#OSDFCon
OPEN SOURCE DIGITAL FORENSICS CONFERENCE

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

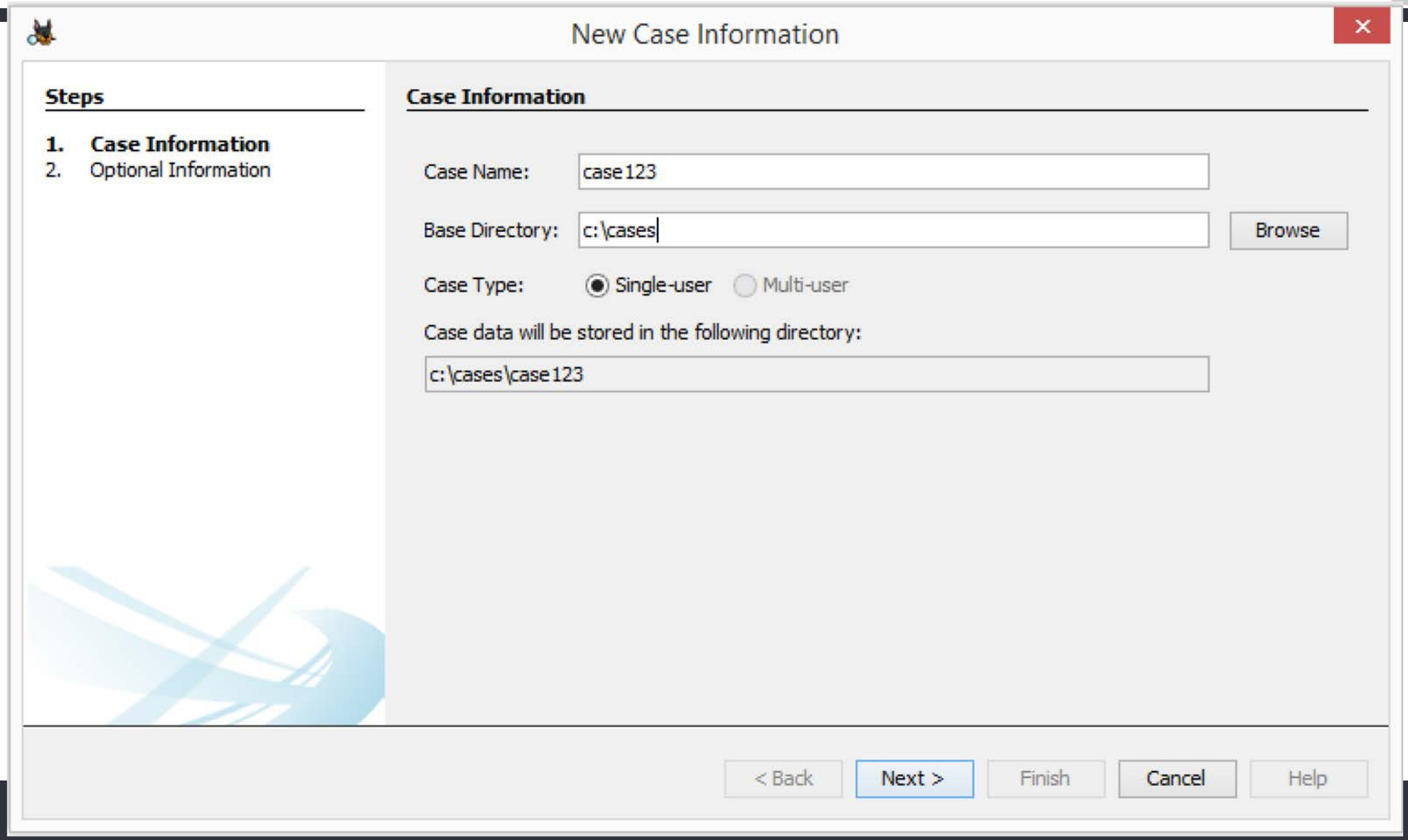
Hash

What is Autopsy?

- Open source digital forensics platform.
- Designed to be:
  - Easy to use
  - 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.

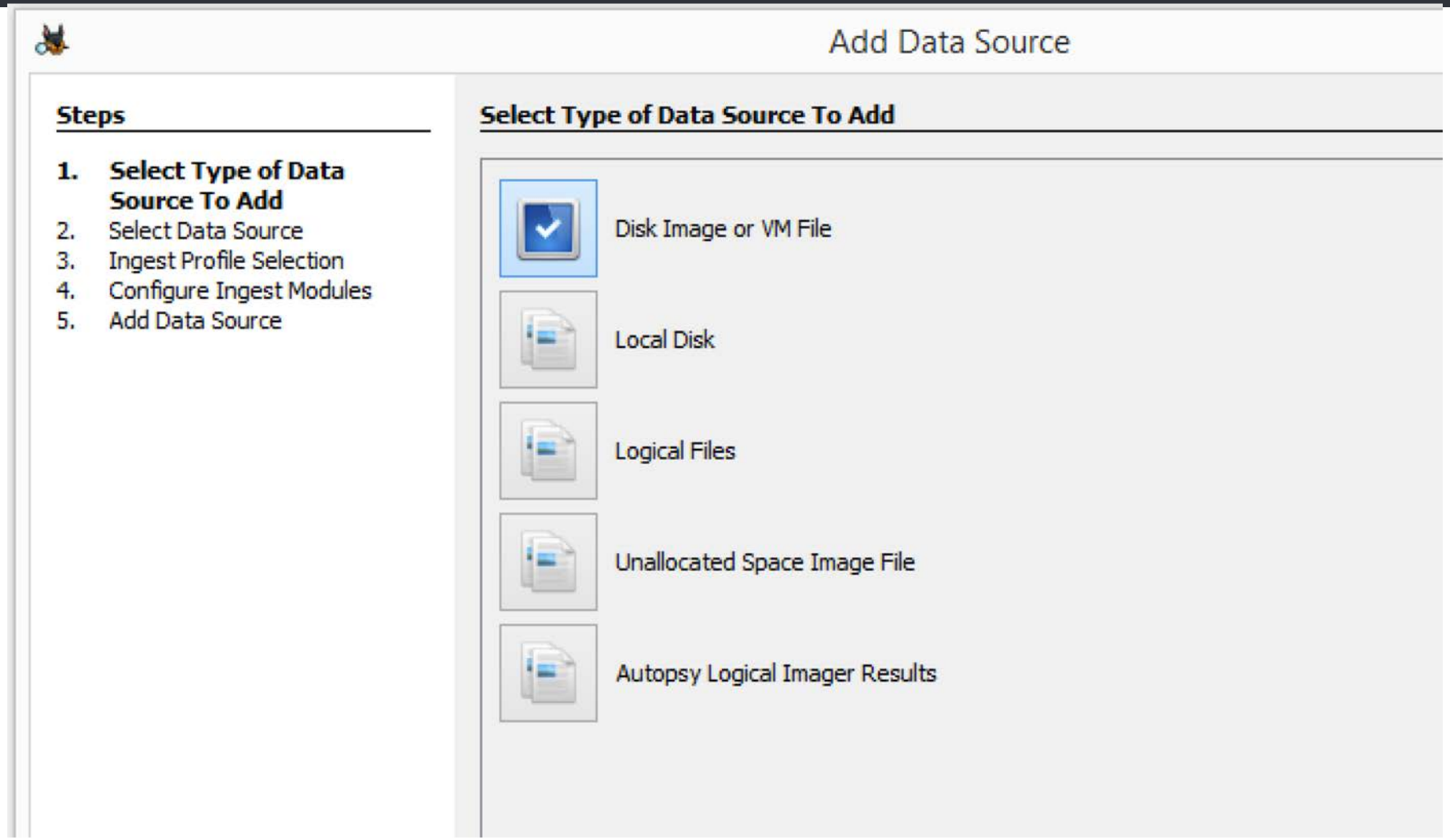
Make A Case


New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
case123
Base Directory:
c:\cases
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
c:\cases\case123
< Back
Next >
Finish
Cancel
Help

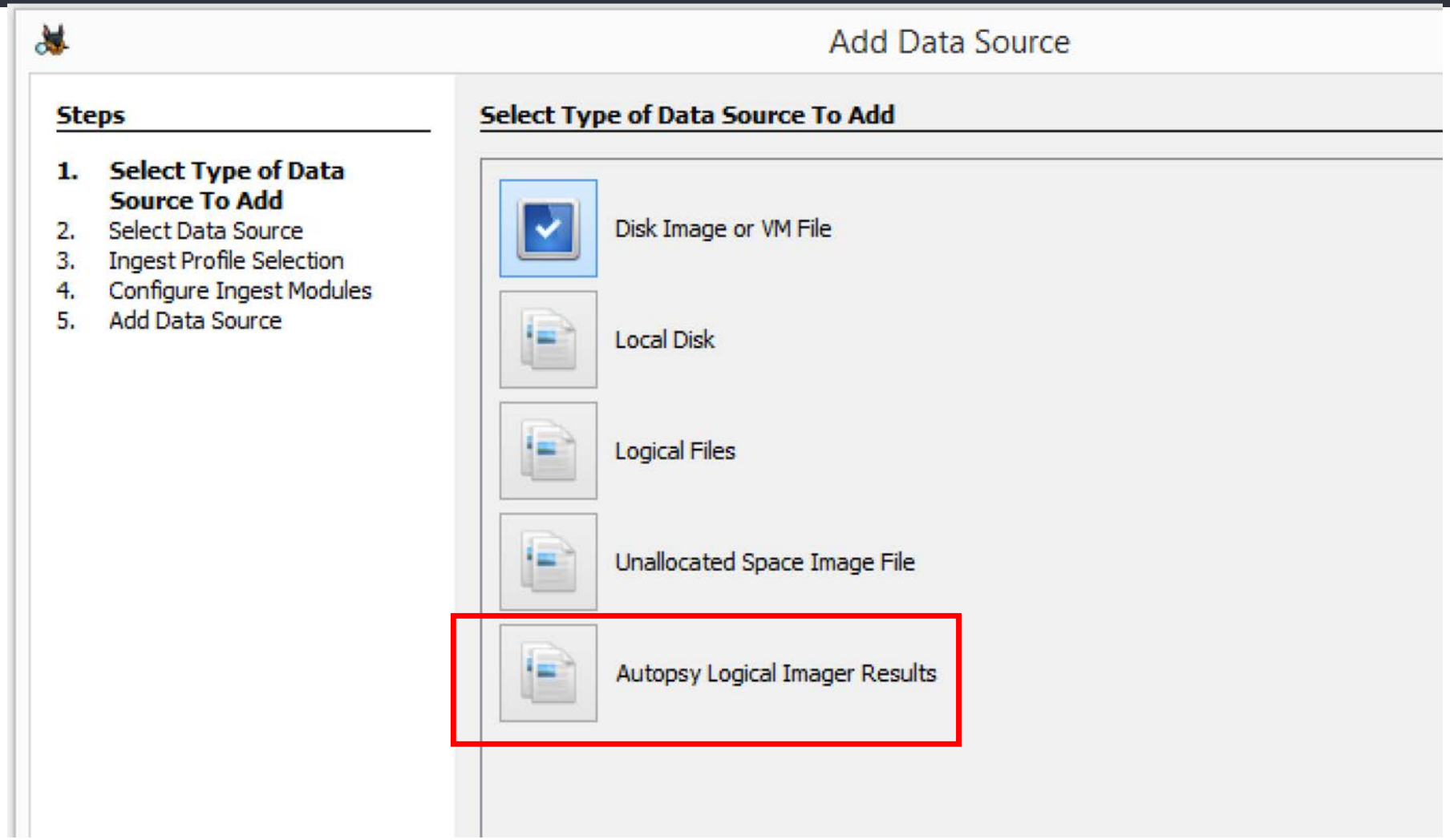
Multi-user Case Documentation

- 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



Add A Data Source

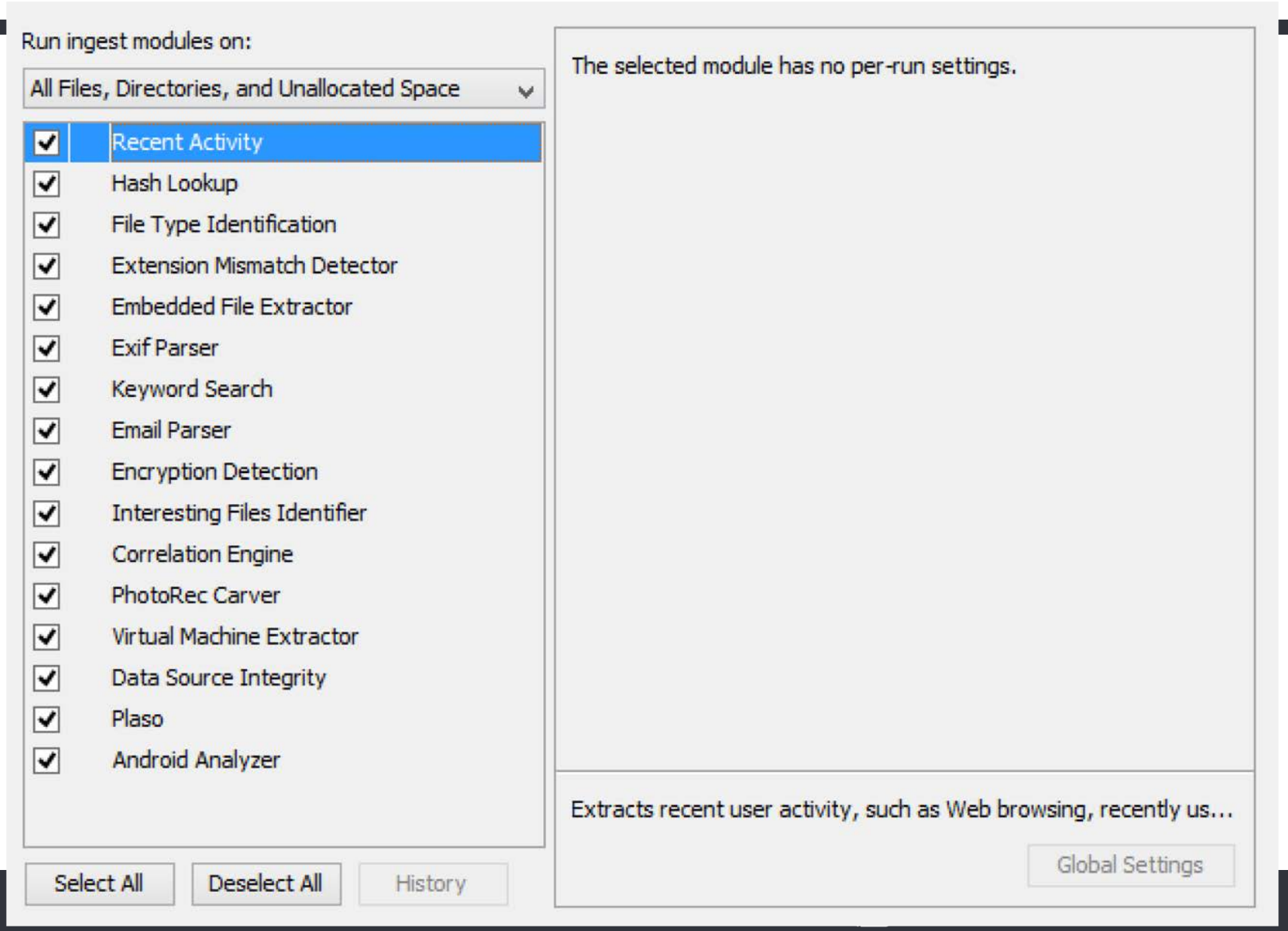


Logical Imager

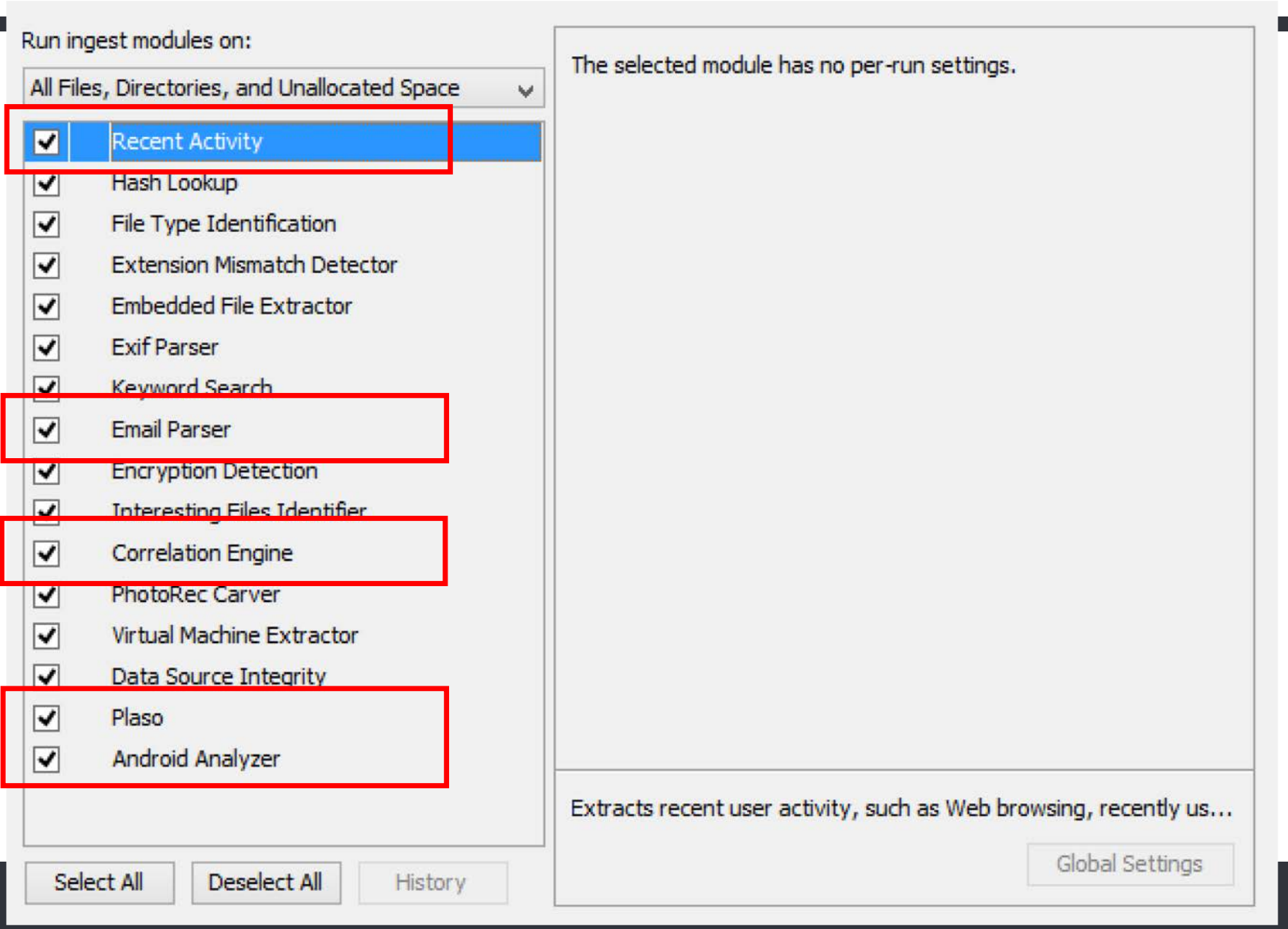
- Command line program that runs on target computer and collects:
  - Files (based on a set of rules)
  - System information (such as users)
- Parses raw drive data and the registry using The Sleuth Kit
- Unique Benefits:
  - Can access locked files and bypass rootkits that hide files
  - Does not update time stamps during search
  - Can access dual boot volumes (Linux for example)
  - 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



Configure Ingest Modules



Recent Activity Module

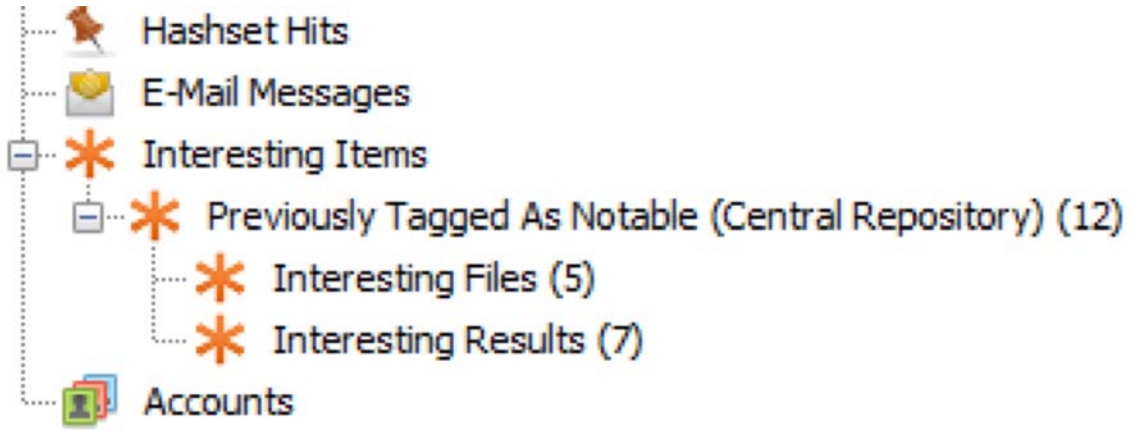
- Lots of features added from our DHS S&T contract.
- All of them came from “What’s Needed” and surveys from past OSDFCons.
- Web: Added Safari and Edge. Added form fill data to Firefox and Chrome. Added cache parsing to Chrome.
- Parse Zone.Identifiers to show source of downloaded files.
- Ported existing 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

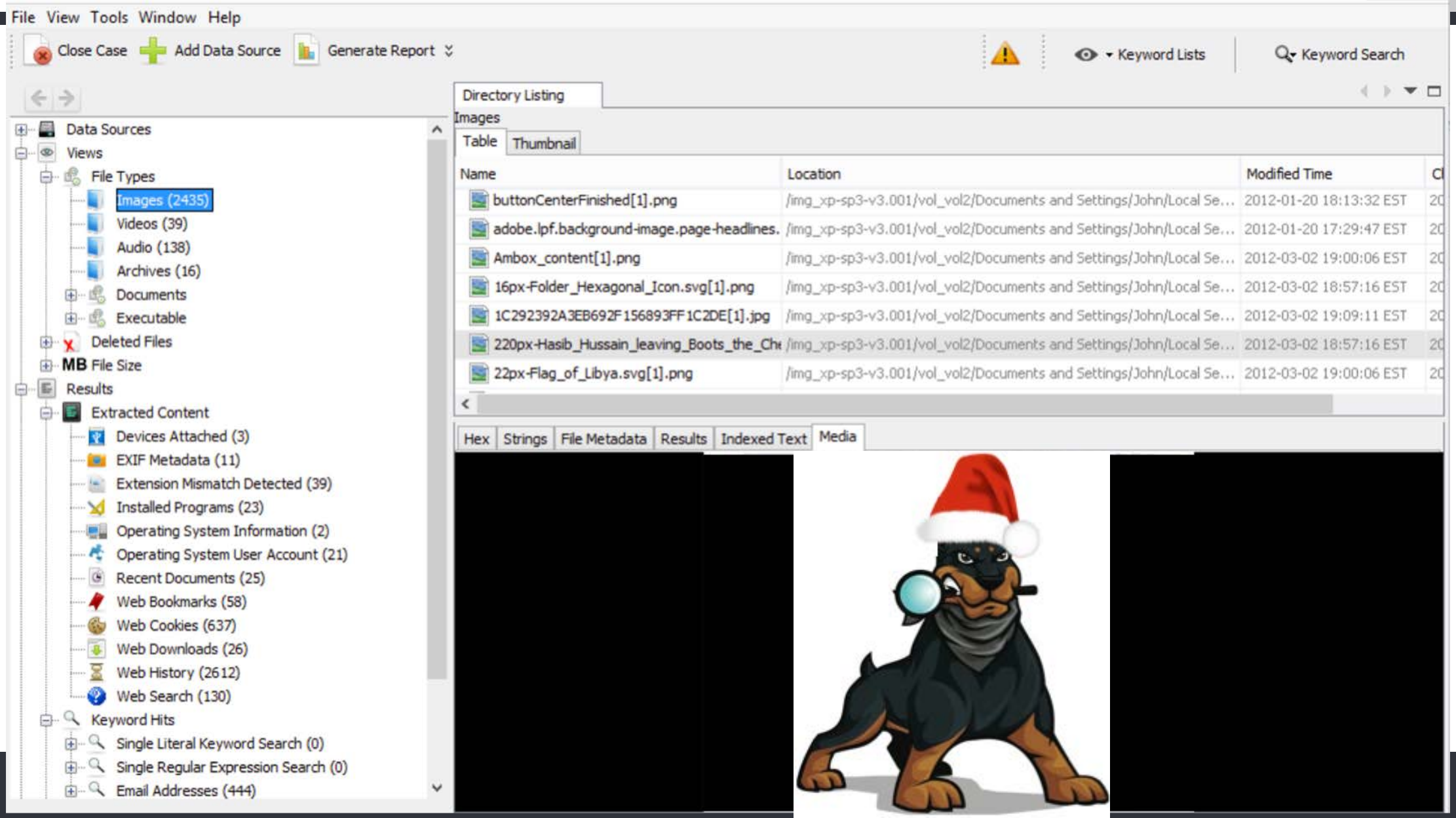
- This module:
  - Saves artifacts to a central database for future correlation
  - Flags artifacts that were previously seen and marked as notable
- Updates:
  - More artifacts: SSID, MAC address, IMEI, IMSI, and ICCID



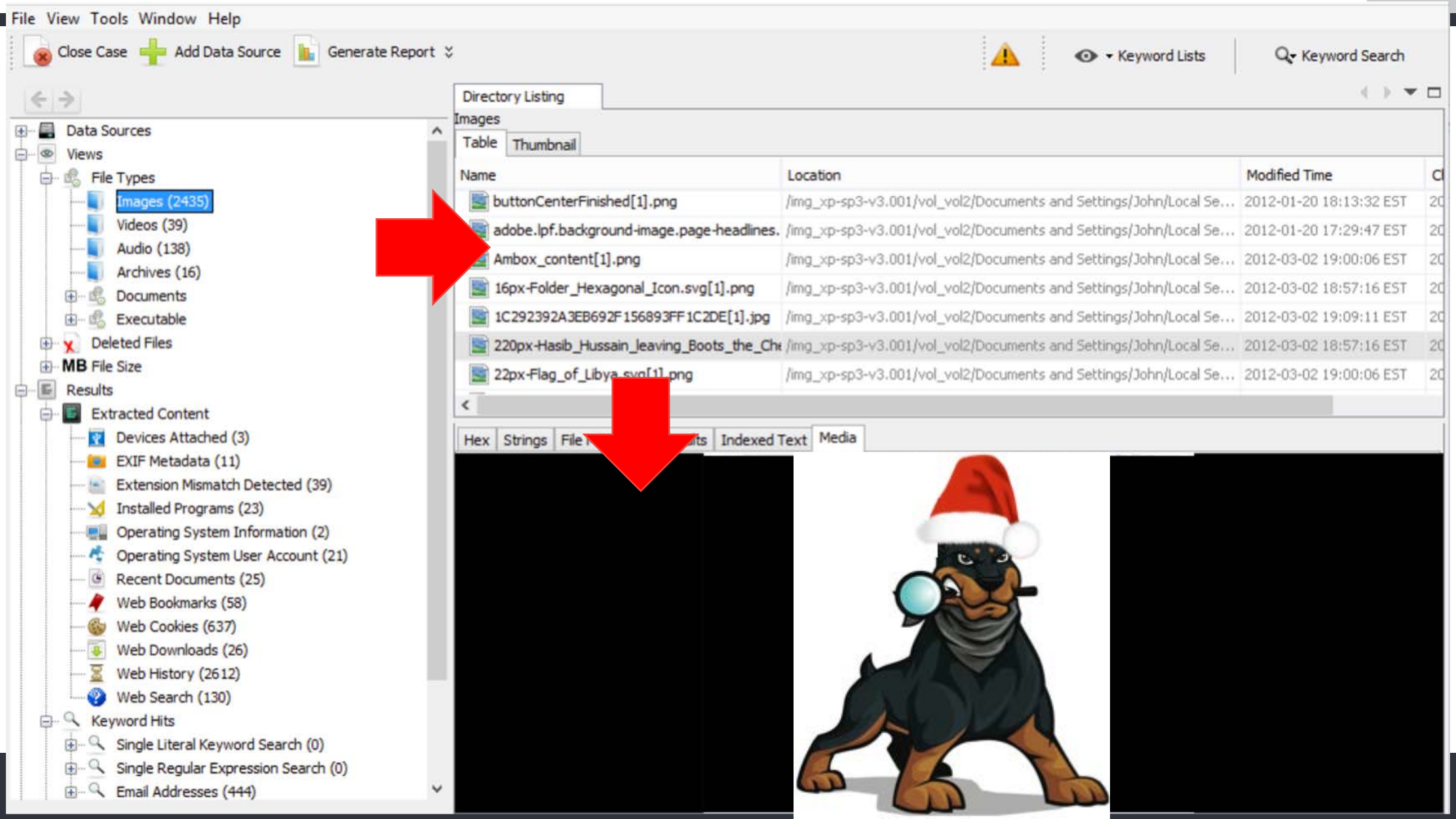
Android Analyzer Module

- Added support for many more apps:
  - Browsers: Android browser, Opera, Samsung SBrowser
  - Messaging: Facebook Messenger, IMO, LINE, Skype, TextNow, Viber, WhatsApp
  - File Transfer: ShareIt, Xender, Zapya
  - …
- Made it even easier to make 3rd party apps. 3 steps:
  - Find and open SQLite and associated WAL files with one call.
  - Query correct tables
  - Add artifacts for contacts, messages, etc. (one call each instead of 8 or 10).
- See talk later today for more details

Case Opens Up

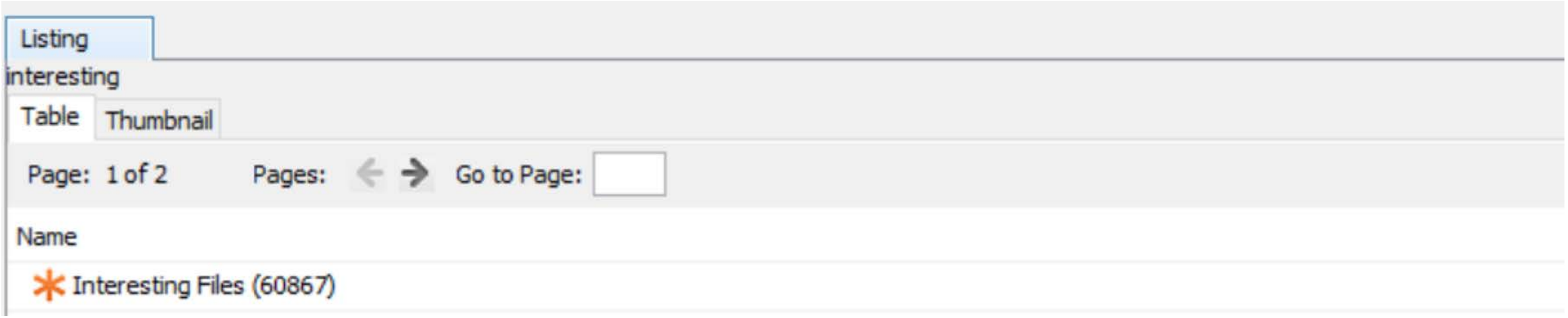


Basic UI Flow

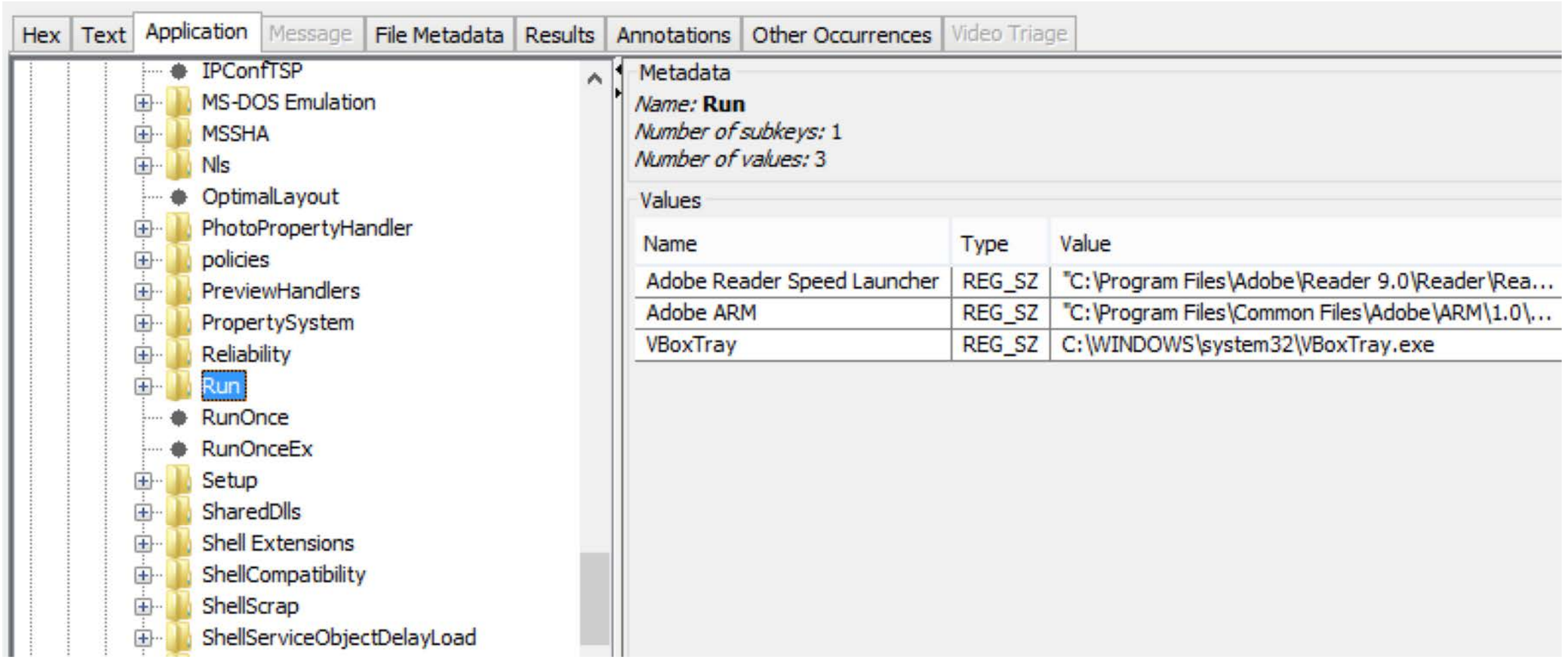


Performance

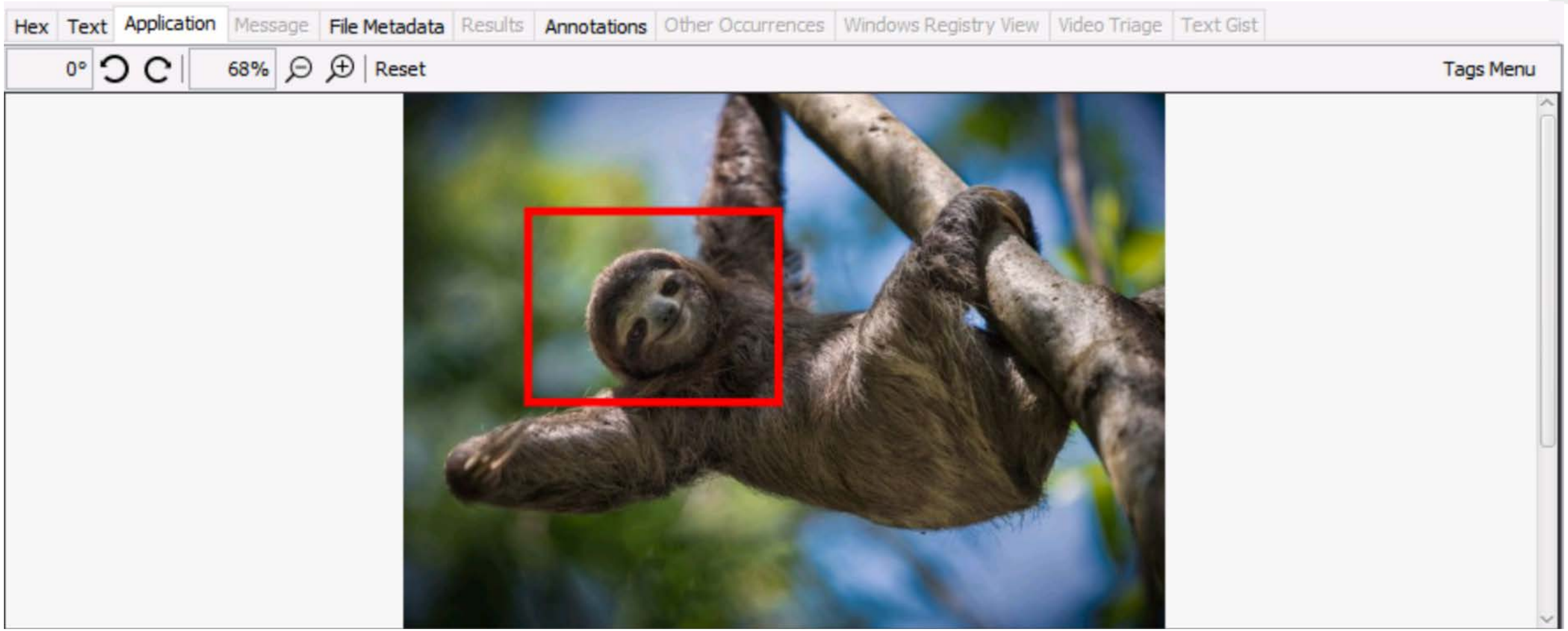
- Several things were done to improve performance with large datasets
- Improved some backend queries
- Added paging everywhere



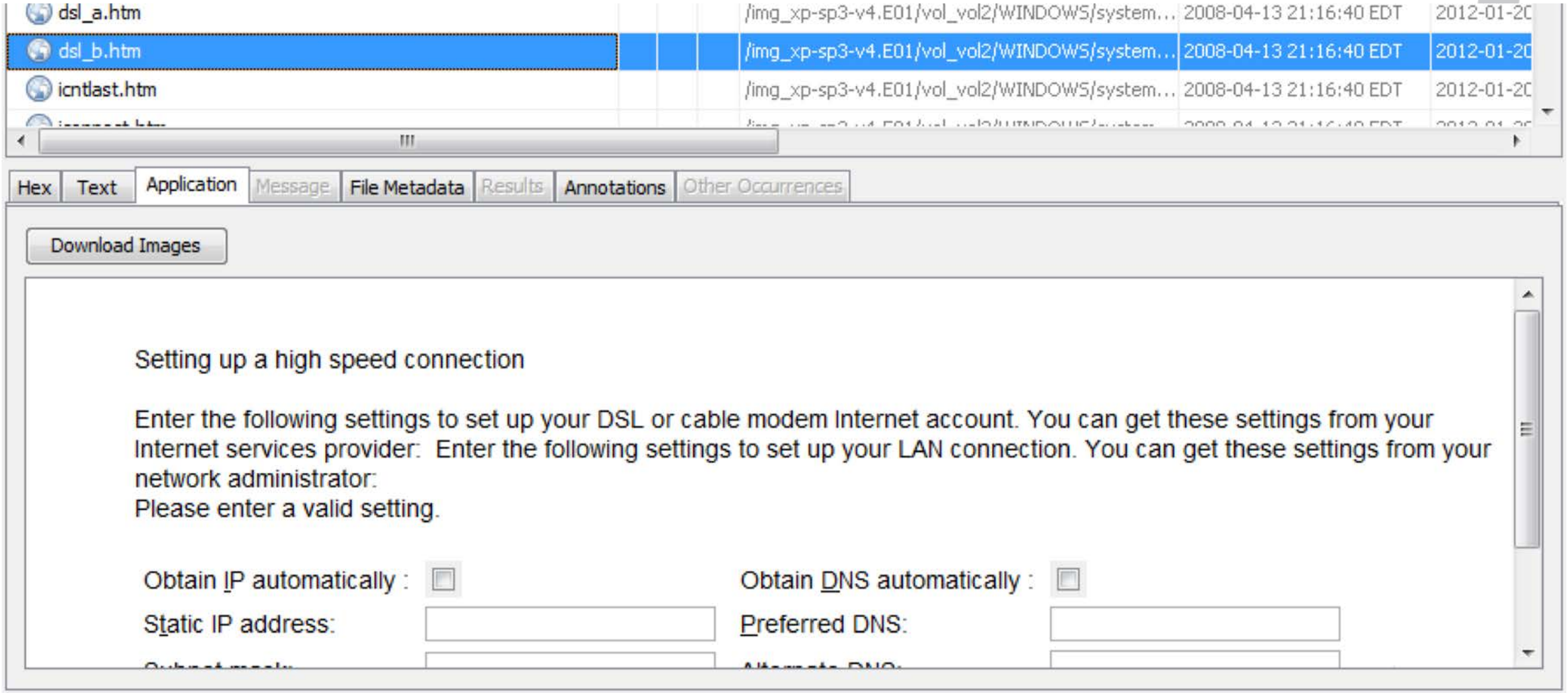
Content Viewer: Added Willi's Registry Viewer



Content Viewer: Image Tags Can Have Boxes

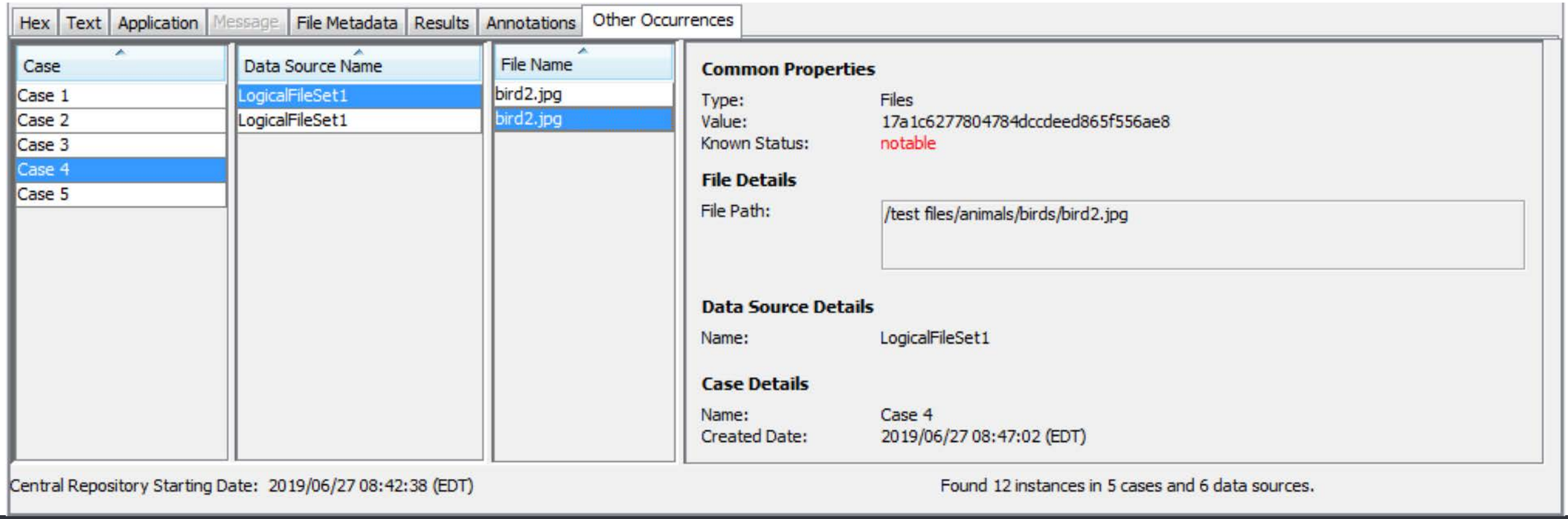


Content Viewer: Added HTML viewer



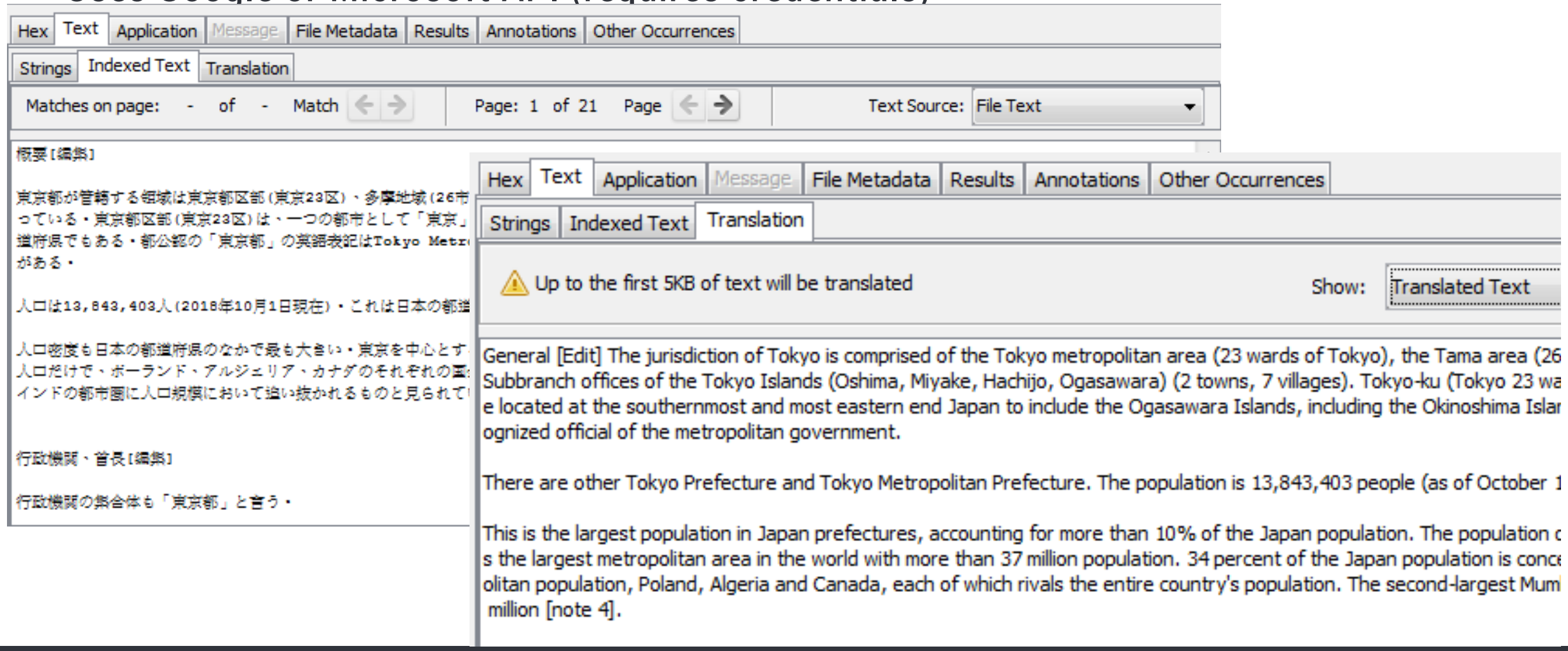
Content Viewer: Other Occurrences

- 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)



Translation: File Names Too

Listing

/LogicalFileSet5/Test files/Translation Testing

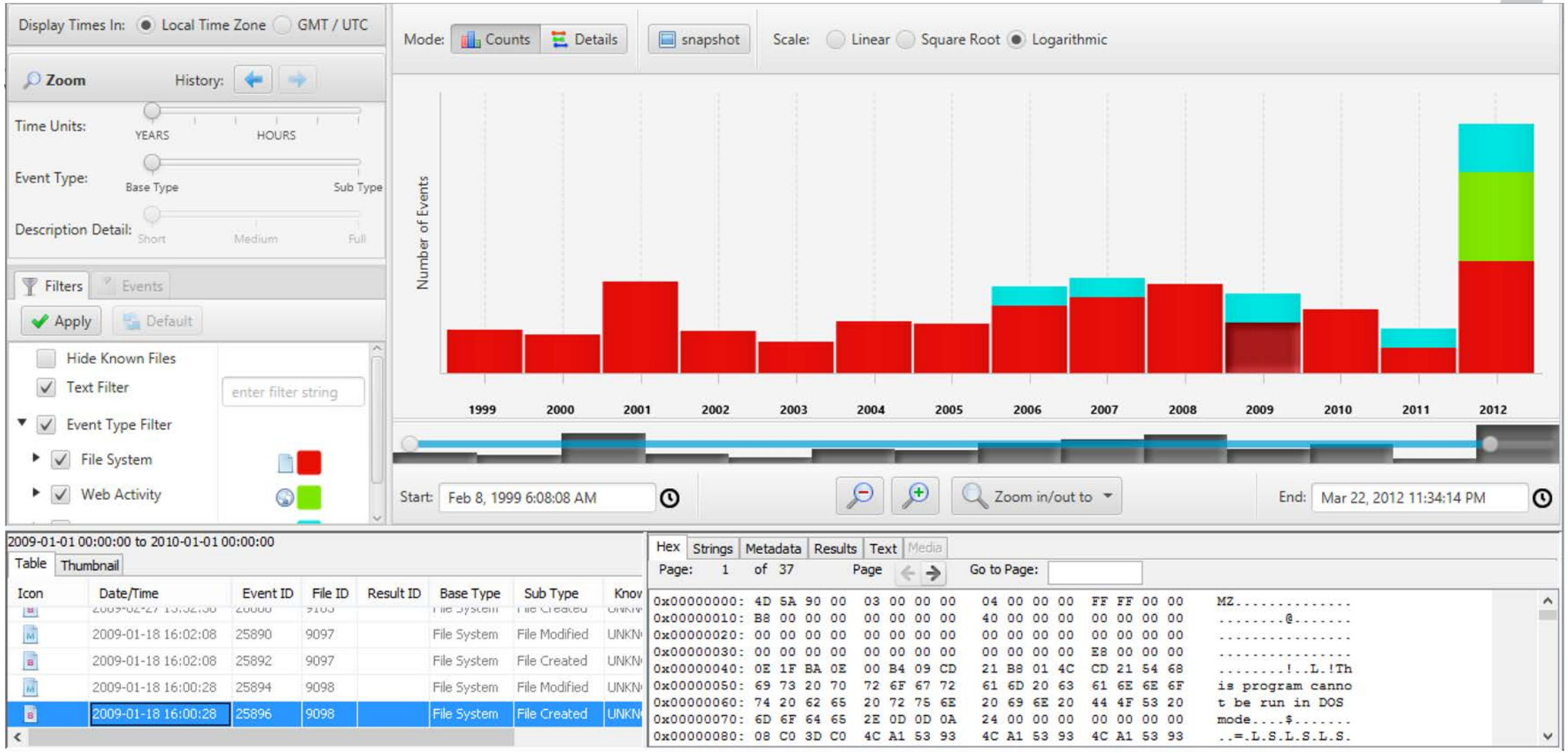
Table | Thumbnail

Name	Original Name	S	C	O	Location
Spain	España				/LogicalFileSet5/Test files/Translation Testing/España
test					/LogicalFileSet5/Test files/Translation Testing/test
Greece	Ελλάδα				/LogicalFileSet5/Test files/Translation Testing/Ελλάδα
Russia's Federation	Росси́йска...				/LogicalFileSet5/Test files/Translation Testing/Росс...
Russia	Росси́я				/LogicalFileSet5/Test files/Translation Testing/Росси́я
Bahrain	البحرين				/LogicalFileSet5/Test files/Translation Testing/البحرين
Japan	日本				/LogicalFileSet5/Test files/Translation Testing/日本
Korean	한국어				/LogicalFileSet5/Test files/Translation Testing/한국어
Four.txt	أربعة.txt				/LogicalFileSet5/Test files/Translation Testing/أربعة.txt

Other Viewers

- Some data types need an interface more specific than the generic tree and table.
- All of those viewers received updates too:
  - Timeline
  - Image Gallery
  - Communications

Timeline

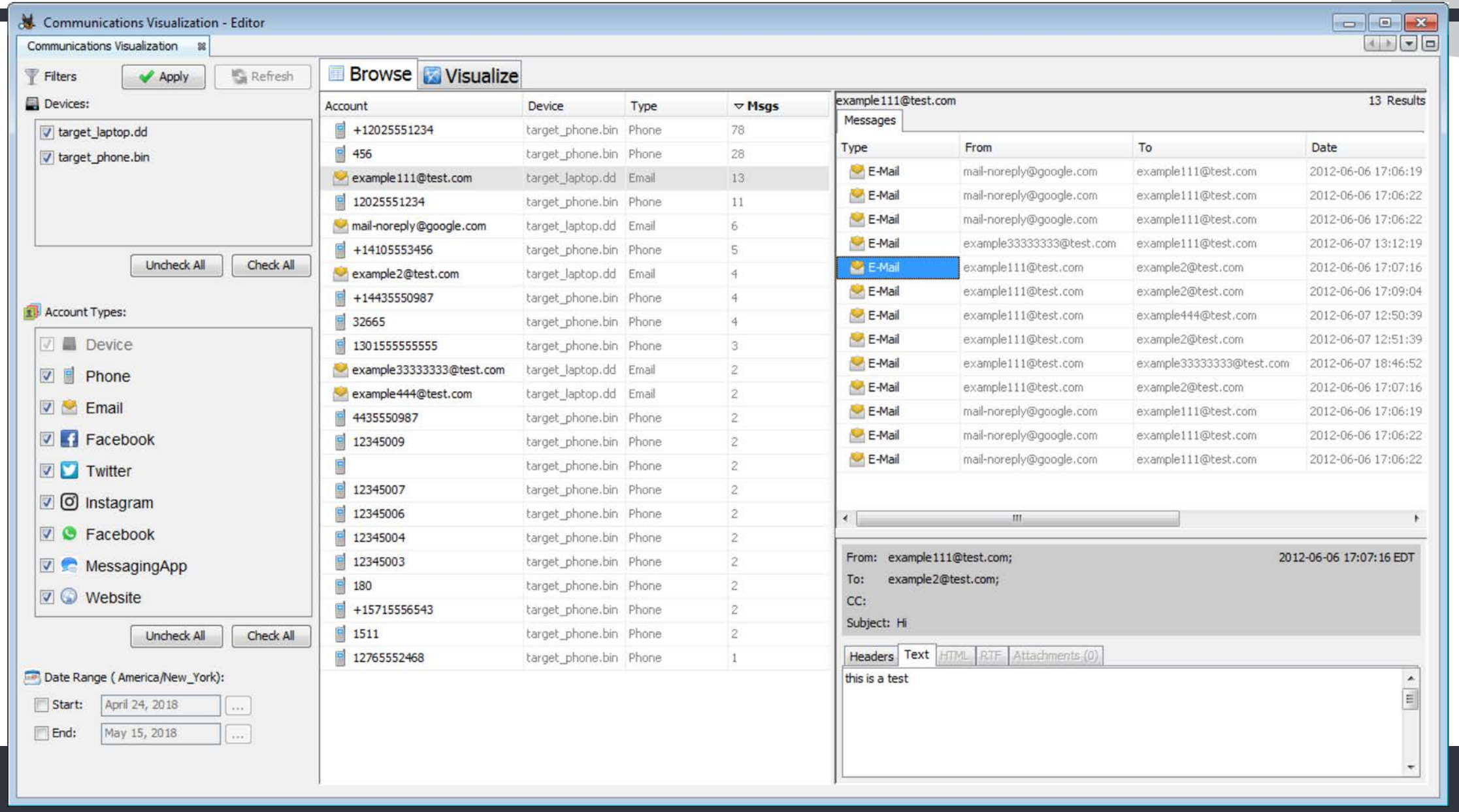
- 
Display Times In: Local Time Zone GMT / UTC
Zoom
History:
Time Units:
YEARS
HOURS
Event Type:
Base Type
Sub Type
Description Detail:
Short
Medium
Full
Filters
Events
Apply
Default
Hide Known Files
Text Filter
enter filter string
Event Type Filter
File System
Web Activity
Mode: Counts Details
snapshot
Scale: Linear Square Root Logarithmic
Number of Events
1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012
Start: Feb 8, 1999 6:08:08 AM
Zoom in/out to
End: Mar 22, 2012 11:34:14 PM
2009-01-01 00:00:00 to 2010-01-01 00:00:00
Table
Thumbnail
Icon
Date/Time
Event ID
File ID
Result ID
Base Type
Sub Type
2009-01-18 16:02:08 25890 9097 File System File Modified
2009-01-18 16:02:08 25892 9097 File System File Created
2009-01-18 16:00:28 25894 9098 File System File Modified
2009-01-18 16:00:28 25896 9098 File System File Created
Hex
Strings
Metadata
Results
Text
Media
Page: 1 of 37
Page
Go to Page:
0x00000000: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ..............
0x00000010: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 ....
0x00000040: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ....!..L.!Th
0x00000050: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
0x00000060: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
0x00000070: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
0x00000080: 08 C0 3D C0 4C A1 53 93 4C A1 53 93 4C A1 53 93 ..=.L.S.L.S.L.S.

Timeline Enhancements

- No longer need to create timeline databases the first time it is opened.
  - 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

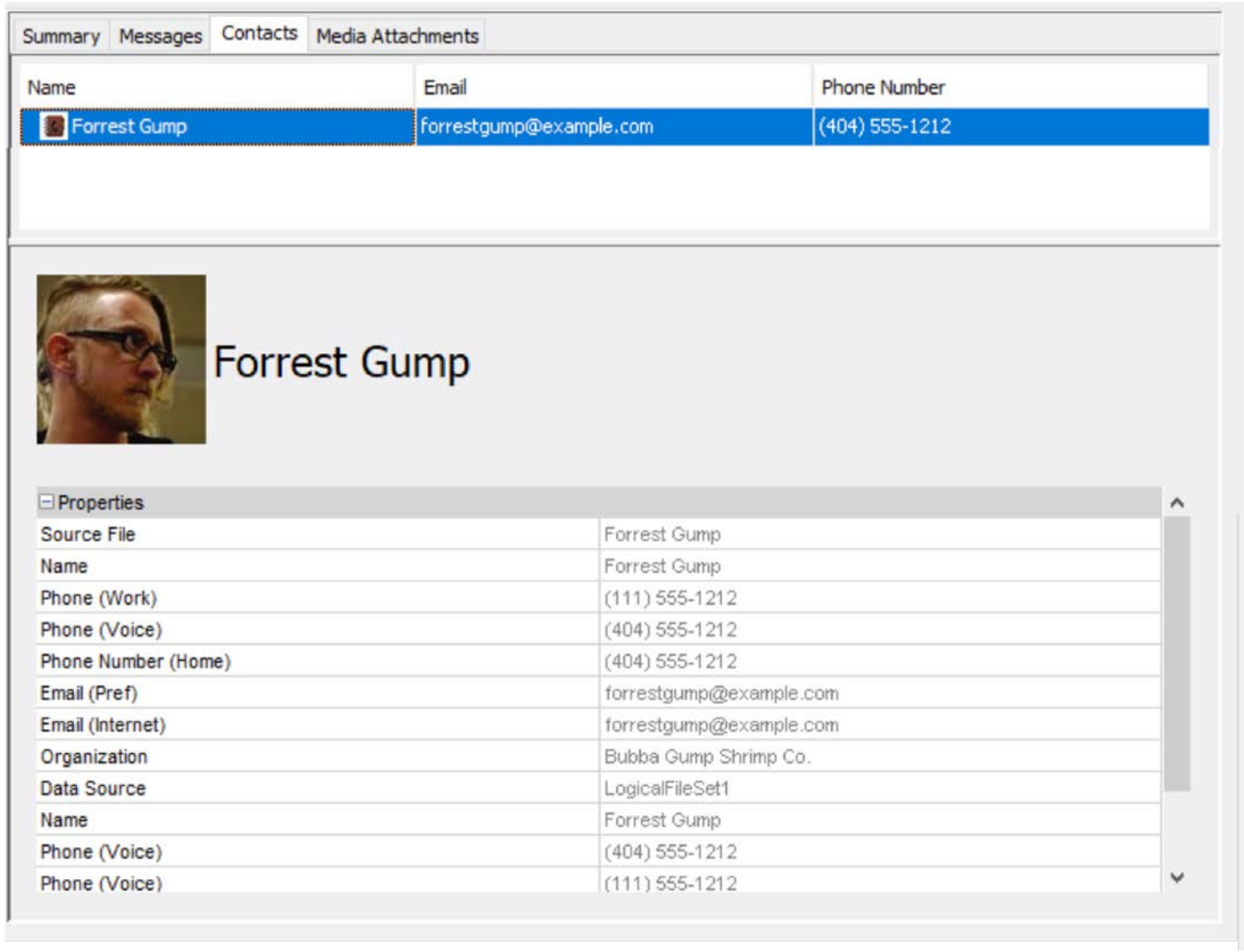


Communications Updates

- 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

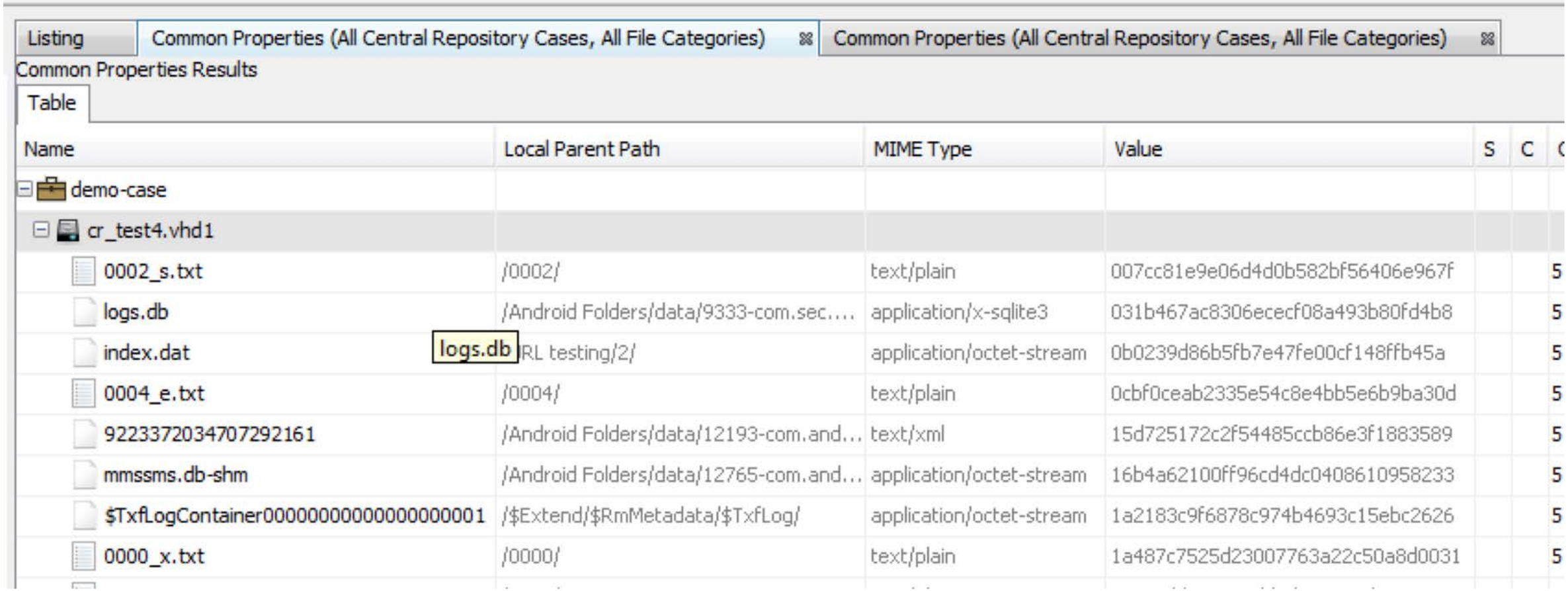
Contacts


Summary
Messages
Contacts
Media Attachments
Name
Email
Phone Number
Forrest Gump
forrestgump@example.com
(404) 555-1212
Forrest Gump
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)
forrestgump@example.com
Email (Internet)
forrestgump@example.com
Organization
Bubba Gump Shrimp Co.
Data Source
LogicalFileSet1
Name
Forrest Gump
Phone (Voice)
(404) 555-1212
Phone (Voice)
(111) 555-1212

Common Property Search

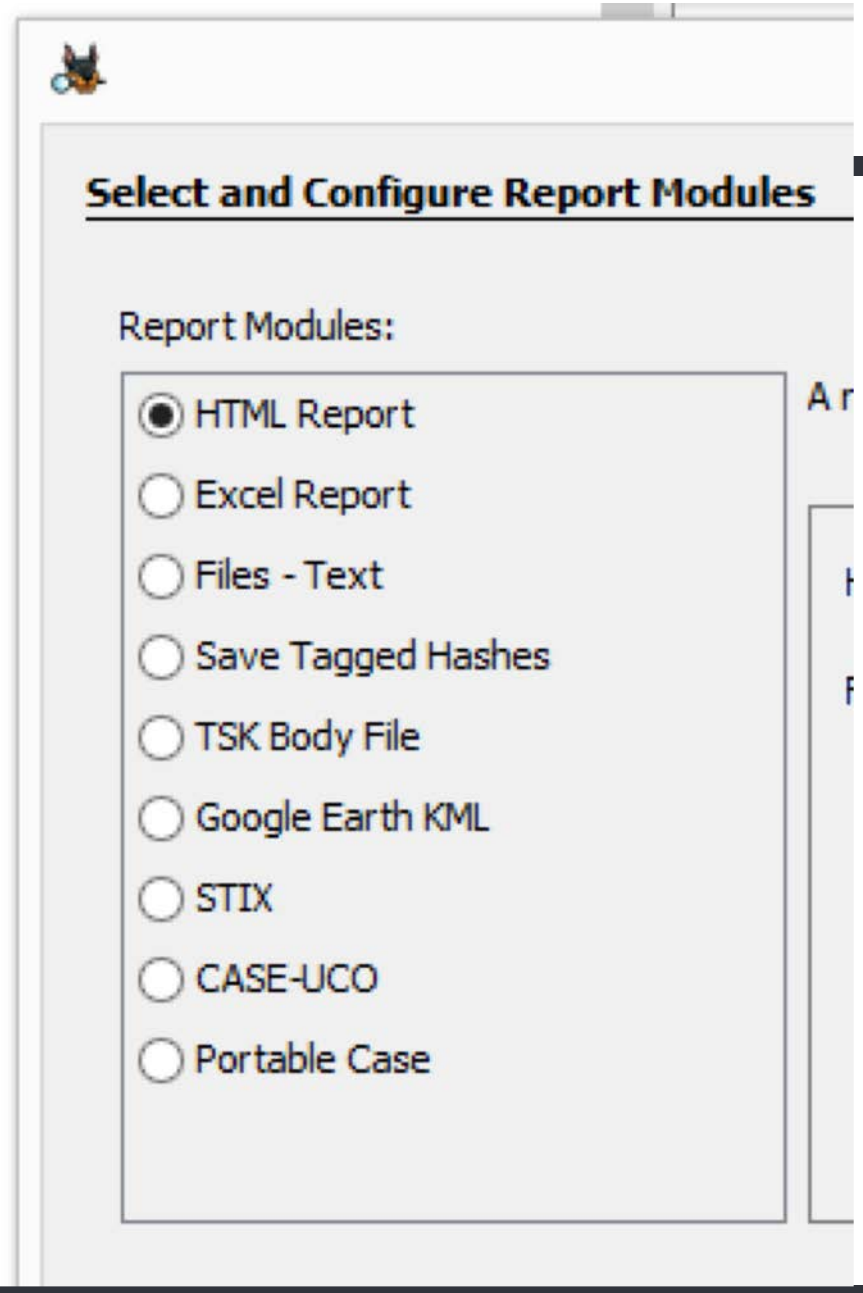
- This feature matches files and other artifacts within a case or with past cases.
  - Finds patterns between devices and cases.
- Updates:
  - Updated the ways the results are shown
  - Can focus on certain file types when matching past cases
  - Can search past cases for specific artifact values (email,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

New Past Case Matching Grouping



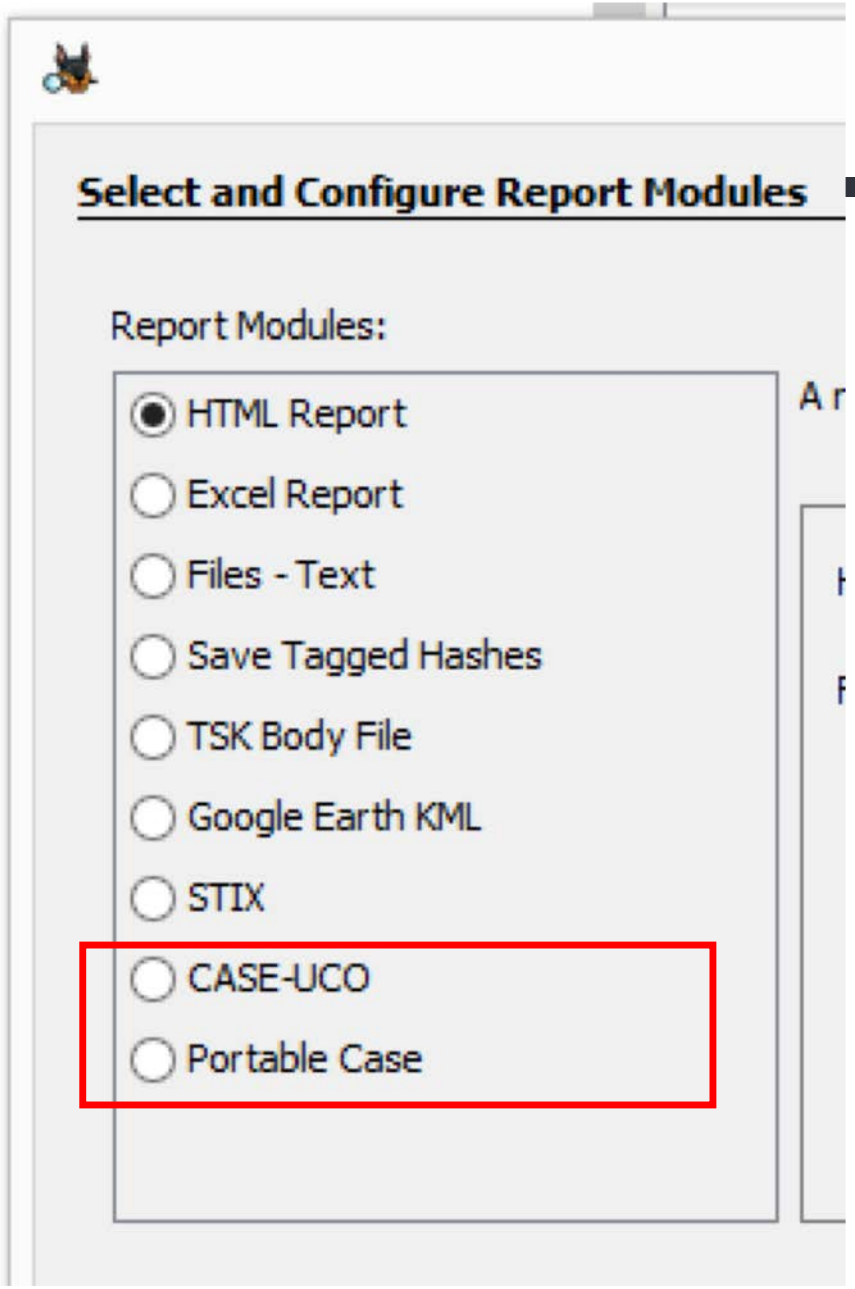
Reporting

- 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.
  - 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:
  - Make Cases and Add Data Sources
  - Run Ingest Modules
  - Generate Reports
- Example:

```
> autopsy64.exe \
    -createCase -caseName="case123" -caseBaseDir="C:\Cases" \
    -addDataSource -dataSourcePath="C:\images\disk.bin" \
    -runIngest -generateReports
```

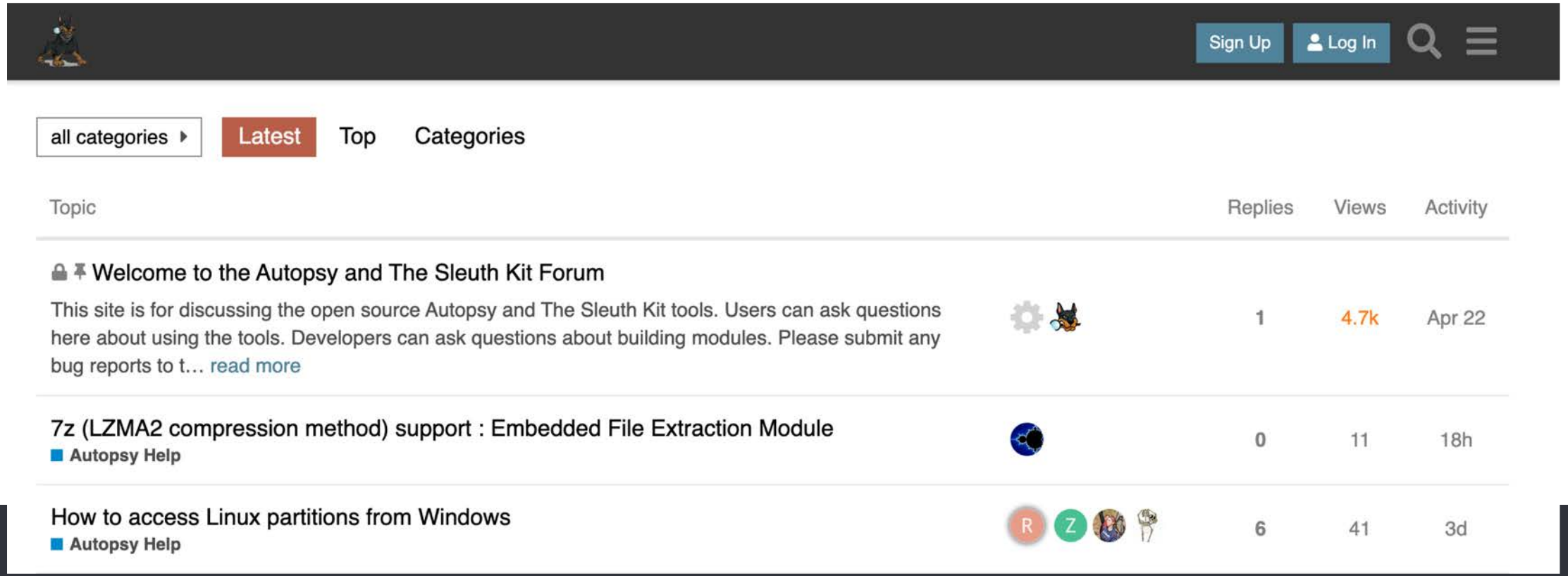
- Requires you to preconfigure what modules to run.

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.
  - 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…)