Autopsy

Before We Get Started

During this class, we will go through the capabilities of Autopsy together

We will use a common case file

But it will take a few minutes to get set up

Let's do that here

Do the following on your Windows RADISHng desktop

Use the File Explorer and go to R:\Share\Labs\Autopsy Lab

Double-click on the 2009 M57-Jean.zip file

Select the Extract All icon on the File ribbon

Extract the files to your Autopsy Base Directory

Use the *Case > New Case* menu item to get the pathname

When it is done, open this case in Autopsy

Earlier Class Session

Original Autopsy

A "sort of" GUI for TSK

Brian Carrier originally created a *"sort of"* GUI that provided a primitive graphical interface for TSK tools

- *Named* **Autopsy Forensic Browser (AFB)**
- *The* **AFB** *interface was originally a web-based interface*
- *Originally ran on most browsers*
  - Natively used TSK-based scripts on Linux and WinXP Service Pack 2 and greater

Original Autopsy

A "sort of" GUI for TSK

The original ***AFB*** was a set of scripts that were run by the web browser

- *The scripts ran*
  - TSK tools
  - Some Linux distro tools
  - Other software
- *This software was used to analyze a drive, partition or file image*

It helped organize a forensic analysis

It was free

Evolution of Autopsy

Eventually, ***AFB*** was rewritten as a native application that would run on Linux, Windows and OS X

Still uses TSK tools, Linux distro tools and other software tools to analyze a drive, partition or file

Continues to be free

Comments About Autopsy

AFB helps organize a forensic analysis

Don't need to know much about TSK and other command line tools

However, in certain situations, such knowledge is useful

Good at timeline analysis

Describes what files were created, modified, accessed and changed in an orderly way

Good at searching and displaying context around search terms in readable format

Rendering is marginal

But 3rd party apps can be configured for better rendering

As new TSK and other free cyber forensics tools become available, they have been selectively integrated into Autopsy

More About Autopsy

Autopsy's Changing Focus

TSK and Autopsy focus on forensic analysis of computer mass storage. E.g.,

Magnetic disks

SSDs

USB drives

SD drives

Slowly, Autopsy has evolved to help forensic analysis of networks, journals, dynamic memory and mobile devices

Other Forensic Software of Note

But there are a Number of Others

EnCase *(Guidance Software → OpenText) [.E01]*

Used to be the most used

Forensic ToolKit (FTK) *(Access Data) [.001]*

Used a lot by the U.S. Federal Government

X-Ways Forensics *(X-Ways Forensics) [.dd]*

WinHex is their hex editor

ProDiscover *(ProDiscover) [.eve]*

ProDiscover Basic version is free

Oxygen Forensics Detective *(Oxygen Forensics)*

Started by focusing on smart phones

Magnet AXIOM software *(Magnet Forensics)*

Started by focusing on smart phones. The newest of these forensic tools

Comments

*All of the above now have suites of **proprietary** tools*

*They are all **good**. They are all **expensive**.*

So What About Autopsy?

Autopsy is based upon integrated command line tools and scripts of

- *TSK + Linux distro tools + other open-source forensic tools*
- *Non-proprietary*
- *Mostly publicly licensed and open source*
- *Not always as up-to-date as the commercial software*
- *Rather slow*
- *Poor rendering*
- *Free*

Autopsy seems to be evolving, albeit slowly

Workflow and Features of *Autopsy*

Autopsy Workflow

Create a Case

A case is a container for one or more data sources

A case must be created before data can be analyzed

Add Data Source(s)

One or more data sources are added to the case.

Data sources include disk images and data files

Analyze with Ingest Modules

Ingest modules operate in the background to analyze the data

Manual Analysis

User navigates the interface, file contents and ingest module results to identify the evidence.

Interesting items can be tagged for later reporting and analysis

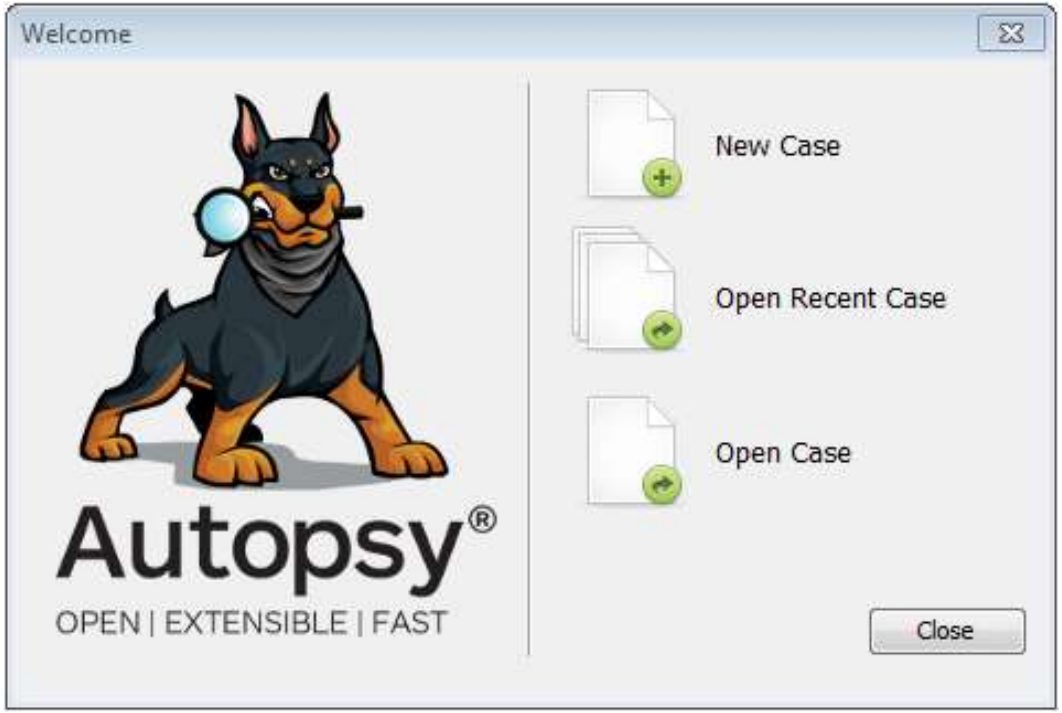
Report Generation

User initiates a final report based on selected tags or results

Autopsy: Creating a Case

Create a Case

Create a case using either the *Case > New Case* menu item or using the splash screen when you start Autopsy

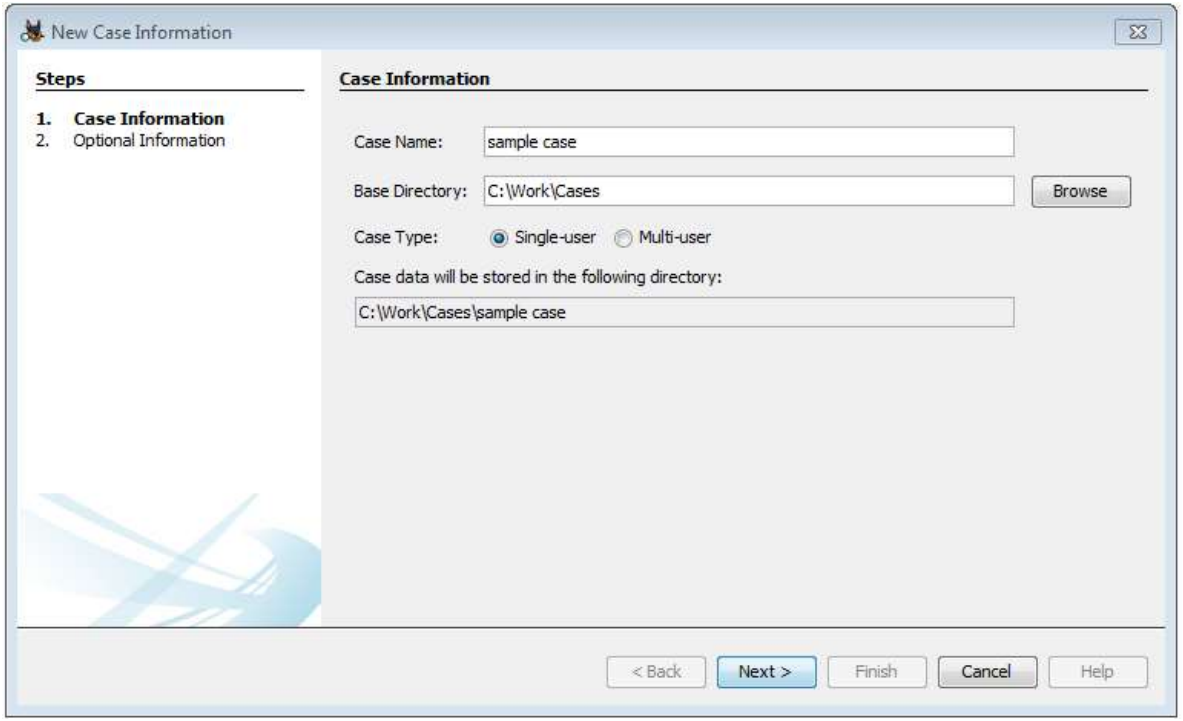


Create a Case

You will now begin the New Case Wizard

Enter a Case Name in the first screen

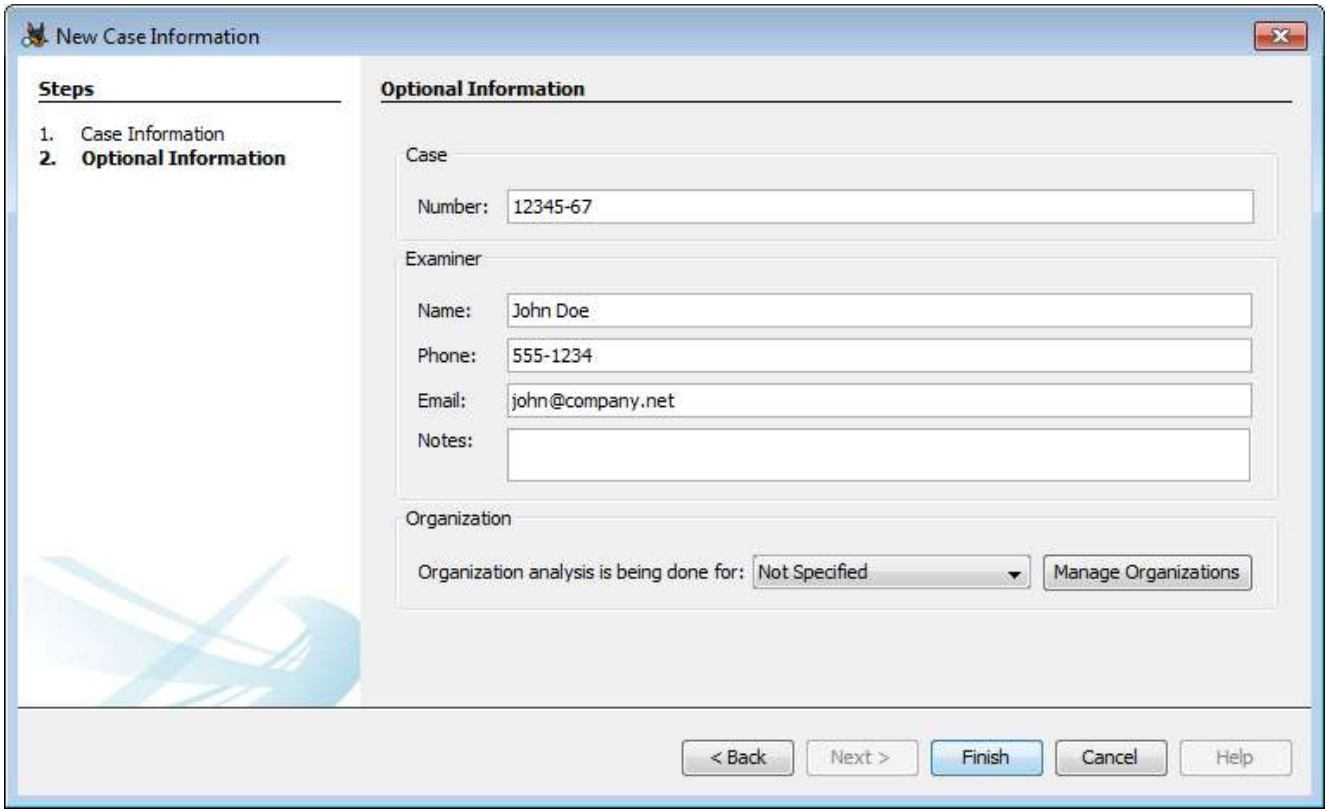
The other information can typically be left to their defaults



Create A Case

Provide a Case Number

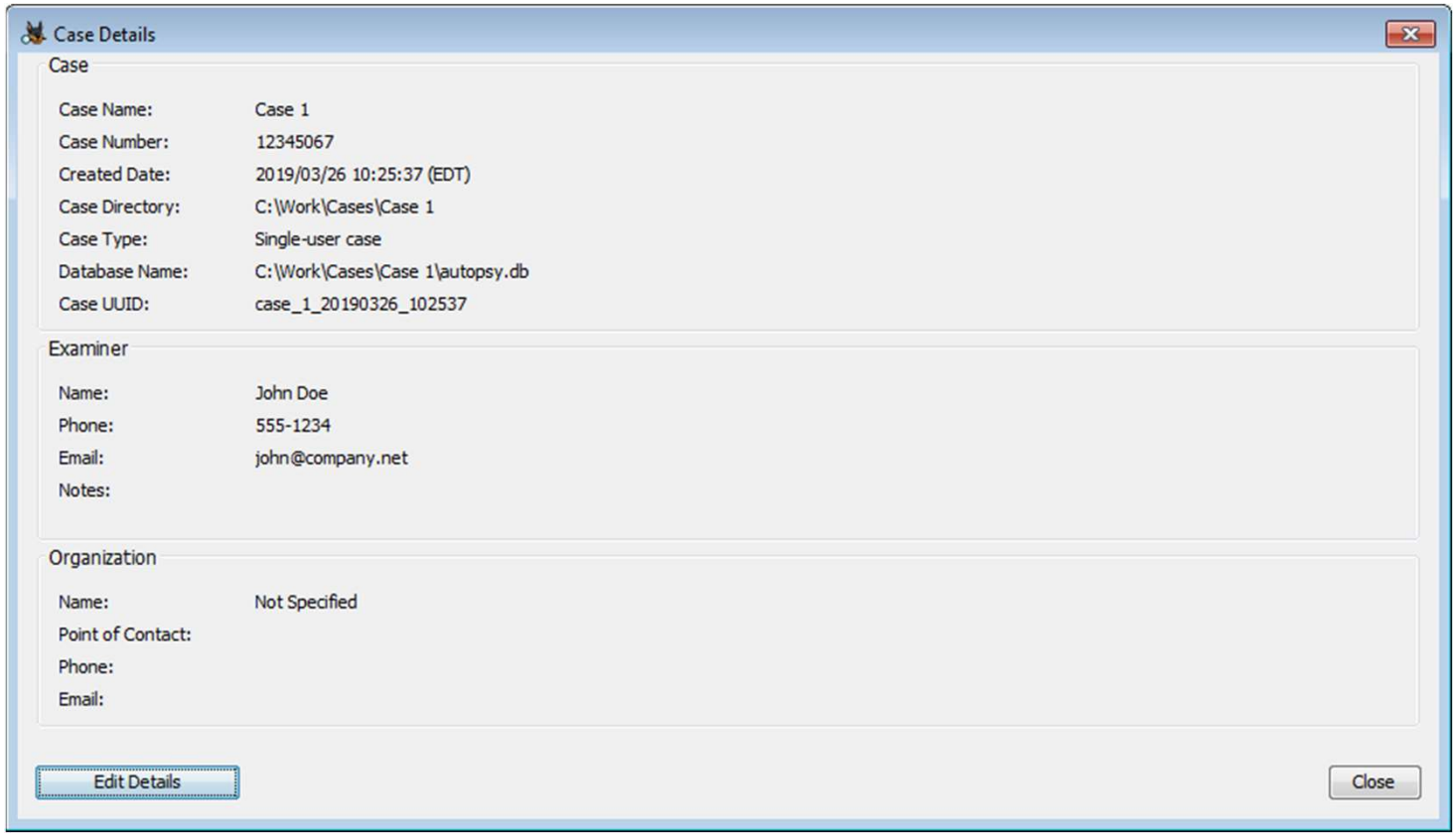
Provide information about yourself (the examiner)



Case Overview

Case Details

You can get the Case Details by using the *Case > Case Details* menu item

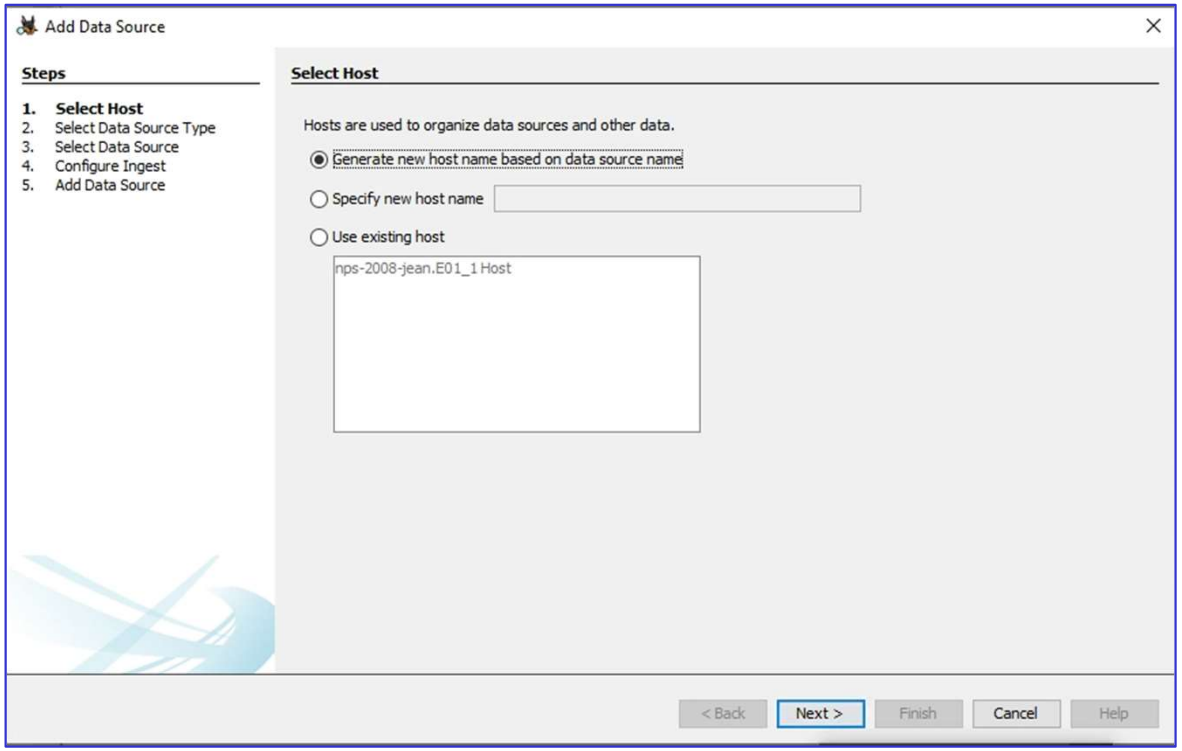


Autopsy: Add Data Source(s)

Adding Data Source(s)

After you create a case, it automatically prompts you to select a host

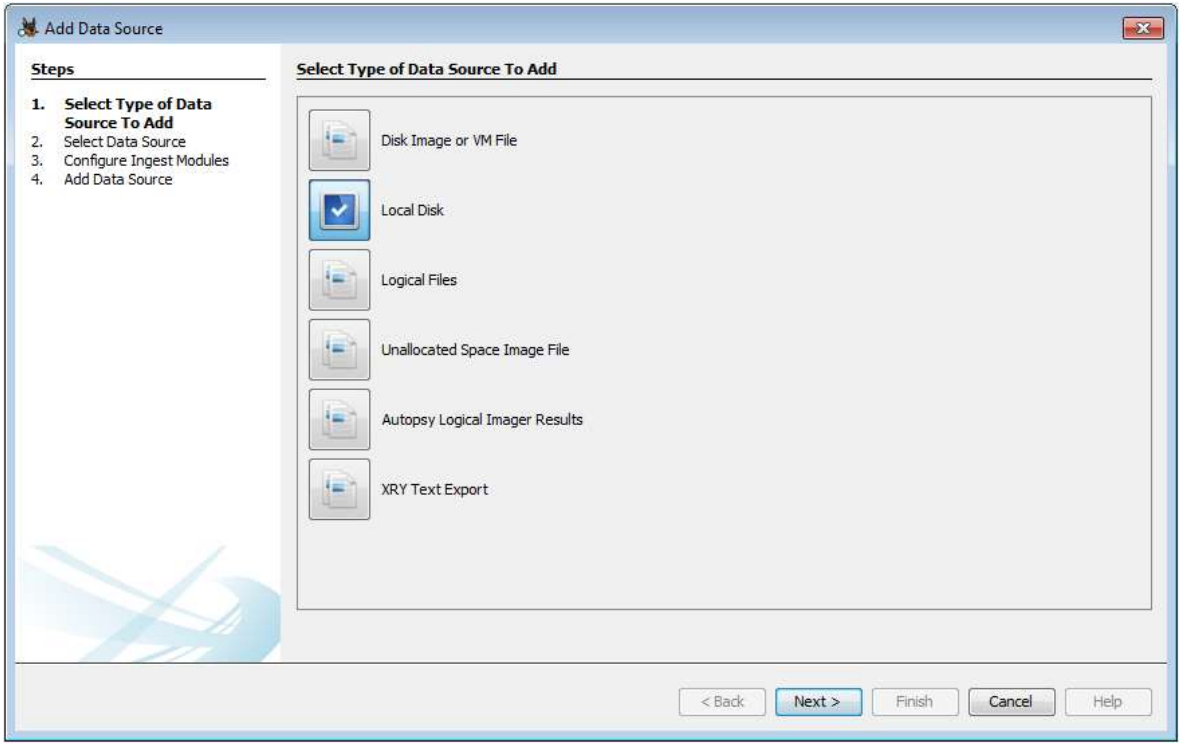
Choose the default option



Adding Data Source(s)

After you create a case, it automatically prompts you to add a data source

You first need to select the type of data source



Adding Data Source(s)

You will then be prompted for the data source

File: Provide file location

Local disk: Select disk

Note that Autopsy supports the following disk formats:

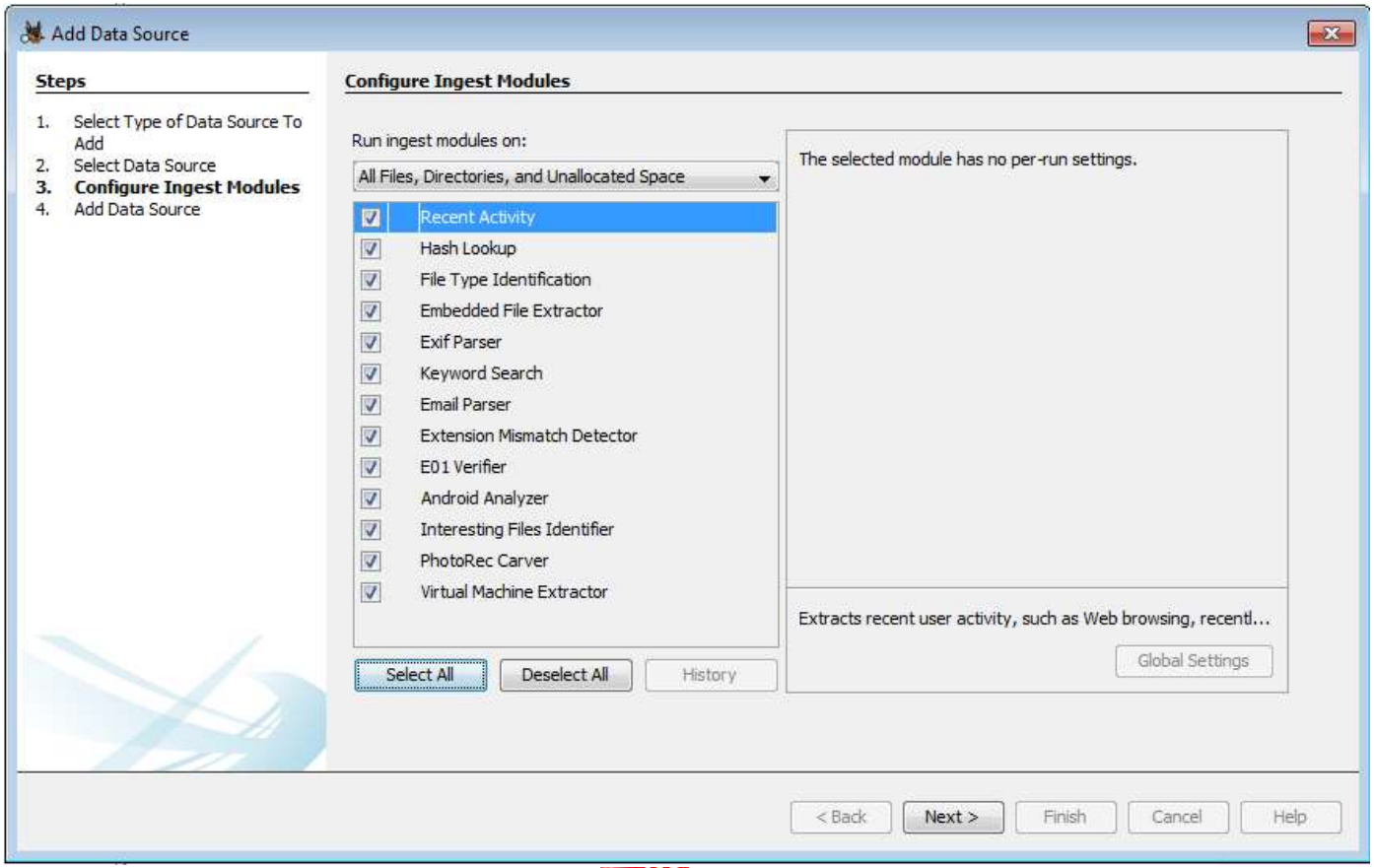
Raw image (single or split)

EnCase (.e01)

Virtual Disk (.vmdk, .vhd)

Adding Data Source(s)

You will then be prompted with a list of ingest modules to enable



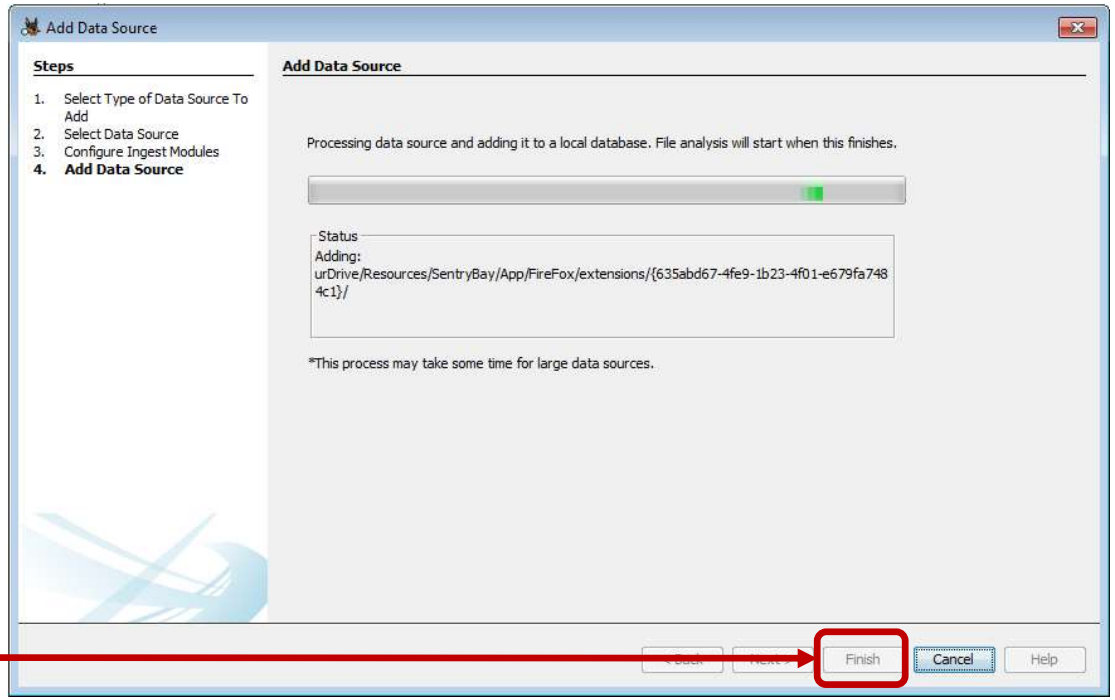
Adding Data Source(s)

Autopsy then

Does a basic examination of the data source

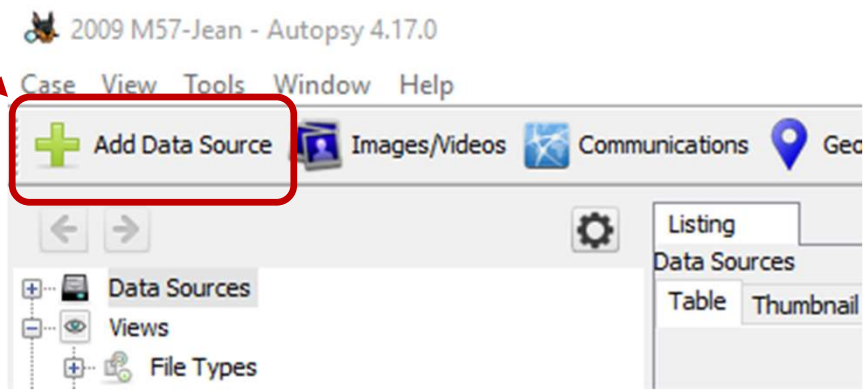
Populates an embedded database with files from the data source

When this is complete, you can continue to the case (by clicking Finish) while the ingest files run in the background



Adding Data Source(s)

You can then add additional data sources by clicking on the *Add Data Source* icon at the top left of the Autopsy Display



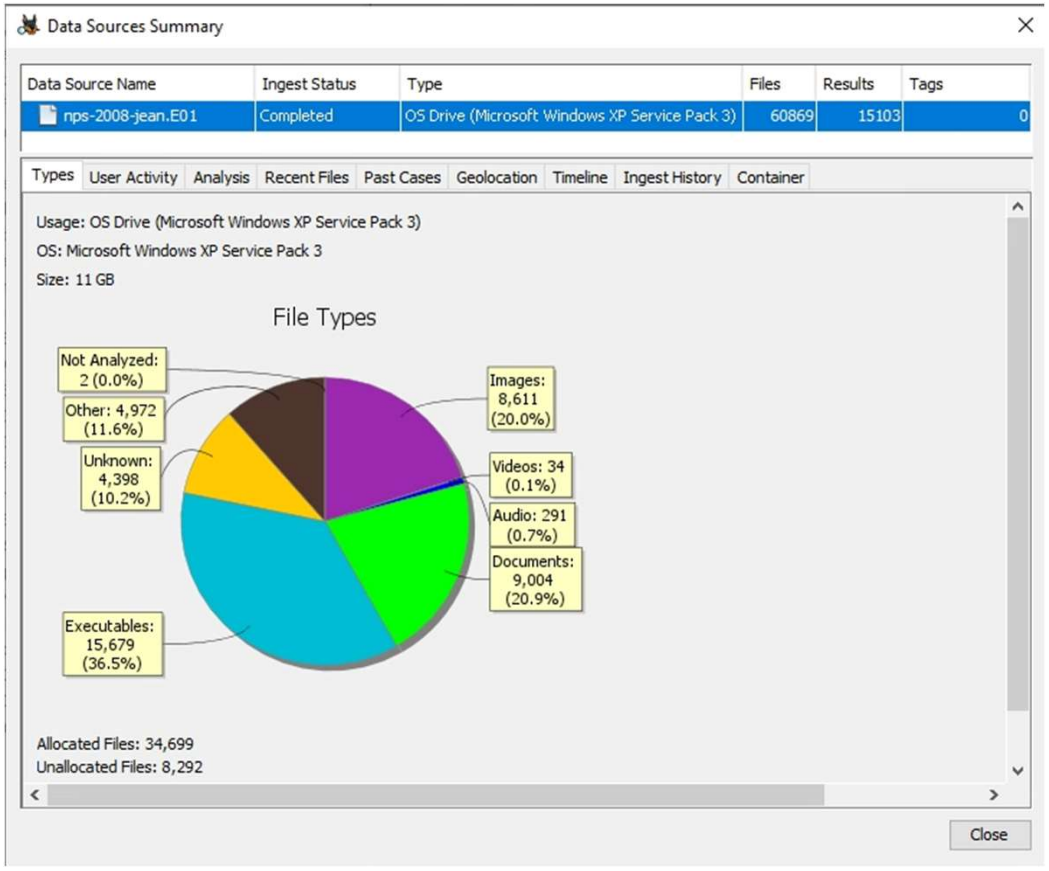
Adding a Data Source

Data Source Summary

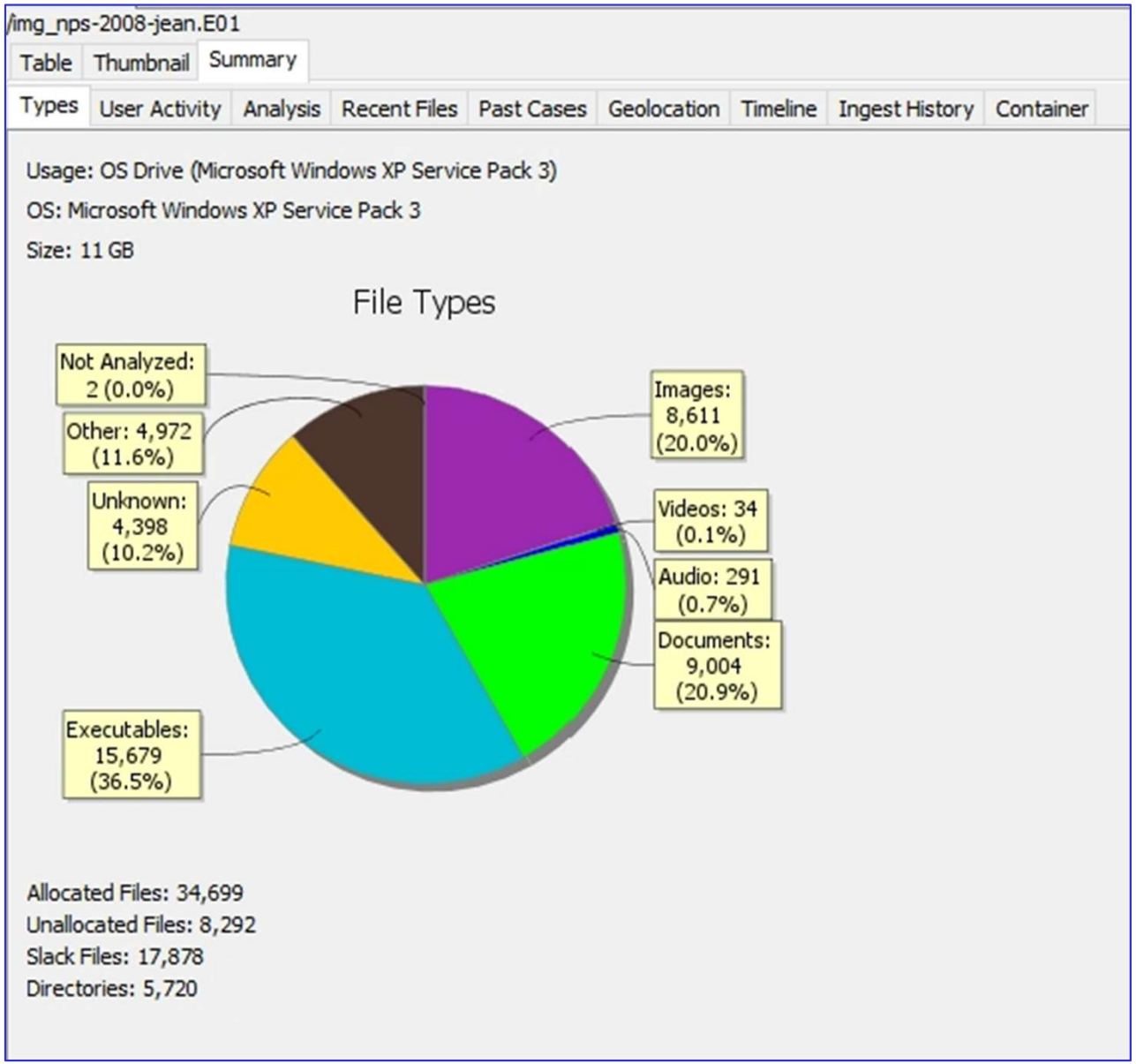
Once the data sources have been added and the ingest modules have completed process, you can get a nice summary of the data used in your case by selecting the *Case > Data Source Summary* menu item

Another way: Select data source in tree viewer and click on *Summary* tab.

Note that the data is summarized by types (available by using the different tabs). The view starts with the *Types* tab



Data Source Summary
Types Tab

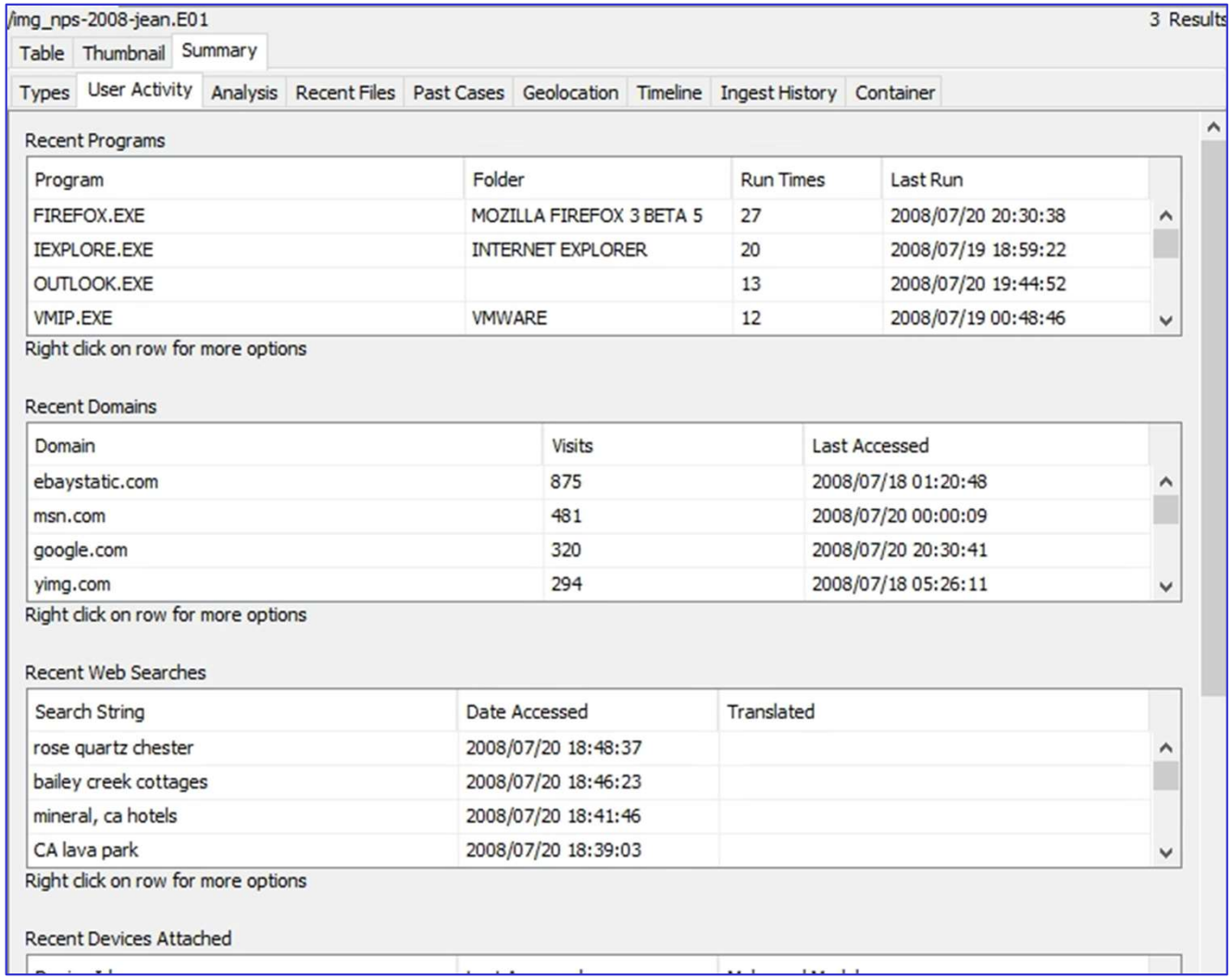


The *Types* tab shows counts of different file types found in the data source.

Data Source Summary
User Activity Tab

The *User Activity* tab shows the most recent results found in the data source.

You can right click on a row to navigate directly to the corresponding result.



Data Source Summary
Recent Files

The *Recent Files* tab shows information on the most recent files open and downloaded.

You can right click on a row to navigate directly to the corresponding result.

/img_nps-2008-jean.E01 — 3 Results

Table | Thumbnail | Summary

Types | User Activity | Analysis | Recent Files | Past Cases | Geolocation | Timeline | Ingest History | Container

Recent Programs

Program	Folder	Run Times	Last Run
FIREFOX.EXE	MOZILLA FIREFOX 3 BETA 5	27	2008/07/20 20:30:38
IEXPLORE.EXE	INTERNET EXPLORER	20	2008/07/19 18:59:22
OUTLOOK.EXE		13	2008/07/20 19:44:52
VMIP.EXE	VMWARE	12	2008/07/19 00:48:46

Right click on row for more options

Recent Domains

Domain	Visits	Last Accessed
ebaystatic.com	875	2008/07/18 01:20:48
msn.com	481	2008/07/20 00:00:09
google.com	320	2008/07/20 20:30:41
yimg.com	294	2008/07/18 05:26:11

Right click on row for more options

Recent Web Searches

Search String	Date Accessed	Translated
rose quartz chester	2008/07/20 18:48:37	
bailey creek cottages	2008/07/20 18:46:23	
mineral, ca hotels	2008/07/20 18:41:46	
CA lava park	2008/07/20 18:39:03	

Right click on row for more options

Recent Devices Attached

Data Source Summary
Analysis & Geolocation

Types | User Activity | Analysis | Recent Files | Past Cases | Geolocation | Timeline | Ingest History | Container | Export

Hashset Hits

Name	Count
Birds	13
Cats	12
bad_stuff	8

Keyword Hits

Name	Count
bomb	189

Interesting Item Hits

Name	Count
No data exists.	

The *Analysis* tab shows the sets with the most results from the *Hash Lookup*, *Keyword Search* and *Interesting Files Identifier* Modules

The *Geolocation* tab uses the coordinates from geolocation results to find the nearest city for each and displays the most recent cities and most common cities.

Types | User Activity | Analysis | Recent Files | Past Cases | Geolocation | Timeline | Ingest History | Container | Export

Recent Cities from Geolocation Results

Closest City	Count
Boston, Massachusetts; United States	7
New York, New York; United States	2
Washington, District of Columbia; United States	1

Locations further than 150km from a city will be listed as 'Unknown'

View in Map

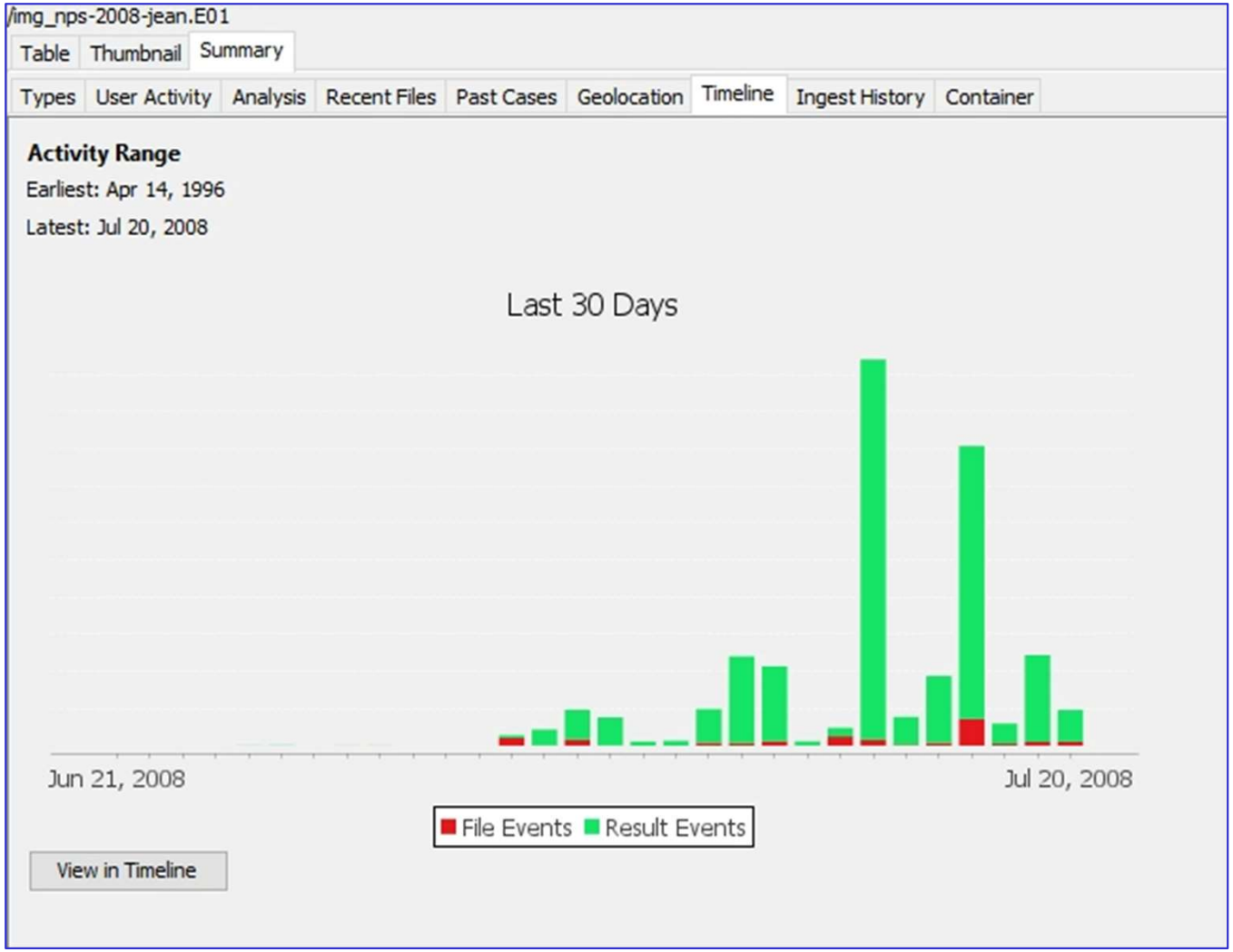
Most Common Cities from Geolocation Results

Closest City	Count
Boston, Massachusetts; United States	7
New York, New York; United States	2
East Los Angeles, California; United States	1
Washington, District of Columbia; United States	1

Locations further than 150km from a city will be listed as 'Unknown'

View in Map

Data Source Summary
Timeline

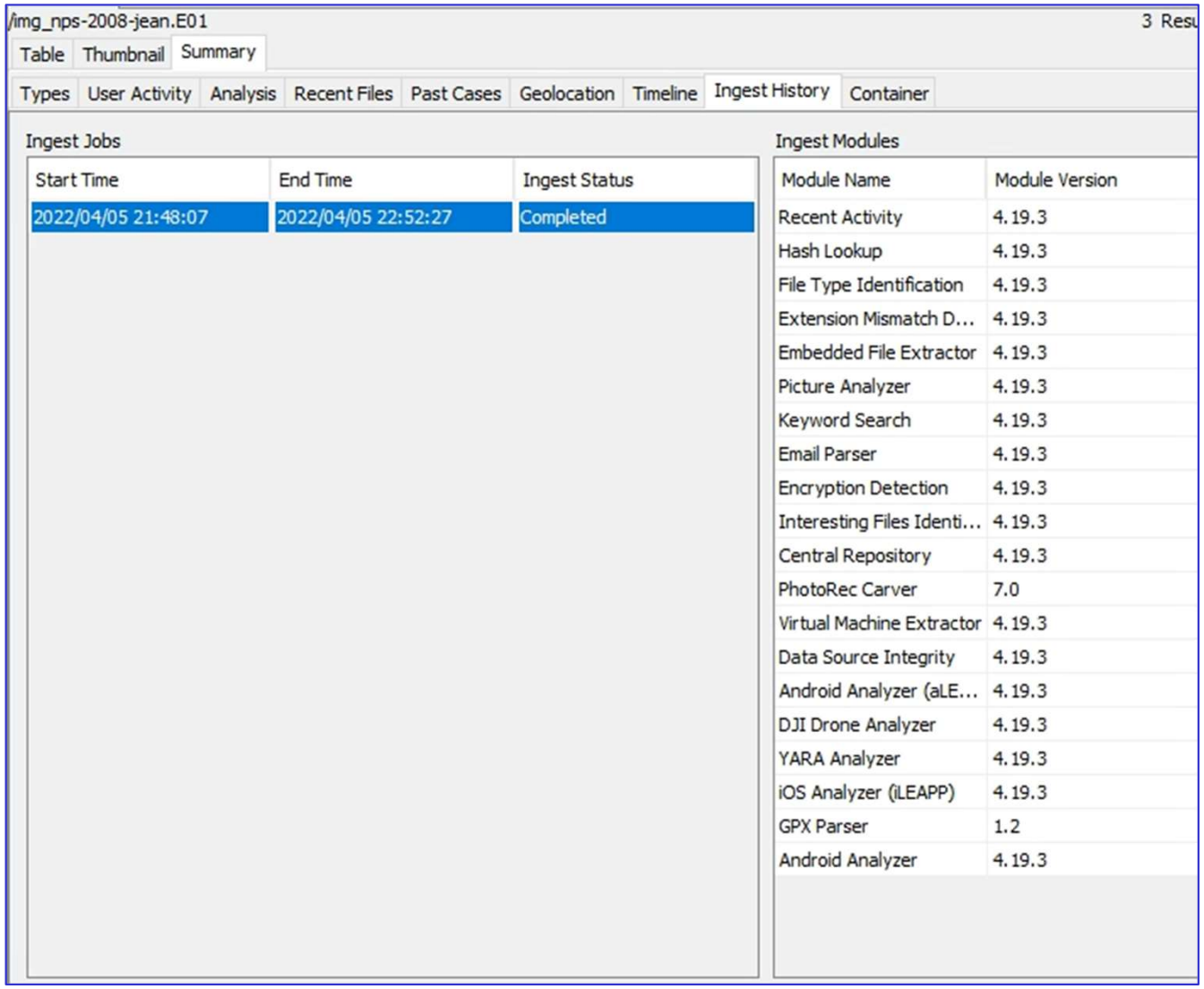


The *Timeline* tab shows a simplified version of the Timeline Viewer.

It will show events for the last 30 days of activity and give the first and last dates of activity.

Data Source Summary
Ingest History

The *Ingest History* tab shows which ingest modules have been run on the data source and the version of each module.



Autopsy: Analyzing with Ingest Modules

Autopsy's Plug-in Architecture

Autopsy has a plug-in architecture that can extend its functionality

"Ingest modules" can be written by the Autopsy team or 3rd party individuals

Some modules are included with Autopsy installation

But several others have been developed. Some references:

https://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules

https://github.com/CarlosLannister/awesome-autopsy-plugins

Ingest Modules

Ingest modules analyze data in a data source

- *They parse the file contents*
- *They do the analysis*

These plug-ins typically run in the background with a status bar on the lower left showing their progress

Examples of ingest modules:

- *Keyword searching*
- *Web artifact extraction*
- *Email parser*

Ingest Modules

They can be executed in one of two ways:

Immediately after you add a data source

By right-clicking on a data source from the tree in the main interface and choosing "Run Ingest Modules"

Ingest Modules

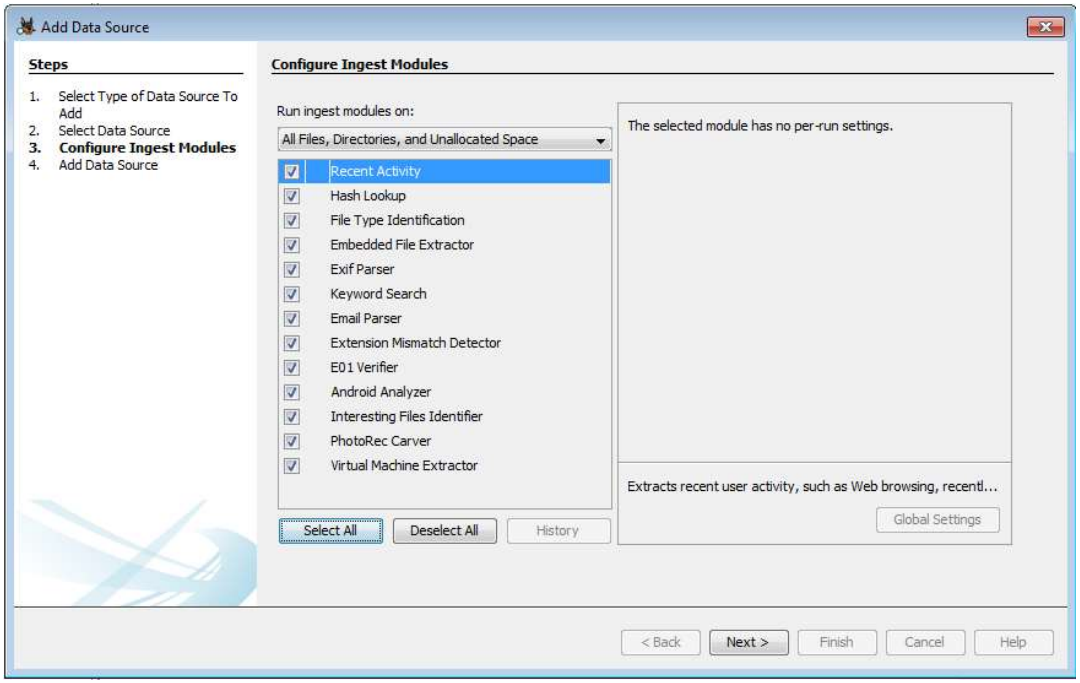
Here is the Ingest Module window that will be displayed using either the two methods described in the last slide

Note that the middle panel allows you to choose which ingest modules to run

Note that the right panel provides

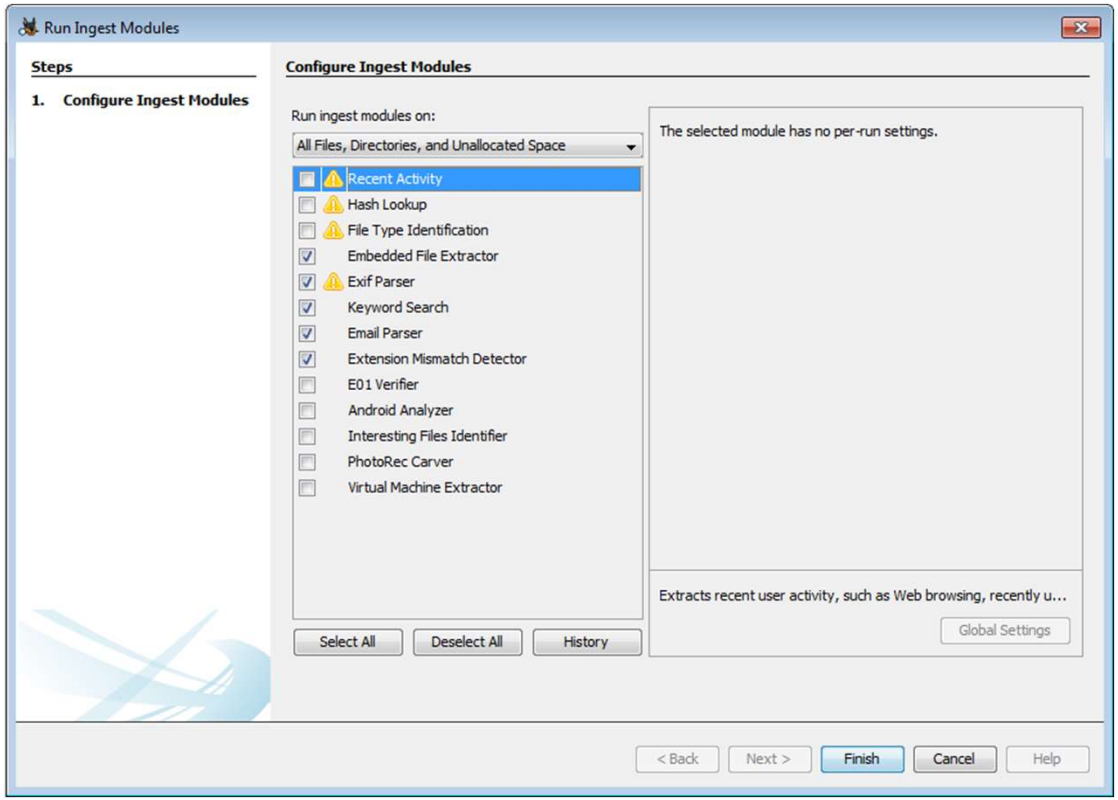
A description of the ingest module

The ability to configure the module (when available)



Ingest Module Status

You can tell if an ingest module has already been run for a particular data source if there is a triangular yellow icon with an exclamation point next to the module



Get Ingest Activity

Use the *Help > Get Ingest Progress Snapshot* menu item to get the current status as shown below:

Ingest Progress Snapshot

Thread ID	Activity	Data Source	File	Start Time	Elapsed Time (...	Job ID
1	IDLE			Fri Jun 03 09:58:04 EDT...	0:00:19.081	0
2	Embedded File Extractor	xp-sp3-v4.001	698E6d01	Fri Jun 03 09:58:22 EDT...	0:00:00.453	3
3	File Type Identification	xp-sp3-v4.001	A3	Fri Jun 03 09:58:23 EDT...	0:00:00.157	3

Job ID	Data Source	Start	Num Processed	Files/Sec	In Progress	Files Queued	Dir Queued	Root Queued	DS Queued
3	xp-sp3-v4.001	09:57:52	786	26.2	50	1	22	25	0

Module	Duration
Embedded File Extractor	0:00:27.256 (47%)
File Type Identification	0:00:12.817 (22%)
Hash Lookup	0:00:10.594 (18%)
Keyword Search	0:00:05.765 (9%)
Exif Parser	0:00:00.845 (1%)

Refresh Close

Manual Analysis

Autopsy Display

The Autopsy display is partitioned into 3 panels

Tree Viewer

- Shows sources of data
- Shows file structure of physical memory and file systems

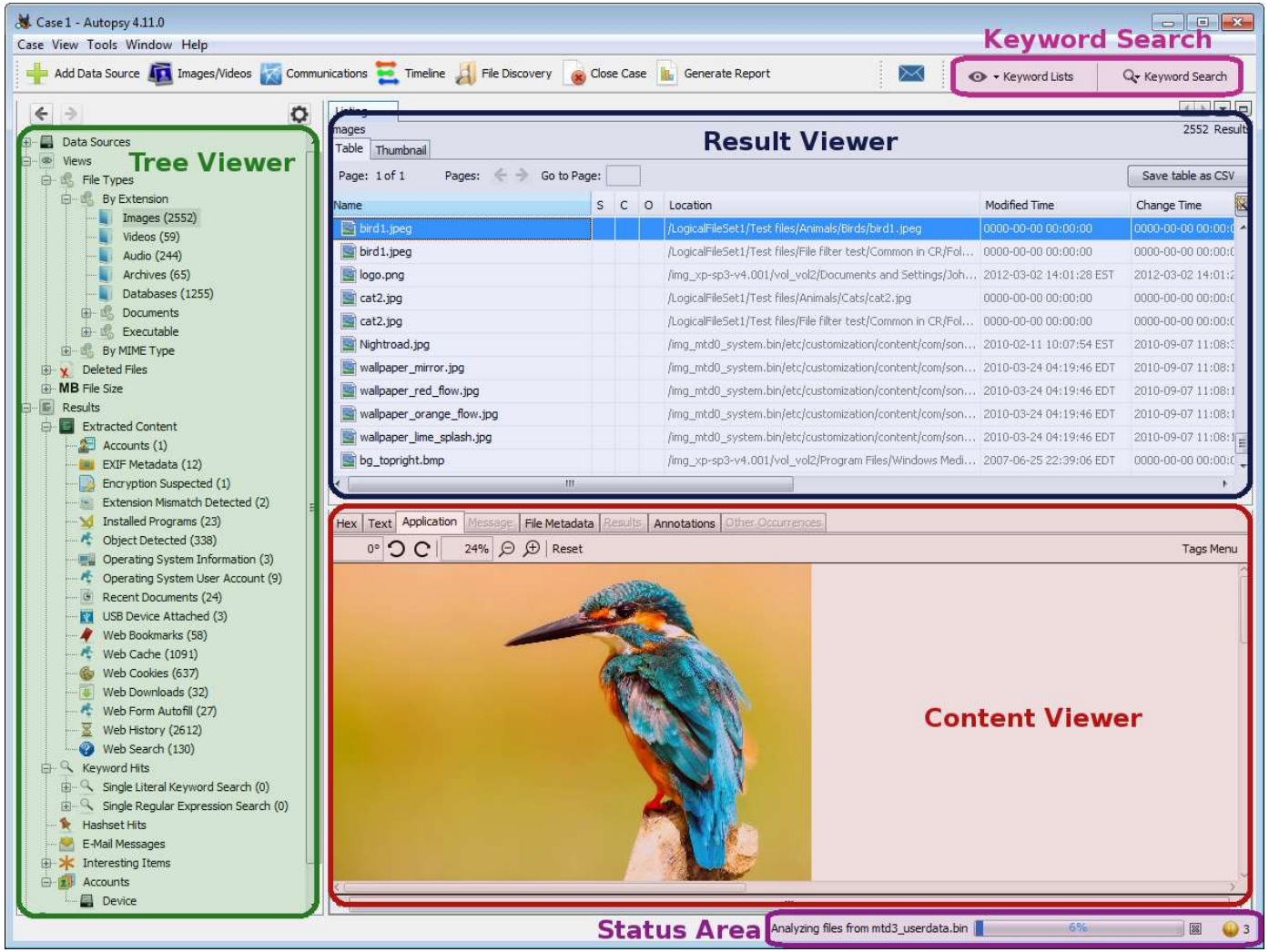
Result Viewer

- Shows details of whatever is highlighted in the left panel

Content Viewer

- Shows details of whatever is highlighted in the upper right panel
- Can use tabs to show various details

Autopsy Display



Manual Analysis: Tree Viewer

Use the tree viewer to browse the files in the data source(s) and find saved results from the ingest modules

The tree has five main areas:

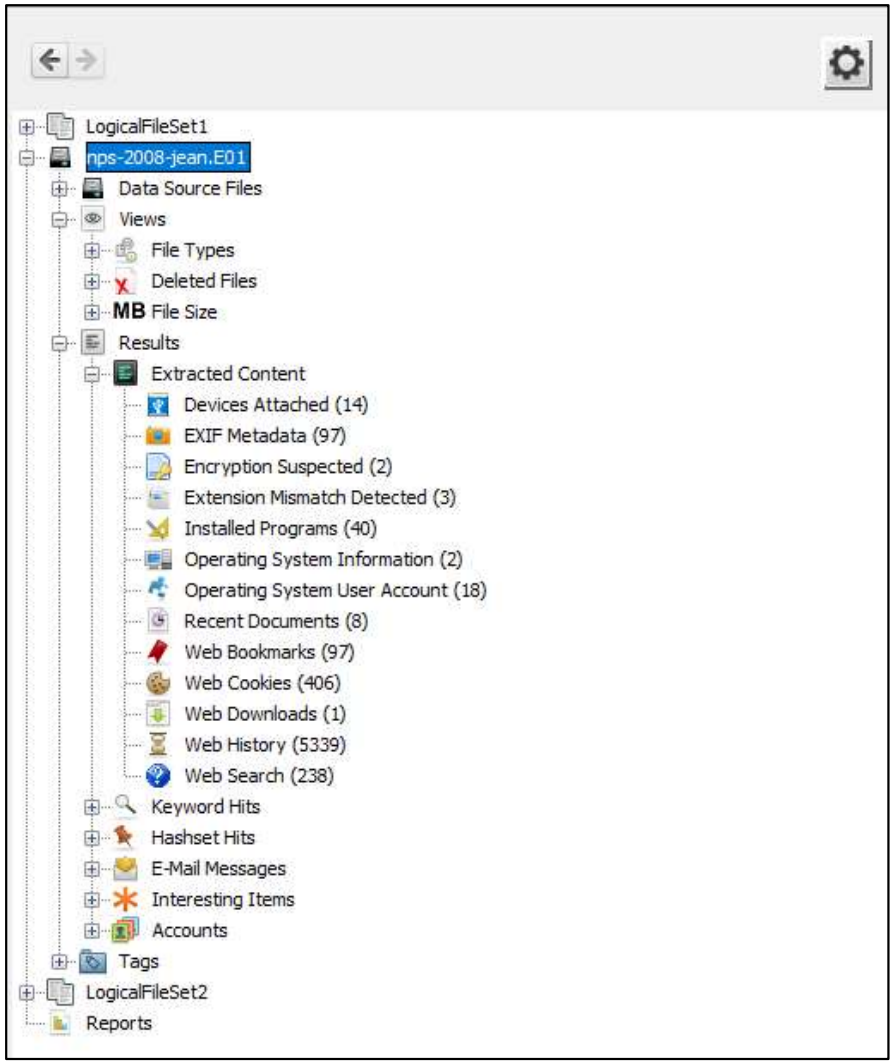
Data Sources

Views

Results

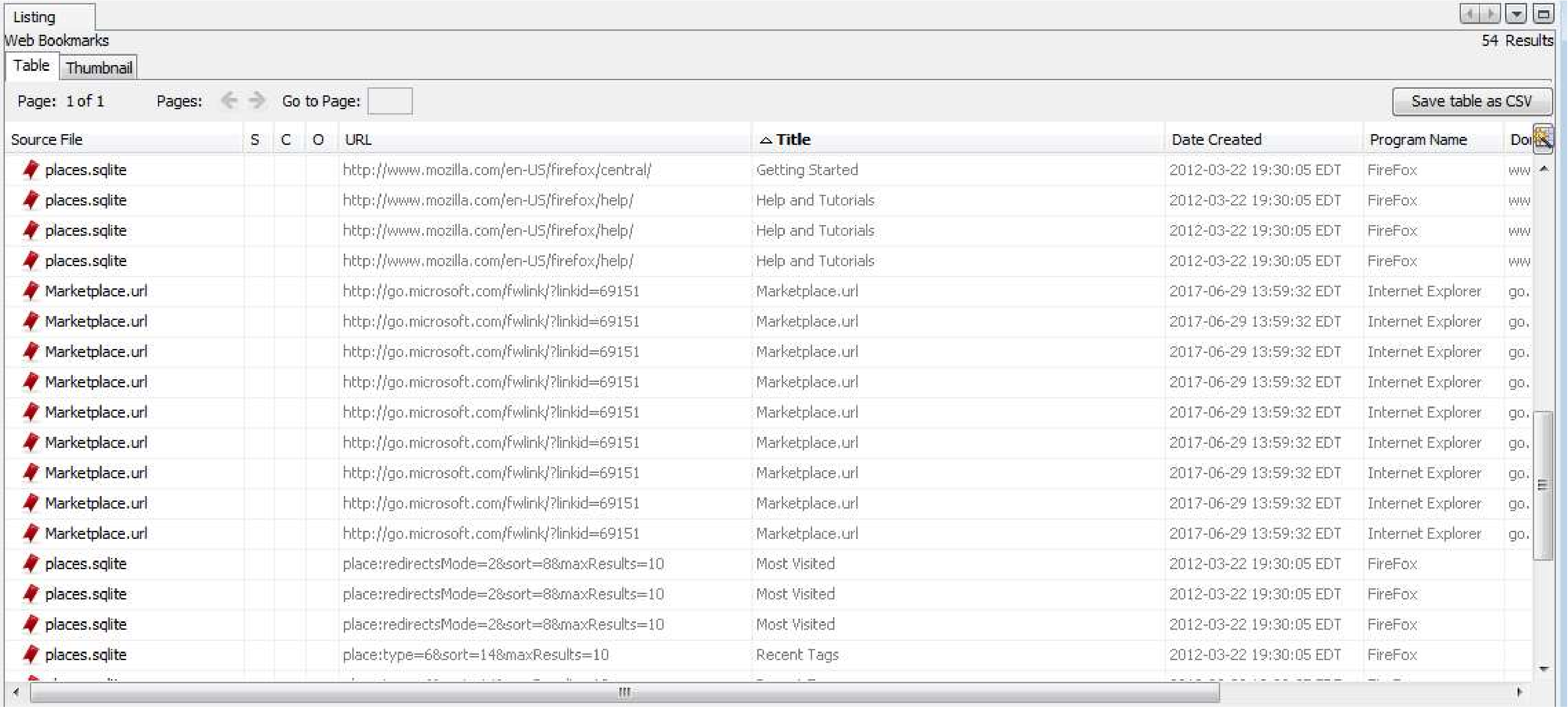
Tags

Reports



Manual Analysis: Result Viewer

The Result Viewer shows the contents of what was selected in the Tree Viewer



Source File	S	C	O	URL	Title	Date Created	Program Name	Do
places.sqlite				http://www.mozilla.com/en-US/firefox/central/	Getting Started	2012-03-22 19:30:05 EDT	FireFox	ww
places.sqlite				http://www.mozilla.com/en-US/firefox/help/	Help and Tutorials	2012-03-22 19:30:05 EDT	FireFox	ww
places.sqlite				http://www.mozilla.com/en-US/firefox/help/	Help and Tutorials	2012-03-22 19:30:05 EDT	FireFox	ww
places.sqlite				http://www.mozilla.com/en-US/firefox/help/	Help and Tutorials	2012-03-22 19:30:05 EDT	FireFox	ww
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
Marketplace.url				http://go.microsoft.com/fwlink/?linkid=69151	Marketplace.url	2017-06-29 13:59:32 EDT	Internet Explorer	go.
places.sqlite				place:redirectsMode=2&sort=8&maxResults=10	Most Visited	2012-03-22 19:30:05 EDT	FireFox	
places.sqlite				place:redirectsMode=2&sort=8&maxResults=10	Most Visited	2012-03-22 19:30:05 EDT	FireFox	
places.sqlite				place:redirectsMode=2&sort=8&maxResults=10	Most Visited	2012-03-22 19:30:05 EDT	FireFox	
places.sqlite				place:type=6&sort=14&maxResults=10	Recent Tags	2012-03-22 19:30:05 EDT	FireFox	

Manual Analysis: SCO Columns

The first three columns after a file name in the table viewer are named “S”, “C”, and “O”

- *(S)core column – indicates whether the item is interesting or notable*
  - Red icon if the hash for this file has been tagged as notable
  - Yellow icon is the file has an interesting item match or been tagged with a non-notable tag
- *(C)omment column – indicates whether the item has a comment in the Central Repository*
- *(O)ther Occurrences column – indicates how many data sources in the Central Repository contain this item*

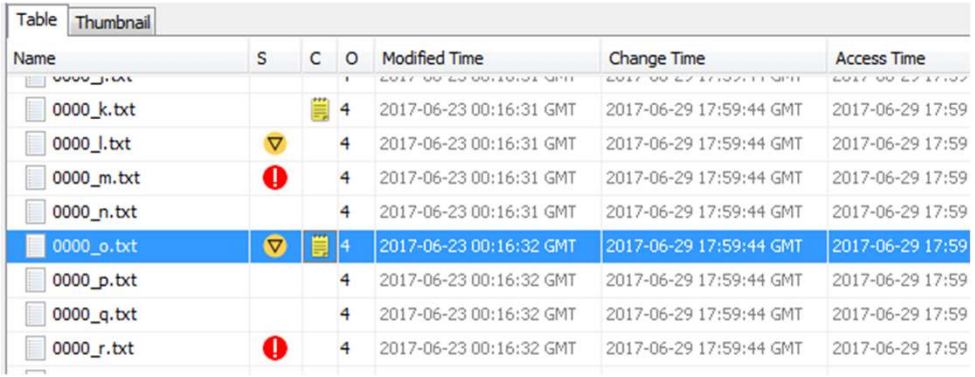


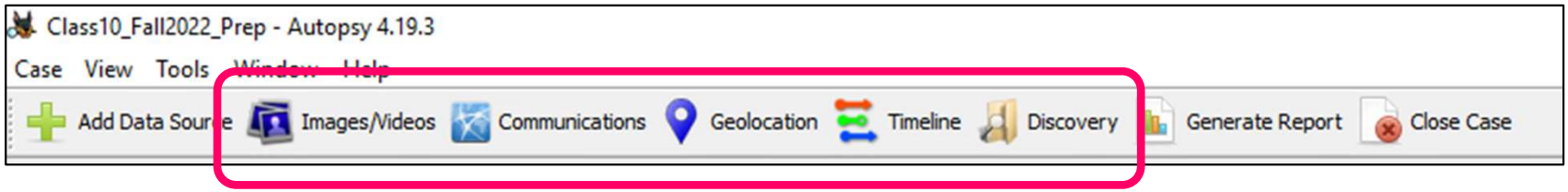
Table | Thumbnail

Name	S	C	O	Modified Time	Change Time	Access Time
0000_k.txt			4	2017-06-23 00:16:31 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_l.txt			4	2017-06-23 00:16:31 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_m.txt			4	2017-06-23 00:16:31 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_n.txt			4	2017-06-23 00:16:31 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_o.txt			4	2017-06-23 00:16:32 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_p.txt			4	2017-06-23 00:16:32 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_q.txt			4	2017-06-23 00:16:32 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59
0000_r.txt			4	2017-06-23 00:16:32 GMT	2017-06-29 17:59:44 GMT	2017-06-29 17:59

Specialized Viewers

Specialized Viewers

Autopsy also has a number of specialized viewers available via the top toolbar



Image/Videos Gallery Module

Communications Visualization Tool

Geolocation

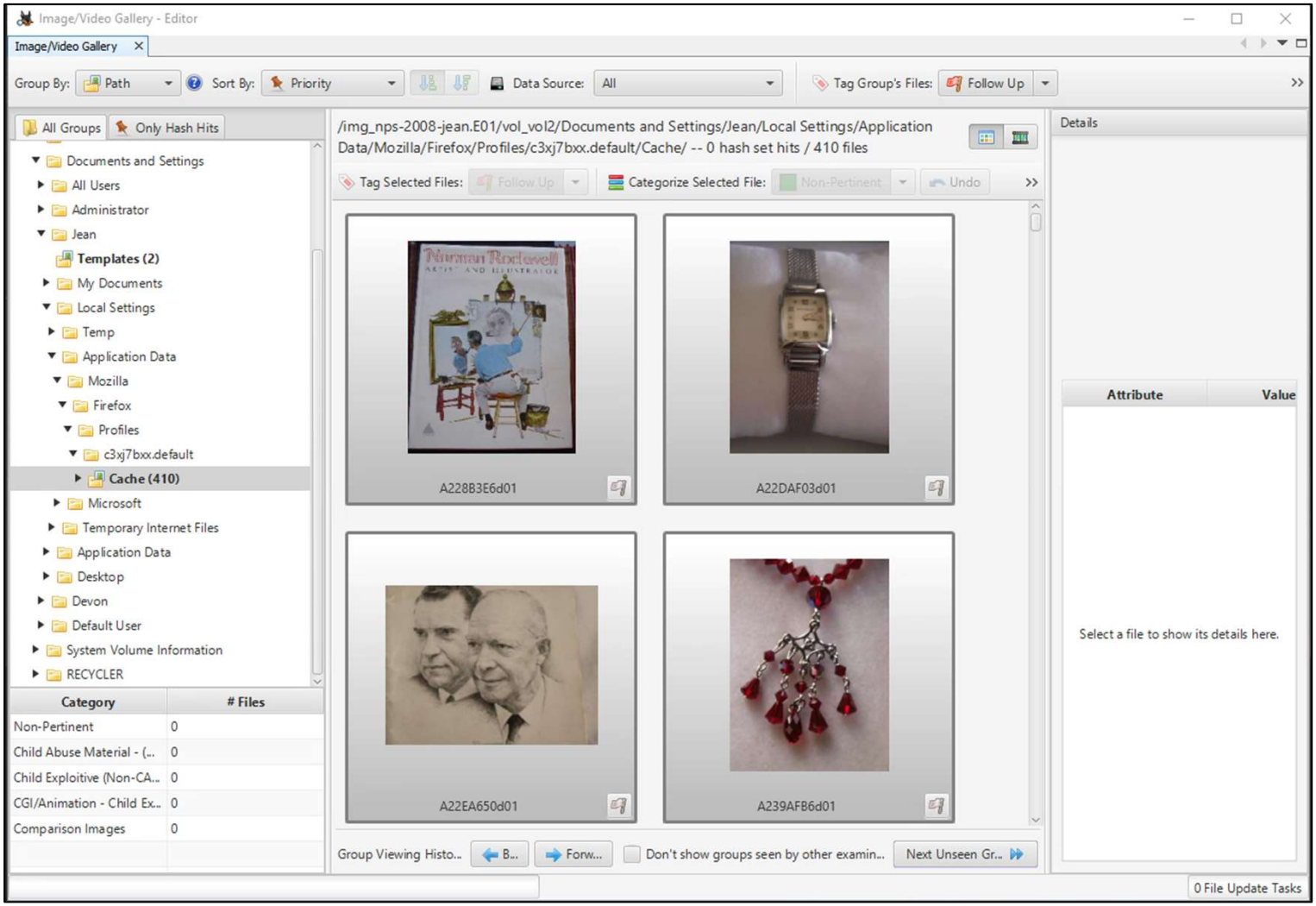
Timeline

Discovery

Image/Video Gallery Module

- This viewer has been designed to aid in investigations involving images and videos
- It offers the following features beyond the normal thumbnail viewing available in other parts of Autopsy
  - *Groups images by folder or other attributes*
    - This helps the investigator break the large set of images into smaller groups
    - It helps focus the investigation on areas with images of interest
  - *Allows investigator to start viewing images immediately upon adding them to the case*
    - You do not need to wait until the entire image is processed by the ingest modules

Image/Video Gallery



Communications Visualization Tool

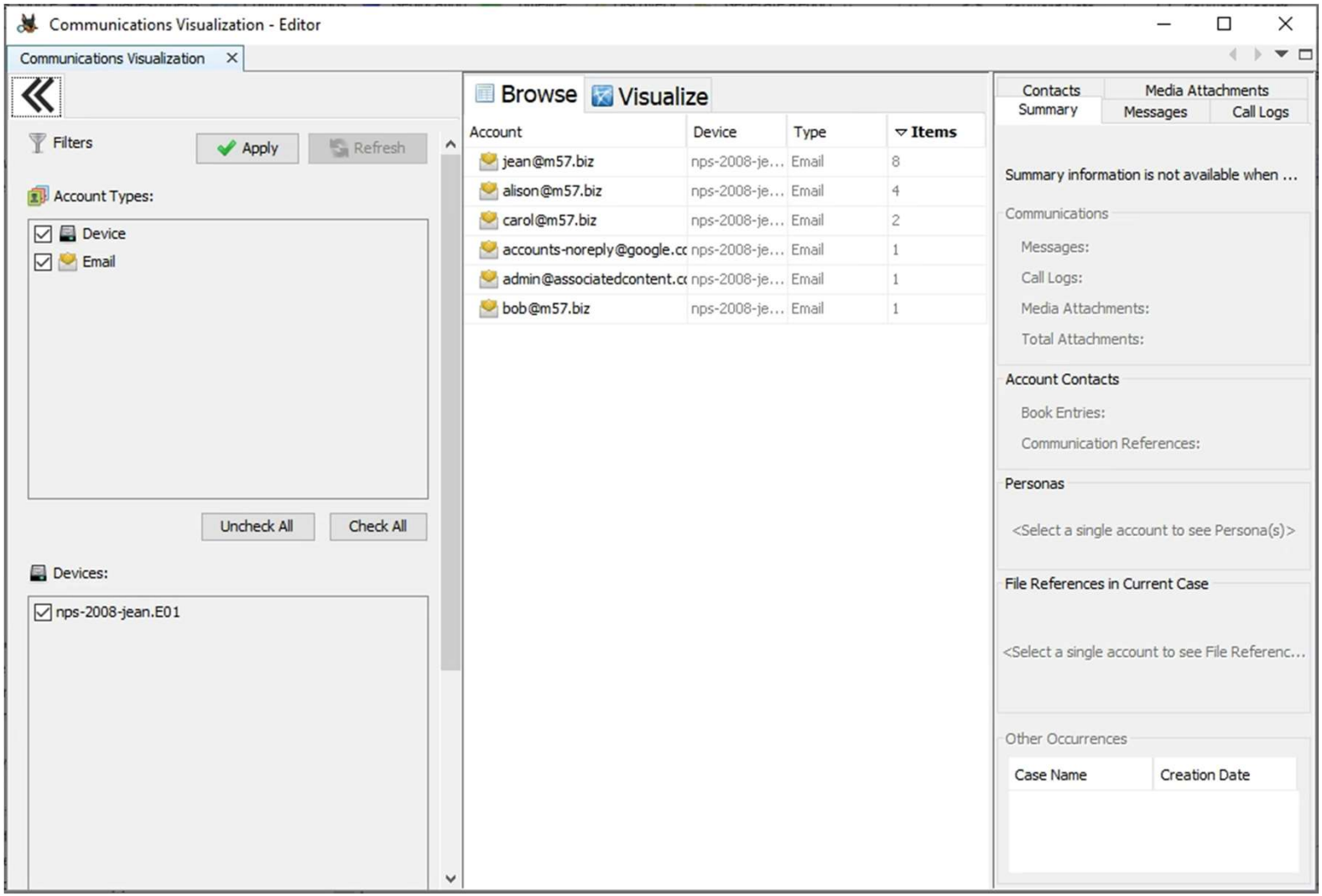
Gives consolidated view of all communication events for the case

Allows an analyst to quickly view communications data such as:

Most commonly used accounts

Communications within a specific time frame

Communication Visualization Tool



Communication Visualization Tool

From left column, choose:

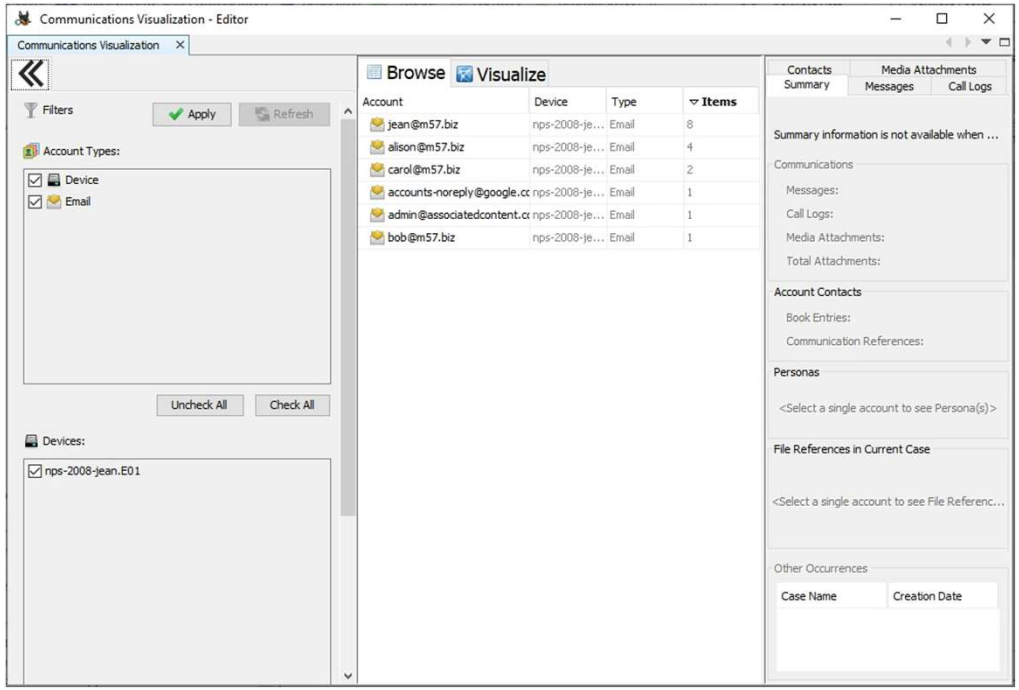
- *Which devices to display*
- *Which types of data to display*
- *A time range (optionally)*

Middle column displays:

- *Each account and its*
  - Device
  - Type
  - Number of associated messages
- *Sorted in descended order of frequency*

Right column

- *Details of results selected in middle column*



Communication Visualizer

Right Column Details

Some Key Tabs:

Summary

- Displays counts of how many times the account has appear in different interactions in the top section
- In the middle it displays the files the account was found in
- At the bottom are cases where this account has been discovered

Messages

- Displays any messages or call logs associated with he account.
- Click on *All Messages* at the bottom to show specifics about messages

Media Attachments

- Shows thumbnails of any media files in messages for that account

Communication Visualizer

Visualizer

The Visualizer tab in the middle manel will show a graph of one or more accounts selected in the Browse tab.

To start, right click on the first account you want to view (in the Browse tab). There are two options

Add selected Account to Visualization

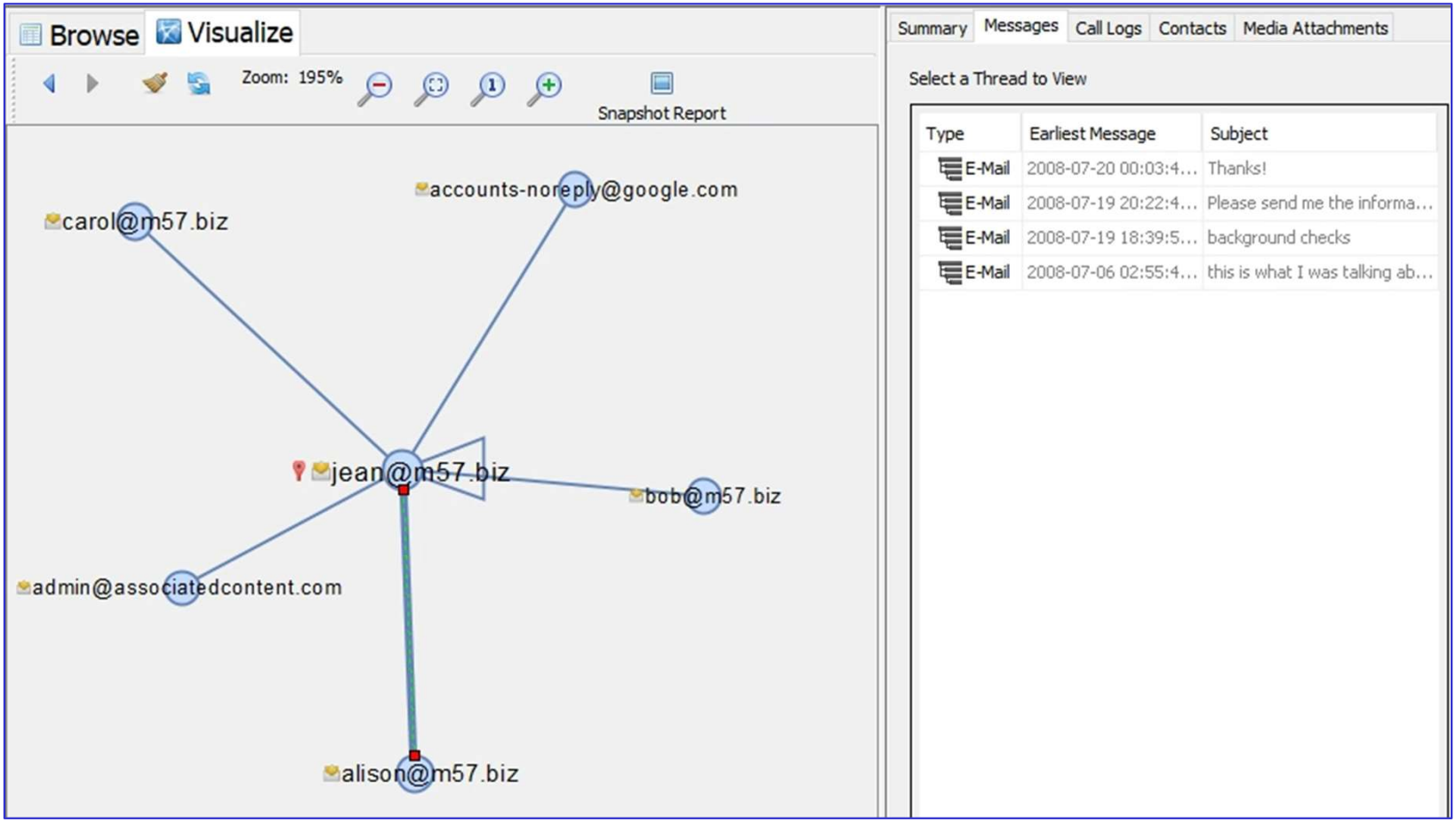
Add this account and its connections to the graph

Visualize Only Selected Account

Clears the graph and only displays the connections for this account

Communication Visualizer
Visualizer

- Click on Node to see communications involving that account
- Click on link to see communications between the two entities
- Click *Snapshot Report* to create an HTML report with the snapshot included

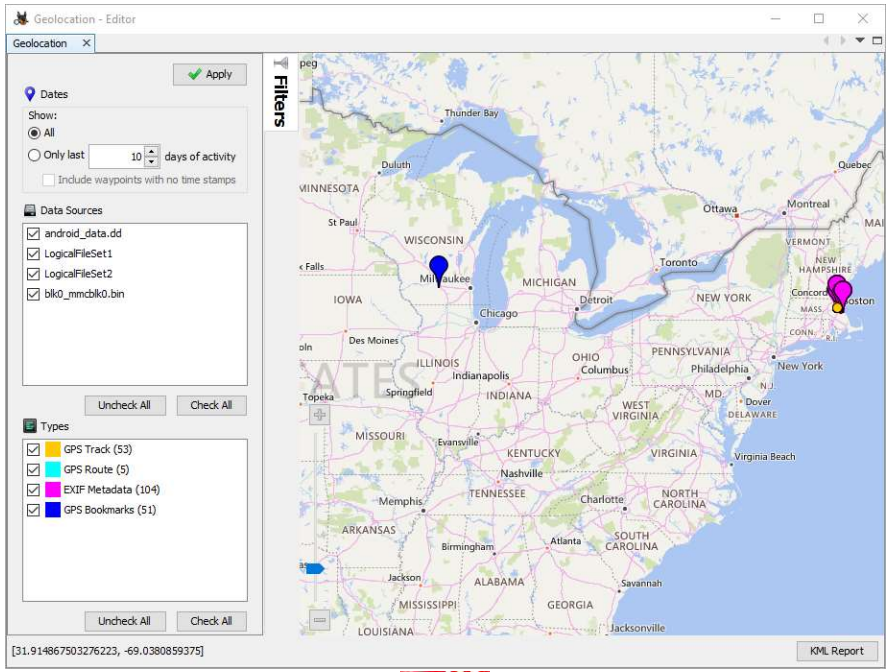


Geolocation Viewer

The Geolocation viewer shows artifacts that have longitude and latitude attributes

They are marked on the map

Offline map data resources are available



Geolocation Viewer

You can move the map by clicking and dragging

Different type of markers (called waypoints) are displayed in different colors

Key is available in lower left of viewer

You can filter based on:

Timeframe

Data Source

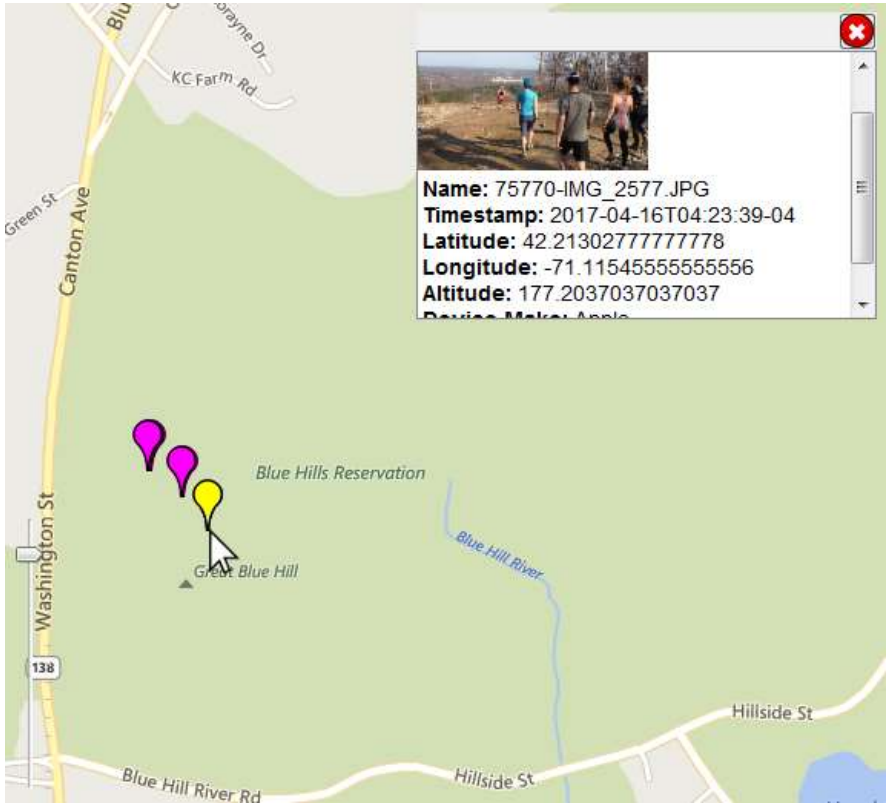
Geolocation Viewer

Details

Left-clicking on waypoint will give you details on a waypoint

The data will be different depending upon type of waypoint.

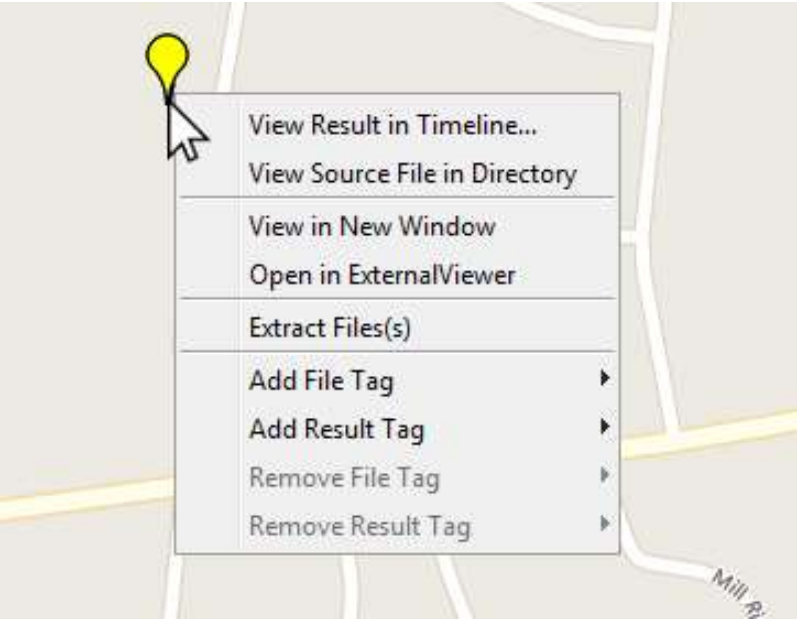
Here is a waypoint associated with an image from the Picture Analyzer Module



Geolocation Viewer

Details

Right-clicking on waypoint will give you a similar menu as you would see in the Result Viewer



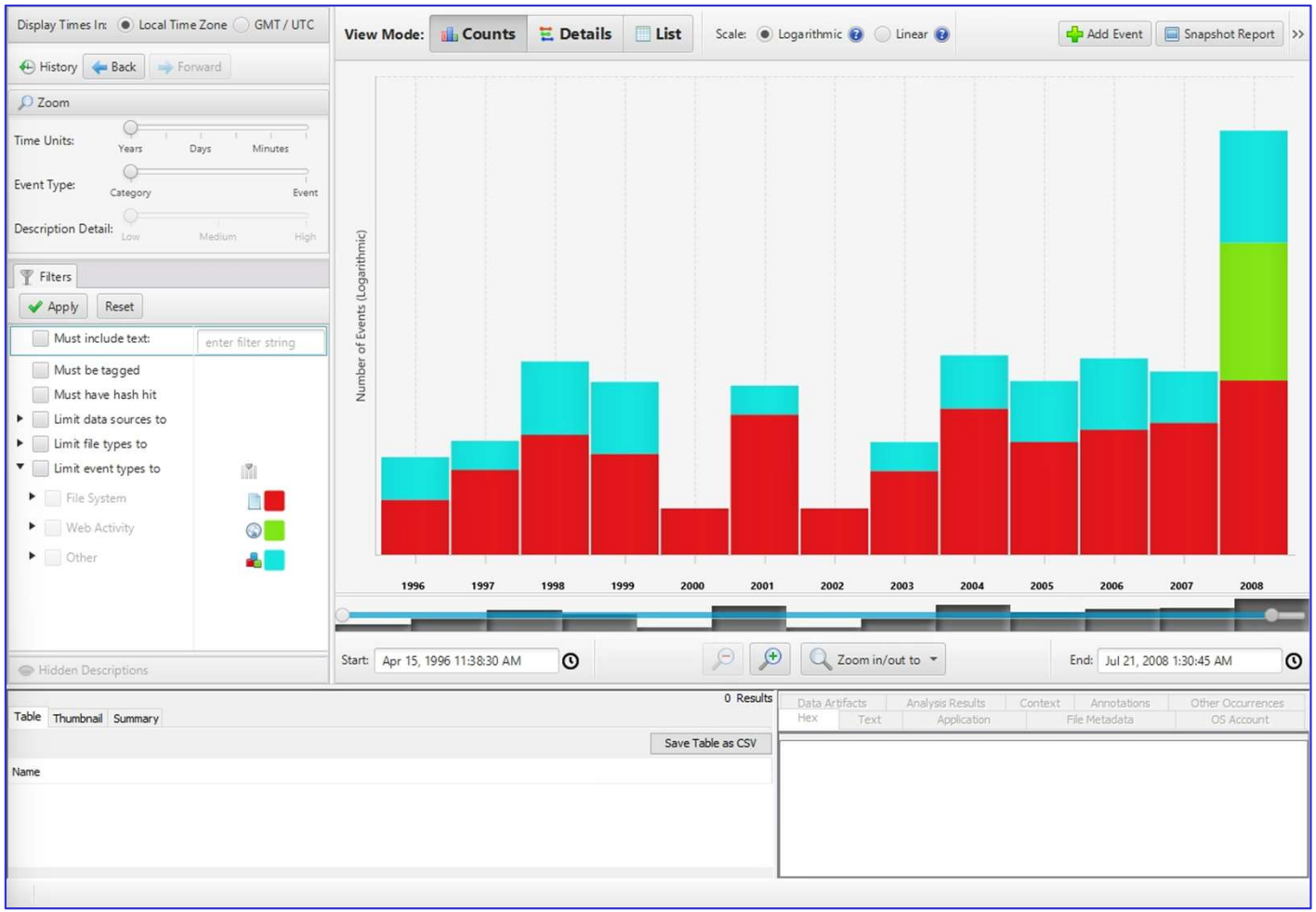
Timelines

- Lawyers who work with Cyber Forensic Investigators really really want to know
  - *What event happened*
  - *When it happened*
  - *Timing relative to other events*
- Autopsy has timeline analysis
  - *Functions specific to timelines*
  - *Easy to understand*
- Can filter on
  - *Times of interest*
  - *Text*
  - *Relation to other events*

Timeline Display

There are three primary views:

- Counts (default)
- Details
- List

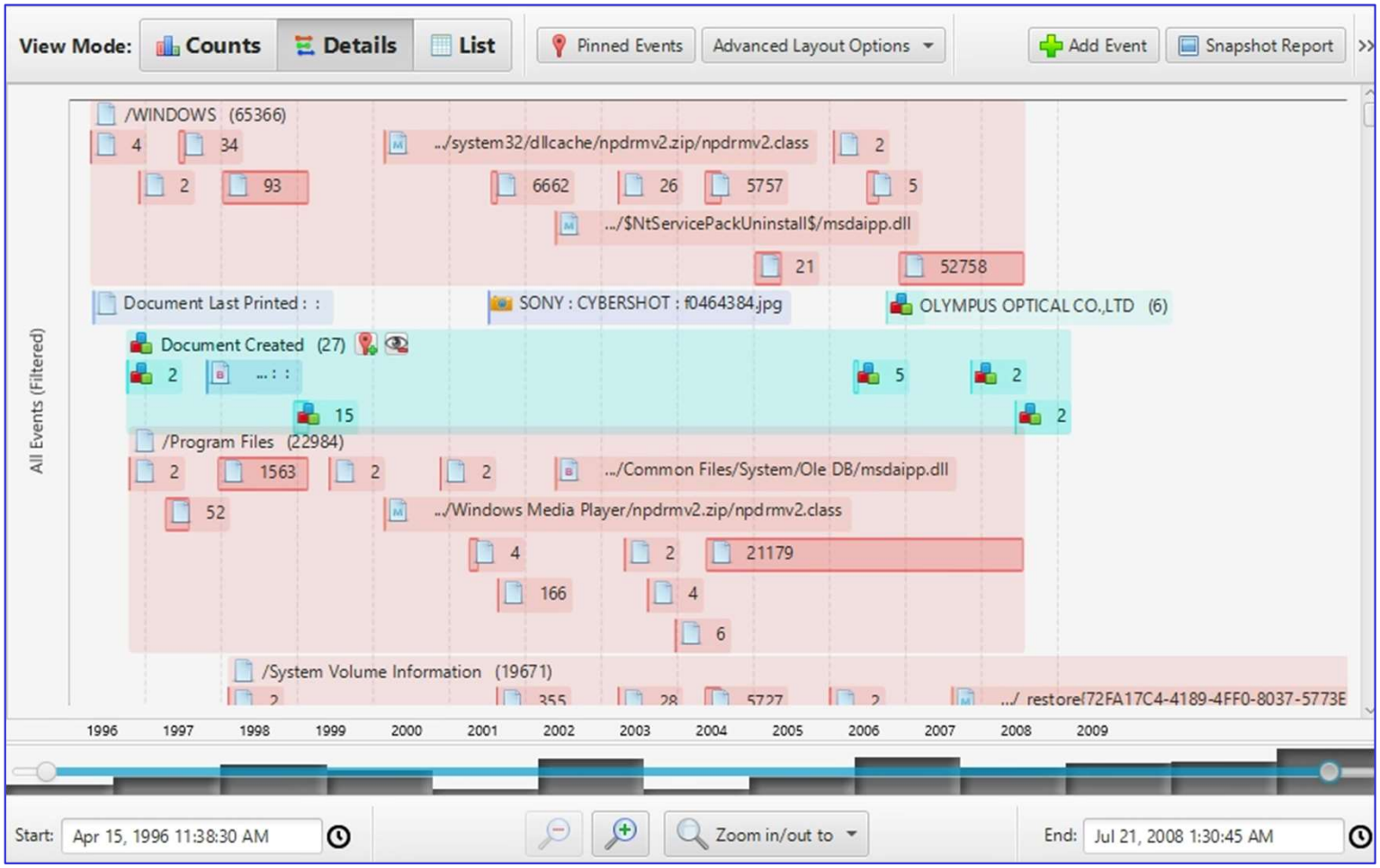


Timeline Display

Details view:

Shows information on events that happened in a specific time period

Best when you've filtered down to a small window in time



Timeline Display

List view:

Shows every event in the order it occurred.

Can be helpful to see which other events happened in the same time frame as an event of interest.

Best used after you've filtered down to a limited number of events.

View Mode: Counts | Details | List | Add Event | Snapshot Report | Refresh View

83,573 events

Date/Time	Event Type	Description	Tagged	Hash Hit
1996-04-15 11:38:30	_BM	/WINDOWS/Fonts/WINGDNG2.TTF		
1996-04-15 11:39:10	_BM	/WINDOWS/Fonts/WINGDNG3.TTF		
1996-04-24 22:07:00	Document Last Printed	Document Last Printed : :		
1996-10-03 21:59:12	Document Created	Document Created : :		
1996-10-14 23:33:28	Document Created	Document Created : :		
1996-10-16 18:00:00	_BM	/Program Files/Microsoft Office/Office/1033/GR8GALRY.GRA		
1996-12-03 06:50:14	_BM	/WINDOWS/system32/VEN2232.OLB		
1997-04-08 08:18:46	_BM	/Program Files/Microsoft Office/Office/Addins/FRMRDRCT.ECF		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART15.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART3.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART14.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART1.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART12.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART4.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART5.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART13.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART2.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART6.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART10.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART8.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART7.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART11.BDR		
1997-06-10 18:00:00	_BM	/Program Files/Microsoft Office/Office/Borders/MSART9.BDR		
1997-06-10 19:37:00	_BM	/WINDOWS/Media/Microsoft Office 2000/GLASS.WAV		

Start: Apr 15, 1996 11:38:30 AM Jump By: Year End: Jul 21, 2008 1:30:45 AM

Discovery

The discovery tools shows images, videos, documents or domains that match a set of filters configured by the user.

You can choose how to group and order your results in order to see the most relevant data first.

There are three basic steps you need to follow to set up the Discovery tool:

Choose the result type

Set up filters

Choose how to group and sort the results

Discovery

Discovery

Step 1: Choose result type

Images | Videos | Documents | Domains

Step 2: Filter which images to show

- [x] File Size:
  - XSmall: 0-16KB
  - Small: 16-100KB
  - Medium: 100KB-1MB
  - Large: 1-50MB
  - XLarge: 50-200MB
  - XXLarge: 200MB+
- [ ] Data Source:
  - LogicalFileSet2 (ID: 43640)
  - xp-sp3-v4.001 (ID: 12714)
  - LogicalFileSet1 (ID: 1)
- [x] Past Occurrences:
  - Known (NSRL)
  - Very Common (100+)
  - Common (11 - 100)
  - Rare (2-10)
  - Unique (1)
- [ ] Possibly User Created
- [ ] Hash Set: Bomb files
- [ ] Interesting Item: Bird files, Cat files
- [ ] Object Detected: haarcascade_eye.xml, haarcascade_frontalcatface.xml
- [ ] Parent Folder: /Windows/ (substring) (exclude), /Program Files/ (substring) (exclude)

(All will be used)

Full | Substring

Include | Exclude

Delete

Add

Step 3: Choose display settings

Group By: File Size

Order Within Groups By: File Size

Order Groups By: Group Name

Search

Report Generation

Including Items in a Report

Tagging (aka bookmarking) allows you to create a reference to a file or object and

Easily find it later

Include it in a report

Tagging Items

When an interesting item is discovered, the user can tag it by right-clicking the item and selecting one of the tag options

When you tag an item identified from the Views section of the tree viewer, you can add a file tag

When you tag an item identified from the Results section of the tree viewer, you have a choice of adding a

File tag (use when the file is of interest)

Result tag (use when the result is of interest)

Tag Names

There are several default tag names:

Bookmark

default tag for marking files of interest

CAT-1 through CAT-5

for law enforcement use

Follow-up

default tag for marking files to follow up on

Notable item

default tag for indicating that an item should be marked as notable in the central repository

You can also create custom tag names

Add a Result Tag

Listing | Common Files (All Data Sources, Documents, Media)

Web Downloads — 2 Results

Table | Thumbnail

Source File	URL	Date Accessed	Path
downloads.sqlite	http://fpdownload.macromedia.com/get/flashplayer/curren...	2008-05-14 01:47:44 EDT	C:/Documents and Settings/Administrator/Desktop/ir
downloads.sqlite	http://fpdownload.macromedia.com/get/flashplayer/curren...	2008-05-14 01:47:44 EDT	C:/Documents and Settings/Administrator/Desktop/ir

- Properties
- View Result in Timeline...
- View Source File in Timeline...
- View Source File in Directory
- View in New Window
- Open in External Viewer
- Extract File(s)
- Add File Tag
- Add Result Tag
- Remove File Tag
- Remove Result Tag
- Add file to hash set

- chicken
- duck
- goose
- horse
- mooo
- rabbit
- Bookmark Ctrl+B
- CAT-1: Child Exploitation (Illegal) (Notable)
- CAT-2: Child Exploitation (Non-Illegal/Age Difficult) (Notable)
- CAT-3: CGI/Animation (Child Exploitive) (Notable)
- CAT-4: Exemplar/Comparison (Internal Use Only)
- CAT-5: Non-pertinent
- Follow Up
- Notable Item (Notable)
- Tag and Comment...
- New Tag...

Hex | Strings | Application | Indexed Text | Message | File Me

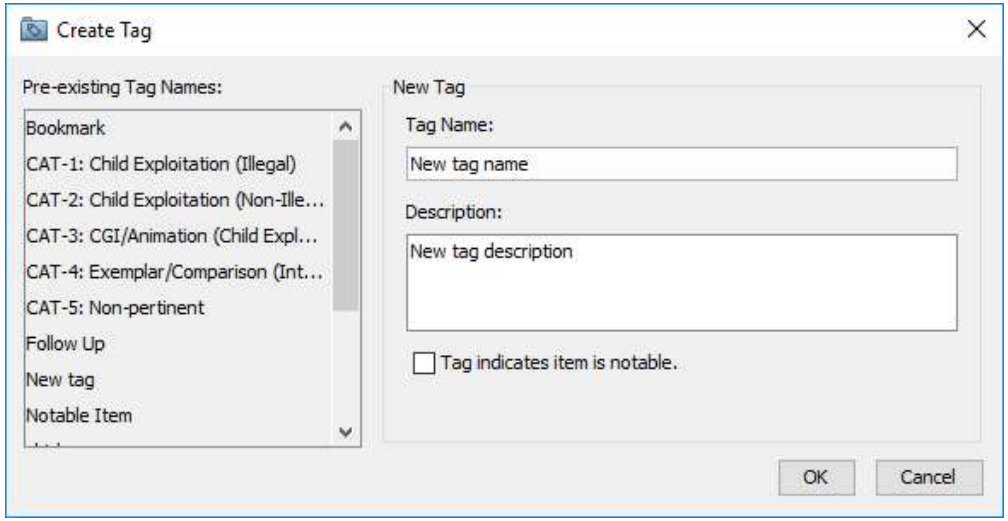
Result: 1 of 1 Result

Type	Value	Source(s)
URL	http://fpdownload.macromedia.com/get/flash	RecentActivity
Date Accessed	2008-05-14 01:47:44	RecentActivity
Path	C:/Documents and Settings/Administrator/Des	RecentActivity
Program Name	FireFox	RecentActivity
Domain	fpdownload.macromedia.com	RecentActivity
Source File Path	/LogicalFileSet2/37-Administrator/Application Data/Mozilla/Firefox/Profiles/towjib3x.default/downloads.sqlite	

Creating a Tag

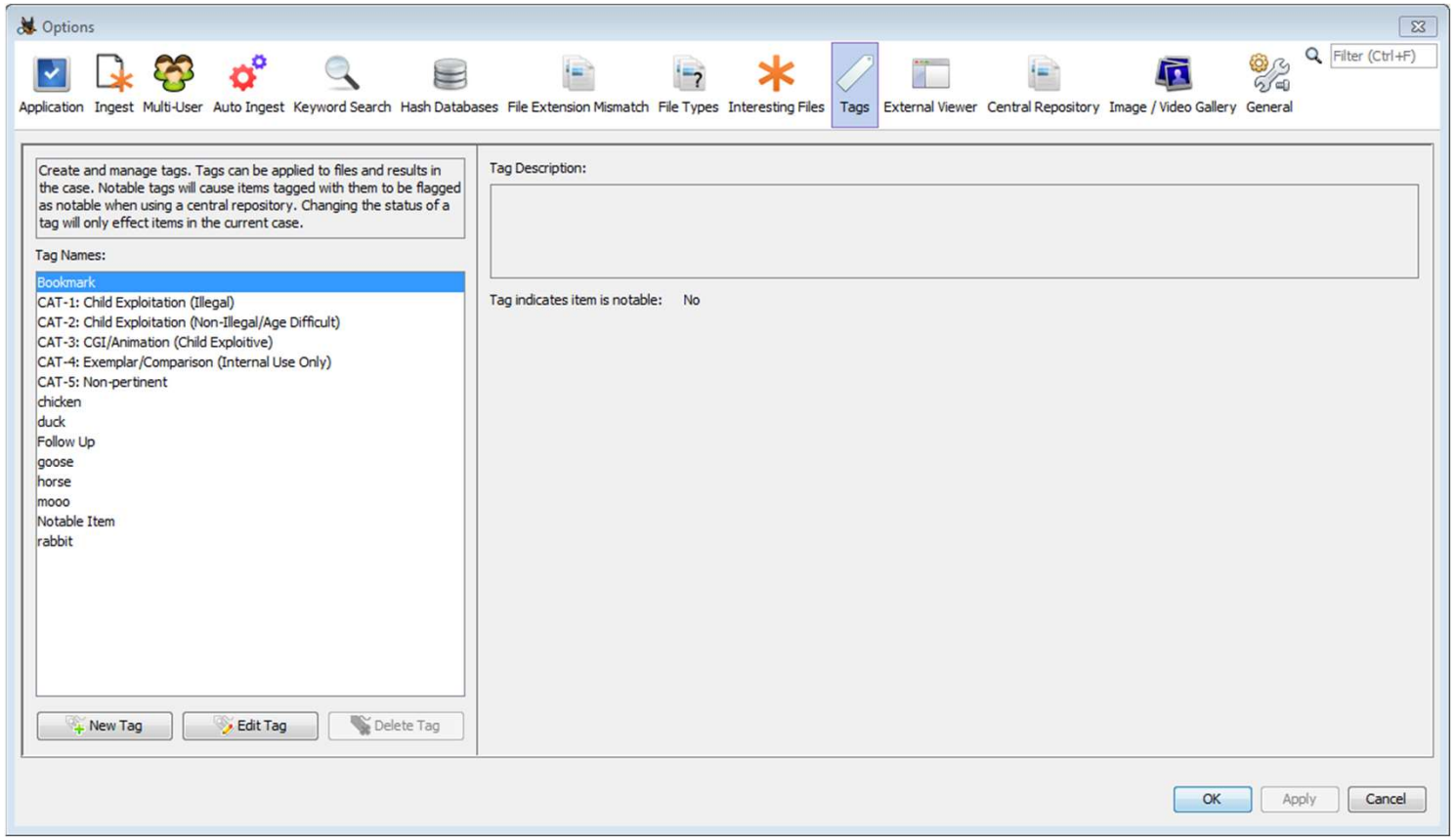
Tag and Comment

New Tag



Managing Tags

The list of tags can be edited through the Tags tab on the Options menu



Reporting

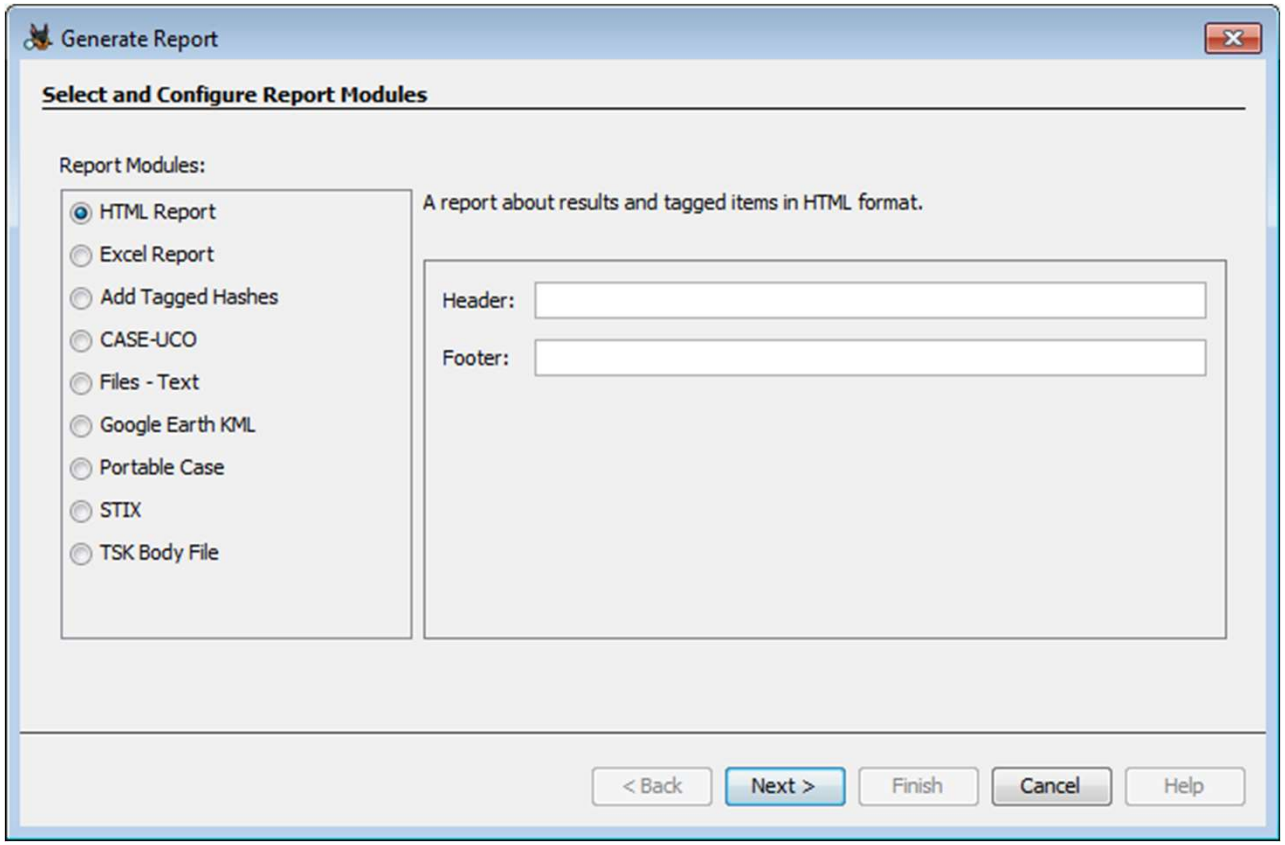
The report modules allow the user to extract key information from a case in a variety of formats

We will walk through a scenario where a report in HTML format is generated

Triggering Report Generation

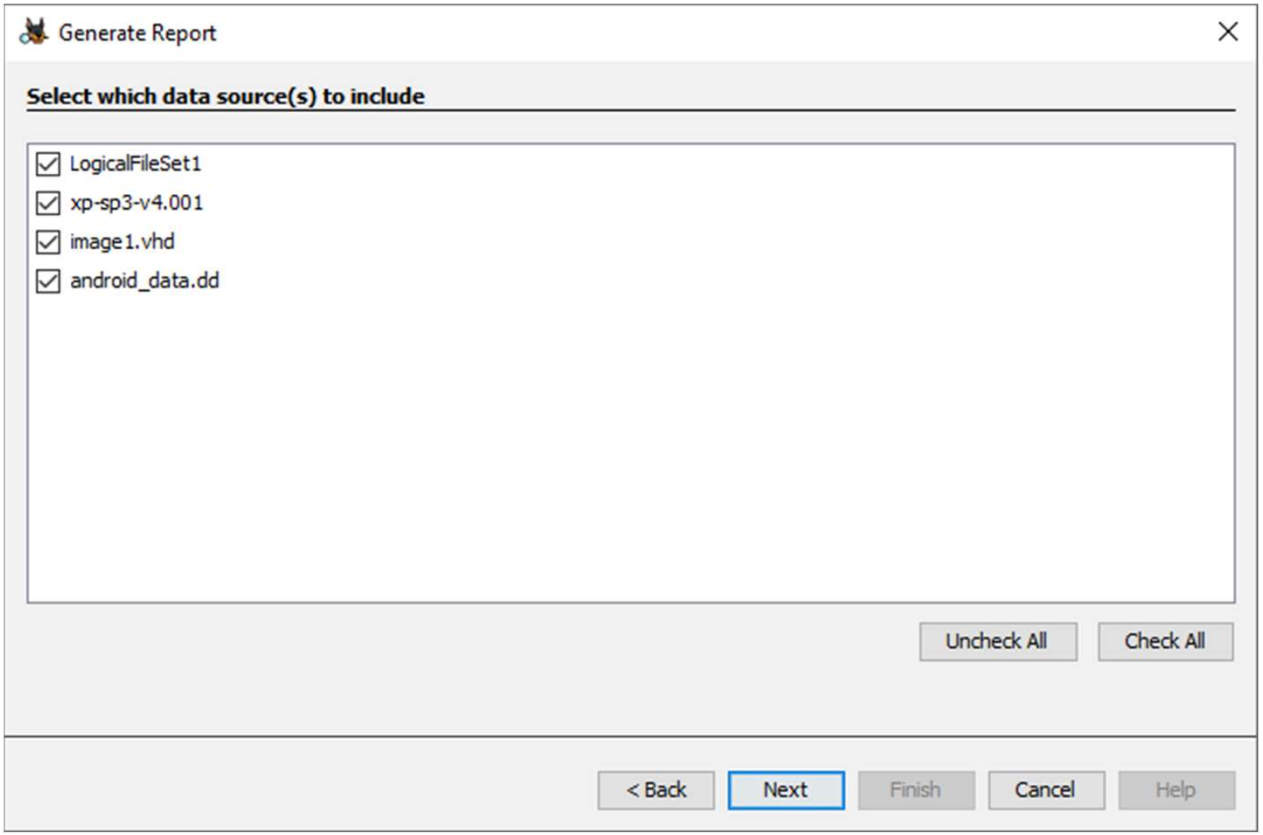
Click on the *Generate Report* above the Result Viewer

You will be presented with the following pop-up window



Reporting

After entering the desired header and footer, you will be asked which data sources to include



Reporting

You then select the data you want to report on by choosing:

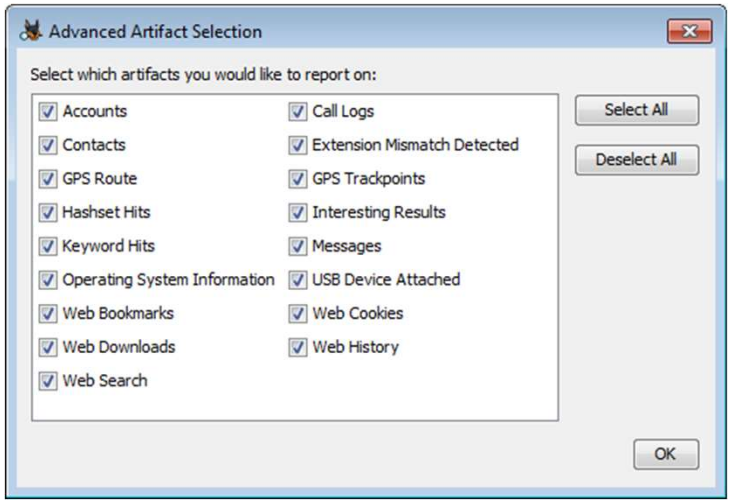
Result types

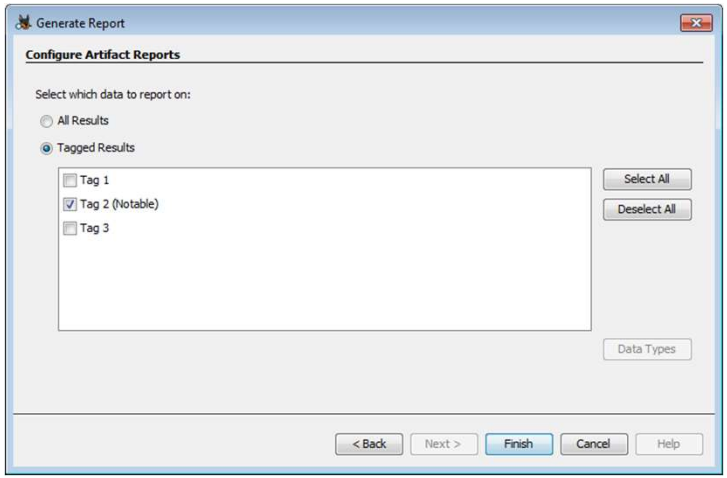
Must select “All Results”, then “Choose Result Types”

Tagged Results

Choice of all tagged results or specific tagged results

You can choose which tags to include in the report





Reporting

The completed report would look similar to this: