

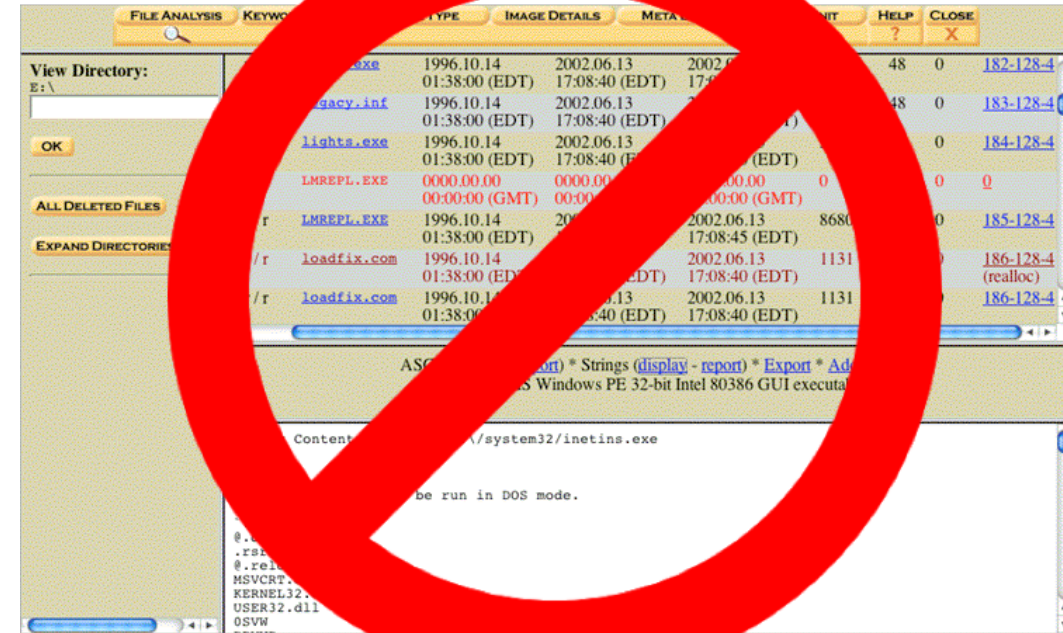
Autopsy's Year in Review

Brian Carrier

November 18, 2020

Goal of this Presentation

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



Autopsy 4

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Listing
EXIF Metadata 12 Results

Table Thumbnail Save Table as CSV

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size
QUPANq5X_normal[1].jpg			7		Desire HD	HTC	xp-sp3-v3.001	1433
data_2_b20204f8			1	2012-02-06 09:51:37 EST	Canon EOS DIGITAL REBEL XS	Canon	xp-sp3-v3.001	2448
ta_520n-tfb-tm[1].jpg			7	2009-08-25 18:22:50 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	113784
ame_8vc-tfb-tm[1].jpg			7	2009-08-25 18:20:18 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	23446
B0137d01			7	2011-02-08 07:50:30 EST	NIKON D700	NIKON CORPORATION	xp-sp3-v3.001	37828
ACC93d01			7	2007-07-21 10:48:42 EDT	Canon EOS-1D Mark III	Canon	xp-sp3-v3.001	385936
F733Fd01			7	2006-03-30 12:34:35 EST	Canon EOS-1Ds Mark II	Canon	xp-sp3-v3.001	26138

Hex Text Application Message File Metadata Results Annotations Other Occurrences Video Triage

0% 107% Reset

Tags Menu

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. IOlahC. 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:

Base Directory:

Case Type:



Single-user



Multi-user

Case data will be stored in the following directory:

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



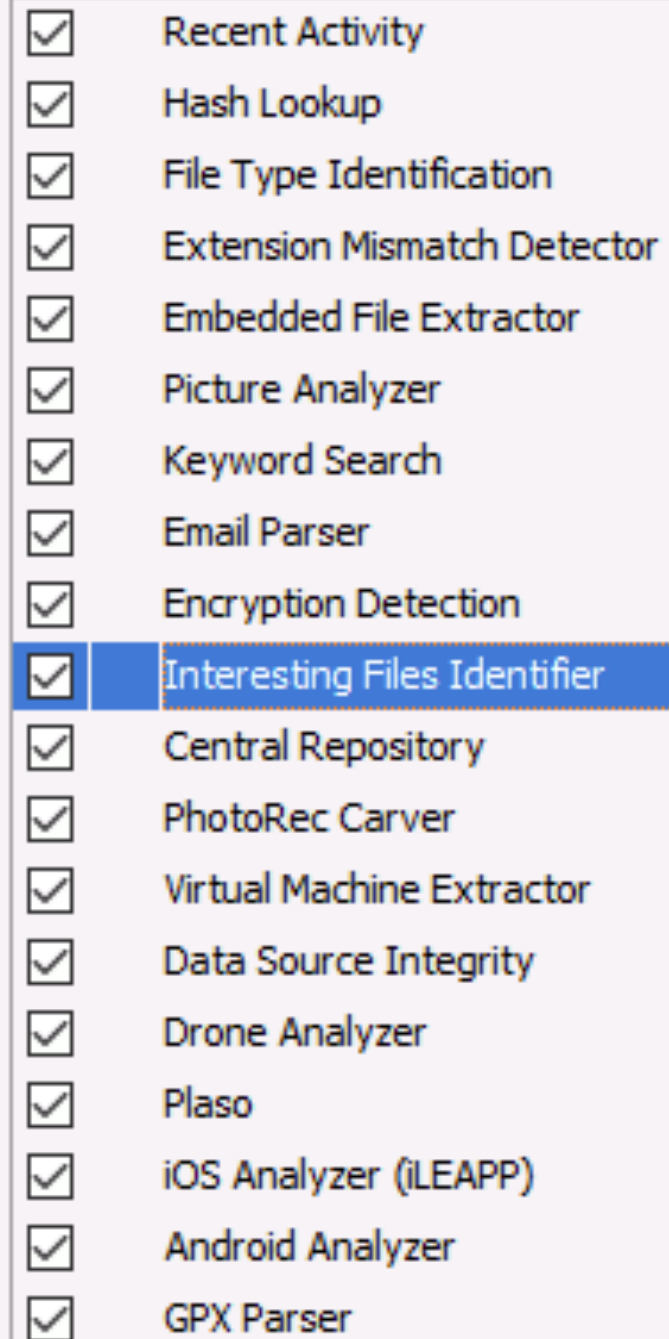
Autopsy Logical Imager Results



XRY Text Export

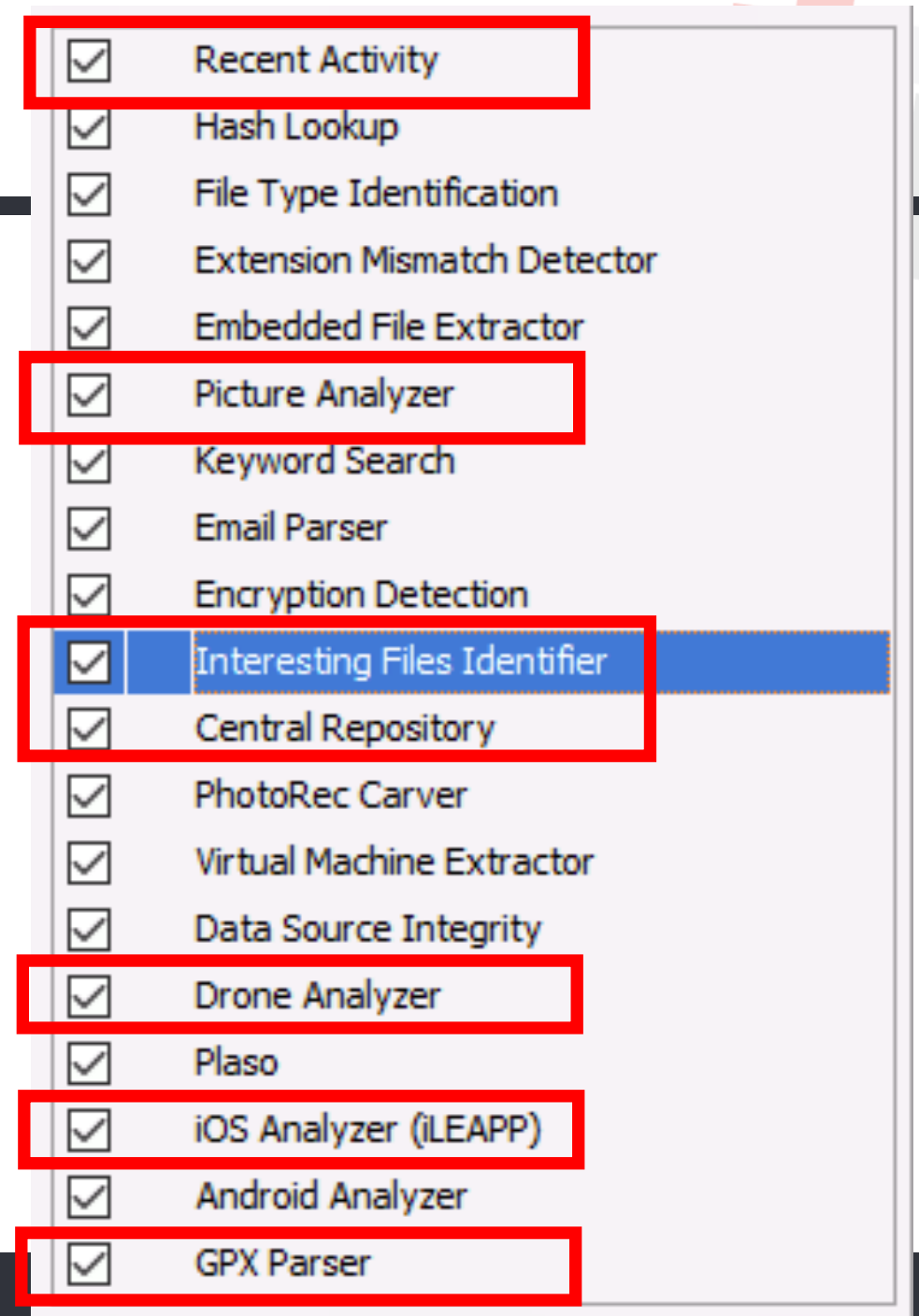
Configure Ingest Modules

- 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



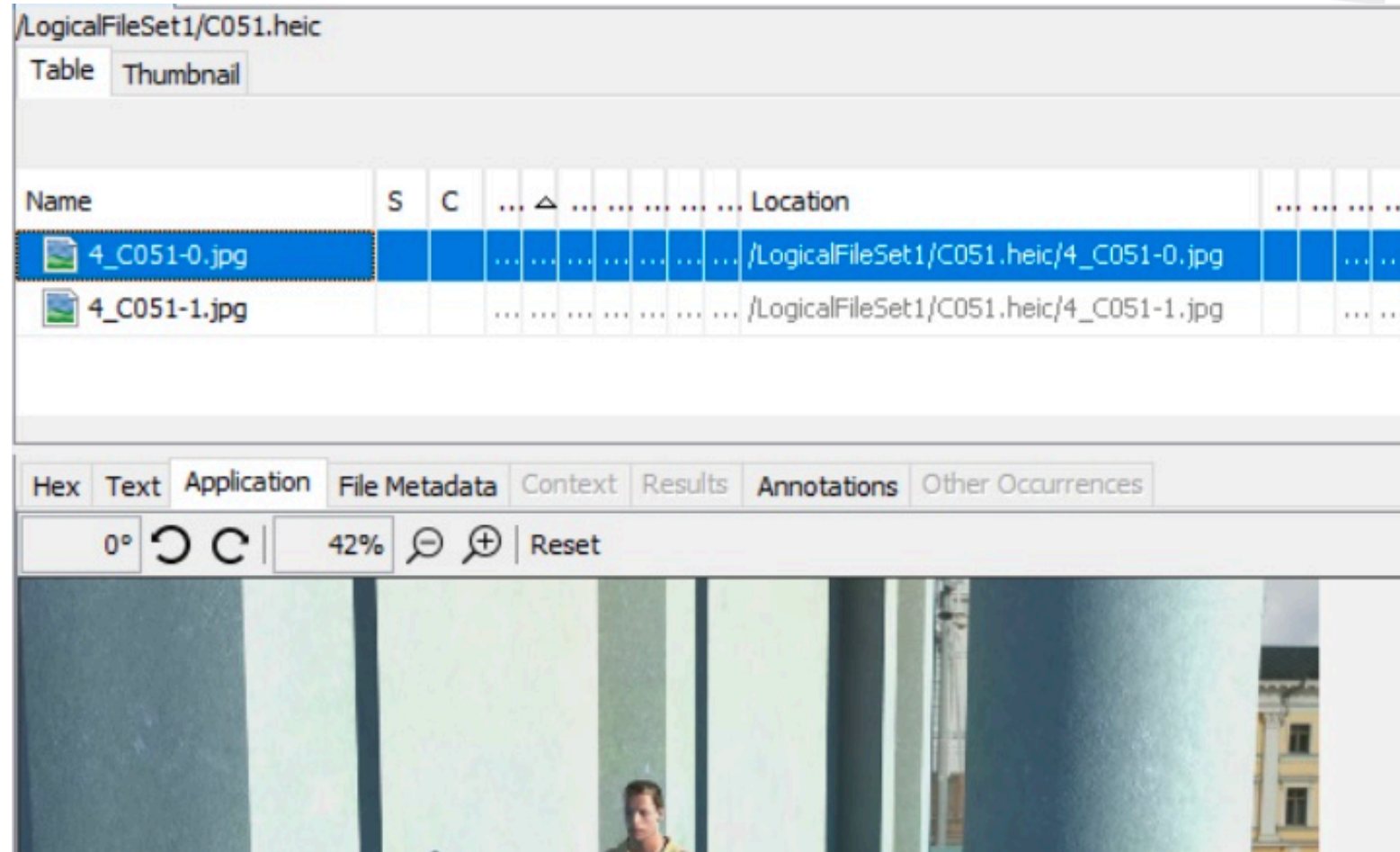
Recent Activity Module

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



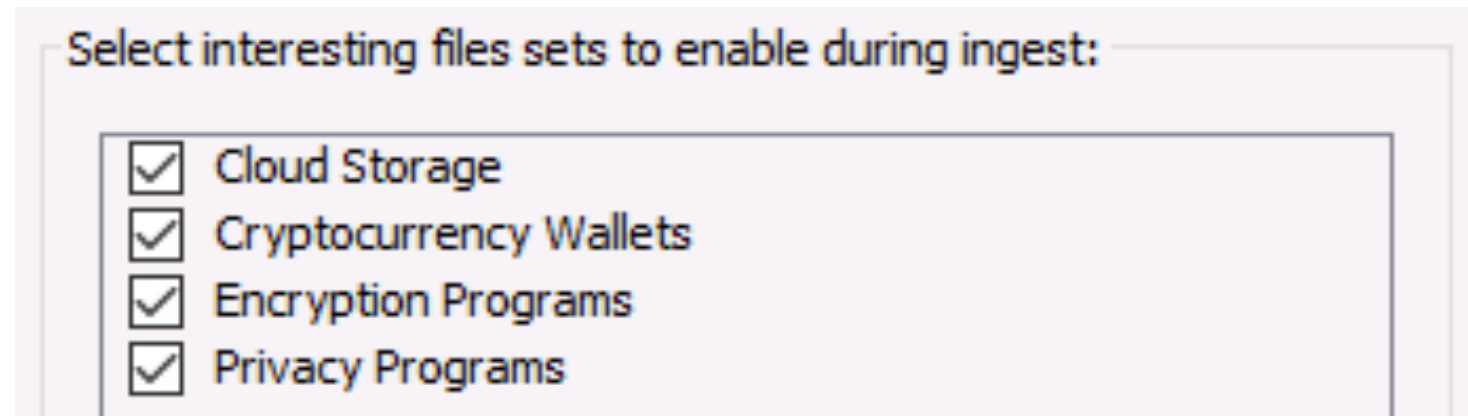
Picture Analyzer

- 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:



- 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

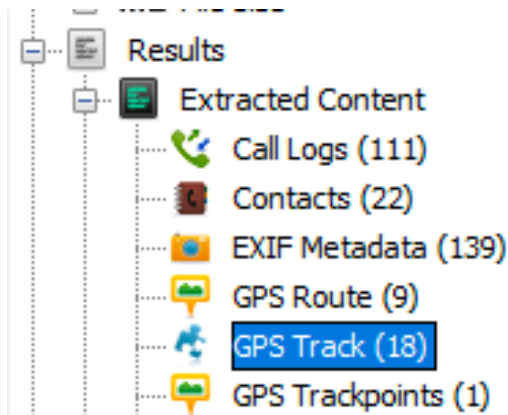
- The rebranded Correlation Engine module.
 - It does a lot more than correlate
- We want make sure you're taking advantage of your past data (see later talk)
 - The repository is enabled by default.
 - Hashes and identifiers are stored by default.
 - It will not correlate though.
- It also stores more account identifiers (email, social media, etc.) for Persona feature.

Ingest Settings

- ☒ Save items to the Central Repository
- ☒ Flag items previously tagged as notable
- ☒ Flag devices previously seen in other cases

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.

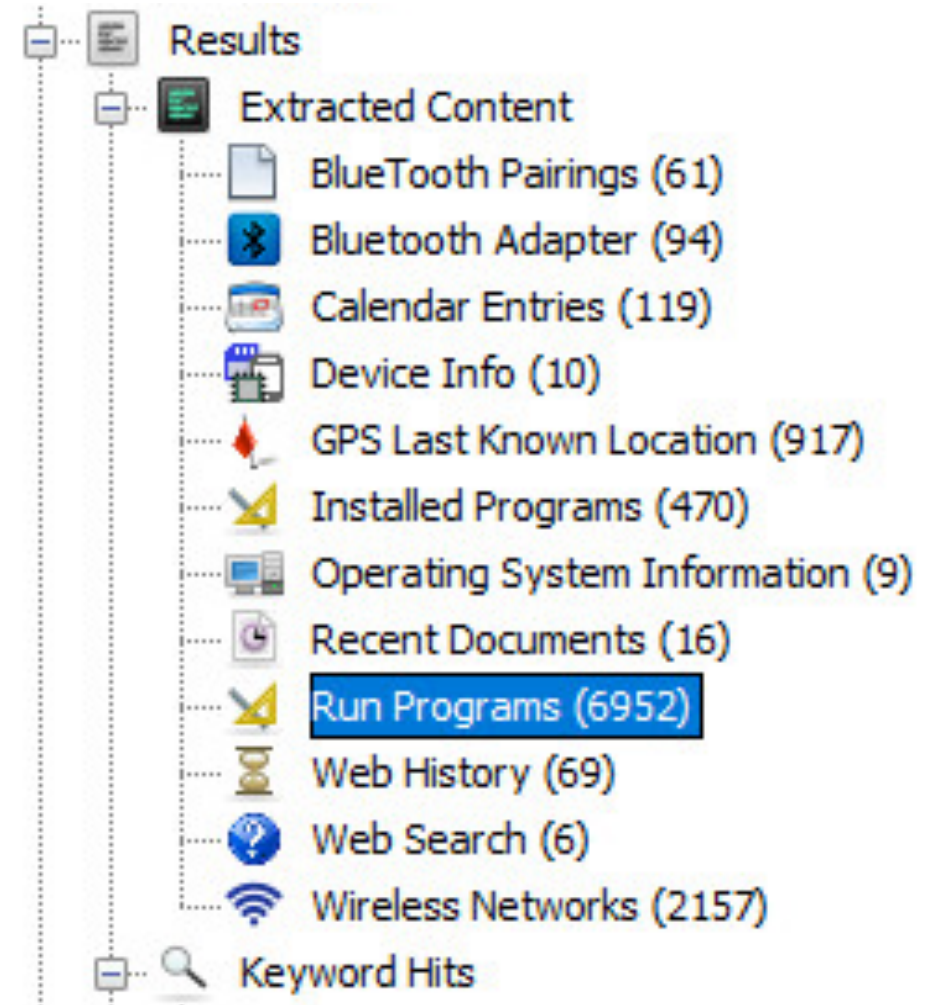


FLY005.DAT			FLY005.DAT	DJIMavicPro.001
FLY006.DAT			FLY006.DAT	DJIMavicPro.001
FLY020.DAT			FLY020.DAT	DJIMavicPro.001
FLY021.DAT			FLY021.DAT	DJIMavicPro.001
FLY022.DAT			FLY022.DAT	DJIMavicPro.001
FLY023.DAT			FLY023.DAT	DJIMavicPro.001
FLY024.DAT			FLY024.DAT	DJIMavicPro.001

- Can also be displayed in the new Map viewer

iOS Analyzer (iLEAPP)

- New module that wraps iLEAPP
- Current version uses TAR input file.
- Next version (4.18 – Jan 2021) supports:
 - Disk images
 - More artifacts
 - aLEAPP
- See Alexis's talk at the end of the day to learn more about these tools



Case Opens Up

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Listing
EXIF Metadata 12 Results

Table Thumbnail Save Table as CSV

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size
QUPANq5X_normal[1].jpg			7		Desire HD	HTC	xp-sp3-v3.001	1433
data_2_b20204f8			1	2012-02-06 09:51:37 EST	Canon EOS DIGITAL REBEL XS	Canon	xp-sp3-v3.001	2448
ta_520n-tfb-tm[1].jpg			7	2009-08-25 18:22:50 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	113784
ame_8vc-tfb-tm[1].jpg			7	2009-08-25 18:20:18 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	23446
B0137d01			7	2011-02-08 07:50:30 EST	NIKON D700	NIKON CORPORATION	xp-sp3-v3.001	37828
ACC93d01			7	2007-07-21 10:48:42 EDT	Canon EOS-1D Mark III	Canon	xp-sp3-v3.001	385936
F733Fd01			7	2006-03-30 12:34:35 EST	Canon EOS-1Ds Mark II	Canon	xp-sp3-v3.001	26138

Hex Text Application Message File Metadata Results Annotations Other Occurrences Video Triage

0% 107% Reset

Tags Menu

Basic UI Flow

The screenshot displays the Basis Technology software interface. The left sidebar contains a tree view with categories like Data Sources, Views, File Types, Deleted Files, MB File Size, Results, and Keyword Hits. The main window is titled 'Listing' and shows 'EXIF Metadata' with 12 results. A red arrow points to the 'Table' tab, which displays a table of file metadata. Another red arrow points to the 'Thumbnail' tab, which shows a large image of a virus particle.

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size
QUUPANq5X_normal[1].jpg			7		Desire HD	HTC	xp-sp3-v3.001	1433
2_b20204f8			1	2012-02-06 09:51:37 EST	Canon EOS DIGITAL REBEL XS	Canon	xp-sp3-v3.001	2448
520n-tfb-tm[1].jpg			7	2009-08-25 18:22:50 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	113784
ame_8vc-tfb-tm[1].jpg			7	2009-08-25 18:20:18 EDT	KODAK EASYSHARE V1003 ZOOM DIGITAL CAMERA	EASTMAN KODAK COMPANY	xp-sp3-v3.001	23446
B0137d01			7	2011-02-08 07:50:30 EST	NIKON D700	NIKON CORPORATION	xp-sp3-v3.001	37828
ACC93d01			7	2007-07-21 10:48:42 EDT	Canon EOS-1D Mark III	Canon	xp-sp3-v3.001	385936
F733Fd01			7	2006-03-30 12:34:35 EST	Canon EOS-1D Mark II	Canon	xp-sp3-v3.001	26138

New “Context” Viewer

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

The screenshot displays the 'Context' tab of a file analysis tool. At the top, a table lists files with their IDs and timestamps. Below this is a navigation bar with tabs: Hex, Text, Application, File Metadata, Context (selected), Results, Annotations, Other Occurrences, and Video Triage. The main content area is divided into two sections: 'Usage' and 'Source'. The 'Usage' section shows 'Unknown'. The 'Source' section lists two 'Program Execution' events, both dated '2019-10-29 15:52:00 EDT', each with a 'Go to Result' button.

File	ID	Timestamp
svchost.exe	4	2019-03-19 00:44:33 EDT
svf.dll	4	2019-03-19 02:23:18 EDT

<

Hex Text Application File Metadata **Context** Results Annotations Other Occurrences Video Triage

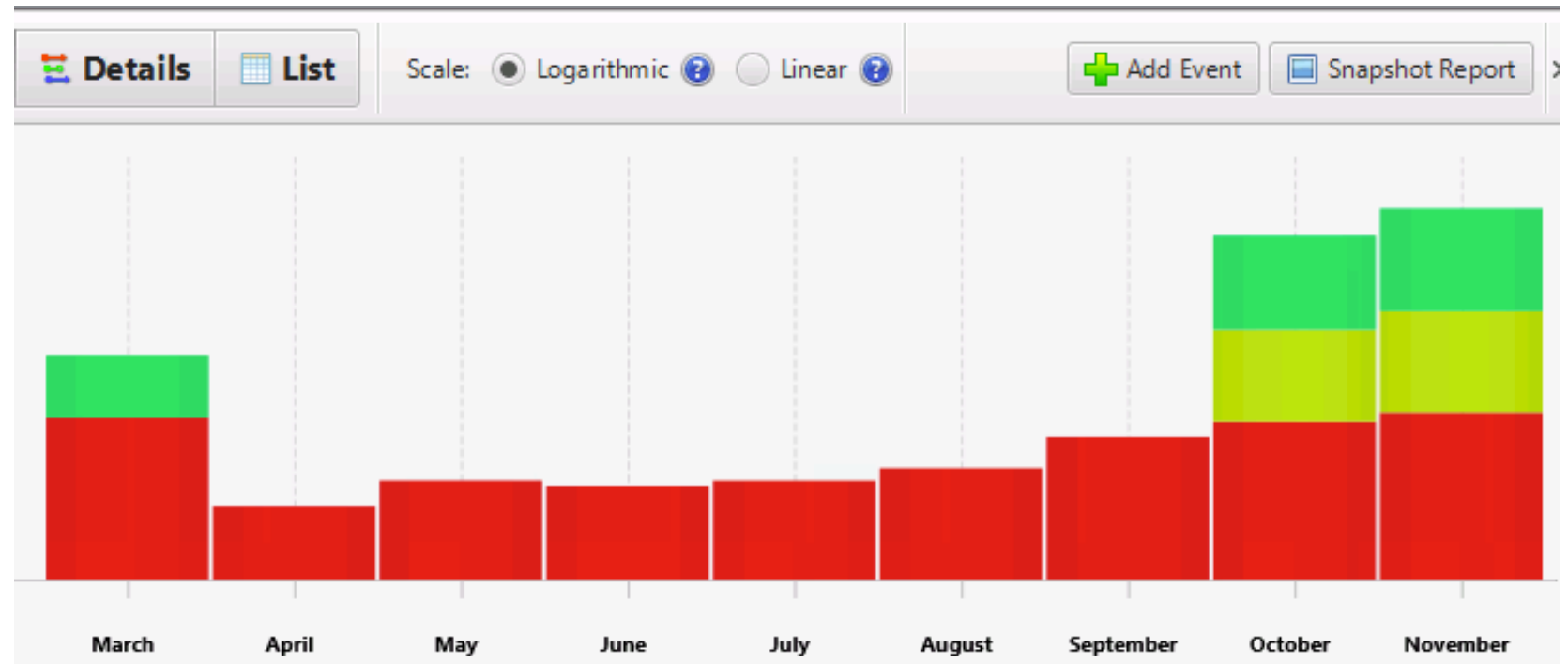
Usage
Unknown

Source
Program Execution: Program Run On 2019-10-29 15:52:00 EDT
[Go to Result](#)
Program Execution: Program Run On 2019-10-29 15:52:00 EDT
[Go to Result](#)

Other Viewers

- Autopsy has other viewers that are more focused for more complex data:

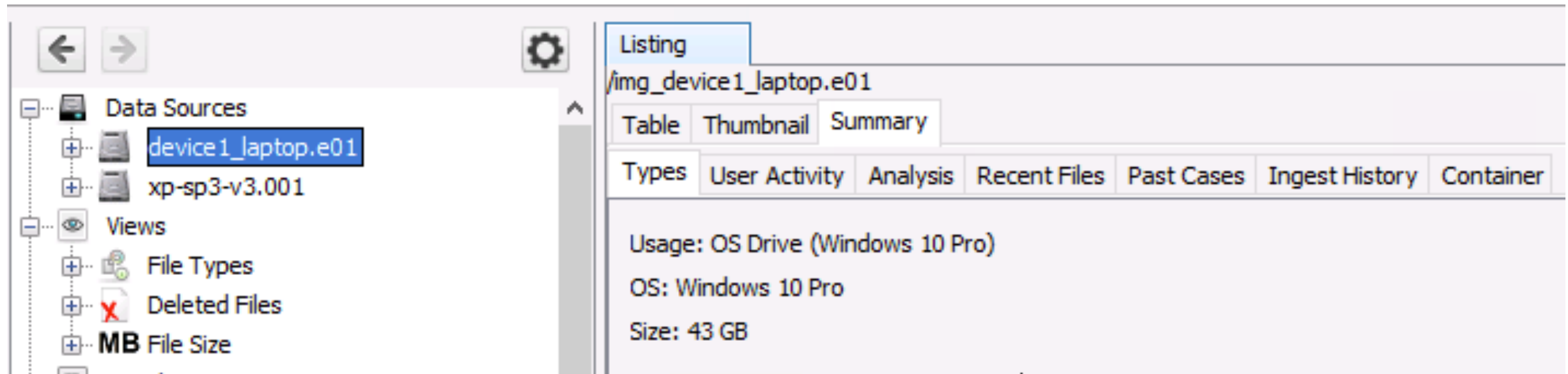
- Communications
- Timeline
- Image Gallery



- Let's look at some new ones and some updates

Data Source Summary

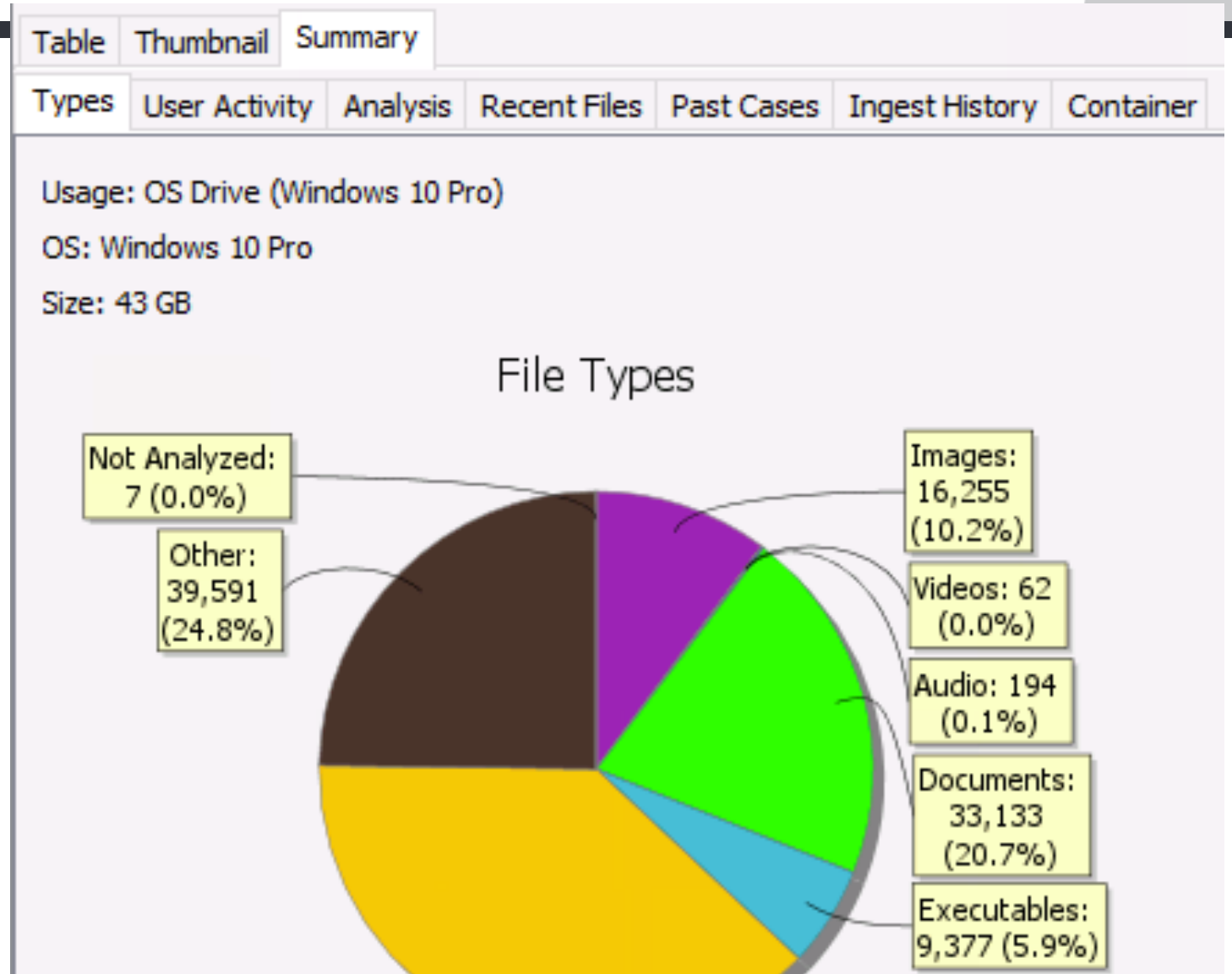
- It's good to start an investigation knowing the rough shape of the data.
- Goal of the Data Source Summary panels is to help you figure that out.
- Click on a data source and choose “Summary”



Data Source Summary Example – Types

Provides overview of:

- OS
- File types
- Number of files




Discovery


Groups

- /img_device1_laptop.e01/vol_... /User Data/Default/Cache (5)
- /img_device1_laptop.e01/vol_... ntRenzk/Desktop/Pictures (4)
- /img_device1_laptop.e01/vol_7/Windows/Web/Screen (4)
- /img_device1_laptop.e01/... one_af74338f76aa2bd0 (4)
- /img_device1_laptop.e01/v ... 3d8bbwe/Assets/Images (2)
- /img_device1_laptop.e01/v ... ilder/ModifierAssets (2)
- /img_device1_laptop.e01/v ... _8wekyb3d8bbwe/Assets (2)
- /img_device1_laptop.e01/vol_... ows/Web/Wallpaper/Theme1 (2)
- /img_device1_laptop.e01 ... ne_a937730822266138 (2)
- /img_device1_laptop.e01/vol_v ... agnosticLogCSP/Collectors (1)
- /img_device1_laptop.e01/vol_... ws/System32/WDI/LogFiles (1)
- /img_xp-sp3-v3.001/vol_2/Do ... Application Data/Microsoft (1)
- /img_xp-sp3-v3.001/vol_2/WINDOWS/Web/Wallpaper (1)

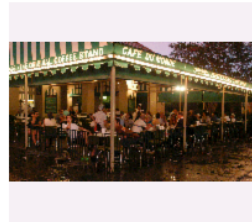
Page: 1 of 1

Pages: 

Go to Page:

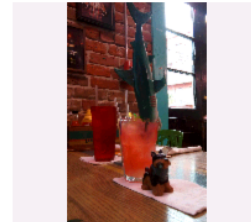
Page Size: 100 

...Data/Default/Cache/f_000158



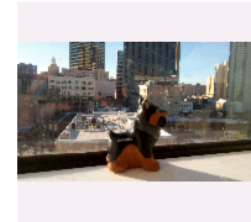
Size: 1 MB

...Data/Default/Cache/f_00022e



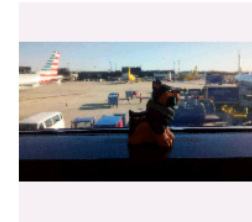
Size: 1 MB

...Data/Default/Cache/f_00022f



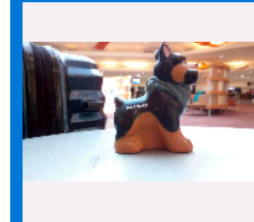
Size: 2 MB

...Data/Default/Cache/f_000230



Size: 1 MB

...Data/Default/Cache/f_000233






Size: 1 MB

Details Area

Instances

/img_device1_laptop.e01/vol_7/Users/AntiRenzk/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000233

Hex Text Application File Metadata Context Results Annotations Other Occurrences Video Triage

0°   31%  Reset



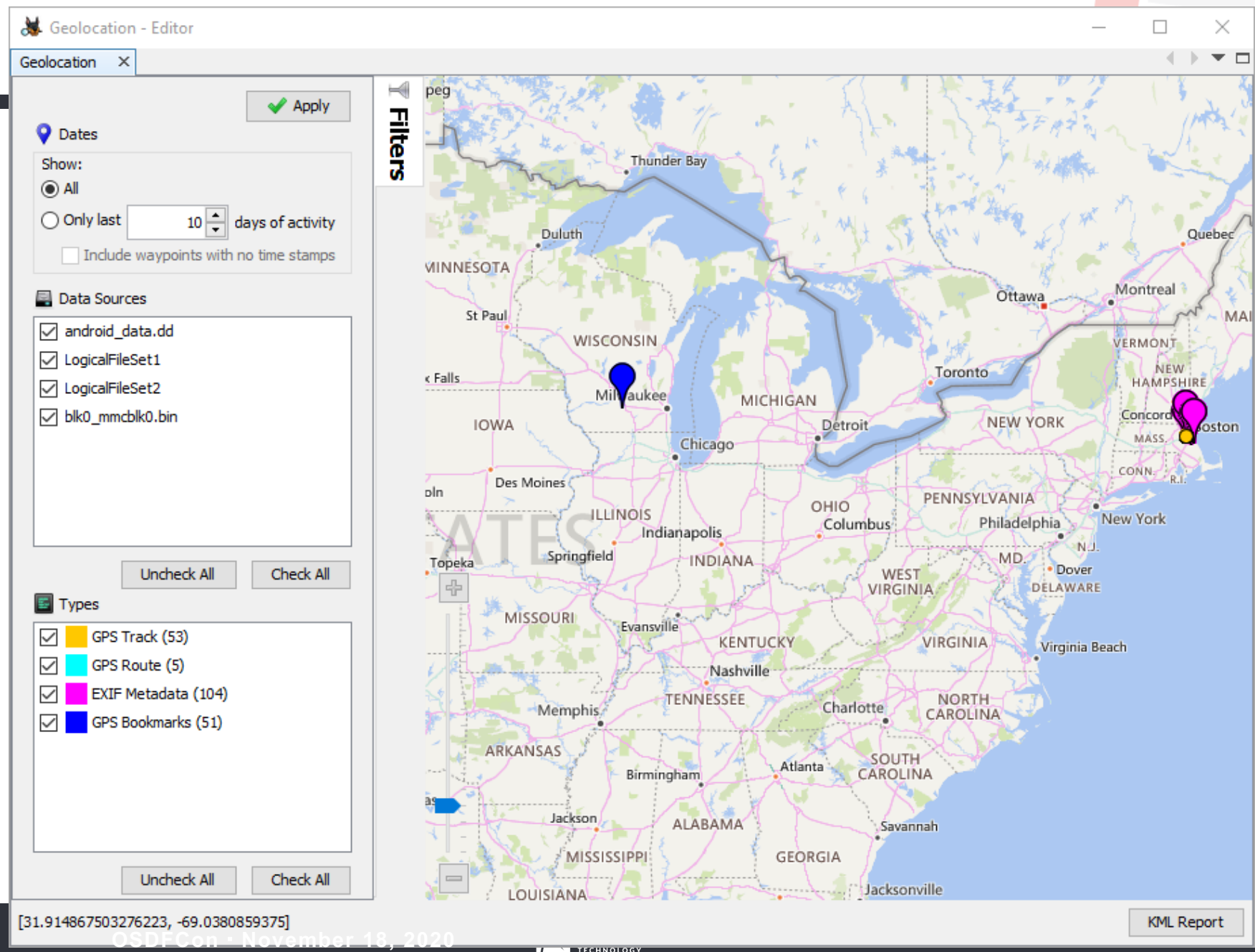
Discovery



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