It now works again and we can use OpenJDK.
• It’s just more complicated based on what distribution you use.
http://forum.sleuthkit.org

- We setup a new forum site this year at Discourse (t).
- Thanks for the free hosting!
- It has had a lot of activity
What’s Coming

• New Search / Discovery UI
• Mobile and drones
• Updated keyword search
• REST APIs
• APFS / Logical Disk Management
• Updated Project Vic integration
• Online training
• …
We Need Your Support

• Nearly all of this was built with support for various organizations.
• It’s always easier if we can point to increased usage and people who depend on this investment.

• If you are law enforcement, please reach out and let us know you are using this and what else you need.
  o We can then relay that to places like DHS S&T.
Download and Contact

- Download the latest version from autopsy.com
- You can get notifications from our email list or Twitter
- Basis Technology provides commercial support

Brian Carrier
brianc <at> basistech <dot> com

Connect on LinkedIn or Twitter
(I’m low volume on both…)