Autopsy’s Year in Review

Brian Carrier

November 18, 2020
Goal of this Presentation

• An update on what’s been added to Autopsy in the past year.
  o 4000+ commits on Github
• An overview of Autopsy for those who think it’s still the 20-year old Linux tool.
Meet Our Dogs

Renzik
Autopsy

Hash
The Sleuth Kit
And Our Newest Basis Family Member…

• Cyber Triage is getting a dog.
• It needs a name.
• Submit your ideas in the Cyber Triage Discord channel.
• If picked, you’ll get a 1-year Cyber Triage license!
• Examples: ROT13. I0lahC. Cy. Siti.
Autopsy Themes Since Last Year

Get More Data

- **More Artifacts**: Parse more data to ensure you have access to as much evidence as possible.

Show Less Data

- **Summary**: Create UIs that summarize artifacts to give you a quick perspective on a data source.
- **Relevance**: Rank data to help you sort through the noise.
New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: case123
Base Directory: C:\cases
Case Type: Single-user

Case data will be stored in the following directory:
C:\cases\case123
Add A Data Source

- APFS Disk Images are now supported. Thanks BlackBag!
- XRY Text File Reports are also new.

### 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
- XRY Text Export
Configure Ingest Modules

- Ingest Modules analyze the files in the data source.
- They add artifacts and other files to the database.
- Many 3rd party plug-in modules are ingest modules.
Configure Ingest Modules

• Ingest Modules analyze the files in the data source.
• They add artifacts and other files to the database.
• Many 3rd party plug-in modules are ingest modules.
• These are new or have changes
Recent Activity Module

• Focuses on user activity (registry, web, etc.)
• Expanded Chromium support:
  o Edge, Opera, Brave, UC, SalamWeb, and Yandex
• More Windows Artifacts:
  o MRUs from Adobe Reader, Media Player, Office, 7Zip, WinRAR, Applets, Microsoft Management Console (MMC) from RegRipper.
  o Prefetch, Background Activity Monitor, and System Resource Usage
Picture Analyzer

• Rebranded “EXIF Module”.
• Also converts HEIC to JPEG and adds them as children
Interesting Item Module

• Flags files based on path and name.
• Now comes with rule sets:

![Select interesting files sets to enable during ingest:]

• Example: Cloud Storage will flag goodsync.exe, googledrivesync.exe, googledrivefs.exe, etc.
Contributing Rules

• Help maintain these rules!
• Or, submit new sets.
• There are instructions in the User Docs
  • Community Contributions
    ○ Translating Documentation and the UI
    ○ Updating the Official Interesting File Sets
  • Troubleshooting

• Basic Idea: Submit a Github Pull Request or Issue!
Central Repository Module

• The rebranded Correlation Engine module.
  o It does a lot more than correlate

• We want make sure you’re taking advantage of your past data (see later talk)
  o The repository is enabled by default.
  o Hashes and identifiers are stored by default.
  o It will not correlate though.

• It also stores more account identifiers (email, social media, etc.) for Persona feature.
Drone Analyzer & GPX

- New module from our previous DHS S&T Contract
  - Uses DatCon to parse DJI drone data
  - Creates Track Points for where the drone was
- GPX module creates track points, way points, etc. from non-drones.
  - Can also be displayed in the new Map viewer
iOS Analyzer (iLEAPPP)

• New module that wraps iLEAPPP
• Current version uses TAR input file.
• Next version (4.18 – Jan 2021) supports:
  o Disk images
  o More artifacts
  o aLEAPPP
• See Alexis’s talk at the end of the day to learn more about these tools
Basic UI Flow
New “Context” Viewer

• Gives you more information about a selected file based on other artifacts.
  o Where did it come from? (Downloads, message attachments, etc.)
  o When or where was it used? (MRU keys, Prefetch, etc.)
Other Viewers

• Autopsy has other viewers that are more focused for more complex data:
  o Communications
  o Timeline
  o Image Gallery

• Let’s look at some new ones and some updates
Data Source Summary

- It’s good to start an investigation knowing the rough shape of the data.
- Goal of the Data Source Summary panels is to help you figure that out.
- Click on a data source and choose “Summary”
Data Source Summary Example – Types

Provides overview of:
- OS
- File types
- Number of files

File Types

- Images: 16,255 (10.2%)
- Videos: 62 (0.0%)
- Audio: 194 (0.1%)
- Documents: 33,133 (20.7%)
- Executables: 9,377 (5.9%)
- Other: 39,591 (24.8%)
- Not Analyzed: 7 (0.0%)
Data Source Summary Example – User Activity

Provides overview of most recent:
- Programs run
- Domains visited
- Web searches
- Devices
- Account types

Focused on final 30 days
Discovery

• The goal of this UI is to help you find relevant data faster.
• You pick:
  o What you want to see
  o How you want to see it
• Example:
  o Show pictures that are rare and big. Organize by parent folder.
  o Show non-common web domains that were visited in past 30-days. Organize by visit count.
• We’ll cover this feature more this afternoon
  o Spoiler Alert: The Central Repository makes this really powerful.
Maps

- New built-in viewer for geolocation-based data:
  - Exif, Drone, GPX, Android, iOS, etc.
- Uses Bing server or OpenStreetMap tiles.
Online Training

• We launched a 1-day online training course.
• It’s free for US Law Enforcement through end of 2020 – From US DHS S&T
• Covers the basics of adding and analyzing data.
• With hands-on exercise – help rescue Renzik!
• $495 / person

http://autopsy.com/training
What’s Coming

• More artifacts – get as much data as possible
• More summarization – provide quick orientation
• More ranking – focus on the relevant data ASAP
  o We’re incorporating in scoring from Cyber Triage
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…)