AUTOPSY FORENSICS
4.9.1

Autopsy User Documentation 4.9.1
Graphical digital forensics platform for The Sleuth Kit and other tools.

Autopsy User's Guide

Overview

This is the User's Guide for the open source Autopsy platform. Autopsy allows you to examine a hard drive or mobile device and recover evidence from it. This guide should help you with using Autopsy. The developer's guide will help you develop your own Autopsy modules.

Autopsy 4 (and 3) are a complete rewrite from Autopsy 2, and none of this document is relevant to Autopsy 2.

Help Topics

The following topics are available here:

If the topic you need is not listed, refer to the Autopsy Wiki or join the SleuthKit User List at SourceForge.

Installing Autopsy

Prerequisites

It is *highly* recommended to remove or disable any antivirus software from computers that will be processing or reviewing cases. Antivirus software will often conflict with forensic software, and may quarantine or even delete some of your results before you get a chance to look at them.

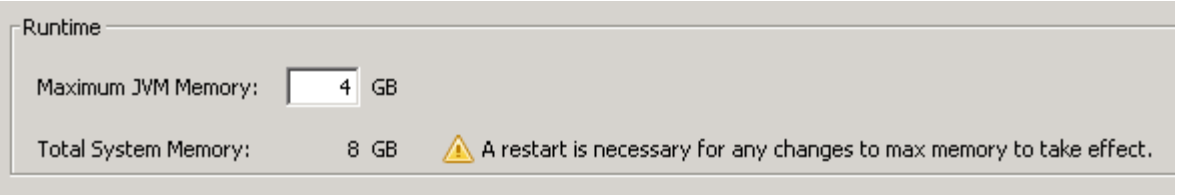
Deployment Types

Starting with Autopsy 4.0, there are two ways to deploy Autopsy:

- **Single-User**: Cases can be open by only a single instance of Autopsy at a time. Autopsy installations do not communicate with each other. This is the easiest to install and deploy. This page outlines that installation process.
- **Multi-User**: Cases can be open by multiple users at the same time and users can see what each other is doing. This collaborative deployment requires installation and configuration of other network-based services. The installation of this deployment is covered in **Setting Up Multi-user Environment**.

System Memory Requirements

The 64 bit version of Autopsy requires a minimum of 8GB RAM (16 GB recommended). When the 64 bit version of Autopsy is installed on Windows it will be limited to a maximum heap size of 4GB leaving the remaining memory for the operating system, the internal Solr text indexing service and other applications. If you wish to change the maximum heap size you can do so after installation by changing the Maximum JVM Memory value in the Runtime section under Tools -> Options -> Application.



Download

Download Autopsy from the website:

http://sleuthkit.org/autopsy/download.php

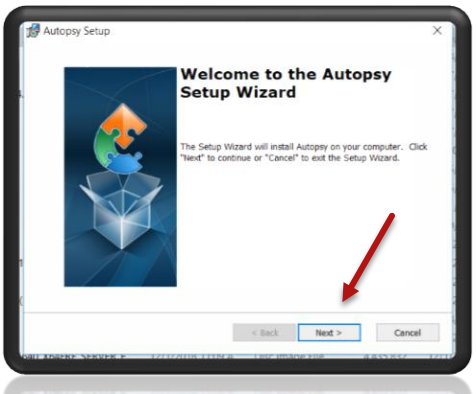
The current version of Autopsy 4 is distributed on sleuthkit.org only as a Windows installer. It can run on Linux and OS X, but requires some manual setup.

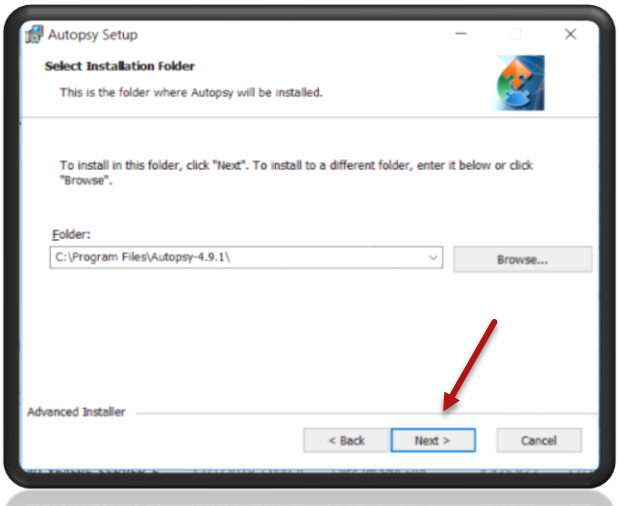
Installation

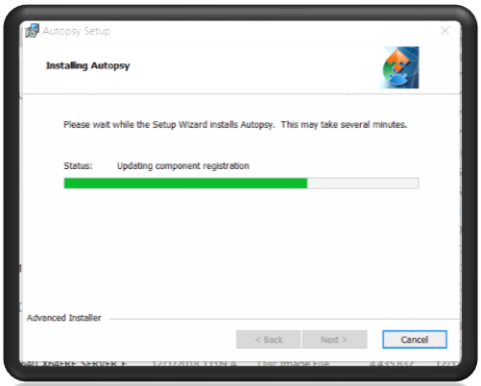
To install Autopsy, perform the following steps:

1. Run the Autopsy *msi* file
2. If Windows prompts with User Account Control, click *Yes*

3. Click through the dialog boxes until you click a button that says *Finish*







4. Autopsy should now be fully installed

Quick Start Guide

Adding a Data Source (image, local disk, logical files)

Data sources are added to a **case**. A case can have a single data source or it can have multiple data sources. Currently, a single report is generated for an entire case, so if you need to report on individual data sources, then you should use one data source per case. If there are many

drives/phones/other data sources for one investigation, then your case should have multiple data sources.

Creating a Case

To create a case, use either the "Create New Case" option on the Welcome screen or from the "Case" menu. This will start the **New Case Wizard**. You will need to supply it with the name of the case and a directory to store the case results into. You can optionally provide case numbers and reviewer names.

Adding a Data Source

The next step is to add an input data source to the case. The **Add Data Source Wizard** will start automatically after the case is created or you can manually start it from the "Case" menu or toolbar. You will need to choose the type of input data source to add (image, local disk, or logical files and folders). Next, supply it with the location of the source to add.

- For a disk image, browse to the first file in the set (Autopsy will find the rest of the files). Autopsy currently supports E01 and raw (dd) files.
- For local disk, select one of the detected disks. Autopsy will add the current view of the disk to the case (i.e. snapshot of the meta-data). However, the individual file content (not meta-data) does get updated with the changes made to the disk. Note, you may need run Autopsy as an Administrator to detect all disks.
- For logical files (a single file or folder of files), use the "Add" button to add one or more files or folders on your system to the case. Folders will be recursively added to the case.

There are a couple of options in the wizard that will allow you to make the ingest process faster. These typically deal with deleted files. It will take longer if unallocated space is analyzed and the entire drive is searched for deleted files. In some scenarios, these recovery steps must be performed and in other scenarios these steps are not needed and instead fast results on the allocated files are needed. Use these options to control how long the analysis will take.

Autopsy will start to analyze these data sources and add them to the case and the internal database. While it is doing that, it will prompt you to configure the Ingest Modules.

Ingest Modules

You will next be prompted to configure the Ingest Modules. Ingest modules will run in the background and perform specific tasks. The Ingest Modules analyze files in a prioritized order so that files in a user's directory are analyzed before files in other folders. Ingest modules can be developed by third-parties. The standard ingest modules included with Autopsy are:

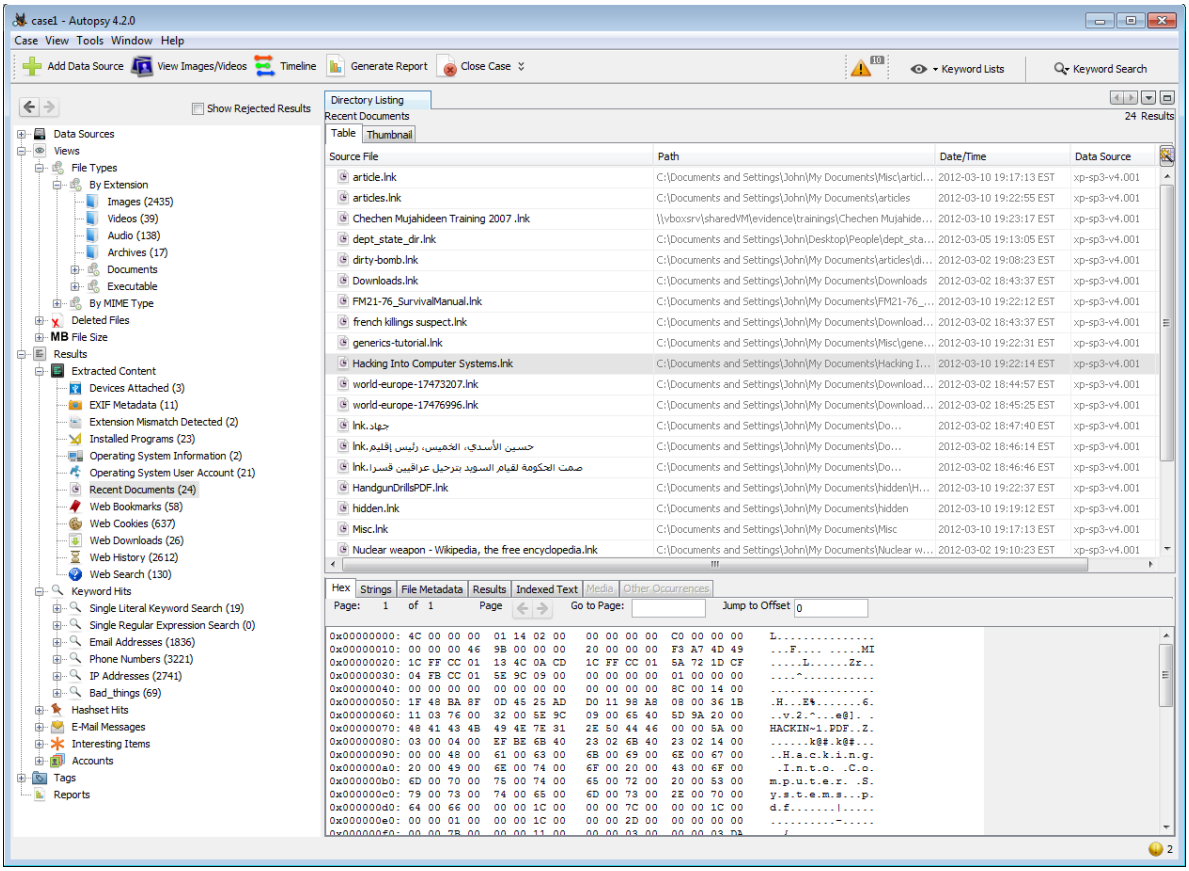
- **Recent Activity Module** extracts user activity as saved by web browsers and the OS. Also runs Regripper on the registry hive.

- **Hash Lookup Module** uses hash sets to ignore known files from the NIST NSRL and flag known bad files. Use the "Advanced" button to add and configure the hash sets to use during this process. You will get updates on known bad file hits as the ingest occurs. You can later add hash sets via the Tools -> Options menu in the main UI. You can download an index of the NIST NSRL from http://sourceforge.net/projects/autopsy/files/NSRL/
- **File Type Identification Module** determines file types based on signatures and reports them based on MIME type. It stores the results in the Blackboard and many modules depend on this. It uses the Tika open source library. You can define your own custom file types in Tools, Options, File Types.
- **Embedded File Extraction Module** opens ZIP, RAR, other archive formats, Doc, Docx, PPT, PPTX, XLS, and XLSX and sends the derived files from those files back through the ingest pipeline for analysis.
- **EXIF Parser Module** extracts EXIF information from JPEG files and posts the results into the tree in the main UI.
- **Keyword Search Module** uses keyword lists to identify files with specific words in them. You can select the keyword lists to search for automatically and you can create new lists using the "Advanced" button. Note that with keyword search, you can always conduct searches after ingest has finished. The keyword lists that you select during ingest will be searched for at periodic intervals and you will get the results in real-time. You do not need to wait for all files to be indexed before performing a keyword search, however you will only get results from files that have already been indexed when you perform your search.
- **Email Parser Module** identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard.
- **Extension Mismatch Detector Module** uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type. Ignores 'known' (NSRL) files. You can customize the MIME types and file extensions per MIME type in Tools, Options, File Extension Mismatch.
- **Data Source Integrity Module** computes a checksum on E01 files and compares with the E01 file's internal checksum to ensure they match.
- **Android Analyzer Module** allows you to parse common items from Android devices. Places artifacts into the BlackBoard.
- **Interesting Files Identifier Module** searches for files and directories based on user-specified rules in Tools, Options, Interesting Files. It works as a "File Alerting Module". It generates messages in the inbox when specified files are found.
- **PhotoRec Carver Module** carves files from unallocated space and sends them through the file processing chain.
- **Correlation Engine Module** adds file hashes and other extracted properties to a central repository.
- **Encryption Detection Module** looks for encrypted files.
- **Virtual Machine Extractor Module** extracts data from virtual machine files

When you select a module, you will have the option to change its settings. For example, you can configure which keyword search lists to use during ingest and which hash sets to use. Refer to the individual module help for details on configuring each module.

While ingest modules are running in the background, you will see a progress bar in the lower right. You can use the GUI to review incoming results and perform other tasks while ingesting at the same time.

Analysis Basics



You will start all of your analysis techniques from the tree on the left.

- The Data Sources root node shows all data in the case.
  - The individual image nodes show the file system structure of the disk images or local disks in the case.
  - The LogicalFileSet nodes show the logical files in the case.
- The Views node shows the same data from a file type or timeline perspective.
- The Results node shows the output from the ingest modules.

When you select a node from the tree on the left, a list of files will be shown in the upper right. You can use the Thumbnail view in the upper right to view the pictures. When you select a file from the upper right, its contents will be shown in the lower right. You can use the tabs in the lower right to view the text of the file, an image, or the hex data.

If you are viewing files from the Views and Results nodes, you can right-click on a file to go to its file system location. This feature is useful to see what else the user stored in the same folder as the file that you are currently looking at. You can also right click on a file to extract it to the local system.

If you want to search for single keywords, then you can use the search box in the upper right of the program. The results will be shown in a table in the upper right.

The tree on the left as well as the table on the right have a **UI Quick Search** feature which can be used to quickly find a visible node.

You can tag (bookmark) arbitrary files so that you can more quickly find them later or so that you can include them specifically in a report.

Ingest Inbox

As you are going through the results in the tree, the ingest modules are running in the background. The results are shown in the tree as soon as the ingest modules find them and report them.

The Ingest Inbox receives messages from the ingest modules as they find results. You can open the inbox to see what has been recently found. It keeps track of what messages you have read.

The intended use of this inbox is that you can focus on some data for a while and then check back on the inbox at a time that is convenient for them. You can then see what else was found while you were focused on the previous task. You may learn that a known bad file was found or that a file was found with a relevant keyword and then decide to focus on that for a while.

When you select a message, you can then jump to the Results tree where more details can be found or jump to the file's location in the filesystem.

Timeline

There is a basic timeline view that you can access via the "Tools", "Make Timeline" feature. This will take a few minutes to create the timeline for analysis. Its features are still in development.

Example Use Cases

In this section, we will provide examples of how to do common analysis tasks.

Web Artifacts

If you want to view the user's recent web activity, make sure that the Recent Activity ingest module was enabled. You can then go to the "Results " node in the tree on the left and then into the "Extracted Data" node. There, you can find bookmarks, cookies, downloads, and history.

Known Bad Hash Files

If you want to see if the data source had known bad files, make sure that the Hash Lookup ingest module was enabled. You can then view the "Hashset Hits" section in the "Results" area of the tree on the left. Note that hash lookup can take a long time, so this section will be updated as long as the ingest process is ongoing. Use the Ingest Inbox to keep track of what known bad files were recently found.

When you find a known bad file in this interface, you may want to right click on the file to also view the file's original location. You may find additional files that are relevant and stored in the same folder as this file.

Media: Images and Videos

If you want to see all images and video on the disk image, then go to the "Views" section in the tree on the left and then "File Types". Select either "Images" or "Videos". You can use the thumbnail option in the upper right to view thumbnails of all images.

Note: We are working on making this more efficient when there are lots of images. We are also working on the feature to display video thumbnails.

You can select an image or video from the upper right and view the video or image in the lower right. Video will be played with sound.

Reporting

A final report can be generated that will include all analysis results. Use the "Generate Report" button to create this. It will create an HTML or XLS report in the Reports folder of the case folder. If you forgot the location of your case folder, you can determine it using the "Case Properties" option in the "Case" menu. There is also an option to export report files to a separate folder outside of the case folder.

Autopsy Workflow

Analyzing data in Autopsy uses the following workflow:

1. **Create a Case**: A case is a container for one or more data sources. One must be created before data is analyzed. See **Cases** for more details.
2. **Adding a Data Source**: One or more data sources are added to the case. Data sources include disk images and local files. See **Data Sources** for more details.
3. **Analyze with Ingest Modules**: After the data source is added, ingest modules operate in the background to analyze the data. Results are posted to the interface in real time and provide alerts as necessary. Example ingest modules include **hash calculation and**

lookup, keyword searching, and web artifact extraction. 3rd-party modules can be developed and added to the pipelines. See Ingest Modules.

4. **Manual Analysis**: The user navigates the interface, file contents, and ingest module results to identify the evidence. Interesting items can be tagged for later reporting and analysis.
5. **Report Generation**: The user initiates a final report based on selected tags or results.

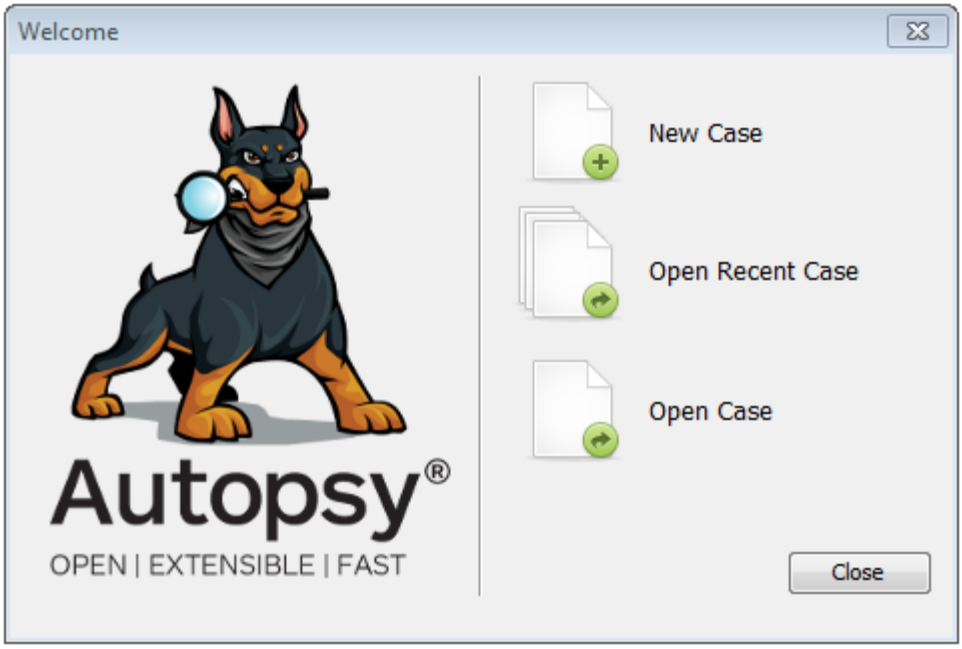
Cases and Adding Data Sources

Cases

You need to create a case before you can analyze data in Autopsy. A case can contain one or more data sources (disk images, disk devices, logical files). The data sources can be from multiple drives in a single computer or from multiple computers. It's up to you.

Each case has its own directory that is named based on the case name. The directory will contain configuration files, a database, reports, and other files that modules generates. The main Autopsy case configuration file has an ".aut" extension.

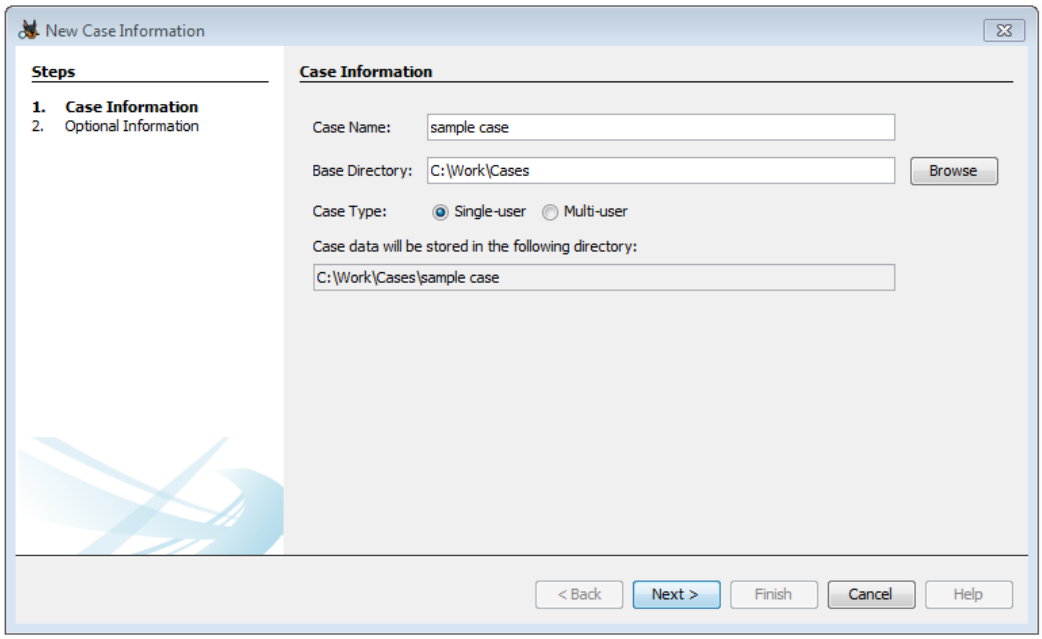
Creating a Case



There are several ways to create a new case:

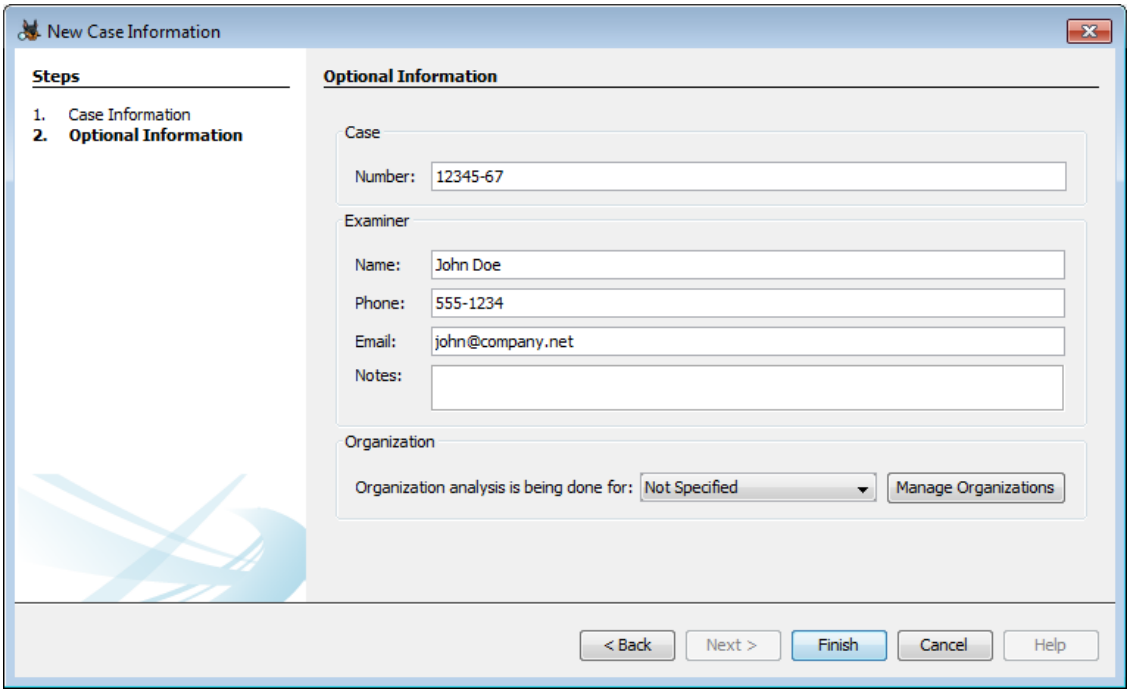
- The opening splash screen has a button to create a new case.
- The "Case", "Create New Case" menu item

The New Case wizard dialog will open and you will need to enter the case name and base directory. A directory for the case will be created inside of the "base directory". If the directory already exists, you will need to either delete the existing directory or choose a different combination of names.



NOTE: You will only have the option of making a multi-user case if you have configured Autopsy with multi-user settings. See **Setting Up Multi-user Environment** for installation instructions and **Creating Multi-user cases** for details on creating multi-user cases.

You will also be prompted for optional information as shown below:



All fields on this panel are optional. Additionally, the Organization section will only be active if the **central repository** is enabled.

After you create the case, you will be prompted to add a data source, as described in **Adding a Data Source**.

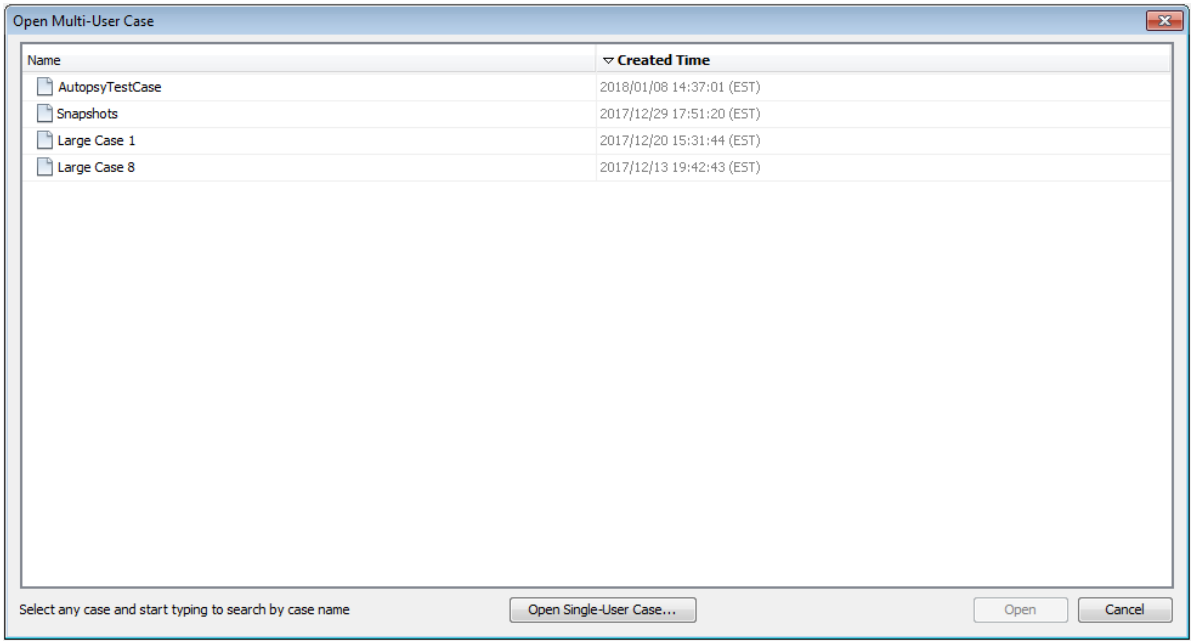
Opening a Case

To open a case, either:

- Choose "Open Case" or "Open Recent Case" from the opening splash screen.
- Choose the "Case", "Open Case" menu item or "Case", "Open Recent Case"

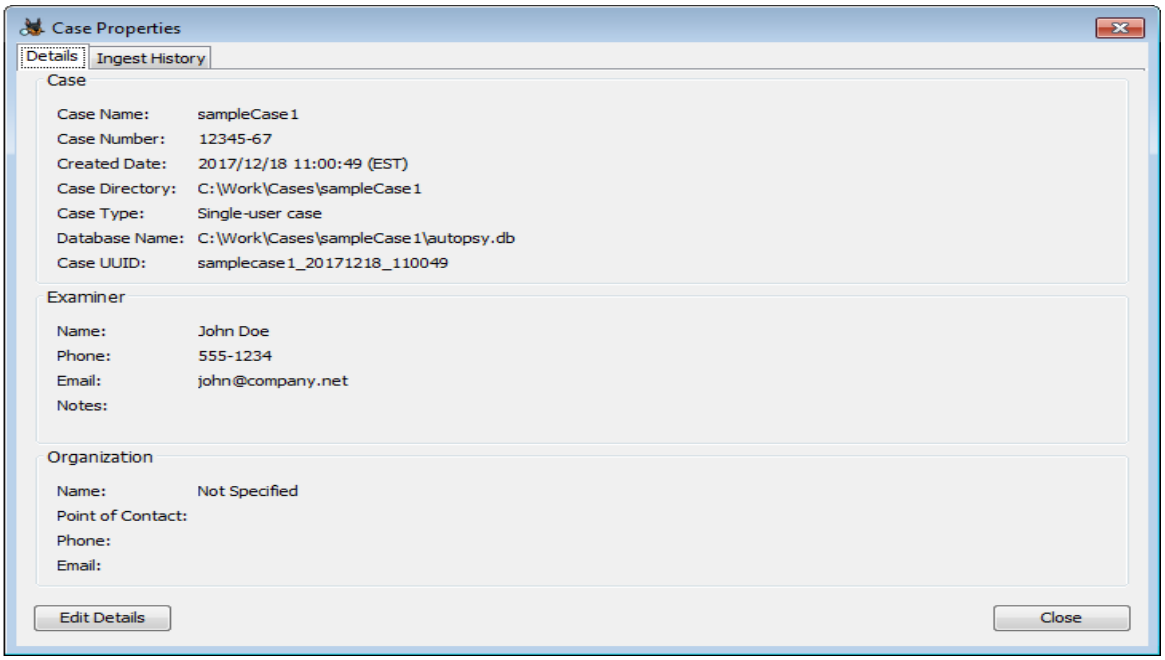
  "Open Recent Case" will always bring up a screen allowing you to select one of the recently opened cases. "Open Case" will do one of two things;

- If multi-user cases are not enabled, it will bring up a file chooser that can be used to browse to the ".aut" file in the case directory of the desired case
- If multi-user cases are enabled, it will bring up the multi-user case selection screen. This uses the coordination services to find a list of multi-user cases. If needed, the "Open Single-User Case" button can be used to bring up the normal file chooser. The multi-user case selection screen has a **UI Quick Search**feature which can be used to quickly find a case in the table. The following shows the multi-user case selection screen:

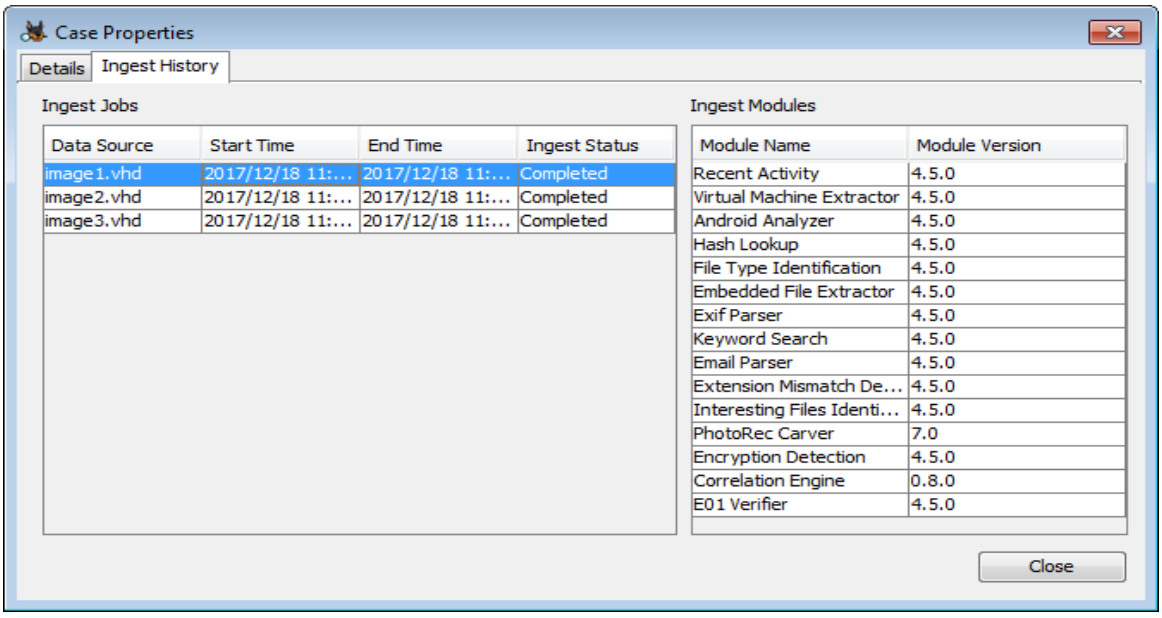


Viewing Case Properties

You can view the case properties by going to the "Case" menu and clicking "Case Properties".



You can use the "Ingest History" tab to view which data sources had which modules run upon them, and when, as shown in the screenshot below.



Data Sources

A data source is the thing you want to analyze. It can be a disk image, some logical files, a local disk, etc. You must open a case prior to adding a data source to Autopsy.

Autopsy supports four types of data sources:

- Disk Image or VM File: A file (or set of files) that is a byte-for-byte copy of a hard drive or media card, or a virtual machine image. (see **Adding a Disk Image**)

- Local Disk: Local storage device (local drive, USB-attached drive, etc.). (see **Adding a Local Disk**)
- Logical Files: Local files or folders. (see **Adding a Logical File**)
- Unallocated Space Image Files: Any type of file that does not contain a file system but you want to run through ingest (see **Adding an Unallocated Space Image File**)

Adding a Data Source

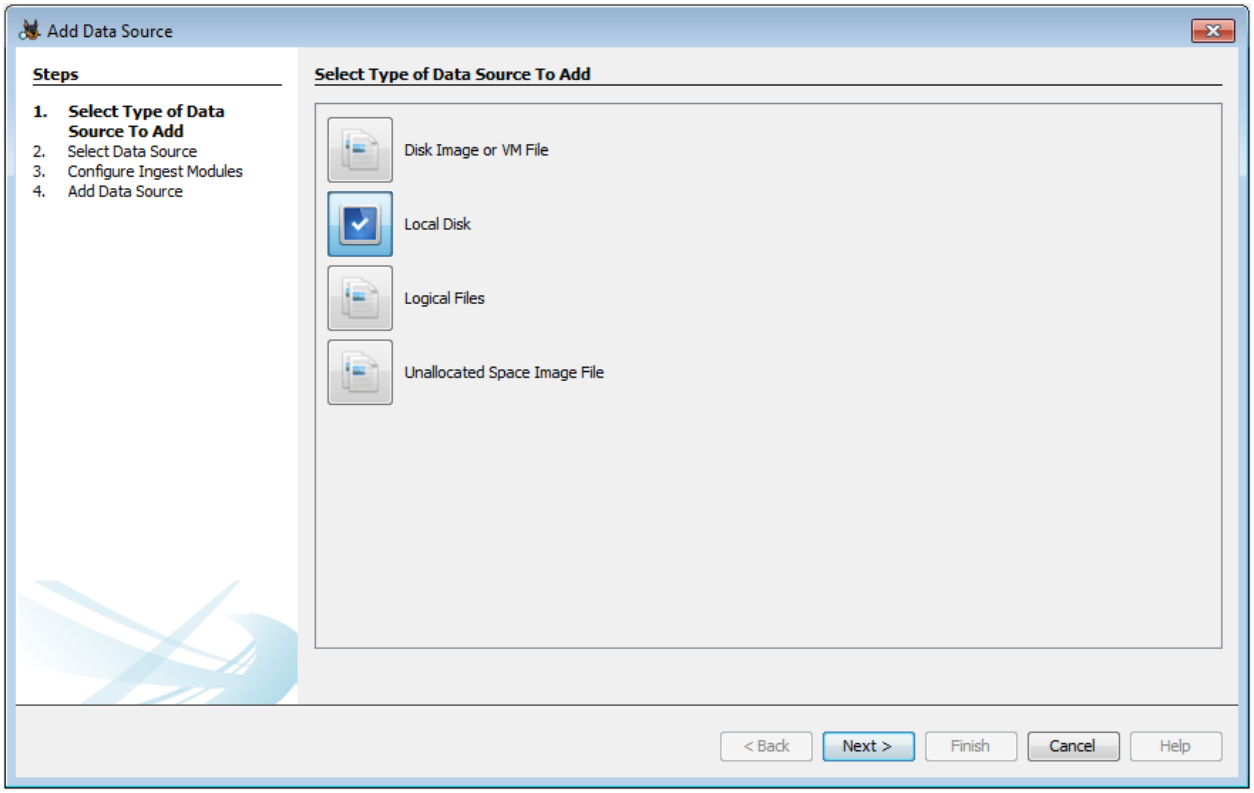
You can add a data source in several ways:

- After you create a case, it automatically prompts you to add a data source.
- There is a toolbar item to add a Data Source when a case is open.
- The "Case", "Add Data Source" menu item when a case is open.

The data source must remain accessible for the duration of the analysis because the case contains a reference to the data source. It does **not** copy the data source into the case folder.

Regardless of the type of data source, there are some common steps in the process:

1) You will select the type of data source.

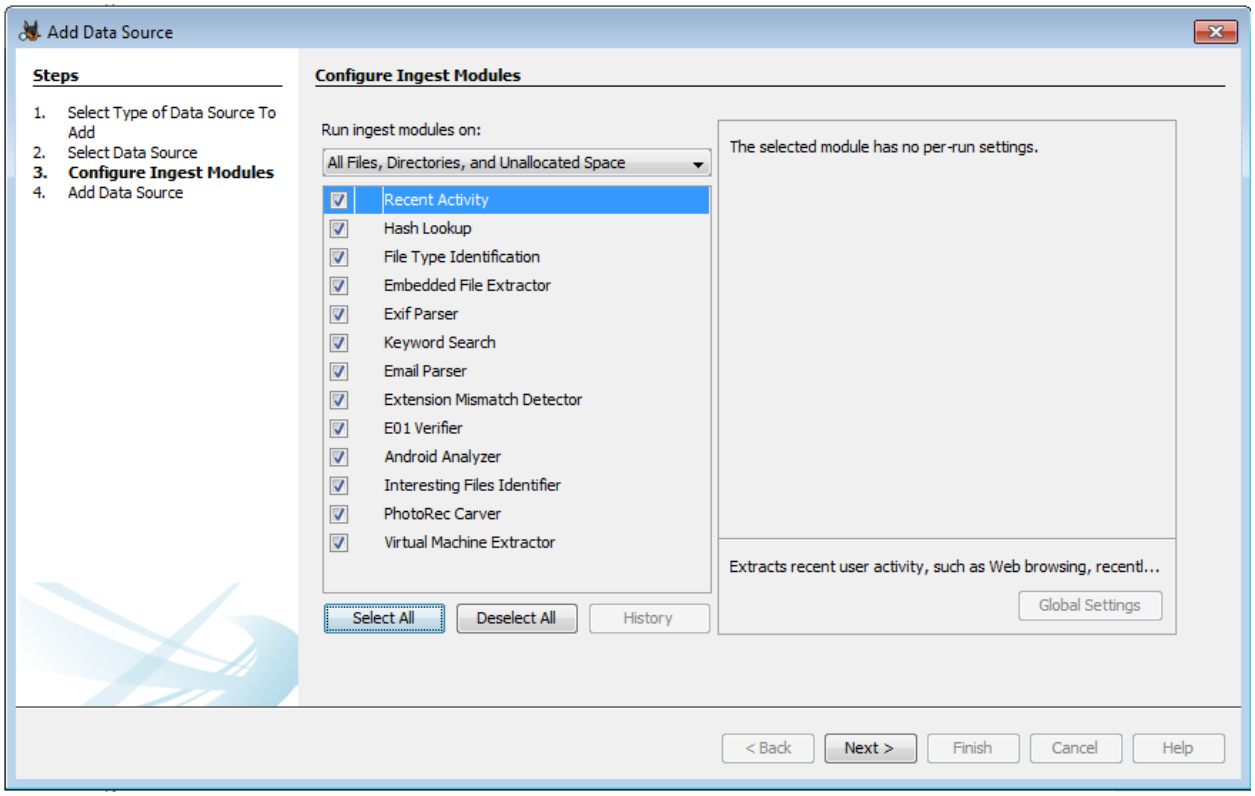


2) You will be prompted to specify the data source to add. This screen varies based on the data source type. Details on adding each type of data source are provided below.

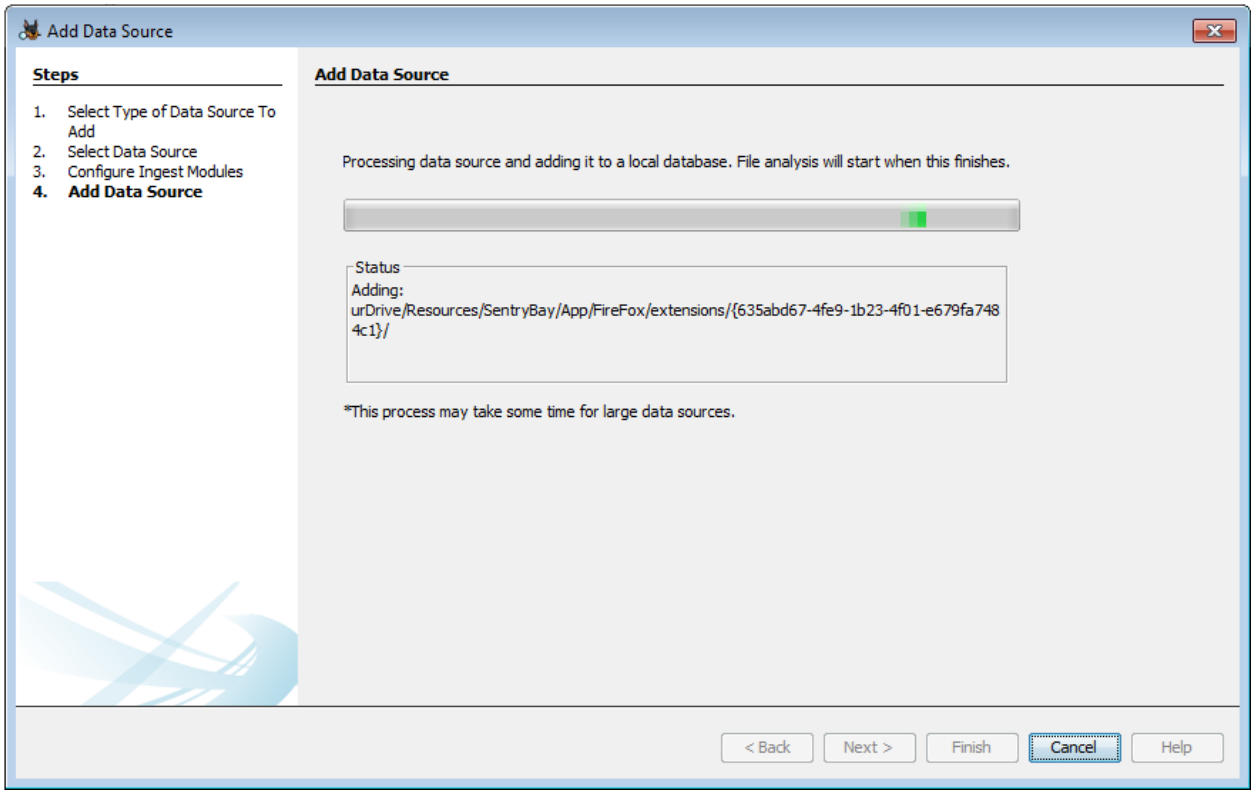
NOTE: If you are adding a data source to a multi-user case, ensure that all Autopsy clients will have access to the data source at the same path. We recommend using UNC paths to ensure this consistent mapping.

3) Autopsy will perform a basic examination of the data source and populate an embedded database with an entry for each file in the data source. No content is analyzed in the process, only the files are enumerated.

4) While it is examining the data source, you will be prompted with a list of ingest modules to enable. If one or more ingest profiles have been saved, there will be a screen before this asking whether to use one of the saved profiles or do a custom setup. See **Ingest Modules** for more information on setting up ingest profiles.



5) After you configure the ingest modules, you may need to wait for Autopsy to finish its basic examination of the data source.



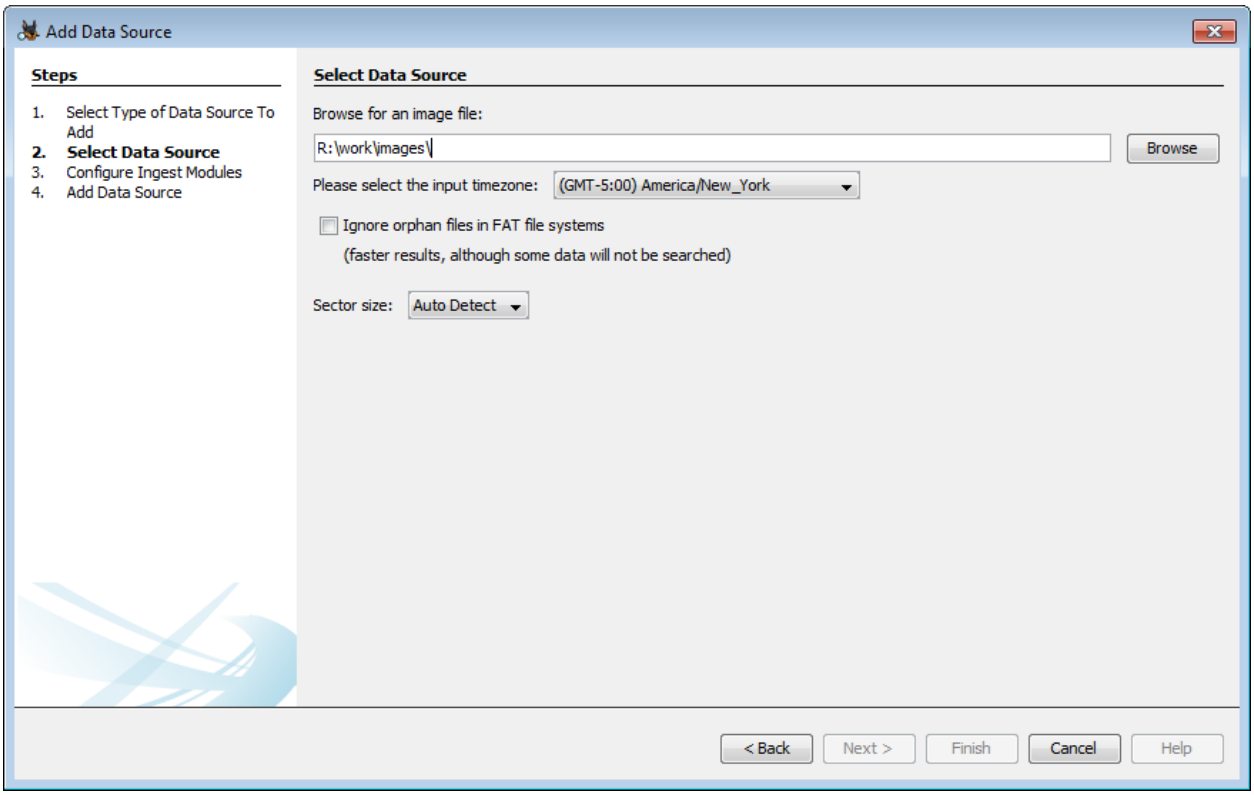
6) After the ingest modules have been configured and the basic examination of the data source is complete, the ingest modules will begin to analyze the file contents.

You cannot remove a data source from a case.

Adding a Disk Image

Autopsy supports disk images in the following formats:

- Raw Single (For example: *.img, *.dd, *.raw, *.bin)
- Raw Split (For example: *.001, *.002, *.aa, *.ab, etc)
- EnCase (For example: *.e01, *.e02, etc)
- Virtual Machines (For example: *.vmdk, *.vhd)



To add a disk image:

1. Choose "Disk Image or VM File" from the data source types.
2. Browse to the first file in the disk image. You need to specify only the first file and Autopsy will find the rest.
3. Choose the timezone that the disk image came from. This is most important for when adding FAT file systems because it does not store timezone information and Autopsy will not know how to normalize to UTC.
4. Choose to perform orphan file finding on FAT file systems. This can be a time intensive process because it will require that Autopsy look at each sector in the device.
5. Optionally choose the sector size. The Auto Detect mode will work correctly on the majority of images, but if adding the data source fails you may want to try the other sector sizes.

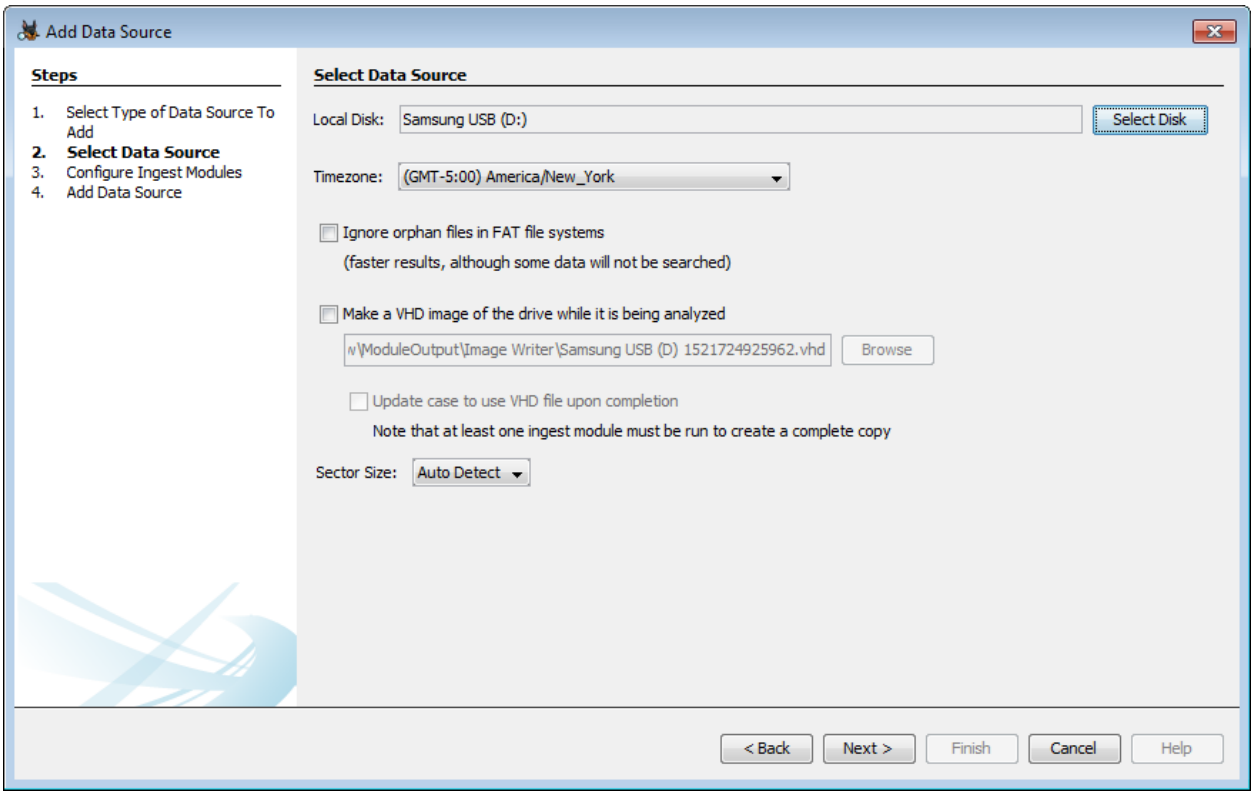
Adding a Local Disk

Autopsy can analyze a local disk without needing to first make an image copy of it. This is most useful when analyzing a USB-attached device through a write blocker.

Note that if you are analyzing a local disk that is being updated, then Autopsy will not see files that are added after you add it as a data source.

You will need to be running Autopsy as an Administrator to view all devices.

There is an option to make a copy of the local disk as a VHD during analysis. This VHD can be loaded in Windows or analyzed through Autopsy. There is an additional option to update the image path in the case database to this newly created file. Enabling this option will allow you to browse the case data normally even after the local disk is removed. Note that at least one ingest module must successfully run in order to generate the complete image copy.



To add a local drive:

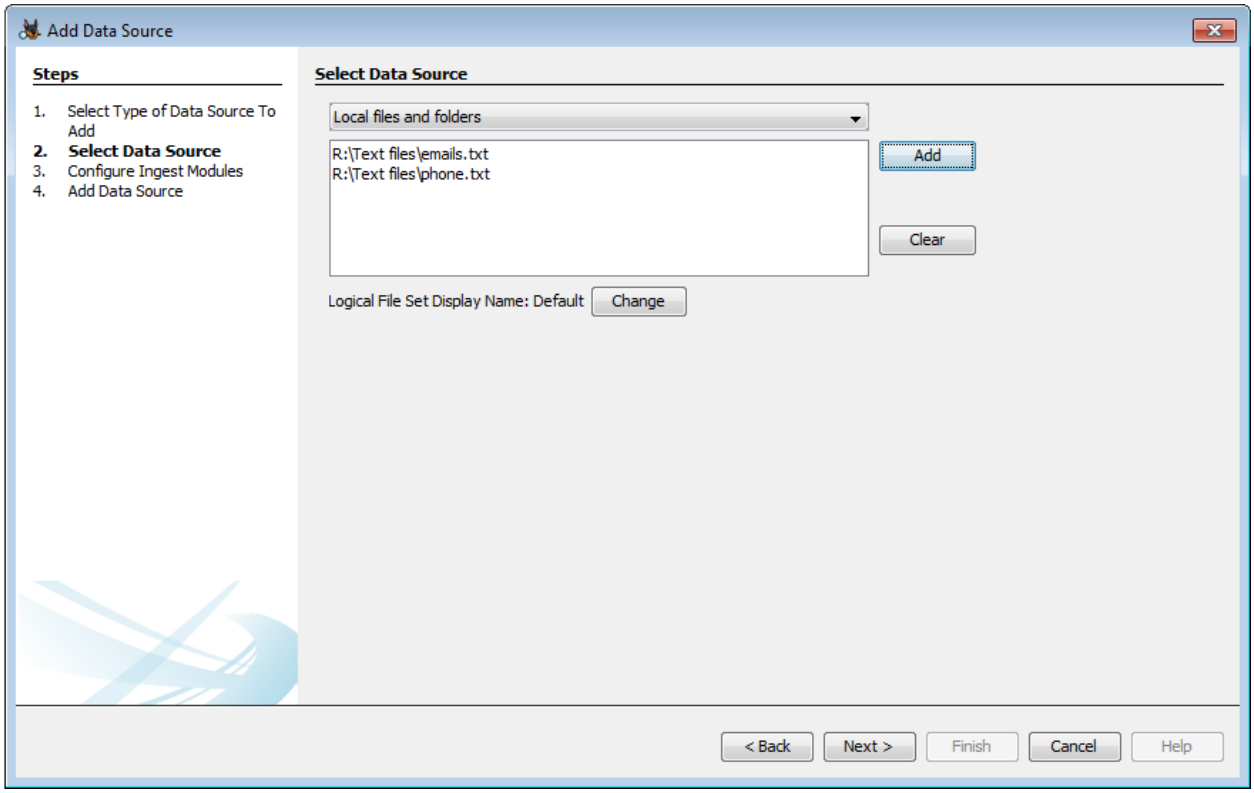
1. Choose "Local Disk" from the data source types.
2. Use the "Select Disk" button to open a dialog showing the local disks. This may take a minute to load. Then select the device from the list.
3. Choose to perform orphan file finding. See comment in **Adding a Disk Image** about this setting.
4. Choose whether to create a VHD copy of the local disk and whether to update the image path.
5. Optionally choose the sector size. The Auto Detect mode will work correctly on the majority of images, but if adding the data source fails you may want to try the other sector sizes.

Adding a Logical File

You can add files or folders that are on your local computer (or on a shared drive) without putting them into a disk image. This is useful if you have only a collection of files that you want to analyze.

Some things to note when doing this:

- Autopsy ignores the time stamps on files that it adds this way because they could be the timestamps when they were copied onto your examination device.
- If you have a USB-attached device that you are analyzing and you choose to add the device's contents using this method, then note that it will not look at unallocated space or deleted files. Autopsy will only be able to see the allocated files. You should add the device as a "Logical Drive" to analyze the unallocated space.
- You can modify the name of the Logical File Set from the default LogicalFileSet# by clicking the "Change" button as shown in the screenshot below:



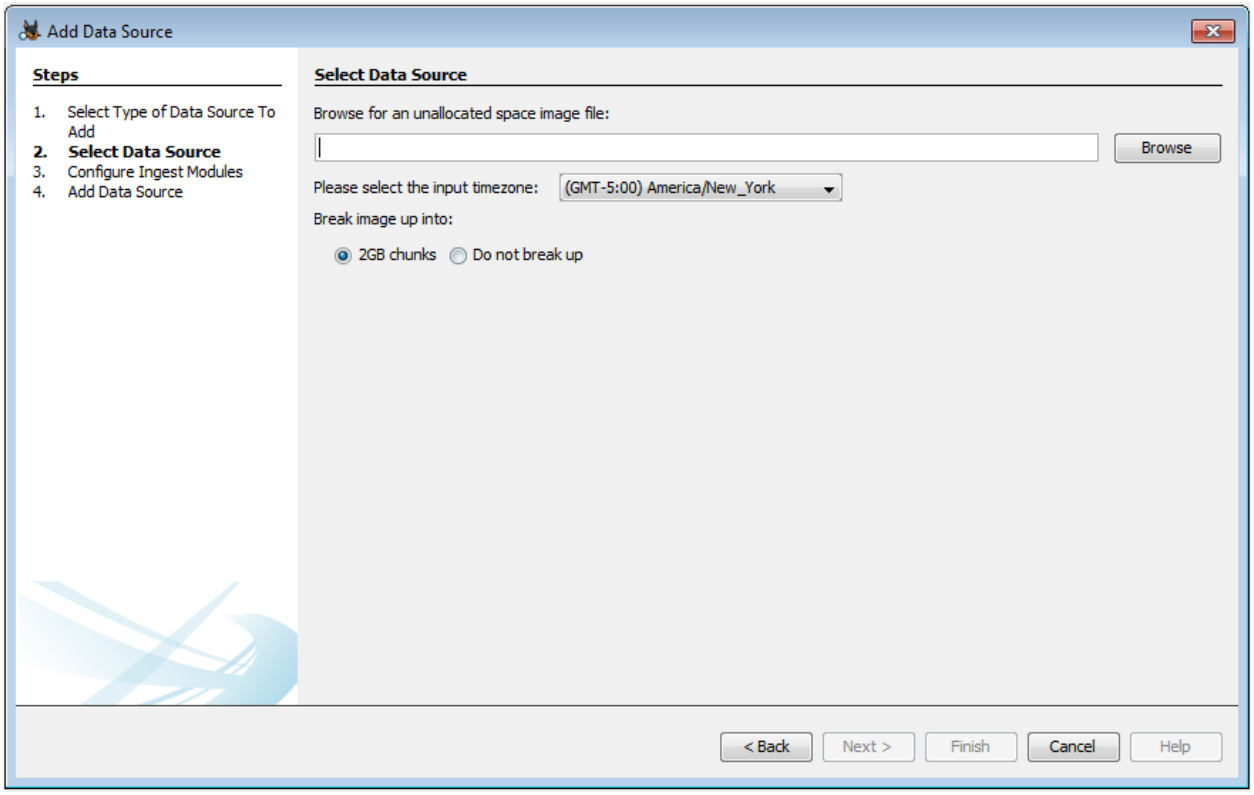
To add logical files:

1. Choose "Logical Files" from the data source types.
2. Leave the top combo box on "Local files and folders"
3. Press the "Add" button and navigate to a folder or file to add. Choosing a folder will cause all of its contents (including sub-folders) to be added.
4. Continue to press "Add" until all files and folders have been selected.

All of the files that you added in the panel will be grouped together into a single data source, called "LogicalFileSet" in the main UI.

There is also limited support for logical evidence (L01) files. To add one as a data source, select "Logical evidence file (L01)" in the top combo box and then browse to your file.

Adding an Unallocated Space Image File



To add unallocated space image files:

1. Choose "Unallocated Space Image File" from the data source types.
2. Browse to the file.
3. Choose whether to break the image up into chunks. Breaking the image up will give better performance since the chunks can be processed in parallel, but there is a chance that keywords or carved files that span chunk boundaries will be missed.

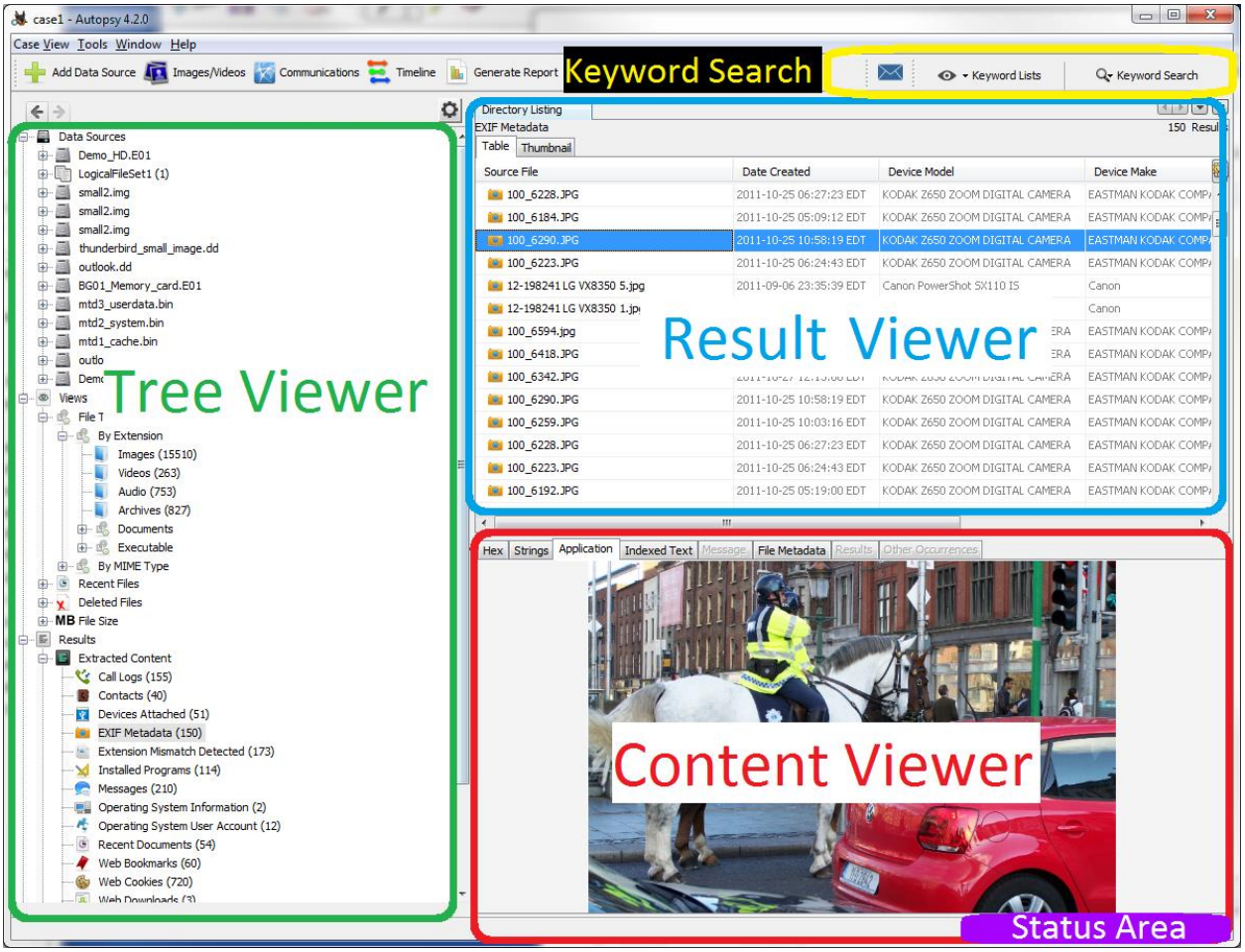
UI Layout

Overview

The major areas in the Autopsy User Interface (UI) are:

- **Tree Viewer**, shown outlined in green below
- **Result Viewer**, shown outlined in blue below
- **Content Viewer**, shown outlined in red below
- **Keyword Search**, shown outlined in yellow below
- **Status Area**, shown in solid purple below

You can customize how data is shown in the UI through the **View Options** panel.



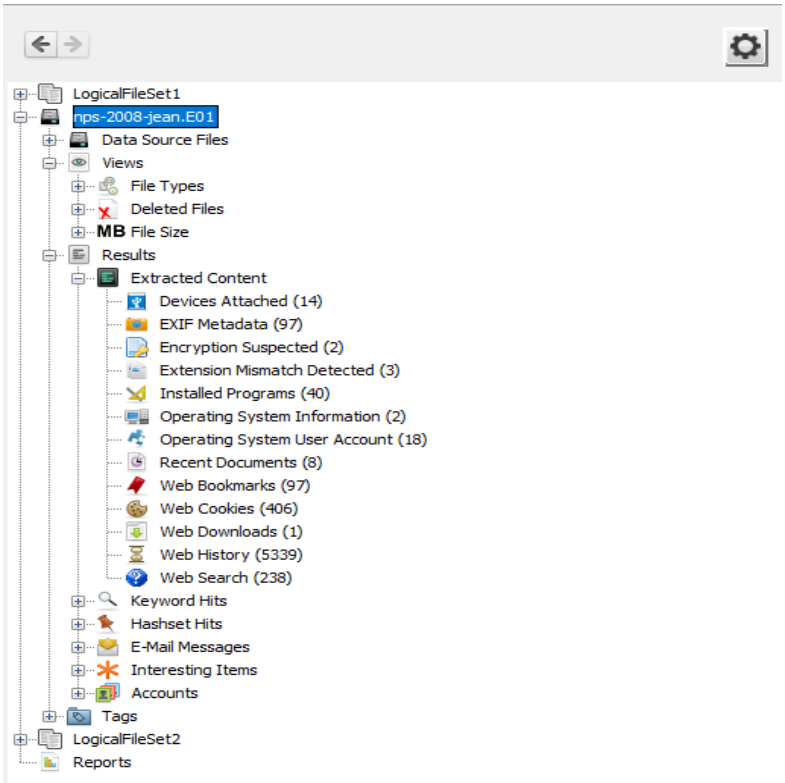
Tree Viewer

More...

The tree on the left-hand side is where you can browse the files in the image and find saved results from automated procedures (ingest). The tree has five main areas:

- **Data Sources:** This shows the directory tree hierarchy of the file systems in the images. You can navigate to a specific file or directory here. Each data source added is represented as a drive. If you add a data source multiple times, it shows up multiple times.
- **Views:** Specific types of files from the data sources are shown here, aggregated by type or other properties. Files here can come from more than one data source. Look here for files of a specific type or property.
- **Results:** Where you can see the results from the background ingest tasks and you can see your previous search results. Go here to see what was found by the ingest modules and to find your previous search results.
- **Tags:** Where files and results that have been **tagged** are shown
- **Reports:** References to reports that you have generated or that ingest modules have created show up here

You can also use the "Group by data source" option available through the **View Options** to move the views, results, and tags subtrees under their corresponding data sources. This can be helpful on very large cases to reduce the size of each node.



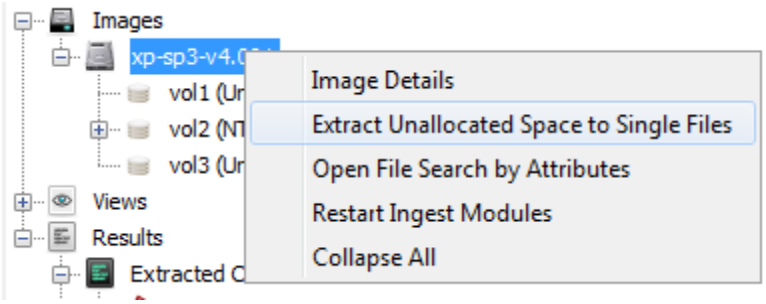
Data Sources

The Data Sources section shows each data source that has been added to the case, in order added (top one is first). Right clicking on the various nodes in the Data Sources section of the tree will allow you to get more options for each data source and its contents.

Unallocated space is chunks of the file system that is currently not being used for anything. Unallocated space can store deleted files and other interesting artifacts. On the actual image, Unallocated space is stored in blocks with distinct locations on the system. However, because of the way various carving tools work, it is more ideal to feed them a single, large unallocated file. Autopsy provides access to both methods of looking at unallocated space.

- **Individual blocks in a volume** There is a folder named "Unalloc". This folder contains all the individual unallocated blocks as the image is storing them. You can right click and extract them the same way you can extract any other type of file in the Directory Tree.
- **Single files** Right click on a volume and select "Extract Unallocated Space as Single File" to concatenate all the unallocated files in the volume into a single, continuous file. (If desired, you can right click on an image, and select "Extract Unallocated Space to Single Files" which will do the same thing, but once for each volume in the image).

An example of the single file extraction option is shown below.



Views

Views filter all the files in the case by some external property of the file, not by any internal analysis of the file.

- **File Type** Sorts files by file extension or MIME type, and shows them in the appropriate group. For example, .mp3 and .wav both end up in the "Audio" group.
- **Recent Files** Displays files that are accessed within the last seven days the user had the device.
- **Deleted Files** Displays files that have been deleted but the names have been recovered.
- **File Size** Sorts files based upon size. This can give you an idea where to look for files you are interested in.

Results

- **Extracted Content:** Many ingest modules will place results here; EXIF data, GPS locations, or Web History for example
- **Keyword Hits:** Keyword search hits show up here
- **Hashset Hits:** Hashset hits show up here
- **E-Mail Messages:** Email messages show up here
- **Interesting Items:** Things deemed interesting show up here
- **Accounts:** Credit card accounts show up here
- **Tags:** Any item you tag shows up here so you can find it again easily

Reports

Reports can be added by **Ingest Modules** or created using the **Reporting** tool.

Result Viewer

More...

The Result Viewer windows are in the upper right area of the interface and display the results from selecting something in the tree. You will have the option to display the results in a variety of formats.

Right Click Functions

Viewers in Result Viewers have certain right-click functions built-in into them that can be accessed when a node a certain type is selected (a file, directory or a result). Here are some examples that you may see:

- Open File in External Viewer: Opens the selected file in an "external" application as defined by the local OS or through the External Viewer tab on the Options menu. For example, HTML files may be opened by IE or Firefox, depending on what the local system is configured to use.
- View in New Window: Opens the content in a new internal Content Viewer (instead of in the default location in the lower right).
- Extract: Make a local copy of the file or directory for further analysis.
- Search for files with the same MD5 Hash: Searches the entire file-system for any files with the same MD5 Hash as the one selected.

Thumbnail Result Viewers

Thumbnail Results Viewer displays the data catalog as a table of thumbnail images in adjustable sizes. This viewer only supports picture files (Currently, only supports JPG, GIF, and PNG formats). Click the Thumbnail tab to select this view. Note that for a large number of images in a directory selected in the Data Explorer, or for a View selected that contains a large number of images, it might take a while to populate this view for the first time before the images are cached.

Example
Below is an example of "Thumbnail Results Viewer" window:

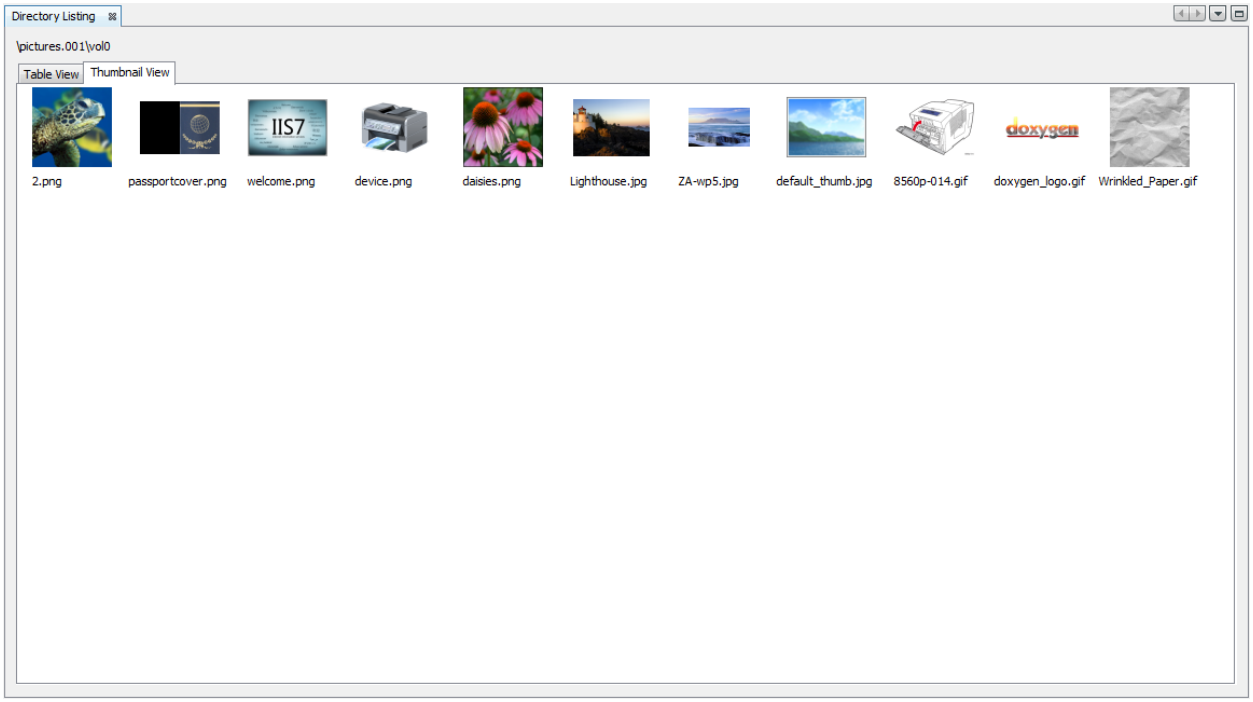
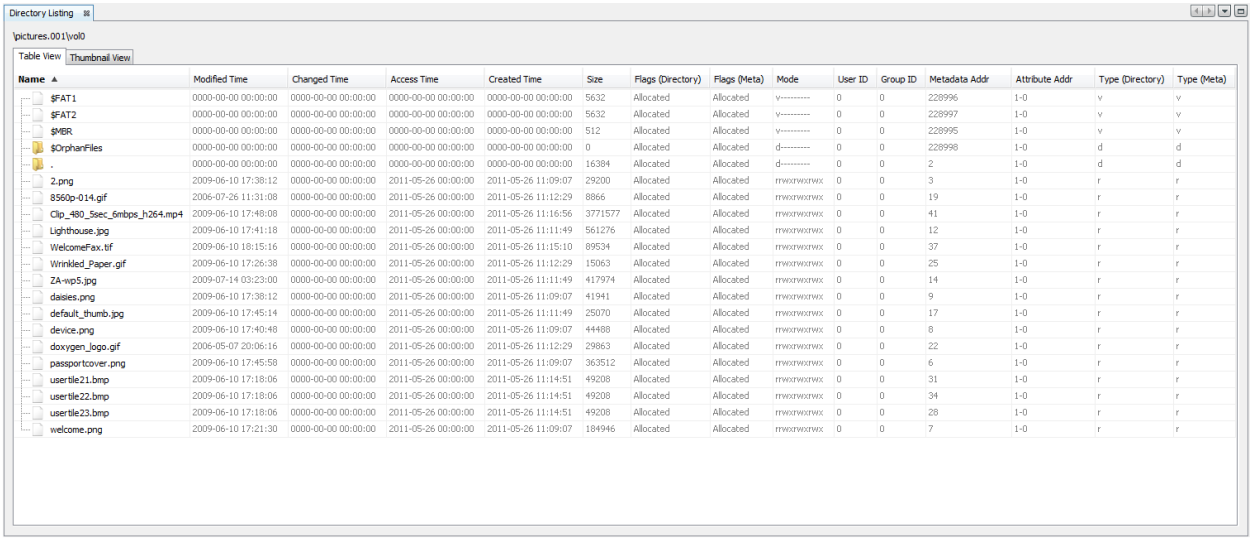


Table Result Viewers

Table Results Viewer (Directory Listing) displays the data catalog as a table with some details (properties) of each file. The properties that it shows are: name, time (modified, changed, accessed, and created), size, flags (directory and meta), mode, user ID, group ID, metadata address, attribute address, and type (directory and meta). Click the Table Viewer tab to select this view.

The Results Viewer can be also activated for saved results and it can show a high level results grouped, or a results at a file level, depending on which node on the Directory Tree is selected to populate the Table Results Viewer.

Example
Below is an example of a "Table Results Viewer" window:



Name	Modified Time	Changed Time	Access Time	Created Time	Size	Flags (Directory)	Flags (Meta)	Mode	User ID	Group ID	Metadata Addr	Attribute Addr	Type (Directory)	Type (Meta)
$FAT1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5632	Allocated	Allocated	v---------	0	0	228996	1-0	v	v
$FAT2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5632	Allocated	Allocated	v---------	0	0	228997	1-0	v	v
$MBR	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	v---------	0	0	228995	1-0	v	v
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d---------	0	0	228998	1-0	d	d
.	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Allocated	Allocated	d---------	0	0	2	1-0	d	d
2.png	2009-06-10 17:38:12	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:09:07	29200	Allocated	Allocated	rrwxrwxrwx	0	0	3	1-0	r	r
8560p-014.gif	2006-07-26 11:31:08	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:12:29	8866	Allocated	Allocated	rrwxrwxrwx	0	0	19	1-0	r	r
Clip_480_5sec_6mbps_h264.mp4	2009-06-10 17:48:08	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:16:56	3771577	Allocated	Allocated	rrwxrwxrwx	0	0	41	1-0	r	r
Lighthouse.jpg	2009-06-10 17:41:18	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:11:49	561276	Allocated	Allocated	rrwxrwxrwx	0	0	12	1-0	r	r
WelcomeFax.tif	2009-06-10 18:15:16	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:15:10	89534	Allocated	Allocated	rrwxrwxrwx	0	0	37	1-0	r	r
Wrinkled_Paper.gif	2009-06-10 17:26:38	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:12:29	15063	Allocated	Allocated	rrwxrwxrwx	0	0	25	1-0	r	r
ZA-wp5.jpg	2009-07-14 03:23:00	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:11:49	417974	Allocated	Allocated	rrwxrwxrwx	0	0	14	1-0	r	r
daisies.png	2009-06-10 17:38:12	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:09:07	41941	Allocated	Allocated	rrwxrwxrwx	0	0	9	1-0	r	r
default_thumb.jpg	2009-06-10 17:45:14	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:11:49	25070	Allocated	Allocated	rrwxrwxrwx	0	0	17	1-0	r	r
device.png	2009-06-10 17:40:48	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:09:07	44488	Allocated	Allocated	rrwxrwxrwx	0	0	8	1-0	r	r
doxygen_logo.gif	2006-05-07 20:06:16	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:12:29	29863	Allocated	Allocated	rrwxrwxrwx	0	0	22	1-0	r	r
passportcover.png	2009-06-10 17:45:58	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:09:07	363512	Allocated	Allocated	rrwxrwxrwx	0	0	6	1-0	r	r
usertile21.bmp	2009-06-10 17:18:06	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:14:51	49208	Allocated	Allocated	rrwxrwxrwx	0	0	31	1-0	r	r
usertile22.bmp	2009-06-10 17:18:06	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:14:51	49208	Allocated	Allocated	rrwxrwxrwx	0	0	34	1-0	r	r
usertile23.bmp	2009-06-10 17:18:06	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:14:51	49208	Allocated	Allocated	rrwxrwxrwx	0	0	28	1-0	r	r
welcome.png	2009-06-10 17:21:30	0000-00-00 00:00:00	2011-05-26 00:00:00	2011-05-26 11:09:07	184946	Allocated	Allocated	rrwxrwxrwx	0	0	7	1-0	r	r

Content Viewer

More...

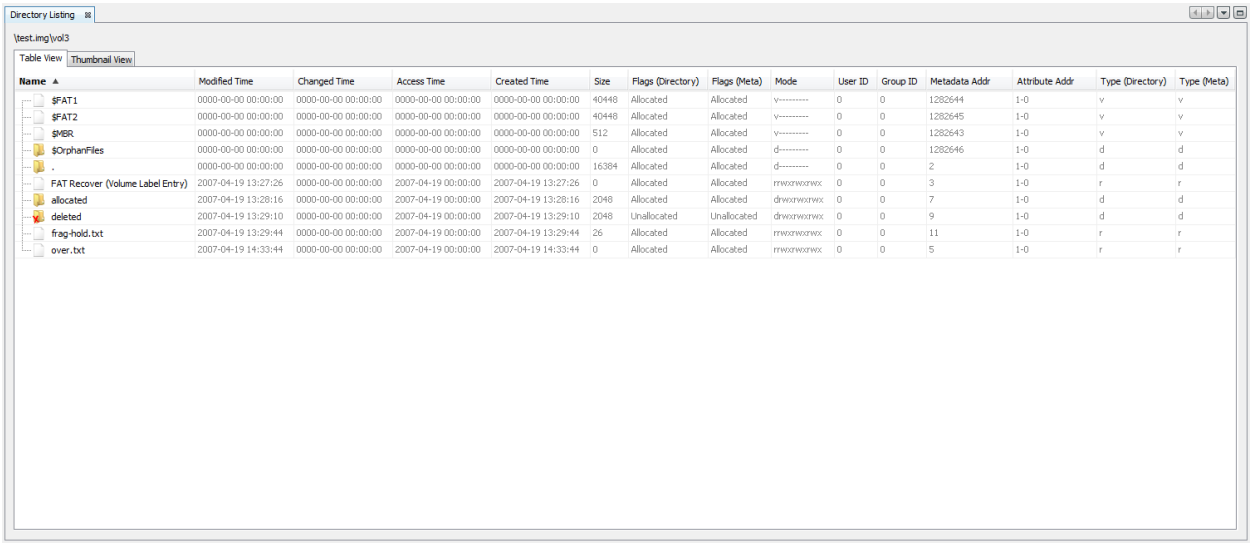
The Content Viewer area is in the lower right area of the interface. This area is used to view a specific file in a variety of formats. There are different tabs for different viewers. Not all tabs support all file types, so only some of them will be enabled. To display data in this area, a file must be selected from the Result Viewer window.

The Content Viewer area is part of a plug-in framework. You can install modules that will add more viewer types. This section describes the viewers that come by default with Autopsy.

Result Content Viewer

Content Viewer shows the artifacts (saved results) associated with the item selected in the Result Viewer.

Example Below is an example of "Result Content Viewer" window:

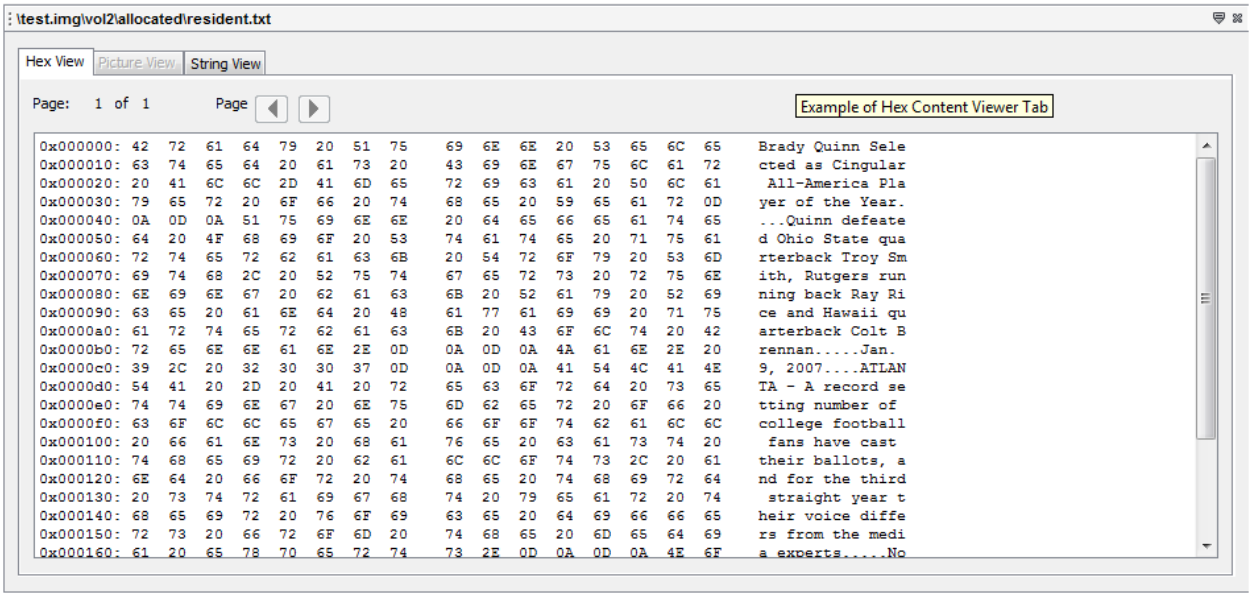


Hex Content Viewer

Hex Content Viewer shows you the raw and exact contents of a file. In this Hex Content Viewer, the data of the file is represented as hexadecimal values grouped in 2 groups of 8 bytes, followed by one group of 16 ASCII characters which are derived from each pair of hex values (each byte). Non-printable ASCII characters and characters that would take more than one character space are typically represented by a dot (".") in the following ASCII field.

Example

Below is an example of "Hex Content Viewer" window:



Media Content Viewer

The Media Content Viewer will show a picture or video file. Video files can be played and paused. The size of the picture or video will be reduced to fit into the screen. If you want more complex analysis of the media, then you must export the file.

If you select an non-picture file or an unsupported picture format on the "Result Viewers", this tab will be disabled.

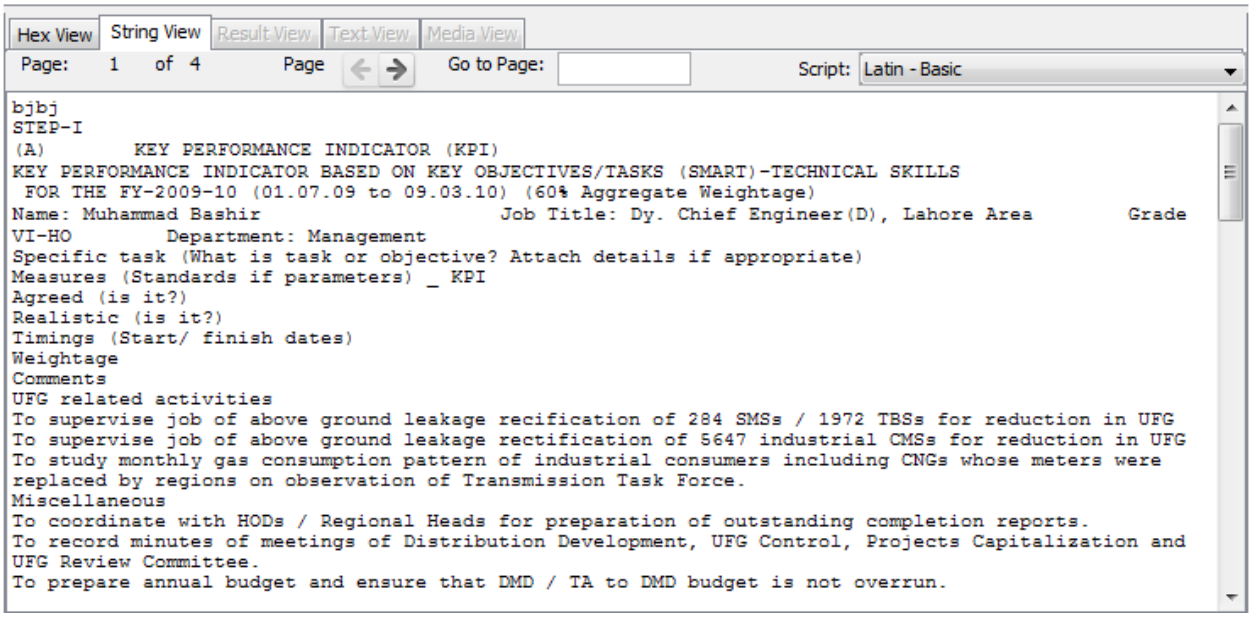
Example
Here's one of the example of the "Media Content Viewer":

String Content Viewer

The String Content Viewer scans (potentially binary) data of the file / folder and searches it for data that could be text. When appropriate data is found, the String Content Viewer shows data strings extracted from binary, decoded, and interpreted as UTF8/16 for the selected script/language.

Note that this is different from the Text Content Viewer, which displays the text for a file that is stored in the keyword search index. The results may be the same or they could be different, depending how the data is interpreted by the indexer.

Example
Below is an example of "String Content Viewer" window:

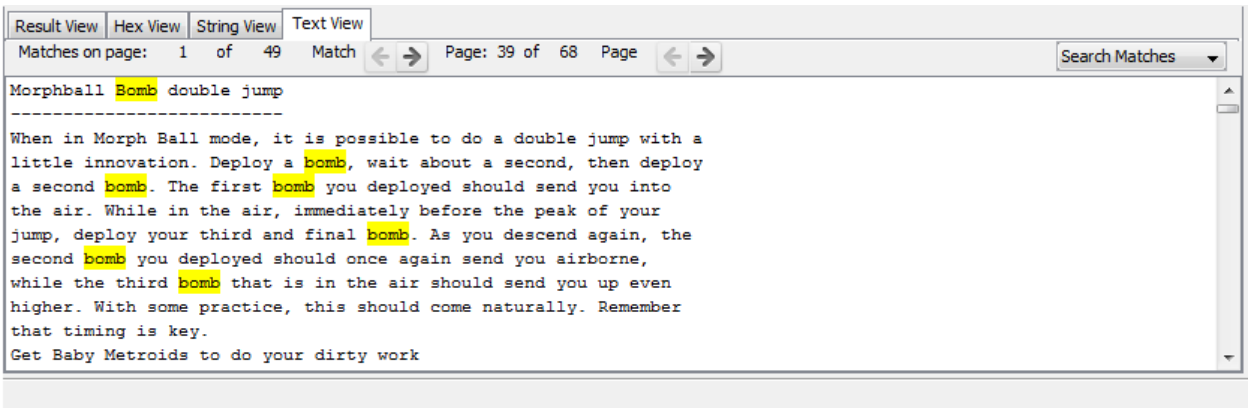


Text Content Viewer

Text Content Viewer uses the keyword search index that may have been populated during Image Ingest. If a file has text stored in the index, then this tab will be enabled and it will be displayed to the user if a file or a result associated with a file is selected.

This tab may have more text on it than the "String View", which relies on searching the file for text-looking data. Some files, like PDF, will not have text-looking data at the byte-level, but the keyword indexing process knows how to interpret a PDF file and produce text. For the files the indexer knows about, there may be the METADATA section at the end of the displayed extracted text. If an indexed document contains any metadata (such as creation date, author, etc), it will be displayed there. Note that, unlike the "String View", the Text View does not have its built-in settings for the script/language to use for extracted strings. This is because the script/language is used at indexing time, and that setting is associated with the Keyword Search indexer, not the viewer.

If this tab is not enabled, then either the file has no text or you did not enable Keyword Search as an ingest module. Note that this viewer is also used to display highlighted keyword hits when operated in the "Search Matches" mode, selected on the right-hand side of the viewer's toolbar.



Keyword Search

Keyword Search allows the user to search for keywords in the data source. It is covered in more detail here: **Keyword Search Module**

Status Area

The Status area will show progress bars while ingest is occuring. This visually indicates to the user what portion of the processing is already complete. The user can click on the progress bars to see further detail or to cancel ingest jobs.

Automated Analysis (Modules)

Ingest Modules

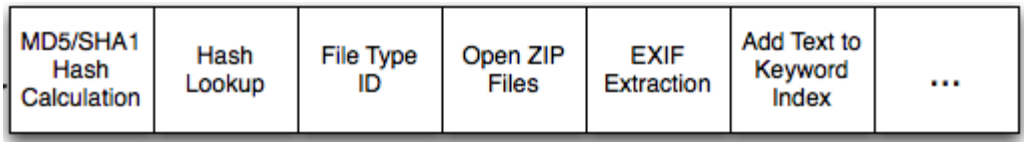
Ingest modules analyze the data in a data source. They perform all of the analysis of the files and parse their contents. Examples include **hash calculation and lookup**, **keyword searching**, and **web artifact extraction**.

Immediately after you add a data source to a case (see **Data Sources**), you will be presented with a dialog to configure the ingest modules to run on it. Once configured, they will run in the background and provide you real-time results when they find relevant information.

This page covers the use of ingest modules. Specific pages will cover the configuration of specific modules. See **Installing 3rd-Party Modules** for details on installing 3rd-party ingest modules.

Multi-threaded and Priority

Ingest modules are configured to find user content quickly. The ingest modules are grouped into pipelines and each file goes down the pipeline, module by module. A pipeline may have modules in the following order:



Multiple pipelines may be running at the same time. By default, two pipelines are running, but you can add more depending on how many cores you have on your system. You can configure the number of pipelines to make in the "Tools", "Options", "General" area.

Autopsy prioritizes user content over other types of files and will send data from the "Documents and Settings" folder or "Users" folder into the pipelines before the "Windows" folder. It prioritizes each folder in the system to ensure that user content is analyzed before other content.

Running Ingest Modules

There are two ways to start ingest modules:

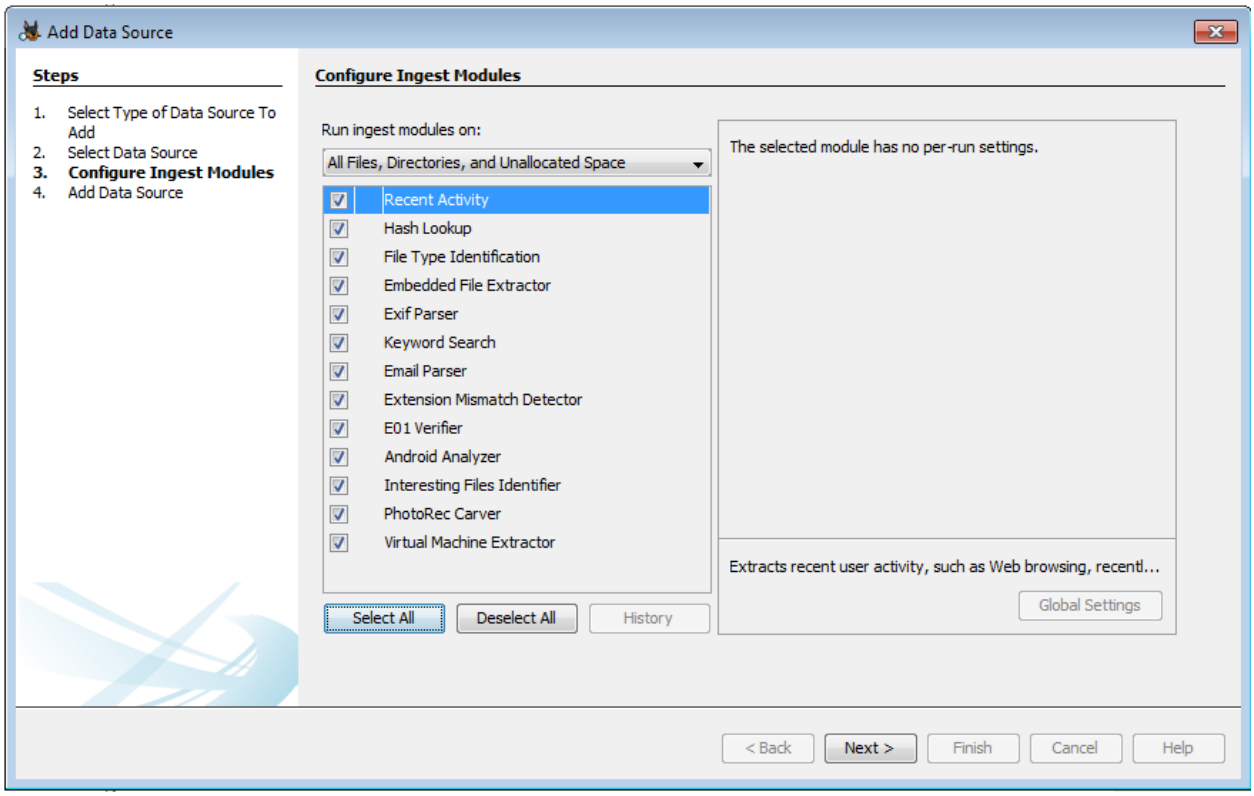
1. Immediately after you add a data source
2. By right-clicking on a data source from the tree in the main interface and choosing "Run Ingest Modules"

Once ingest is started, you can review the currently running ingest tasks in the task bar on the bottom-right corner of the main window. The ingest tasks can be cancelled by the user if so desired.

Note: sometimes the cancellation process may take several seconds or more to complete cleanly, depending on what the ingest module was currently doing.

Configuring Ingest Modules

You will be presented with an interface to configure the ingest modules. From here, you can choose which type of files to analyze and enable or disable each module. Some modules will have further configuration settings.



The selection box at the top controls which files the ingest modules will run on. The two built-in options are "All files, directories, and unallocated space" and "All Files and Directories."

The **Custom File Filters** section describes how to create custom file filters. The chosen filter applies to all ingest modules.

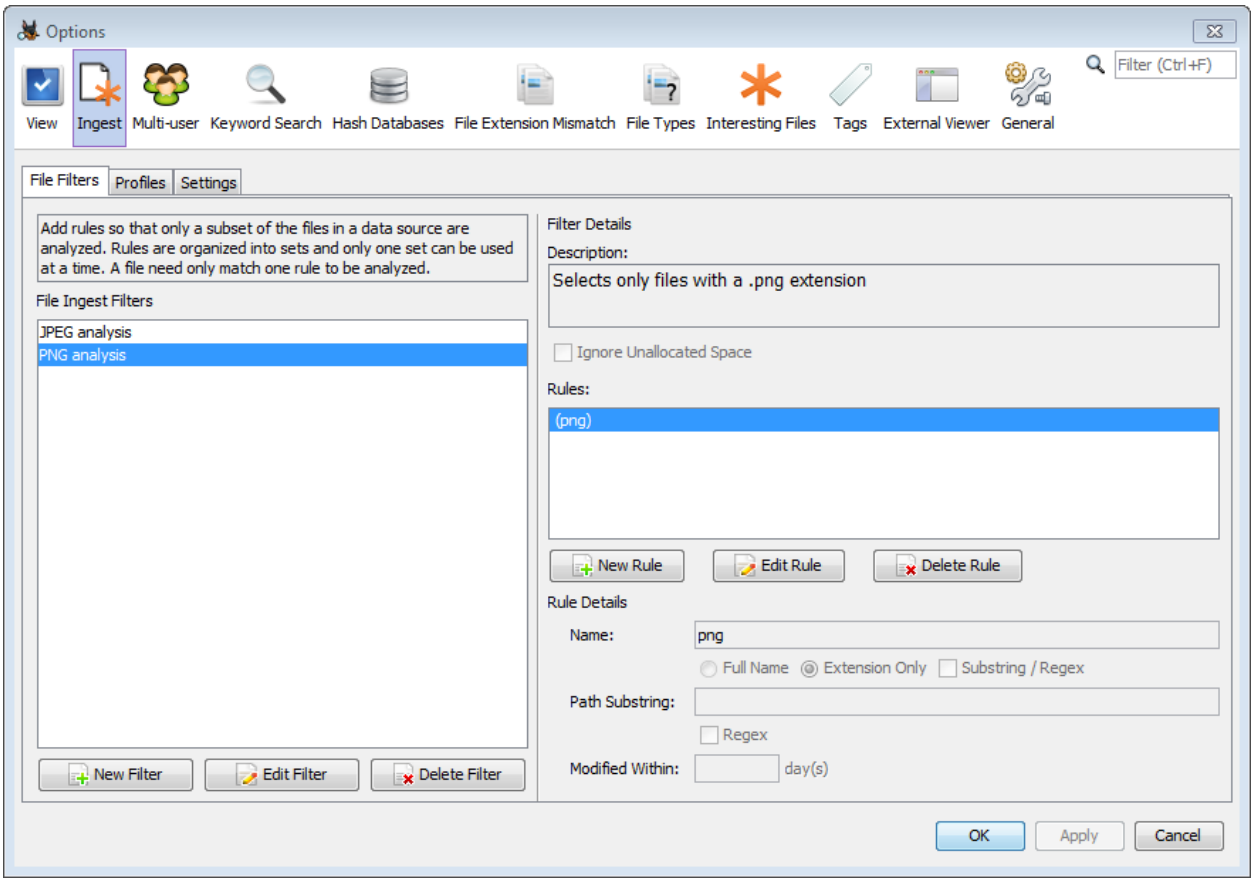
There are two places to configure ingest modules. When you select the module name, you may have some "run time" options to configure in the panel to the right. These are generally settings that you may want to change from image to image.

There may also be an "Advanced" button that is enabled in the lower corner. Pressing this button allows you to change global settings that are not specific to a single image. This advanced configuration panel can often be found in the "Tools", "Options" menu too.

As an example, the hash lookup module will allow you to enable or disable hash sets in the "run time" options panel, but requires you to go to the "Advanced" dialog to add or remove hash sets from the Autopsy configuration.

Custom File Filters

The file filters panel can be opened from the ingest module selection panel or through the Ingest tab on the main options panel. File filters allow ingest modules to be run on only a subset of the files. In the example below, a filter has been set up to only run on files with a "png" extension.

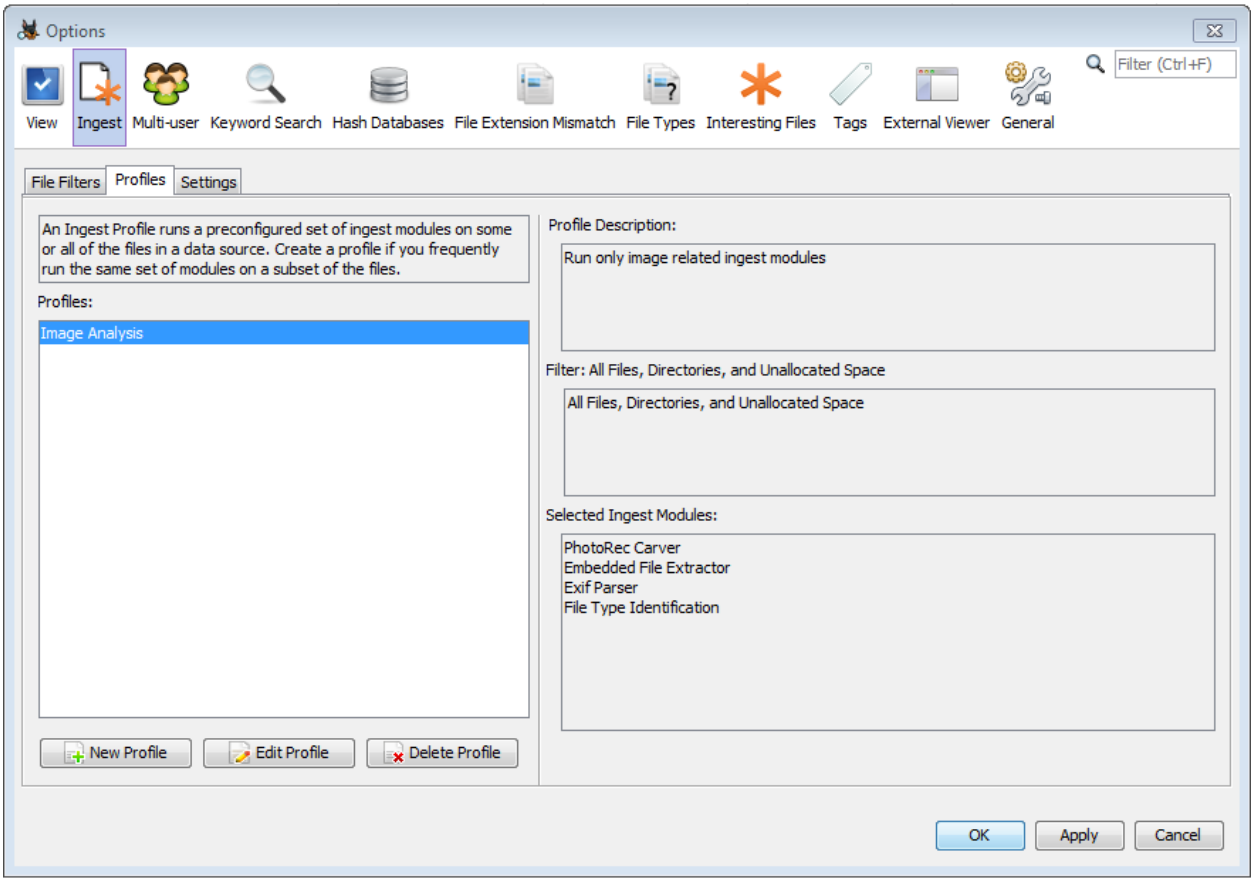


Each filter contains one or more rules for selecting files based on a combination of file name, path, and how recently the file was modified. Only one rule needs to match for the file to pass.

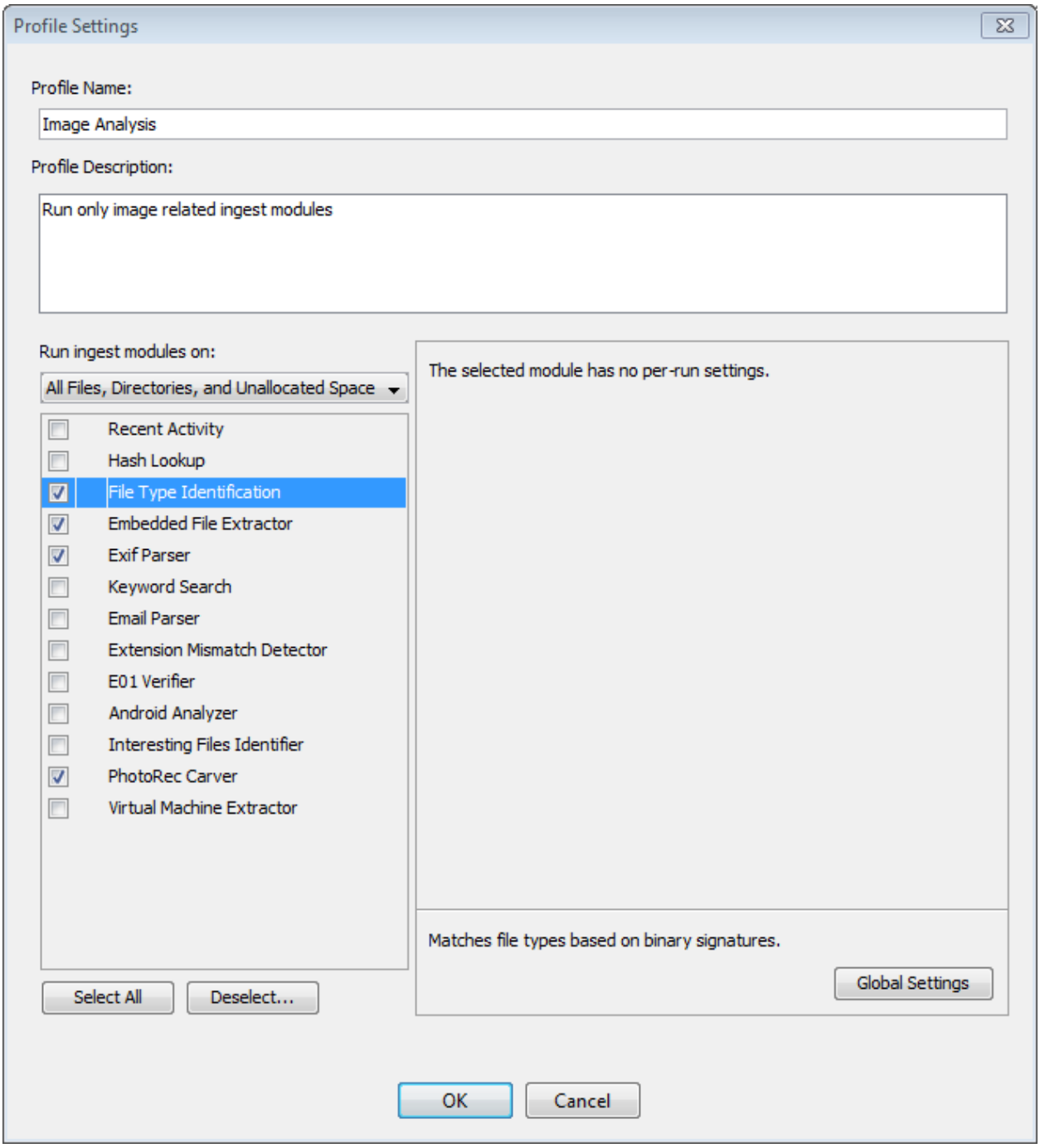
Additionally, you can enter multiple comma-separated file extensions. All files will still be displayed in the tree view, but the ingest modules will only run on a subset. If we use the previous example and run the hash module, only files ending in .png will have their hash computed.

Using Ingest Profiles

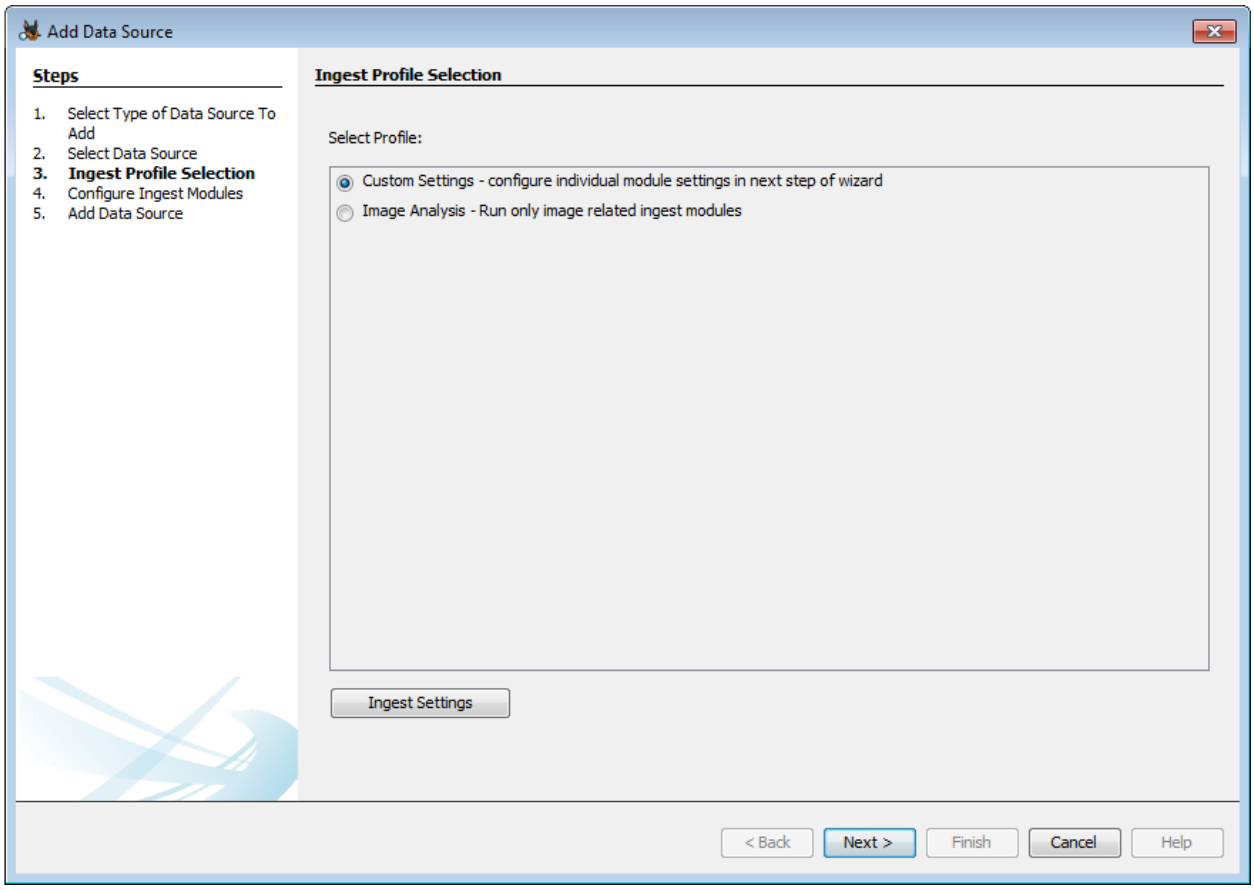
Ingest profiles allow you to quickly choose a defined set of ingest modules to run. This can be useful if you run different sets of ingest modules (or different configurations of those ingest modules) on different types of data. Ingest profiles can be configured through the Ingest tab on the options panel.



Each profile can specify different per-run settings for each ingest module, and you can choose use either a predefined or custom file filter (see **Custom File Filters**).



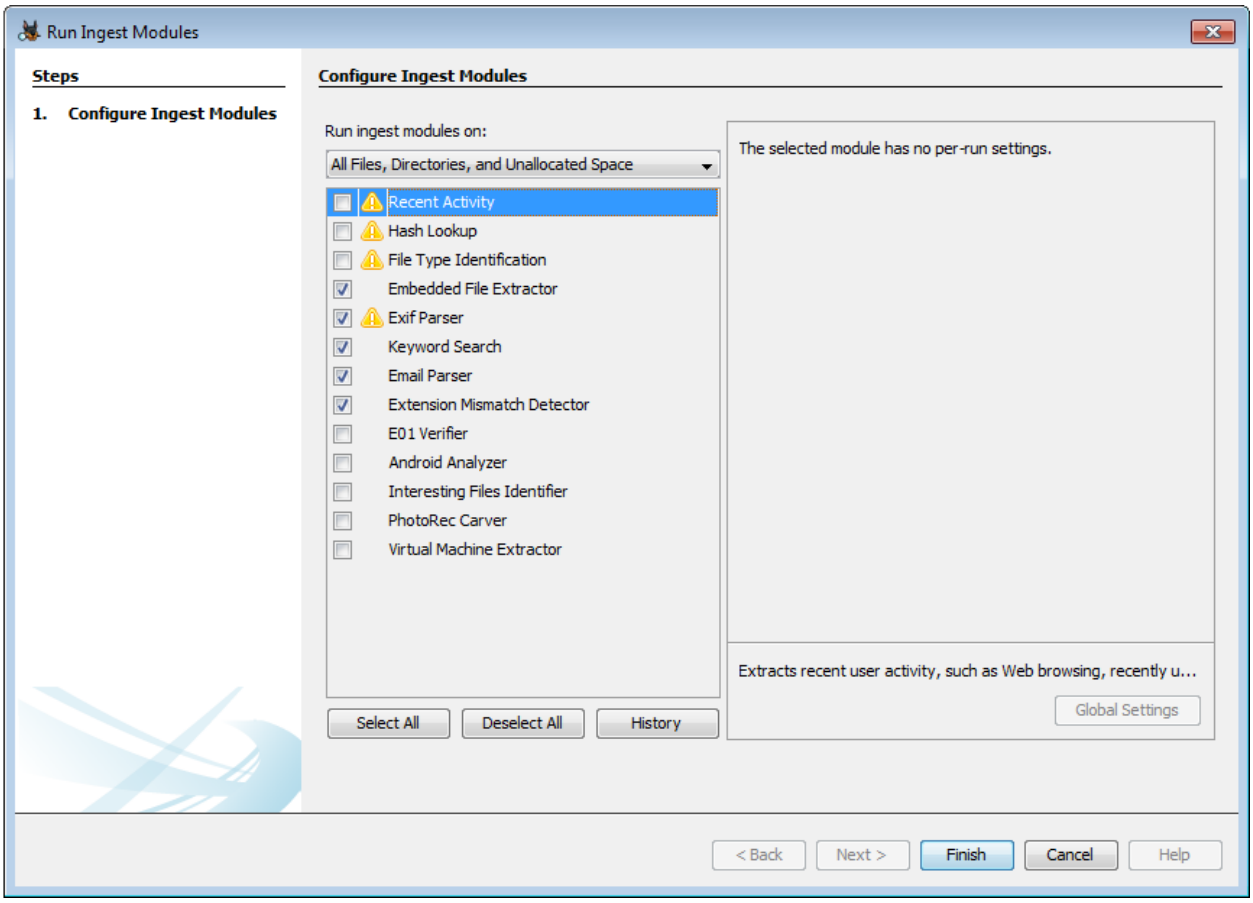
If any custom profiles are present, there will be a new screen in the add data source wizard.



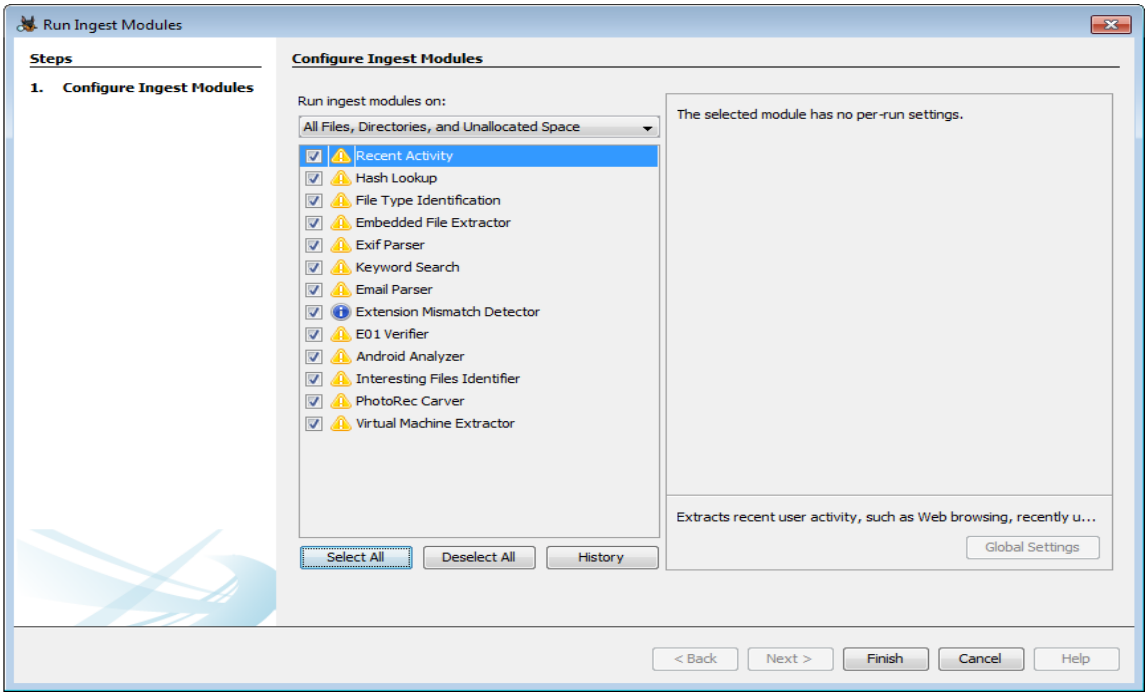
If you choose custom settings it will bring up the normal ingest module selection panel. If you choose a user-defined profile the ingest module screen will be skipped entirely and the ingest modules from that profile will be run on the data source. The profile selection panel will also appear when running ingest by right-clicking on a data source from the tree.

Notification of Ingest Already Run

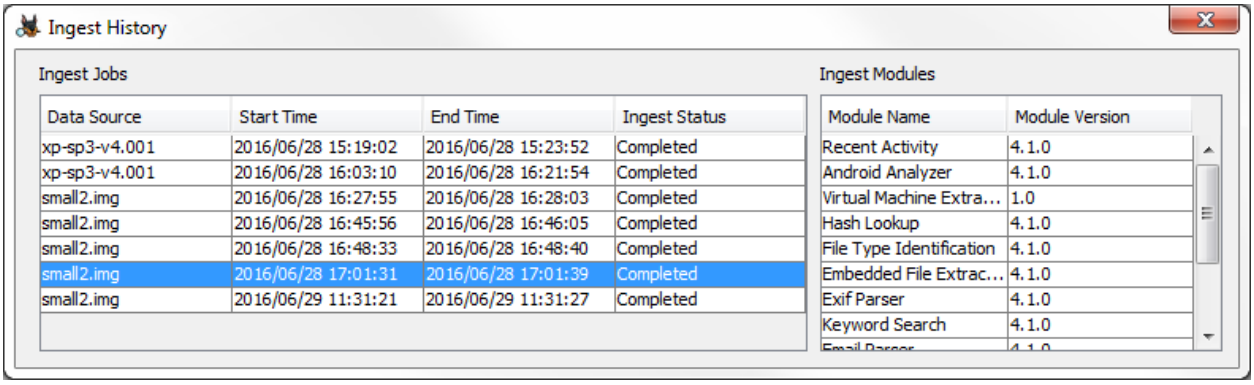
If an ingest module has already been run for a particular data source, you will see a triangular yellow icon with an exclaimation point next to the module in the "Run Ingest Modules" dialog, as shown in the screenshot below.



If an older version of an ingest module has been run for a particular data source, you will see a round blue icon with an "i" next to the module in the "Run Ingest Modules" dialog, as shown in the screenshot below.



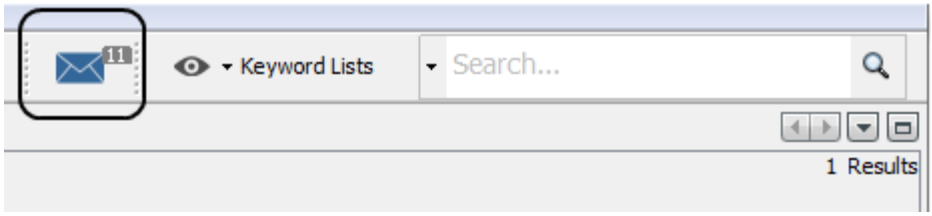
Clicking "View Ingest History" will show you the ingest history in tabular form, allowing you to see which modules were run on which data sources and when, as shown in the screenshot below.

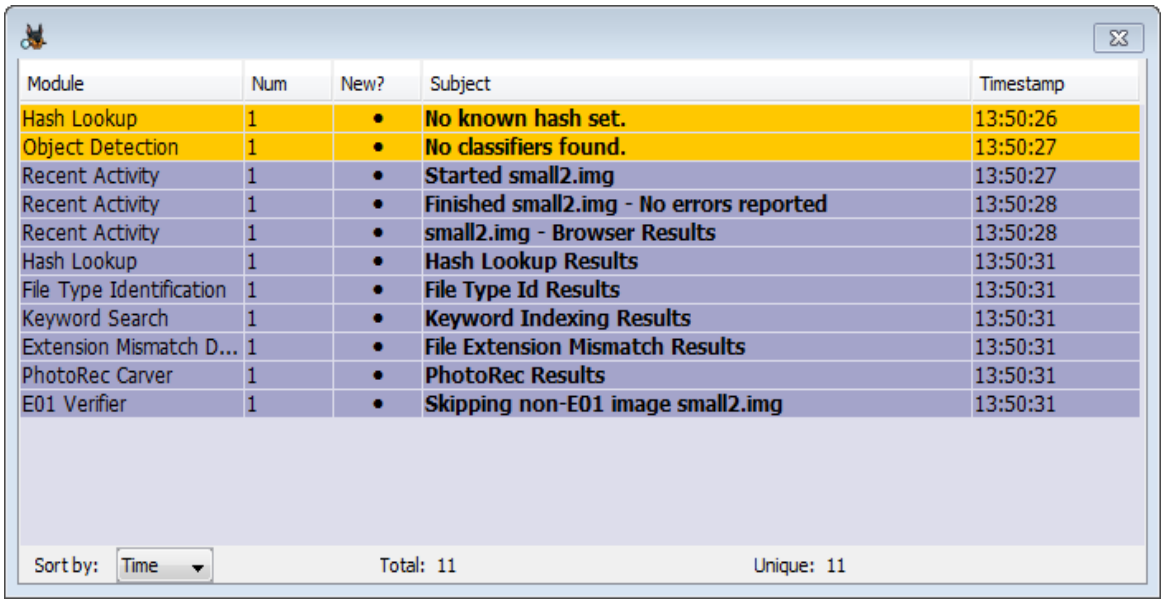


Viewing Ingest Module Results

Ingest modules run in the background. An ingest module can provide you results in a variety of ways, but we recommend specific methods:

1. If they post results to the Blackboard, then you will find them in the "Results" area of the tree in the main interface.
2. They can send a message to the Ingest Inbox so that you get a message each time something really important is found.



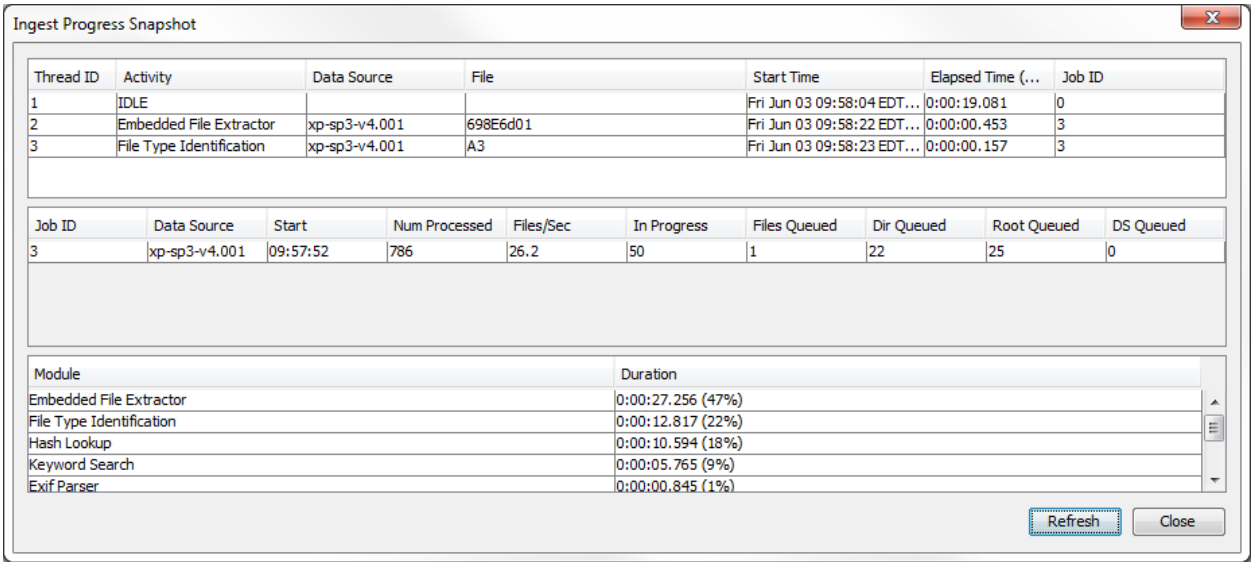


3. If the module is a wrapper around another forensics tool, they may simply provide a link to the output of that tool, in which case you will see a new entry in the "Reports" area of the tree.

All of the official Autopsy modules send results to the blackboard, but if you install third-party apps, then they may choose any approach – including a pop-up window each time they find something.

Viewing Ongoing Ingest Activity

While Ingest is running, one can use the "Ingest Progress Snapshot" tool to see what activity is going on at the moment. Click on "Help", "Get Ingest Progress Snapshot" to view the dialog shown in the screenshot below.



To refresh the view, use the "Refresh" button.

Recent Activity Module

What Does It Do?

The Recent Activity module extracts user activity as saved by web browsers (including web searches), installed programs, and the operating system. It also runs Regripper on the Registry hive.

This allows you to see what activity has occured in the last seven days of usage, what web sites were vistied, what the machine did, and what it connected to.

Configuration

There is nothing to configure for this module.

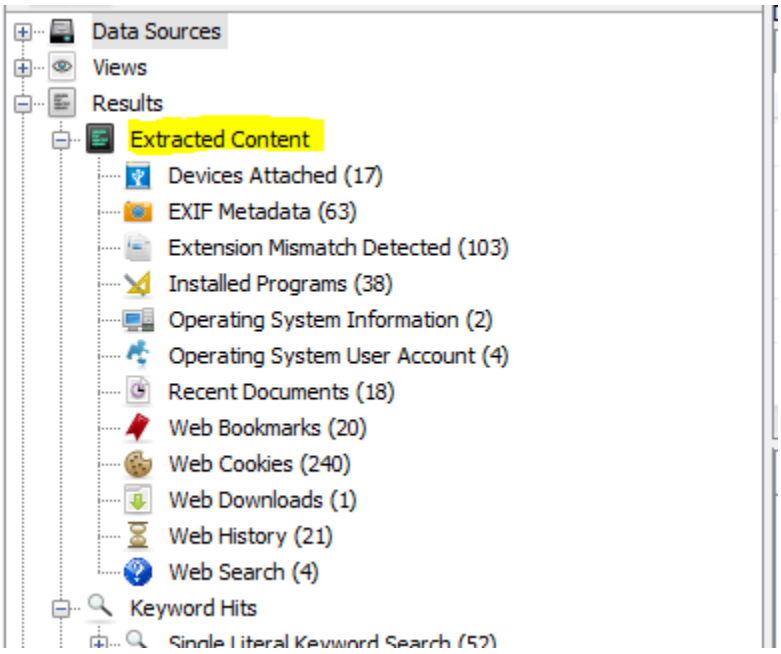
Using the Module

Ingest Settings

There are no run-time settings for this module.

Seeing Results

Results show up in the tree under "Extracted Content".



Hash Lookup Module

What Does It Do?

The Hash Lookup Module calculates MD5 hash values for files and looks up hash values in a database to determine if the file is notable, known (in general), or unknown.

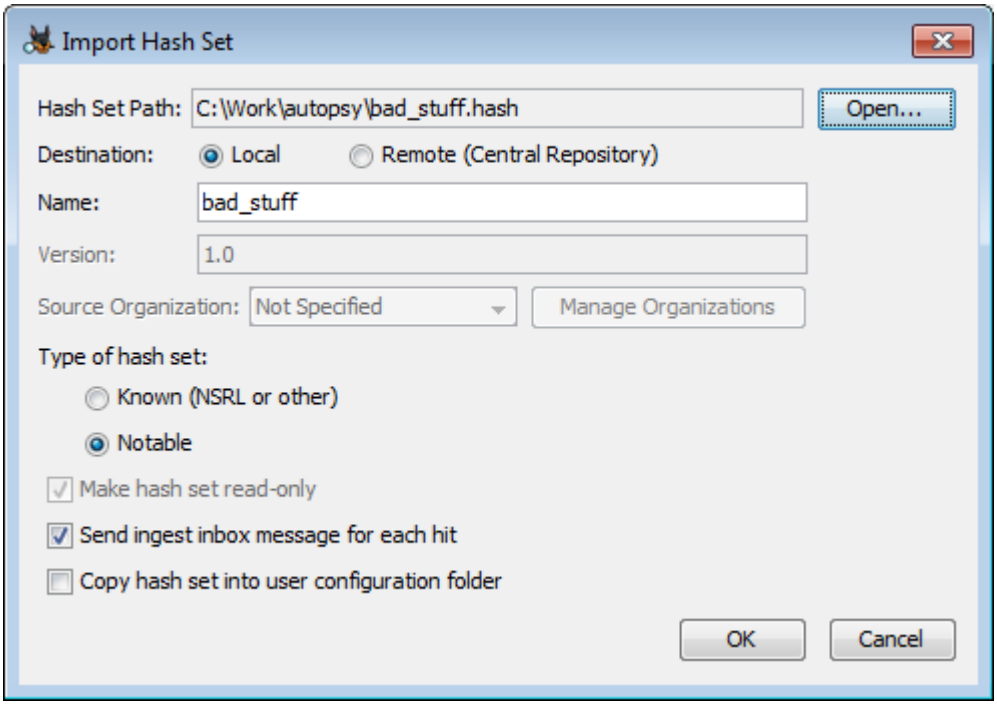
Configuration

The Hash Sets tab on the Options panel is where you can set and update your hash set information. Hash sets are used to identify files that are 'known' or 'notable'.

- Known good files are those that can be safely ignored. This set of files frequently includes standard OS and application files. Ignoring such uninteresting-to-the-investigator files, can greatly reduce image analysis time.
- Notable (or known bad) files are those that should raise awareness. This set will vary depending on the type of investigation, but common examples include contraband images and malware.

Importing Hash Sets

To import an existing hash set, use the "Import Database" button on the Hash Sets options panel. This will bring up a dialog to import the file.



Database Path - The path to the hash set you are importing. Autopsy supports the following formats:

- Text: One hash starting each line. For example, the output from running the md5, md5sum, or md5deep program on a set of files (*.txt)
- Index only: Generated by Sleuth Kit/Autopsy. The NSRL is available in this format for use with Autopsy (**see below**) (*.idx)
- Sleuth Kit/Autopsy format database: SQLite hash sets created by Autopsy (*.kdb)
- EnCase: An EnCase hash set file (*.hash)
- HashKeeper: Hash set file conforming to the HashKeeper standard (*.hsh)

Destination - The Destination field refers to where the hash set will be stored.

- Local: The hash set file will be used from original the location on disk
- Remote: The hash set will be copied into the **central repository**. When using a PostgreSQL central repository, this allows multiple users to easily share the same hash sets.

Name - Display name of the hash set. One will be suggested based on the file name, but this can be changed.

Version - The version of the hash set can only be entered when importing the hash set into the central repository. Additionally, no version can be entered if the hash set is not read-only.

Source Organization - The organization can only be entered when importing the hash set into the central repository. See the section on **managing organizations** for more information.

Type of database - All entries in the hash set should either be "known" (can be safely ignored) or "notable" (could be indicators of suspicious behavior).

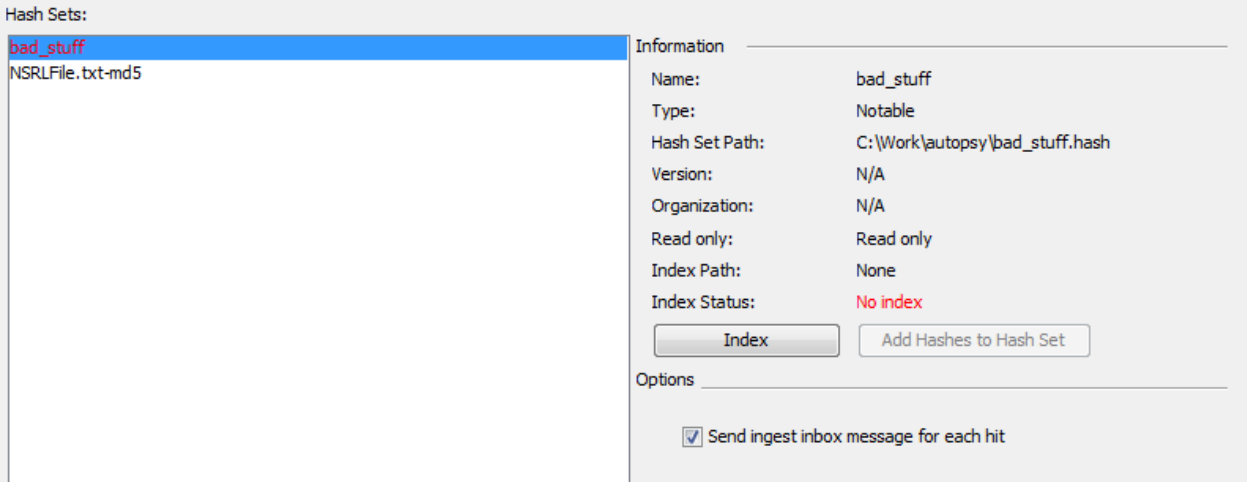
Make database read-only - The read-only setting is only active when importing the hash set into the central repository. A read-only database can not have new hashes added to it through either the Hash Sets options panel or the context menu. For locally imported hash sets, whether they can be written to is dependent on the type of hash set. Autopsy format databases (*.kdb) can be edited, but all other types will be read-only.

Send ingest inbox message for each hit - Determines whether a message is sent for each matching file. This can not be enabled for a "known" hash set.

Copy hash set into user configuration folder - Makes a copy of the hash set instead of using the existing one. This is intended to be used with a **Live Triage** drive.

Indexing

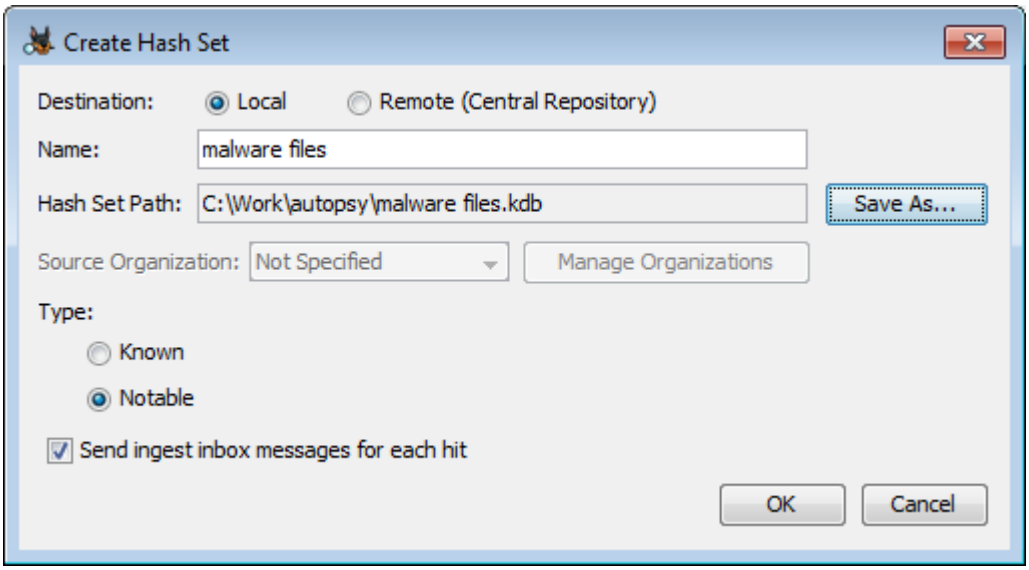
After importing the hash set, you may have to index it before it can be used. For most hash set types, Autopsy needs an index of the hash set to actually use a hash set. It can create the index if you import only the hash set. Any hash sets that require an index will be displayed in red, and their "Index Status" will indicate that an index needs to be created. This is done simply by using the Index button.



Autopsy uses the hash set management system from The Sleuth Kit. You can manually create an index using the 'hfind' command line tool or you can use Autopsy. If you attempt proceed without indexing a hash set, Autopsy will offer to automatically produce an index for you. You can also specify only the index file and not use the full hash set - the index file is sufficient to identify known files. This can save space. To do this, specify the .idx file from the Hash Sets option panel.

Creating Hash sets

New hash sets can be created using the "New Hash Set" button. The fields are mostly the same as the **import dialog** described above.



In this case, the Database Path is where the new database will be stored. If the central repository is being used then this field is not needed.

Using Hash Sets

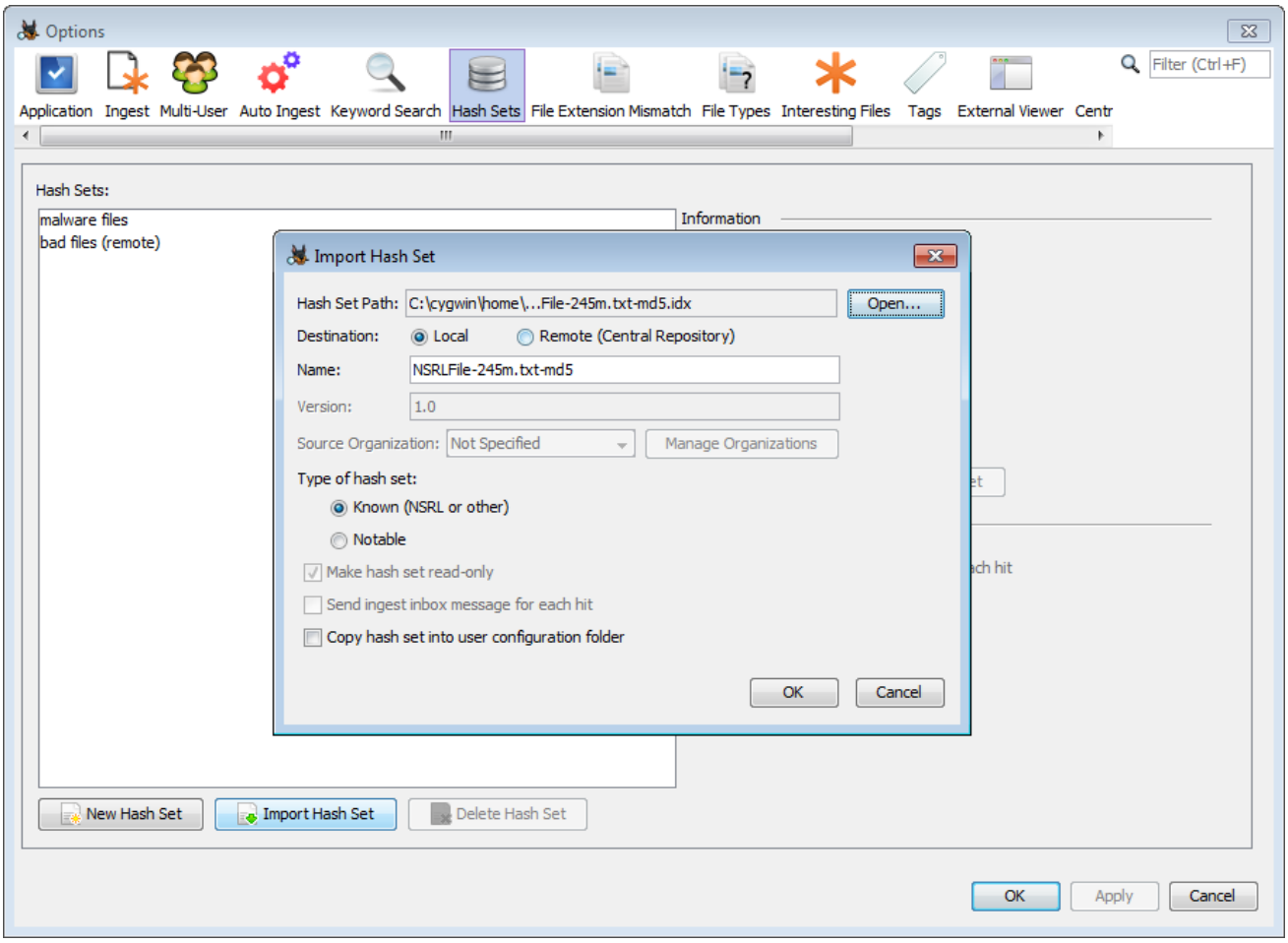
There is an **ingest module** that will hash the files and look them up in the hash sets. It will flag files that were in the notable hash set and those results will be shown in the Results tree of the **Tree Viewer**. Other ingest modules are able to use the known status of a file to decide if they should

ignore the file or process it. You can also see the results in the **File Search** window. There is an option to choose the 'known status'. From here, you can do a search to see all 'notable' files. From here, you can also choose to ignore all 'known' files that were found in the NSRL. You can also see the status of the file in a column when the file is listed.

NIST NSRL

Autopsy can use the NIST NSRL to detect 'known files'. The NSRL contains hashes of 'known files' that may be good or bad depending on your perspective and investigation type. For example, the existence of a piece of financial software may be interesting to your investigation and that software could be in the NSRL. Therefore, Autopsy treats files that are found in the NSRL as simply 'known' and does not specify good or bad. Ingest modules have the option of ignoring files that were found in the NSRL.

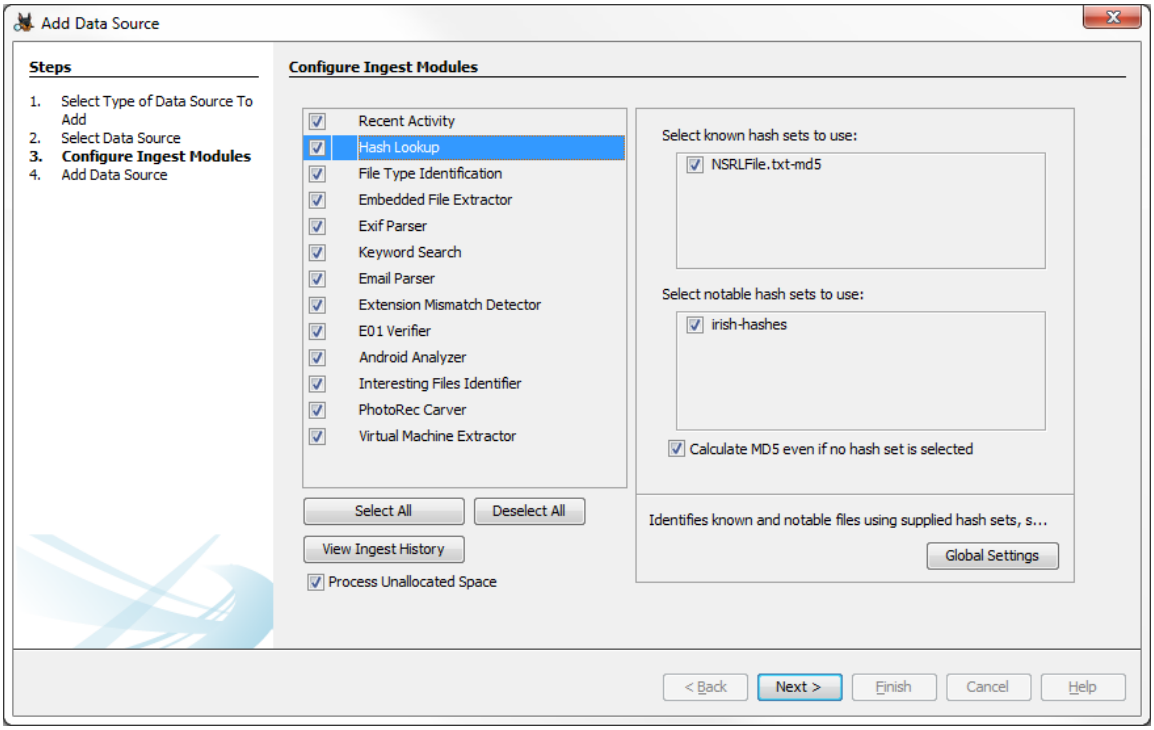
To use the NSRL, you may download a pre-made index from http://sourceforge.net/projects/autopsy/files/NSRL. Download the **NSRL-XYZm-autopsy.zip** (where 'XYZ' is the version number. As of this writing, it is 247) and unzip the file. Use the "Tools", "Options" menu and select the "Hash Sets" tab. Click "Import Database" and browse to the location of the unzipped NSRL file. You can change the Hash Set Name if desired. Select the type of database desired, choosing "Send ingest inbox message for each hit" if desired, and then click "OK".



Using the Module

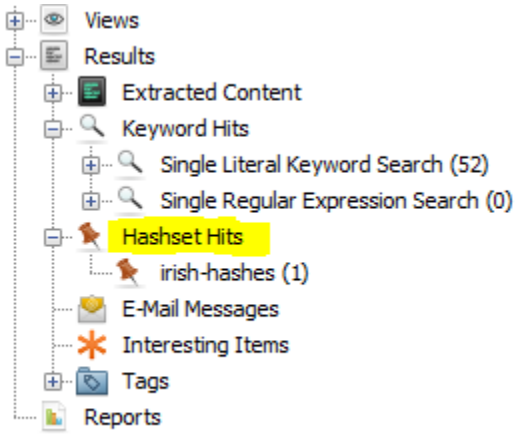
Ingest Settings

When hash sets are configured, the user can select the hash sets to use during the ingest process.



Seeing Results

Results show up in the tree as "Hashset Hits", grouped by the name of the hash set.



File Type Identification Module

What Does It Do?

The File Type ID module identifies files based on their internal signatures and does not rely on file extensions. Autopsy uses the Tika library to do its primary file ID detection and that can be customized with user-defined rules.

You should enable this module because many other modules depend on its results to determine if they should analyze a file. Some examples include:

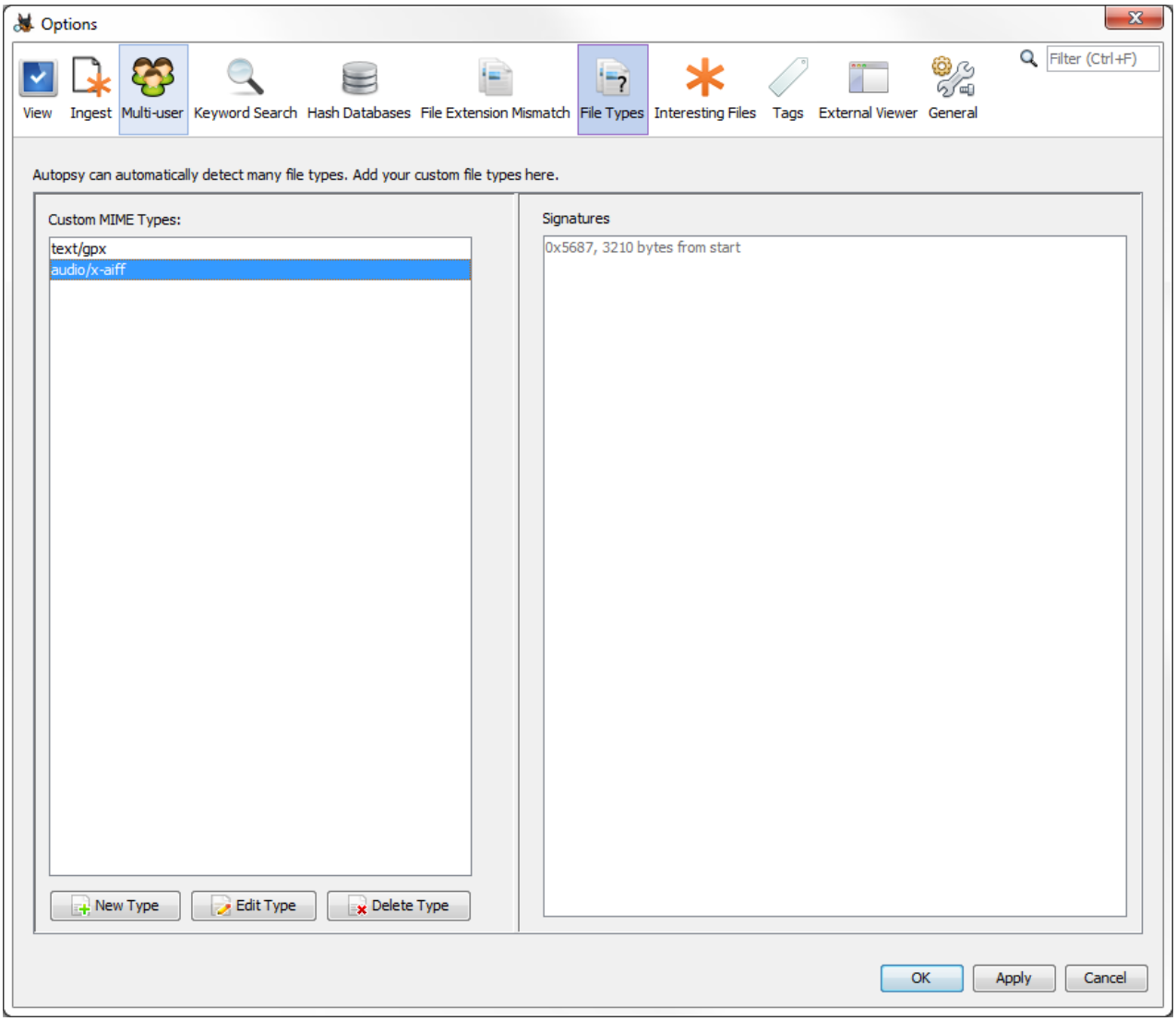
- **Extension Mismatch Detector Module**

- **Keyword Search Module**

Configuration

You do not need to configure anything with this module unless you want to define your own types. To define your own types, go to "Tools", "Options", "File Type Id" panel.

From there, you can define rules based on the offset of the signature and if the signature is a byte sequence of an ASCII string.



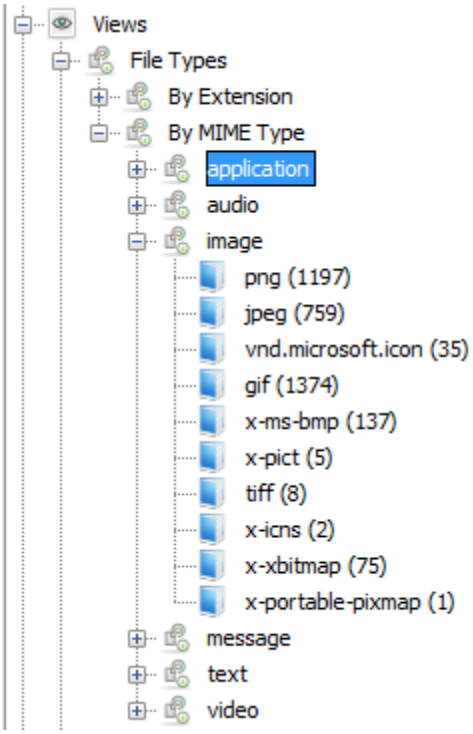
Using the Module

Ingest Settings

There are no run-time settings for this module when you run it on a data source. All user-defined and Tika rules are always applied.

Seeing Results

The results can be seen in the views area of the tree, under Views->File Types->By MIME Type.



Note that only user-defined MIME types of the form (media type)/(media subtype) will be displayed in the tree.

To see the file type of an individual file, view the "Results" tab in the lower right when you navigate to the file. You should see a page in there that mentions the file type.

Embedded File Extraction Module

What Does It Do??

The Embedded File Extractor module opens ZIP, RAR, other archive formats, Doc, Docx, PPT, PPTX, XLS, and XLSX and sends the derived files from those files back through the ingest pipeline for analysis.

This module expands archive files to enable Autopsy to analyze all files on the system. It enables keyword search and hash lookup to analyze files inside of archives

NOTE: Certain media content embedded inside Doc, Docx, PPT, PPTX, XLS, and XLSX might not be extracted.

Configuration

There is no configuration required.

Using the Module

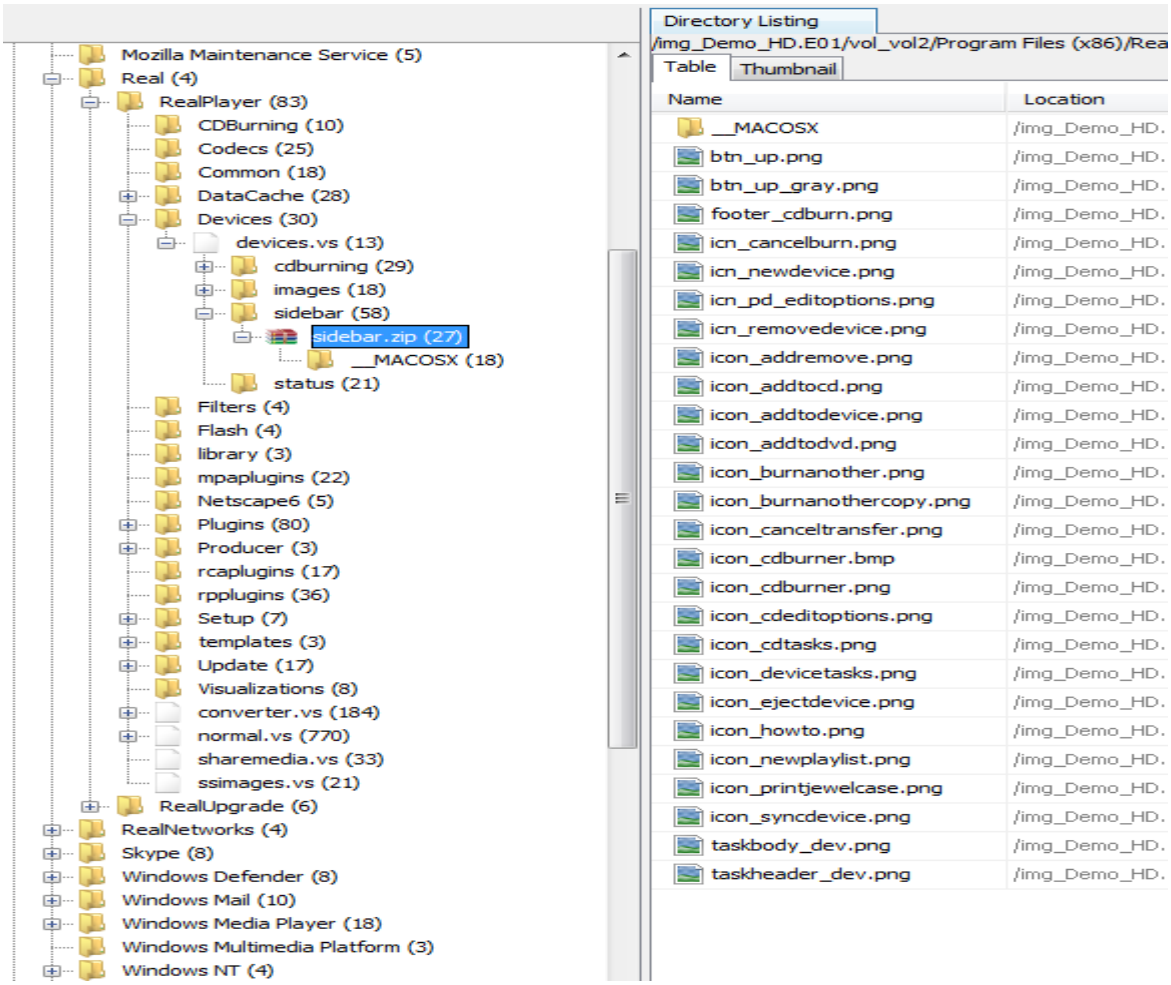
Select the checkbox in the Ingest Modules settings screen to enable the Archive Extractor.

Ingest Settings

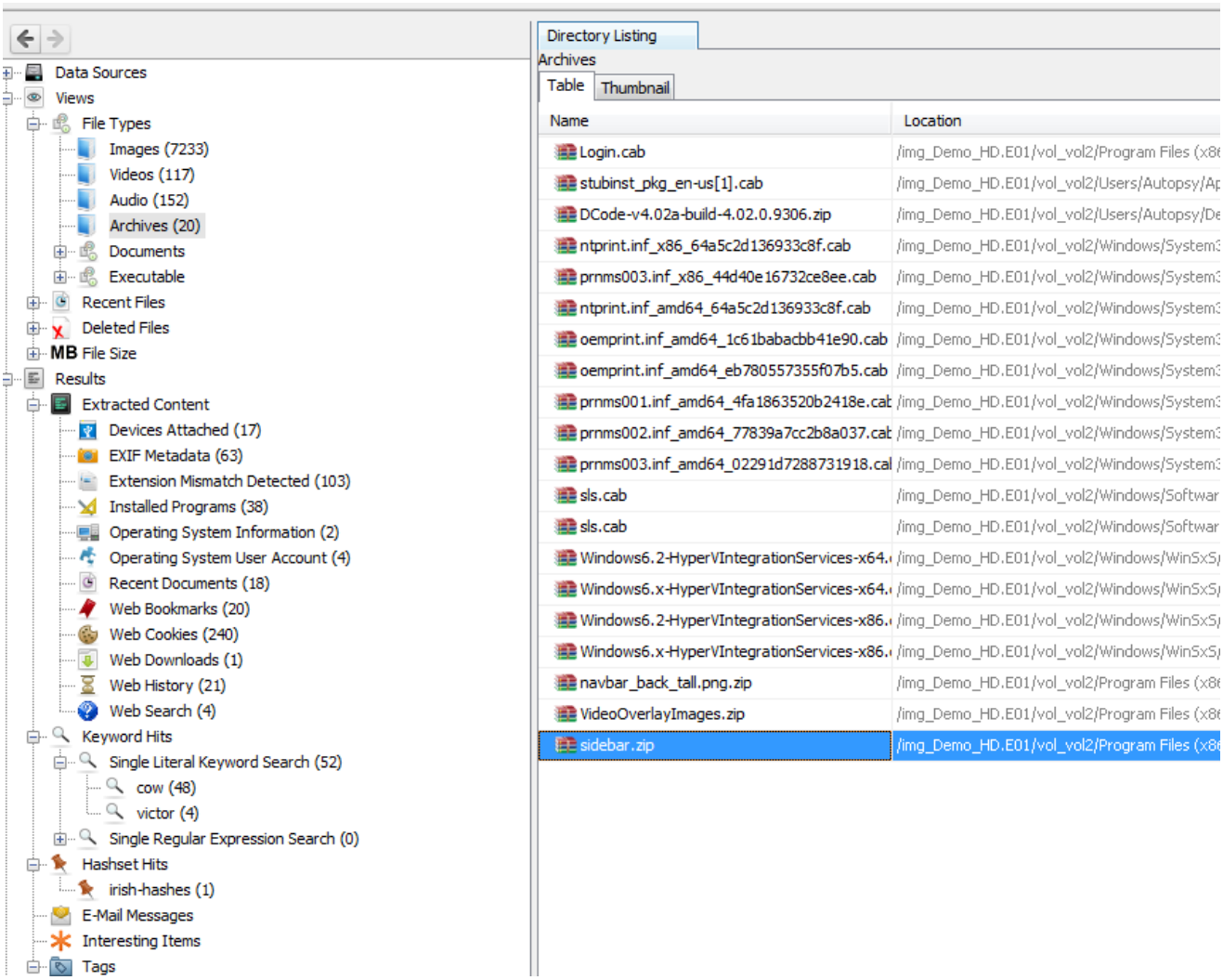
There is no runtime ingest settings required.

Seeing Results

Each file extracted shows up in the data source tree view as a child of the archive containing it,

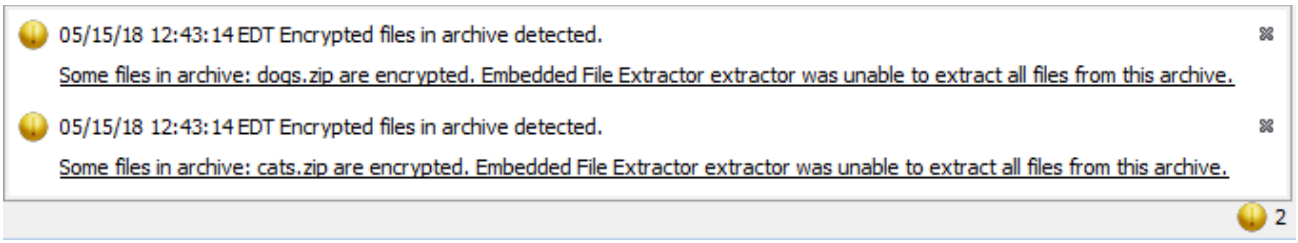


and as an archive under "Views", "File Types", "Archives".

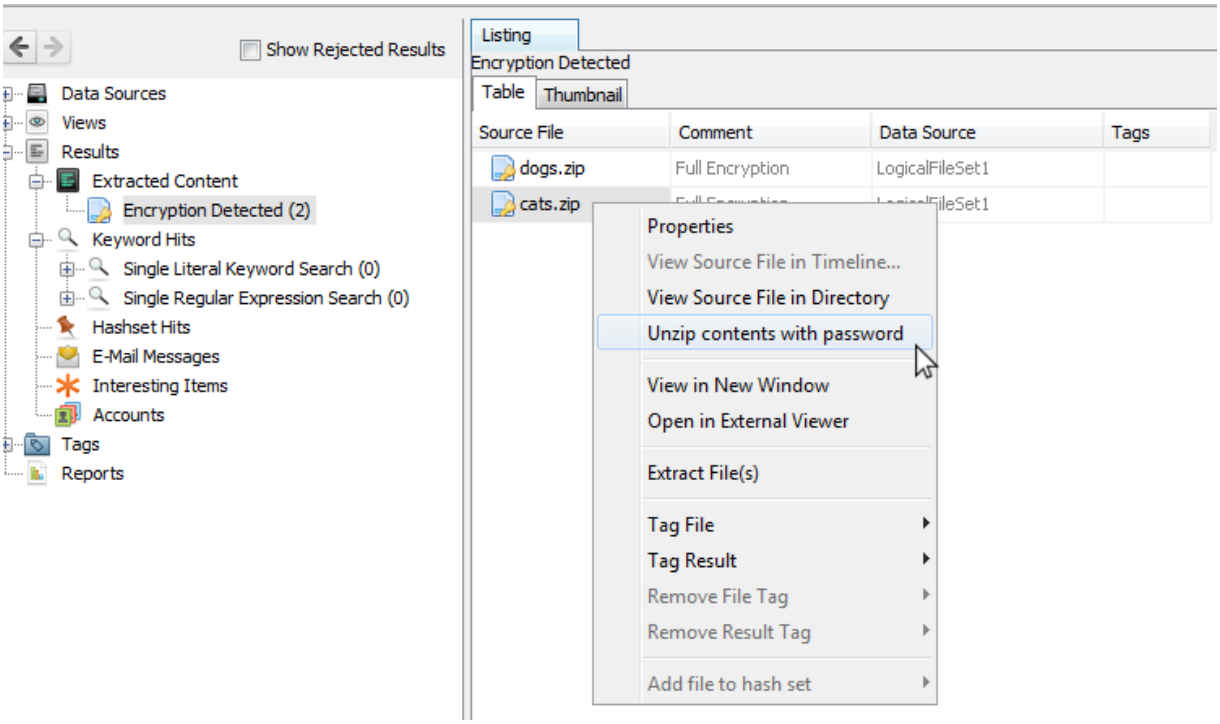


Encrypted Archives

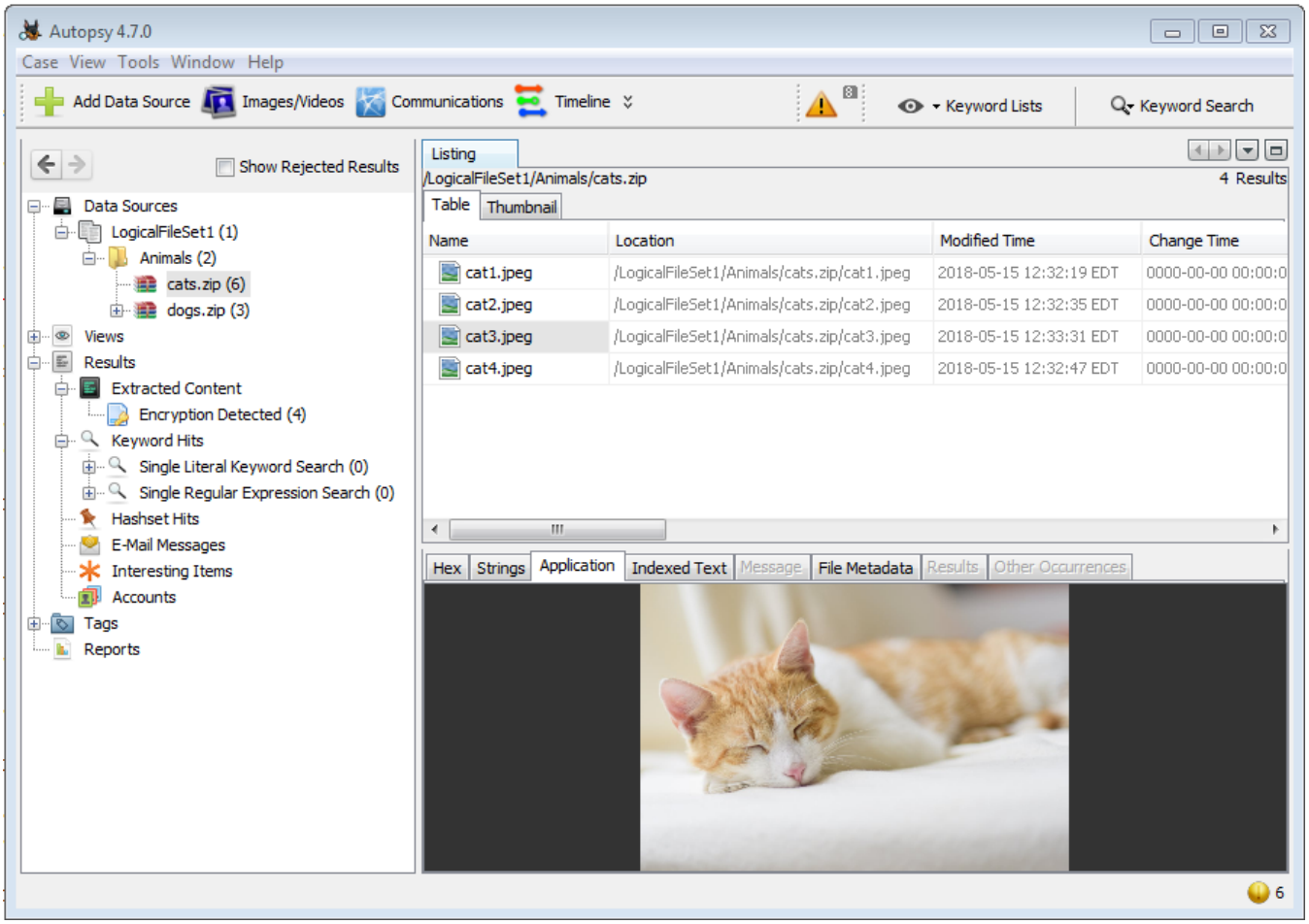
When the Embedded File Extractor module encounters an encrypted archive, it will generate a warning bubble in the bottom right of the main screen:



After ingest, you can attempt to decrypt these archives if you know the password. Find the archive (either in the **tree view** or **result view**) and right-click on it, then select "Unzip contents with password".



After entering the password, you can select which ingest modules to run on the newly extracted files. When finished, you can browse to the encrypted archive in the tree view to see the newly extracted files. If the archive was already open in the tree, you may have to close and open the case in order to see the new data.



EXIF Parser Module

What Does It Do??

The EXIF Parser module extracts EXIF (Exchangeable Image File Format) information from ingested pictures. This information can contain geolocation data for the picture, time, date, camera model and settings (exposure values, resolution, etc) and other information. The discovered attributes are added to the BlackBoard.

This can tell you where and when a picture was taken and give clues to the camera that took it.

Configuration

There is no configuration required.

Using the Module

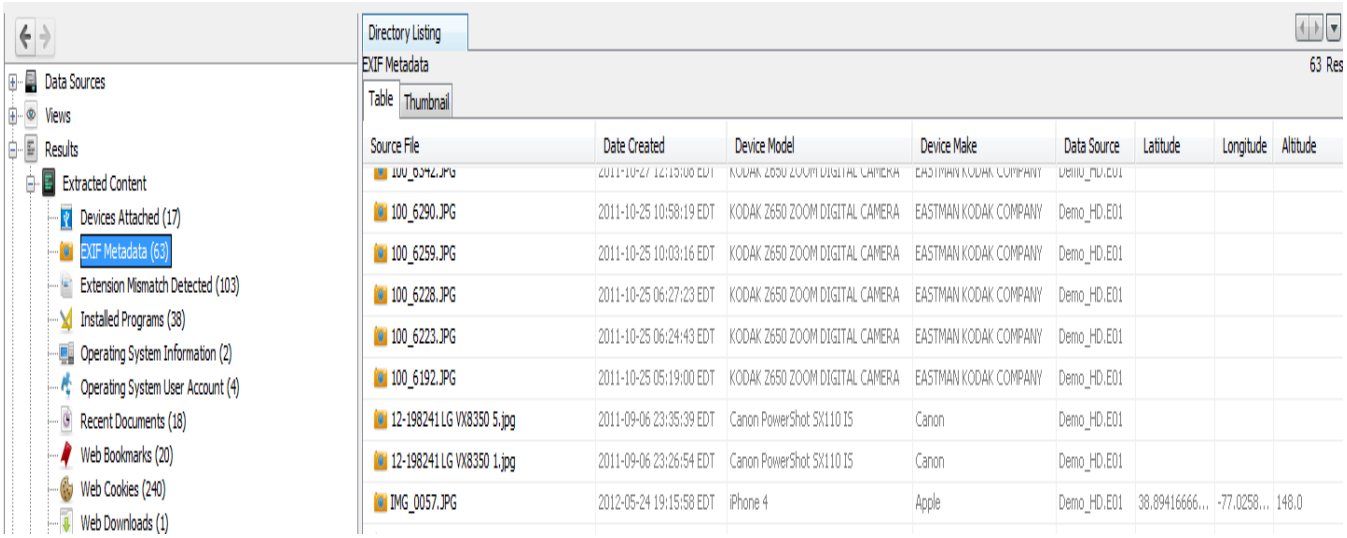
Select the checkbox in the Ingest Modules settings screen to enable the EXIF Parser.

Ingest Settings

There is no runtime ingest settings required.

Seeing Results

Results are shown in the Results tree.



Keyword Search Module

What Does It Do?

The Keyword Search module facilitates both the **ingest** portion of searching and also supports manual text searching after ingest has completed (see **Ad Hoc Keyword Search**). It extracts text from files being ingested, selected reports generated by other modules, and results generated by other modules. This extracted text is then added to a Solr index that can then be searched.

Autopsy tries its best to extract the maximum amount of text from the files being indexed. First, the indexing will try to extract text from supported file formats, such as pure text file format, MS Office Documents, PDF files, Email, and many others. If the file is not supported by the standard text extractor, Autopsy will fall back to a string extraction algorithm. String extraction on unknown file formats or arbitrary binary files can often extract a sizeable amount of text from a file, often enough to provide additional clues to reviewers. String extraction will not extract text strings from encrypted files.

Autopsy ships with some built-in lists that define regular expressions and enable the user to search for Phone Numbers, IP addresses, URLs and E-mail addresses. However, enabling some of these very general lists can produce a very large number of hits, and many of them can be false-positives. Regular expressions can potentially take a long time to complete.

Once files are placed in the Solr index, they can be searched quickly for specific keywords, regular expressions, or keyword search lists that can contain a mixture of keywords and regular expressions. Search queries can be executed automatically during the ingest run or at the end of the ingest, depending on the current settings and the time it takes to ingest the image.

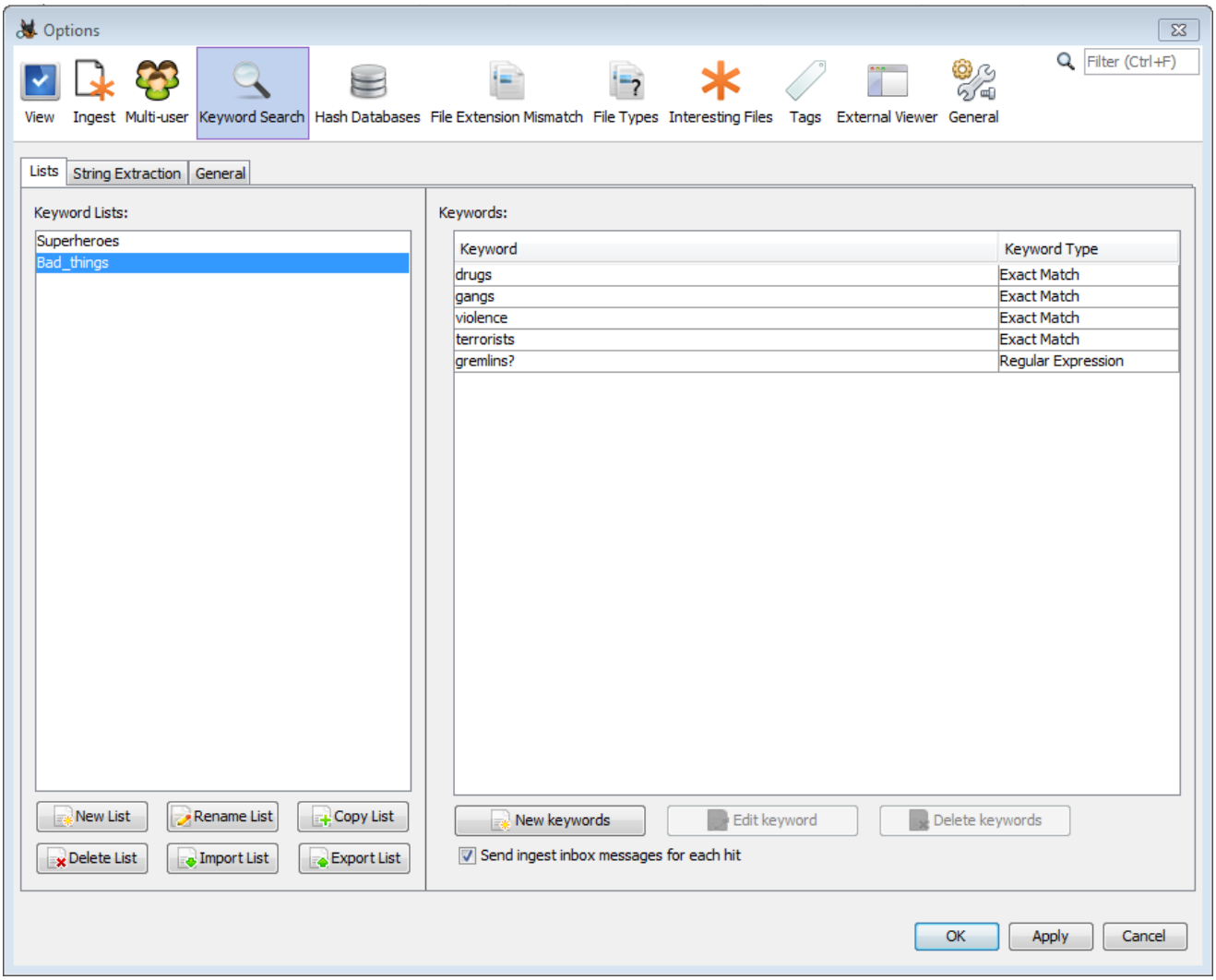
Keyword Search Configuration Dialog

The keyword search configuration dialog has three tabs, each with its own purpose:

- The **Lists tab** is used to add, remove, and modify keyword search lists.
- The **String Extraction tab** is used to enable language scripts and extraction type.
- The **General Settings tab** is used to configure the ingest timings and display information.

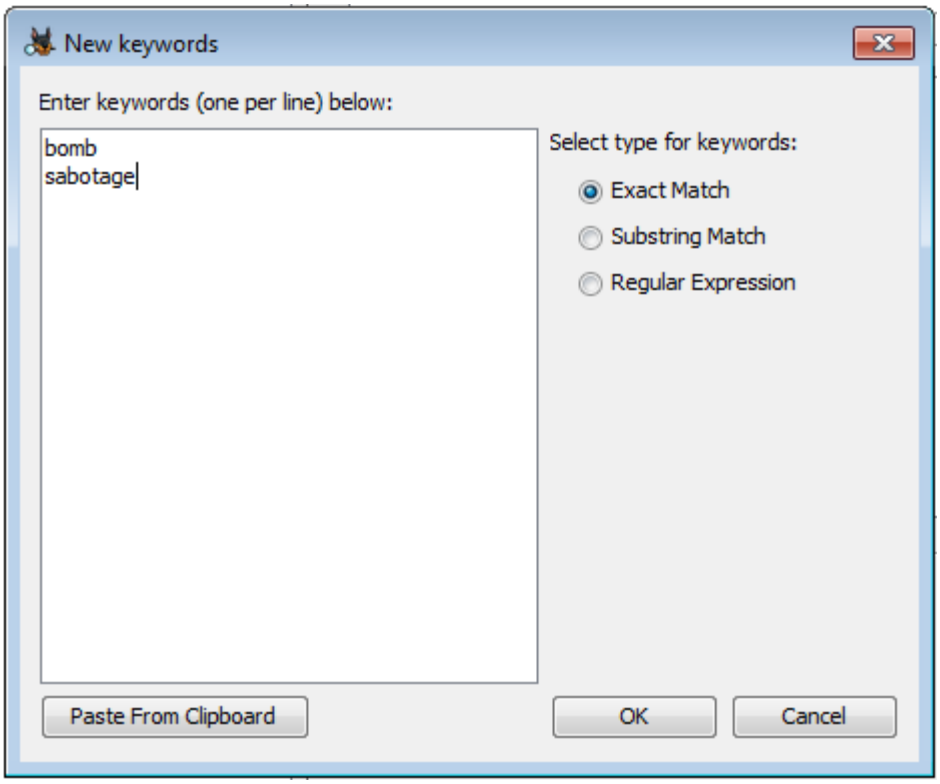
Lists tab

The Lists tab is used to create/import and add content to keyword lists. To create a list, select the 'New List' button and choose a name for the new Keyword List. Once the list has been created, keywords can be added to it (see **Creating Keywords** for more information on keyword types). Lists can be added to the keyword search ingest process; searches will happen at regular intervals as content is added to the index.



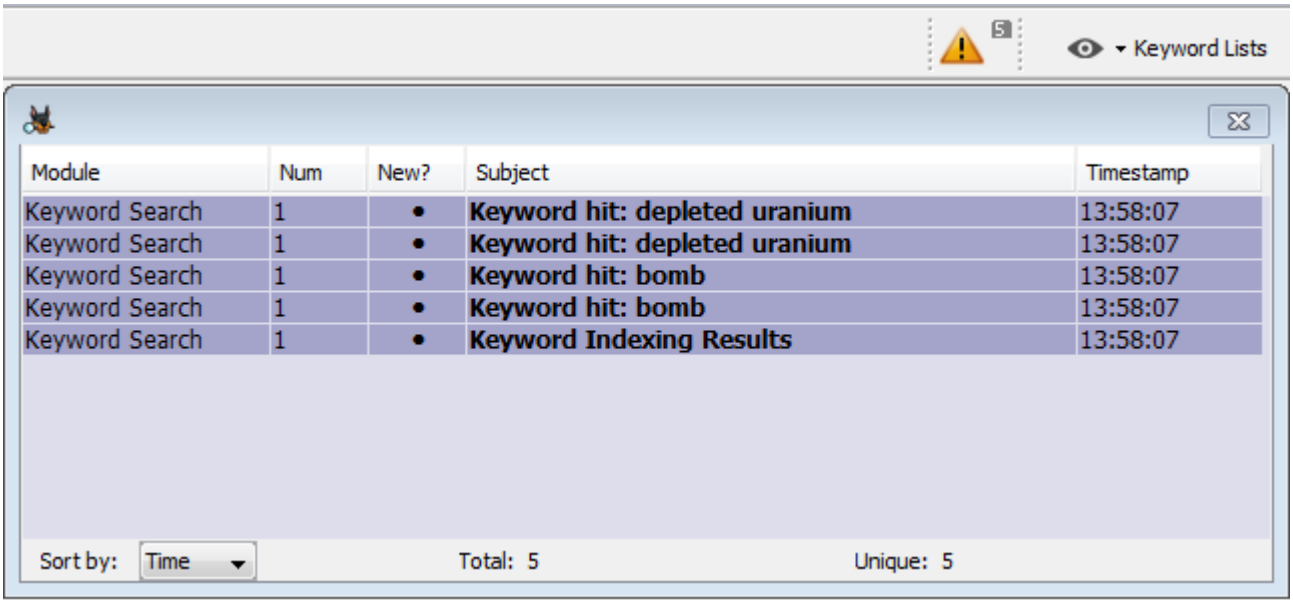
The lists of keywords can be found on the left side of the panel. New lists can be created, existing lists can be renamed, copied, exported, or deleted, and lists can be imported. Autopsy supports importing Encase tab-delimited lists as well as lists created previously with Autopsy. For Encase lists, folder structure and hierarchy is ignored. There is currently no way to export lists for use with Encase, but lists can be exported to share between Autopsy users.

Once a keyword list is selected all keywords in that list will be displayed on the right side of the tab. The "New Keywords" button can be used to add one or more entries to the list, and the "Edit keyword" and "Delete keywords" buttons can alter the existing entries.



New entries can be typed into the dialog or pasted from the clipboard. All entries added at once must be the same type of match (exact, substring, or regex), but the dialog can be used multiple times to add keywords to the keyword list. Refer to the **Creating Keywords** section for an explanation of each keyword type.

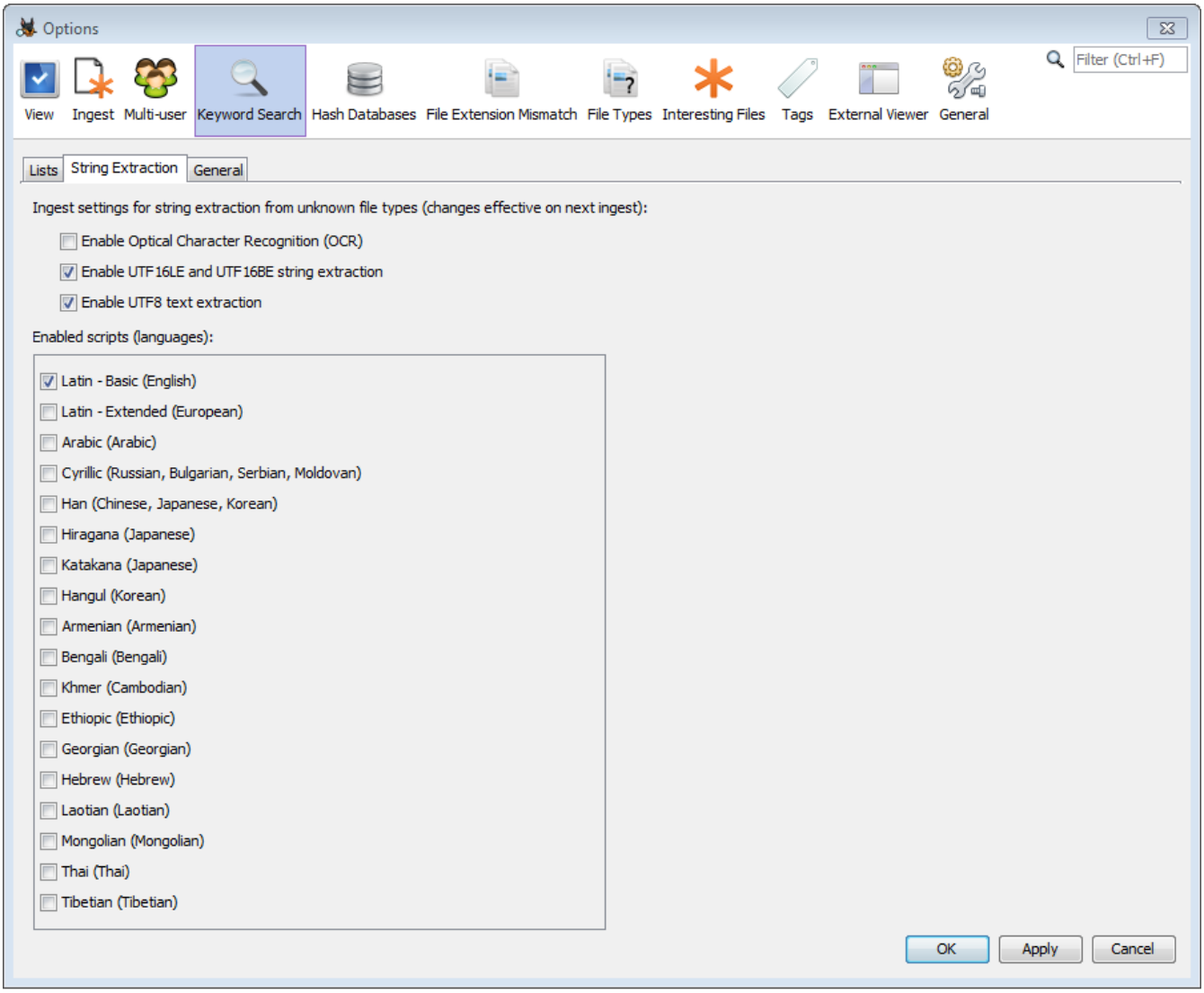
Under the Keyword list is the option to send ingest inbox messages for each hit. If this is enabled, each keyword hit for that list will be accessible through the yellow triangle next to the Keyword Lists button. This feature gives you a quick way to view your most important keyword search results.



String Extraction tab

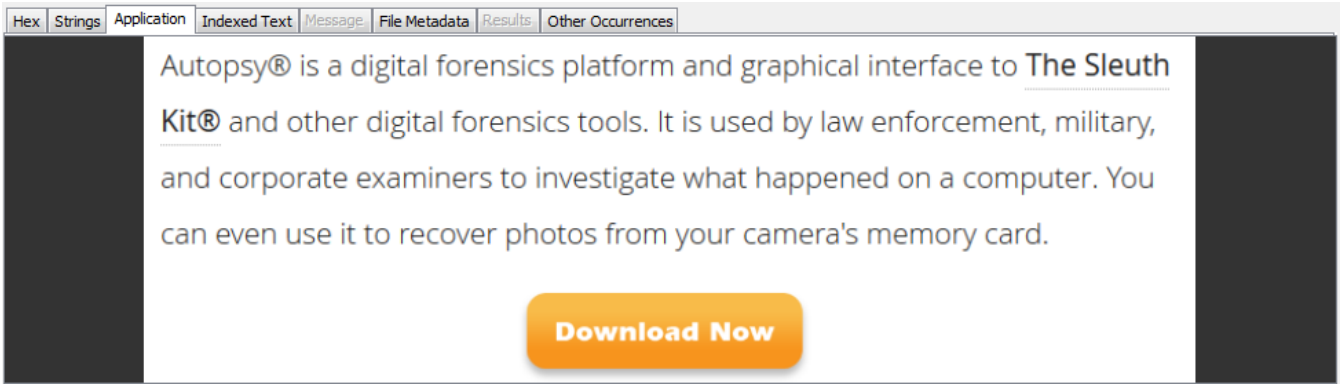
The string extraction setting defines how strings are extracted from files from which text cannot be extracted normally because their file formats are not supported. This is the case with arbitrary binary files (such as the page file) and chunks of unallocated space that represent deleted files. When we extract strings from binary files we need to interpret sequences of bytes as text differently, depending on the possible text encoding and script/language used. In many cases we don't know in advance what the specific encoding/language the text is encoded in. However, it helps if the investigator is looking for a specific language, because by selecting less languages the indexing performance will be improved and the number of false positives will be reduced.

The default setting is to search for English strings only, encoded as either UTF8 or UTF16. This setting has the best performance (shortest ingest time). The user can also use the String Viewer first and try different script/language settings, and see which settings give satisfactory results for the type of text relevant to the investigation. Then the same setting that works for the investigation can be applied to the keyword search ingest.

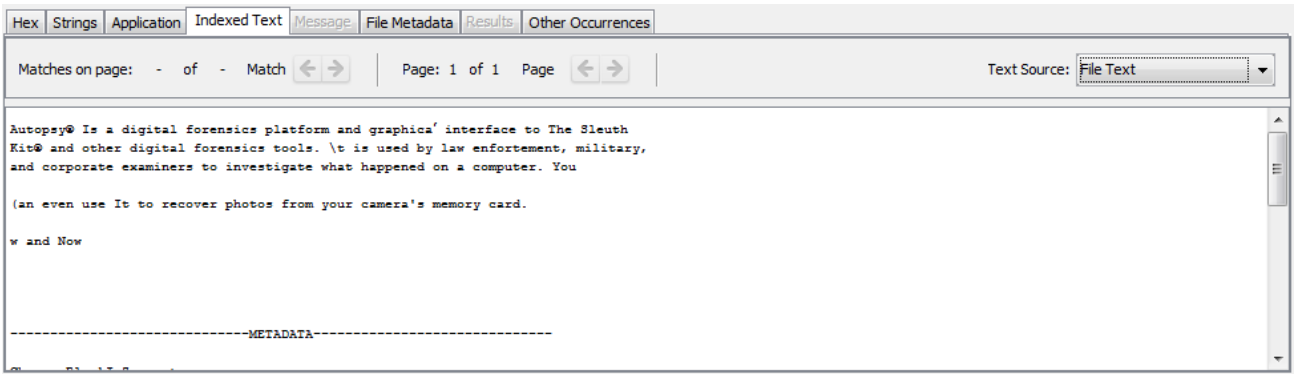


There is also a setting to enable Optical Character Recognition (OCR). If enabled, text may be extracted from supported image types. Enabling this feature will make the keyword search module

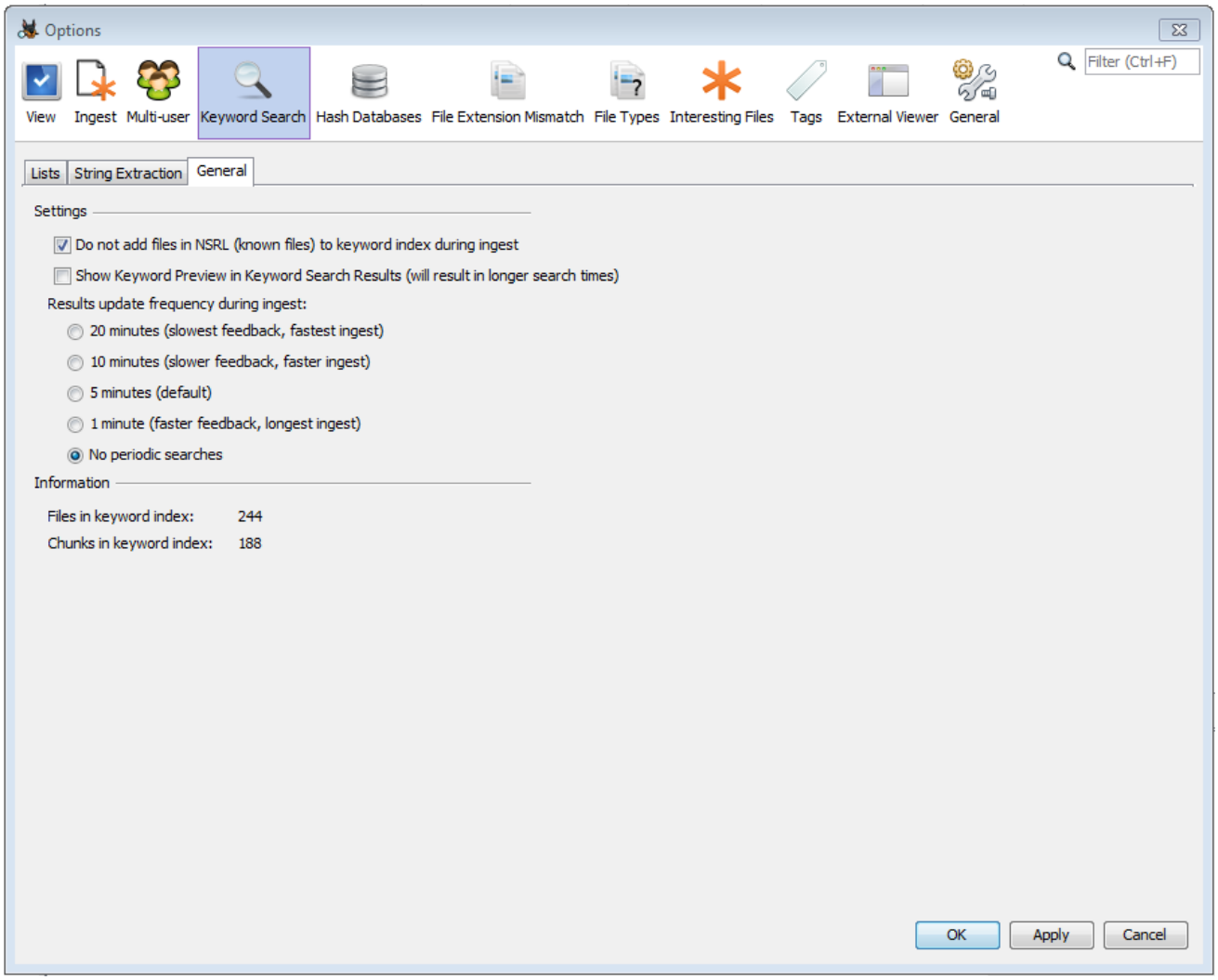
take longer to run, and the results are not perfect. The following shows a sample image containing text:



The "Indexed Text" tab shows the results when running the keyword search module with the OCR option enabled. If we were to use Keyword Search to look for the word "forensics", this file would be a match.



General Settings tab



NIST NSRL Support

The hash lookup ingest service can be configured to use the NIST NSRL hash set of known files. The keyword search advanced configuration dialog "General" tab contains an option to skip keyword indexing and search on files that have previously marked as "known" and uninteresting files. Selecting this option can greatly reduce size of the index and improve ingest performance. In most cases, user does not need to keyword search for "known" files.

Result update frequency during ingest

To control how frequently searches are executed during ingest, the user can adjust the timing setting available in the keyword search advanced configuration dialog "General" tab. Setting the number of minutes lower will result in more frequent index updates and searches being executed and the user will be able to see results more in real-time. However, more frequent updates can affect the overall performance, especially on lower-end systems, and can potentially lengthen the overall time needed for the ingest to complete.

One can also choose to have no periodic searches. This will speed up the ingest. Users choosing this option can run their keyword searches once the entire keyword search index is complete.

Using the Module

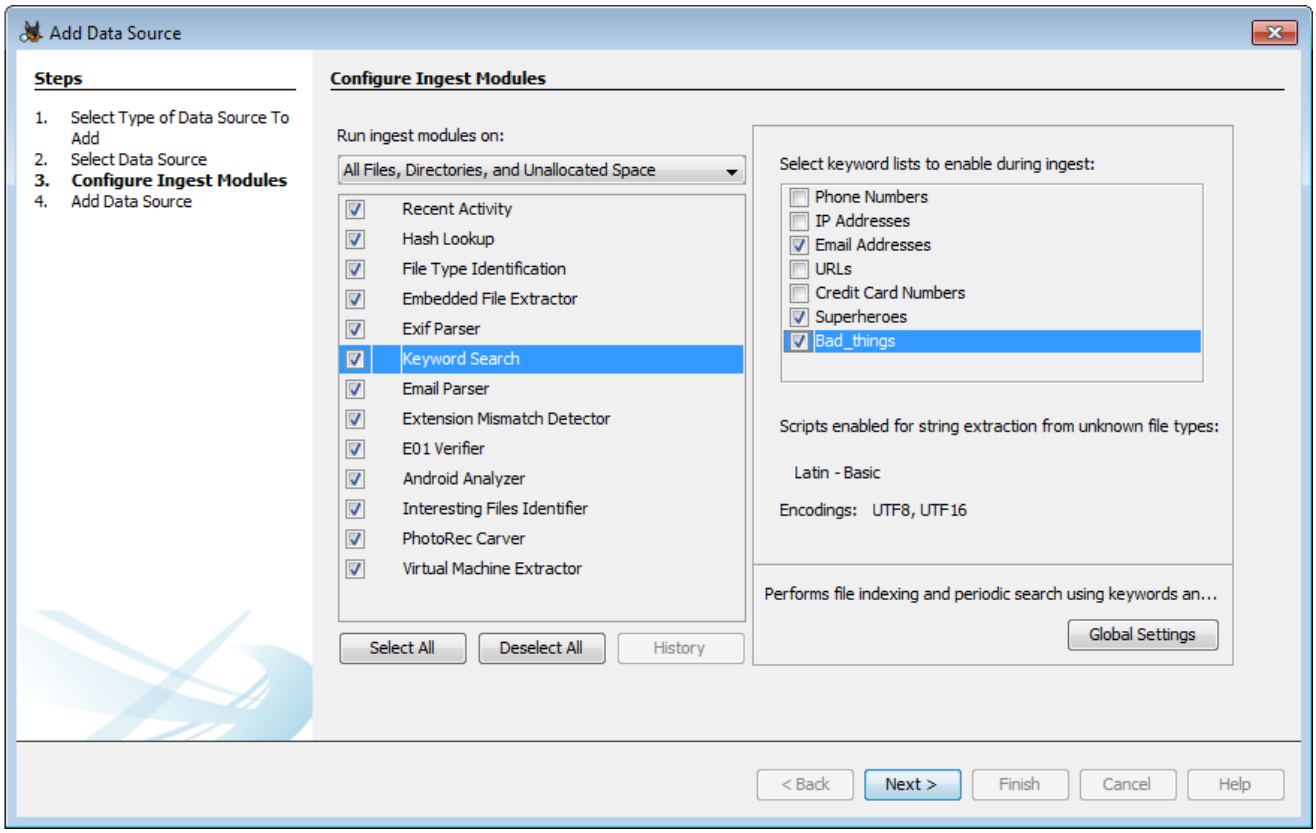
Search queries can be executed manually by the user at any time, as long as there are some files already indexed and ready to be searched. Searching before indexing is complete will naturally only search indexes that are already compiled.

See **Ingest** for more information on ingest in general.

Once there are files in the index, **Ad Hoc Keyword Search** will be available for use to manually search at any time.

Ingest Settings

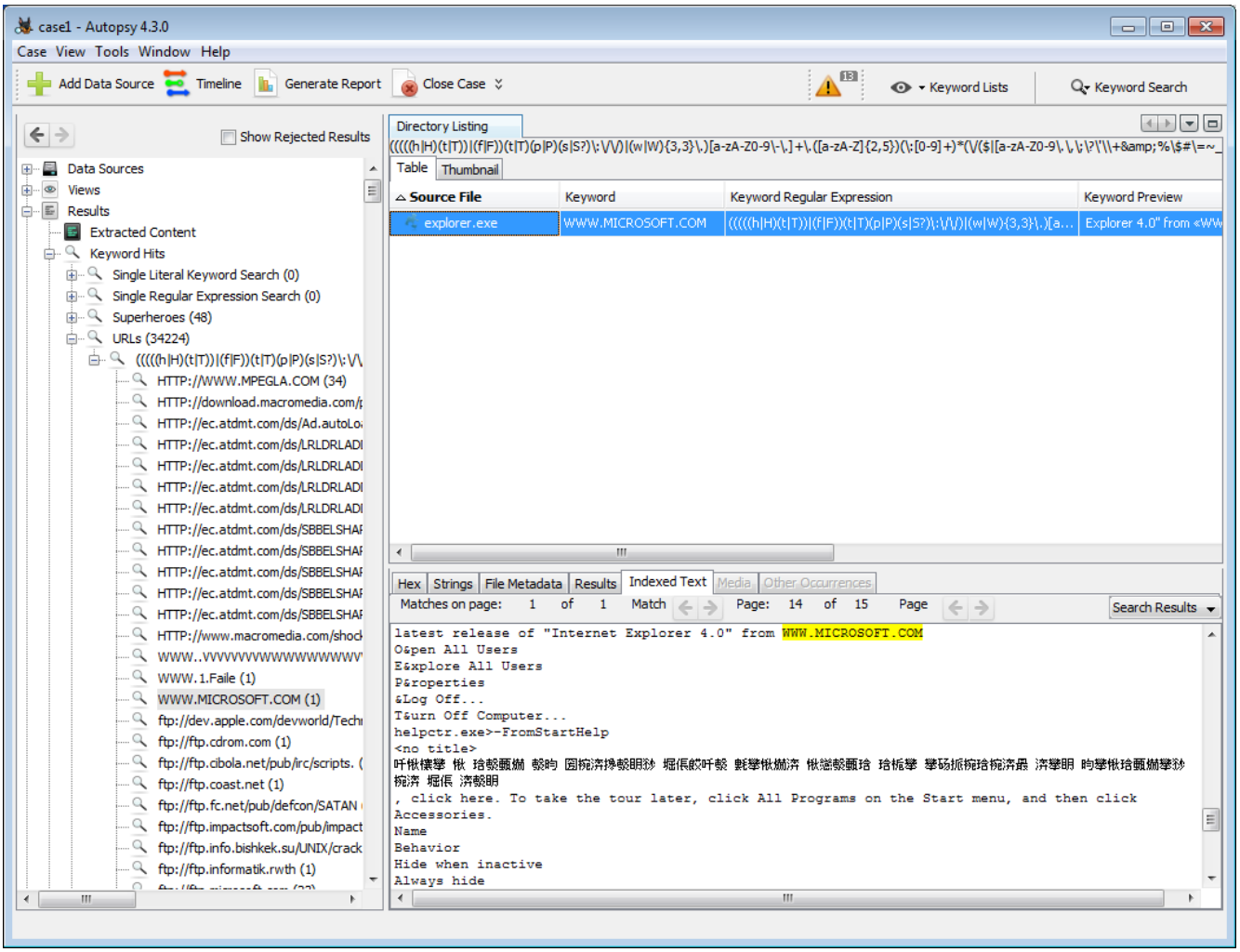
The Ingest Settings for the Keyword Search module allow the user to enable or disable the specific built-in search expressions, Phone Numbers, IP Addresses, Email Addresses, and URLs. Using the Advanced button (covered below), one can add custom keyword groups.



Seeing Results

The Keyword Search module will save the search results regardless whether the search is performed by the ingest process, or manually by the user. The saved results are available in the Directory Tree in the left hand side panel.

The keyword results will appear in the tree under "Keyword Hits". Each keyword search term will display the number of matches, and can be expanded to show the matches. From here, clicking on one of the matches will show a list of files on the right side of the screen. Select a file and go to the Indexed Text tab to see exactly where the matches occurred in the file.



Email Parser Module

What Does It Do?

The Email Parser module identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them, adding the results to the Blackboard. This module skips known files and creates a Blackboard artifact for each message. It adds email attachments as derived files.

This allows the user to identify email-based communications from the system being analyzed.

Configuration

There is no configuration required.

Using the Module

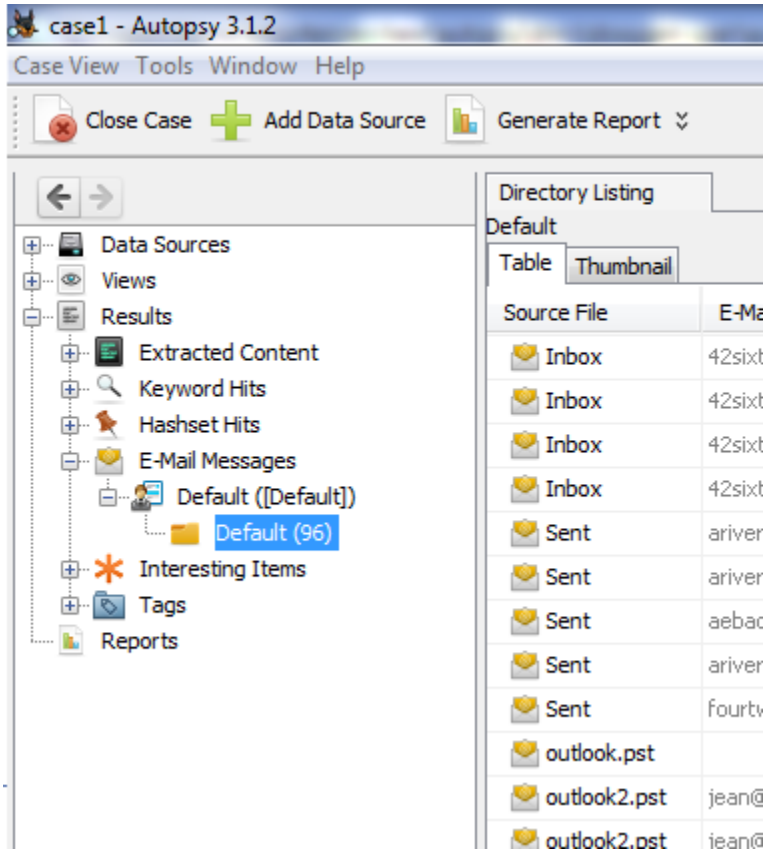
Explore the "Results", "E-Mail Messages" portion of the tree to review the results of this module.

Ingest Settings

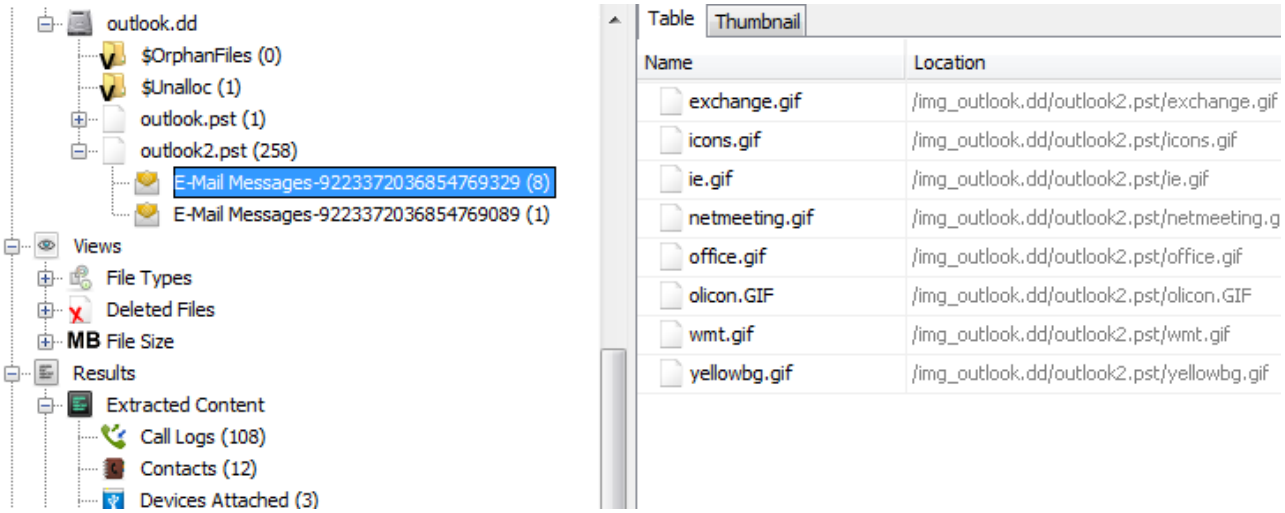
There are no runtime ingest settings required.

Seeing Results

The results of this show up in the "Results", "E-Mail Messages" portion of the tree.



The results can also be seen by browsing to the source file in the Data Sources tree, which will display the messages in the Results Viewer to the right. Any messages with attachments will be shown under the source file, and the attachments can be seen in the Result Viewer by selecting the message.



Extension Mismatch Detector Module

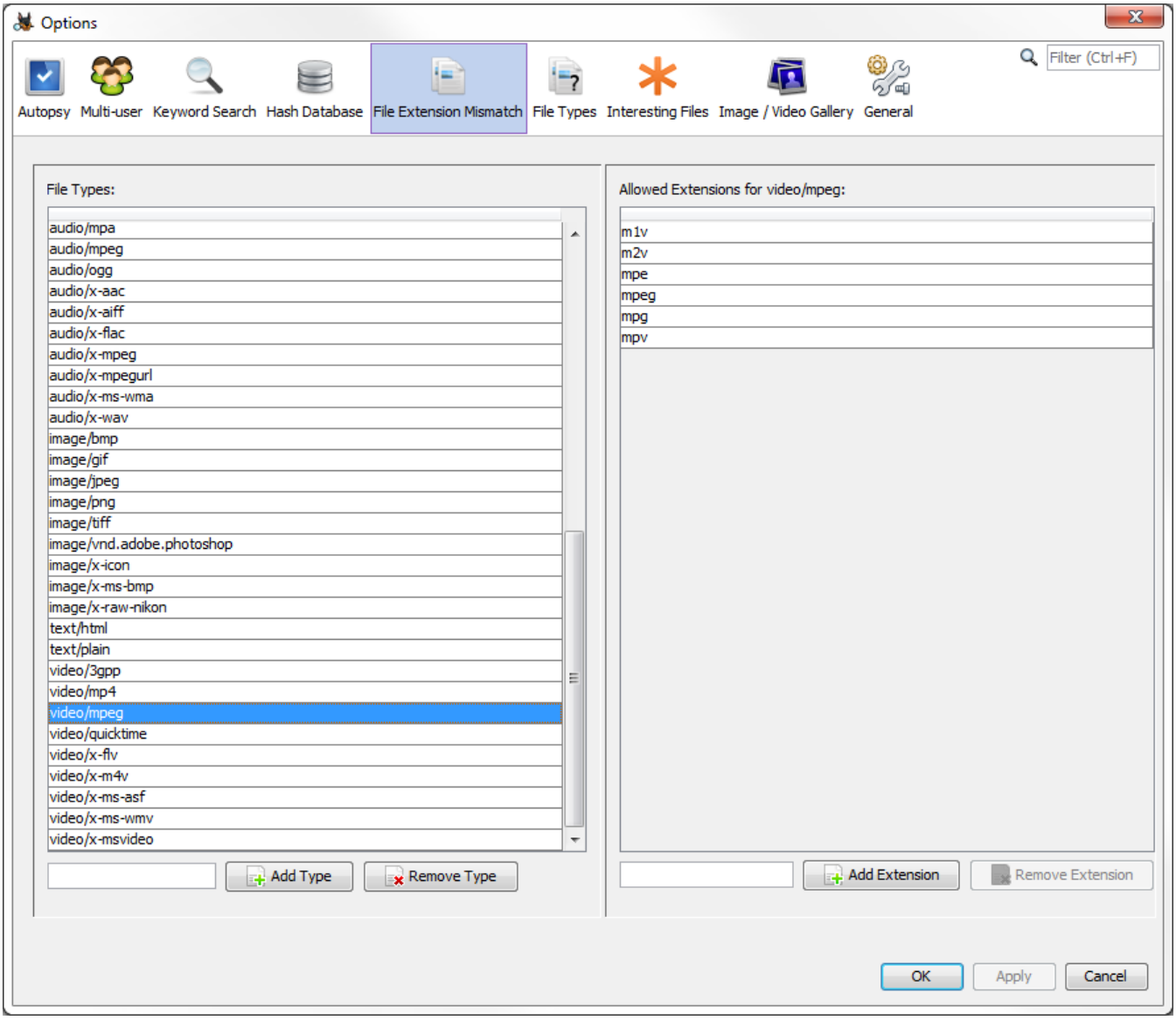
What Does It Do?

Extension Mismatch Detector module uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type. It ignores 'known' (NSRL) files. You can customize the MIME types and file extensions per MIME type in "Tools", "Options", "File Extension Mismatch".

This detects files that someone may be trying to hide.

Configuration

One can add and remove MIME types in the "Tools", "Options", "File Extension Mismatch" dialog box, as well as add and remove extensions to particular MIME types.

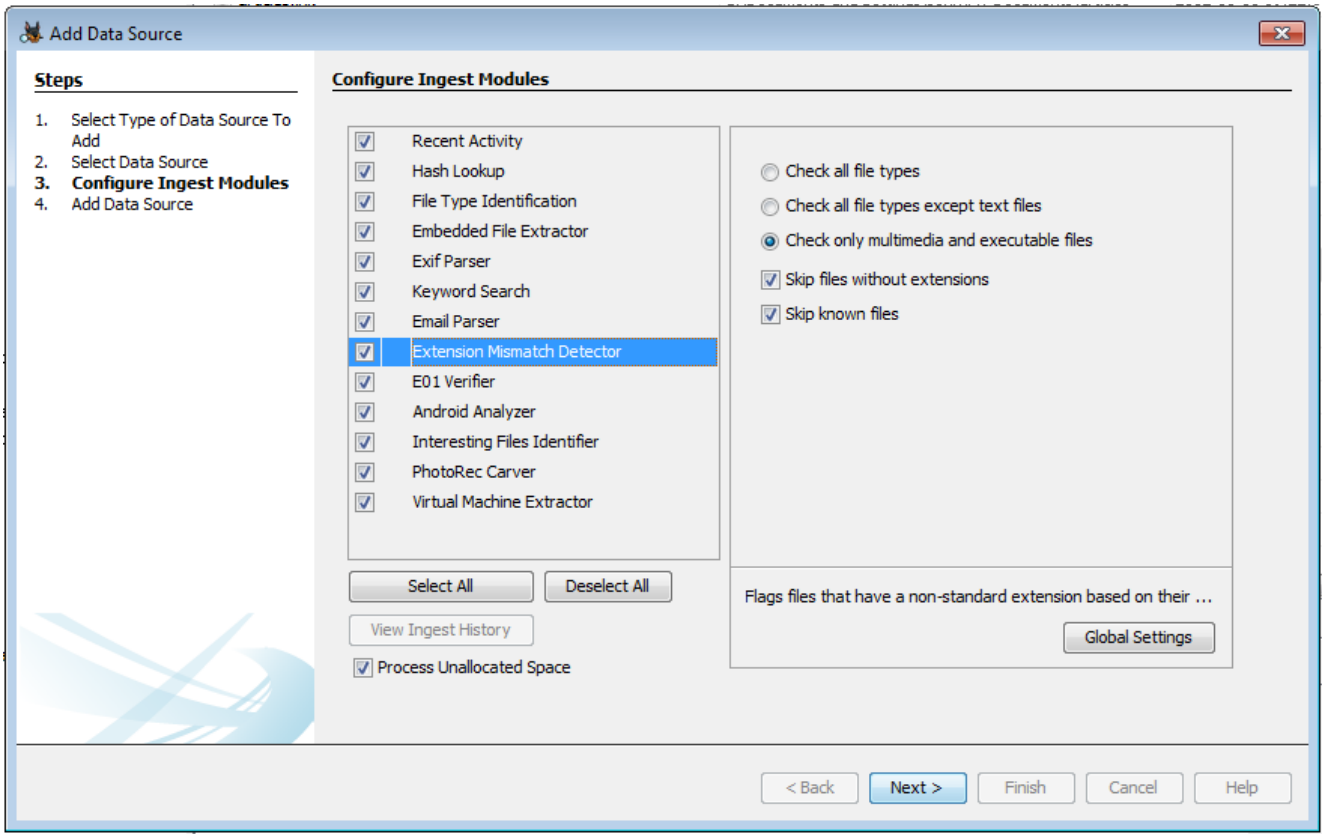


Using the Module

Note that you can get a lot of false positives with this module. You can add your own rules to Autopsy to reduce unwanted hits.

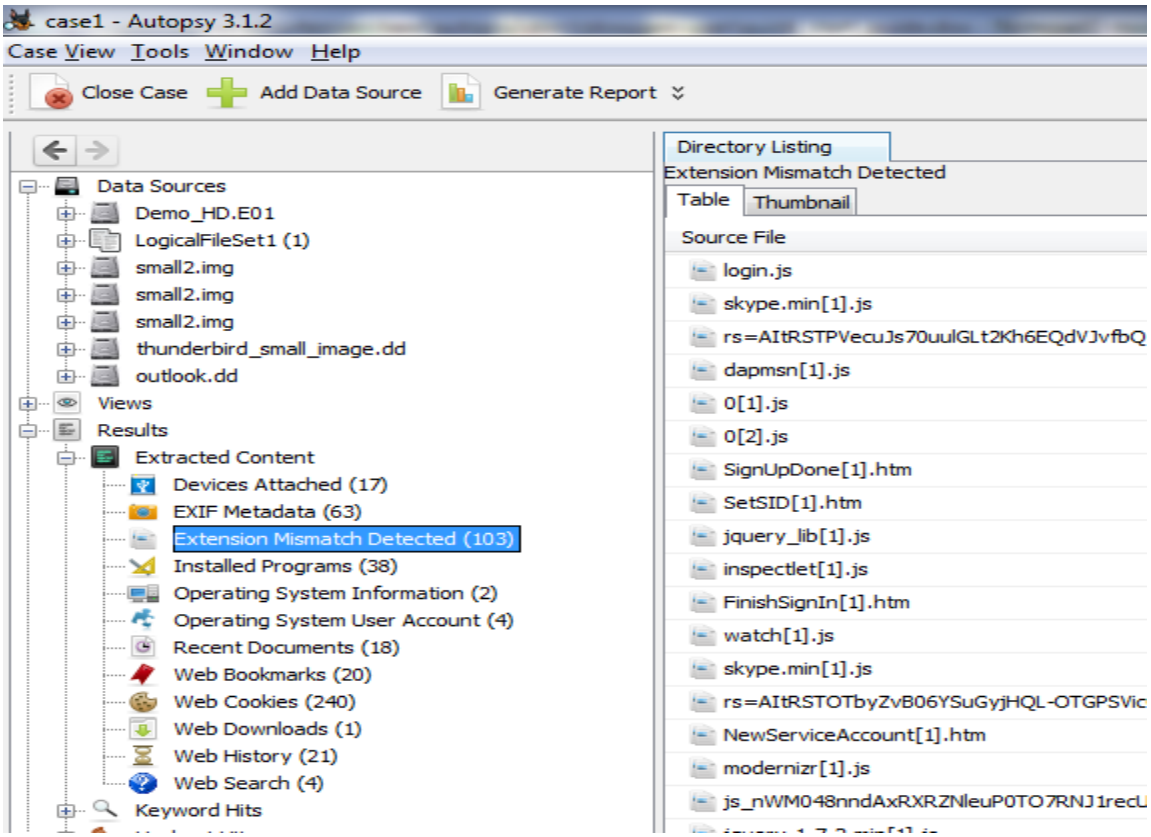
Ingest Settings

In the ingest settings, the user can choose whether to run on all files, all files except text files, or only multimedia or executable files. Additionally, the user can choose to skip all files without an extension, and to skip any known files identified by the hash lookup module, if it is enabled.



Seeing Results

Results are shown in the Results tree under "Extension Mismatch Detected".



Data Source Integrity Module

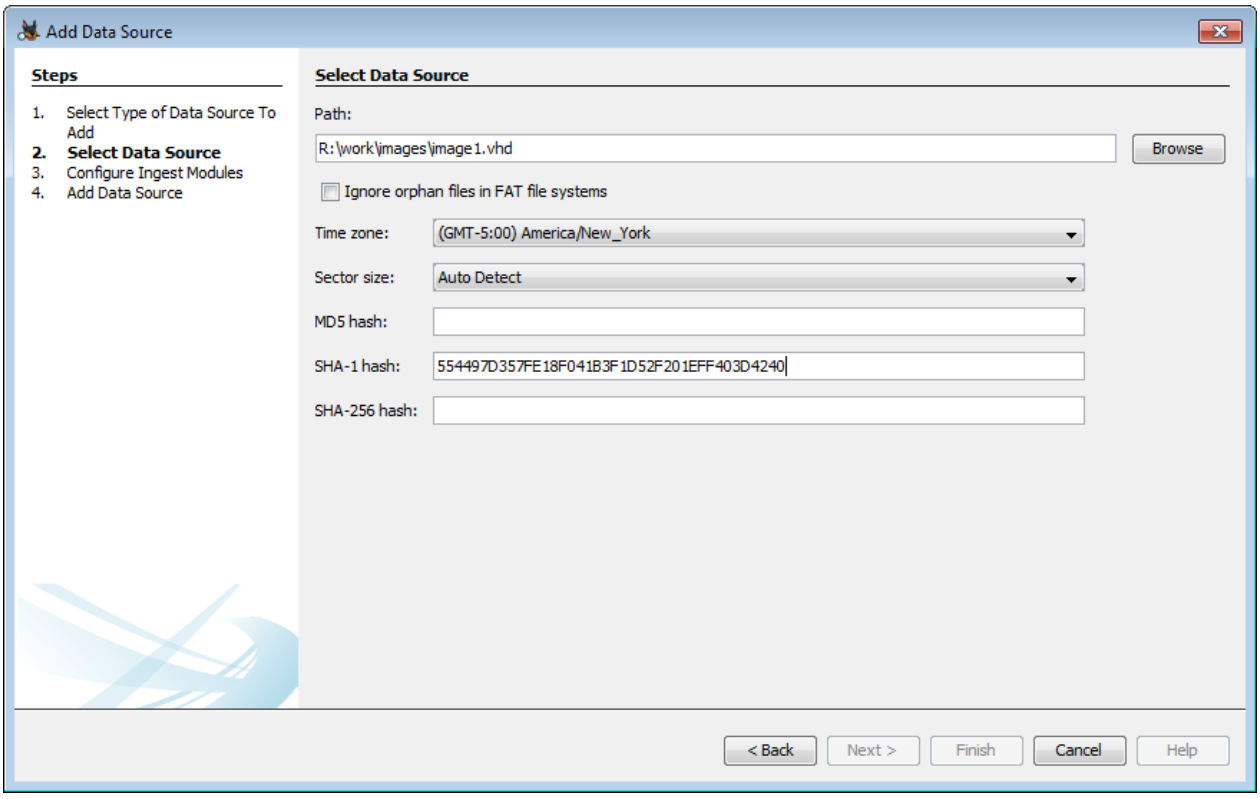
Overview

The Data Source Integrity module has two purposes:

- If the data source has any hashes associated with it (either user-entered or contained in an E01 file), it will verify these hashes
- If the data source has no associated hashes, it will calculate the hashes and store them in the database

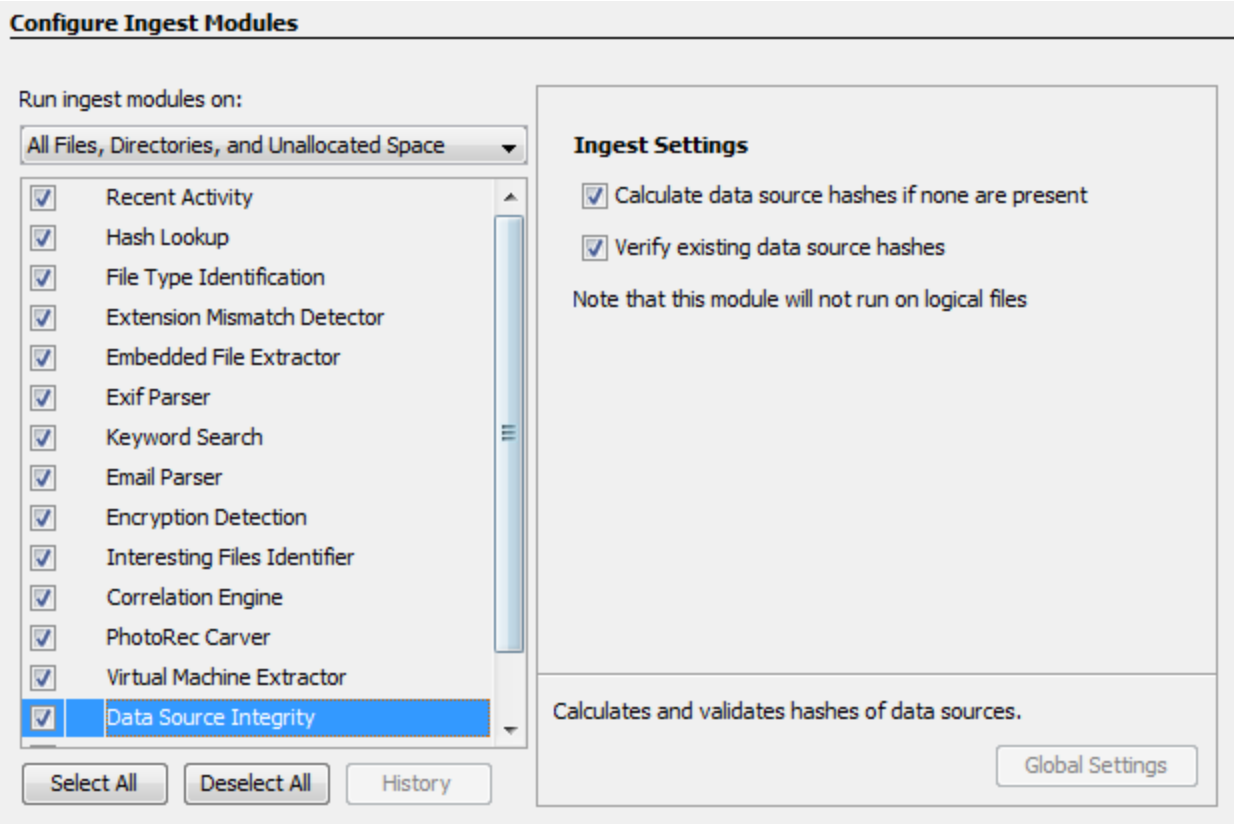
Running the module

If you wish to verify hashes, the first step is to enter hashes for your disk image (unless you have an E01 file - the hash is included in the data source). You can do this in the Add Data Source wizard where you select your disk image.



You can enter any combination of hashes to be verified.

You'll next need to configure the ingest module.

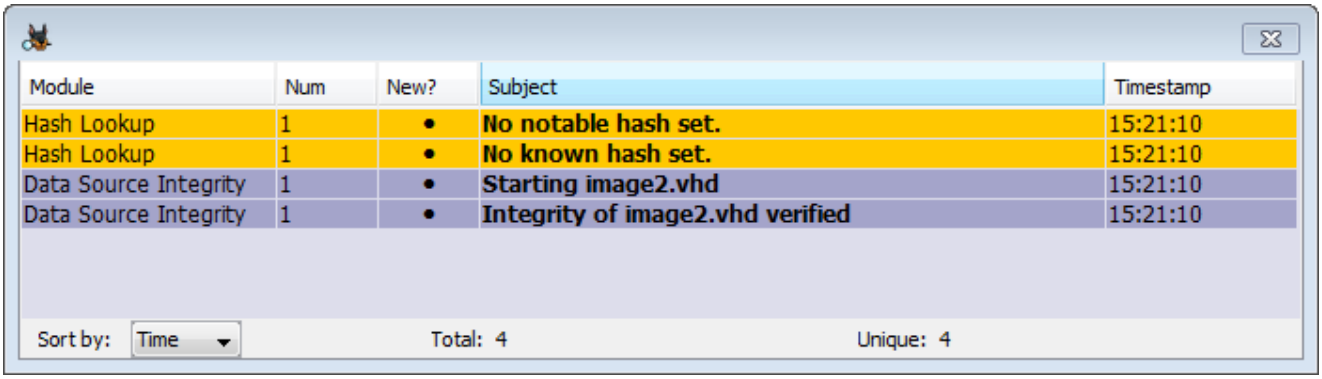


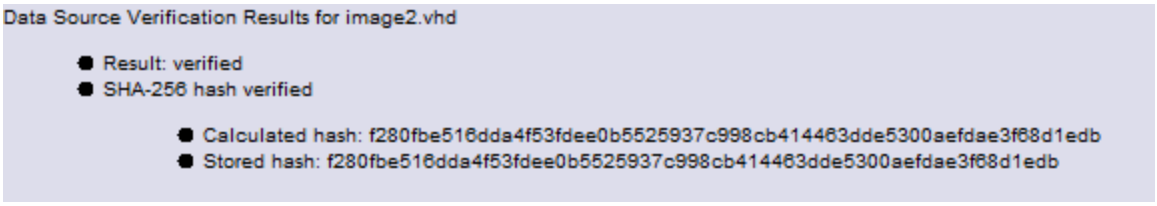
Note that this is simply enabling one or both behaviors, not choosing which one to run (compute vs. verify). That is determined solely by whether the data source has associated hashes. Uncheck-ing both boxes but leaving the module enabled will lead to an ingest module startup error

Viewing results

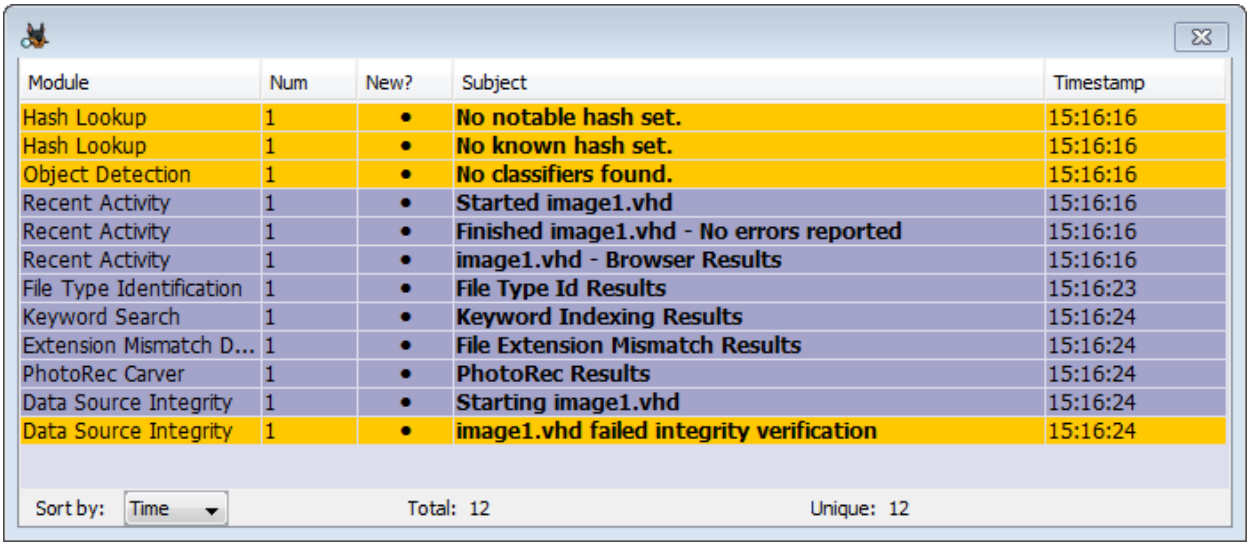
Hash verification

When verifying, if the check succeeds you'll see an inbox message confirming it. If you open the message you'll see the stored and computed hash values.



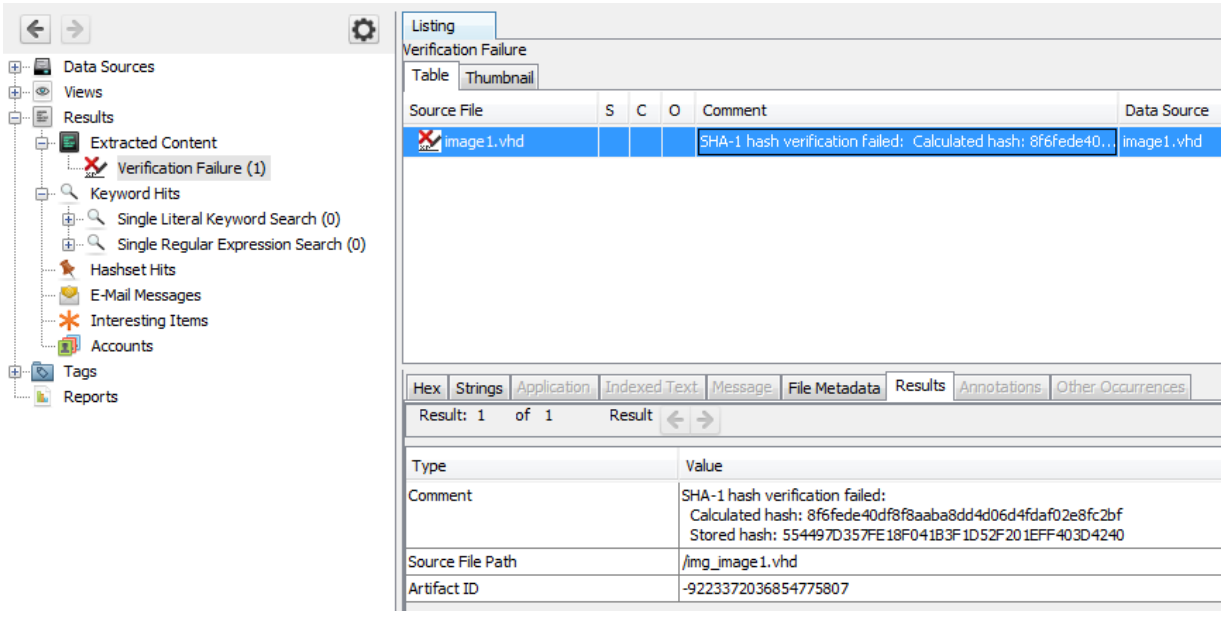


If the verification fails, you'll see an inbox message in yellow and the same message in a pop-up warning bubble.



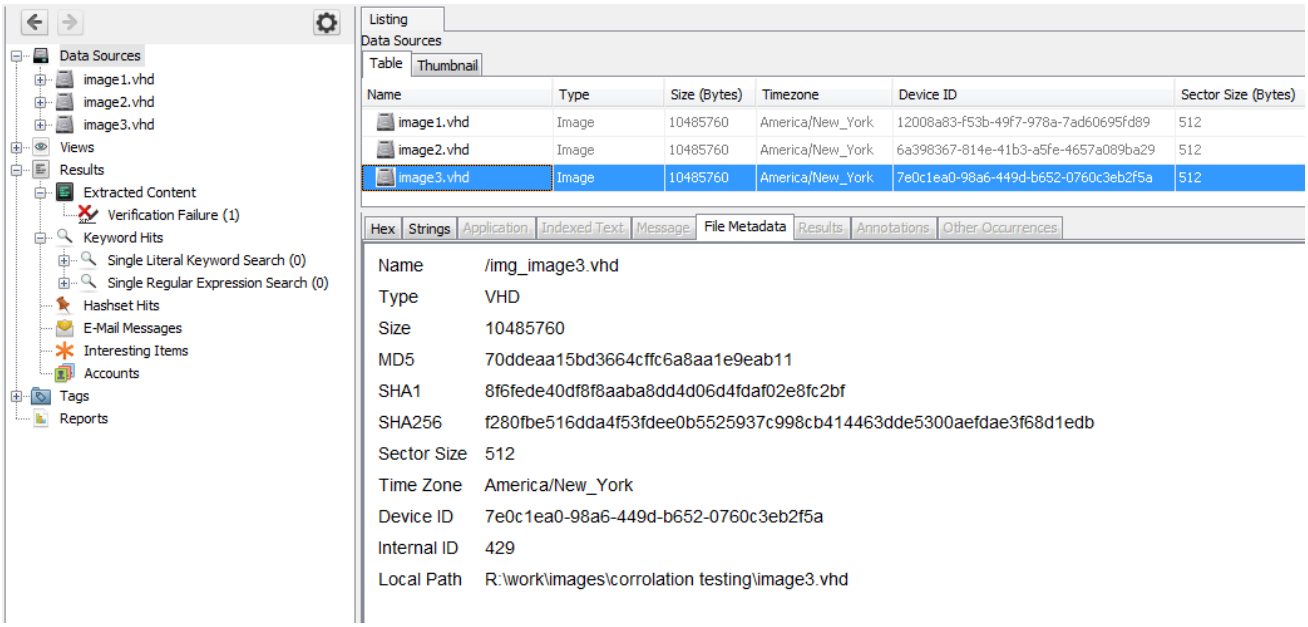
Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	**No notable hash set.**	15:16:16
Hash Lookup	1	•	**No known hash set.**	15:16:16
Object Detection	1	•	**No classifiers found.**	15:16:16
Recent Activity	1	•	**Started image1.vhd**	15:16:16
Recent Activity	1	•	**Finished image1.vhd - No errors reported**	15:16:16
Recent Activity	1	•	**image1.vhd - Browser Results**	15:16:16
File Type Identification	1	•	**File Type Id Results**	15:16:23
Keyword Search	1	•	**Keyword Indexing Results**	15:16:24
Extension Mismatch D...	1	•	**File Extension Mismatch Results**	15:16:24
PhotoRec Carver	1	•	**PhotoRec Results**	15:16:24
Data Source Integrity	1	•	**Starting image1.vhd**	15:16:24
Data Source Integrity	1	•	**image1.vhd failed integrity verification**	15:16:24

The inbox messages will disappear after the case is closed, so the module also adds a "Verification Failed" artifact added to the case.



Hash computation

To view the calculated hashes, select "Data Sources" in the tree, select your data source in the result viewer, and then open the "File Metadata" tab. If you're in "Group by data source" mode (see **View Options**), select "Data Source Files" under the data source you want to examine.



Android Analyzer Module

What Does It Do?

The Android Analyzer module allows you to analyze SQLite and other files from an Android device. It works on Physical dumps from most Android devices (note that we do not provide an acquisition method). Autopsy will not support older Android devices that do not have a volume system. These devices will often have a single physical image file for them and there is no information in the image that describes the layout of the file systems. Autopsy will therefore not be able to detect what it is.

The module should be able to extract the following:

- Text messages / SMS / MMS
- Call Logs
- Contacts
- Tango Messages
- Words with Friends Messages
- GPS from the browser and Google Maps
- GPS from cache.wifi and cache.cell files

NOTE: These database formats vary by version of OS and different vendors can place the databases in different places. Autopsy may not support all versions and vendors.

NOTE: This module is not exhaustive with its support for Android. It was created as a starting point for others to contribute plug-ins for 3rd party apps. See the Developer docs for information on writing modules.

Configuration

There is no configuration required.

Using the Module

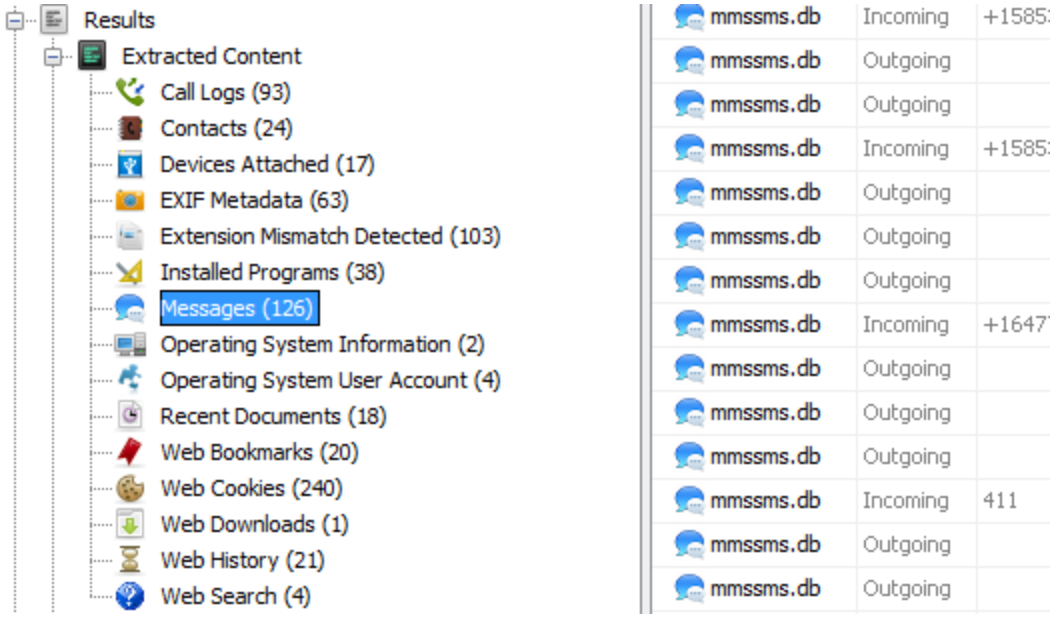
Simply add your physical images or file system dumps as data sources and enable the Android Analyzer module.

Ingest Settings

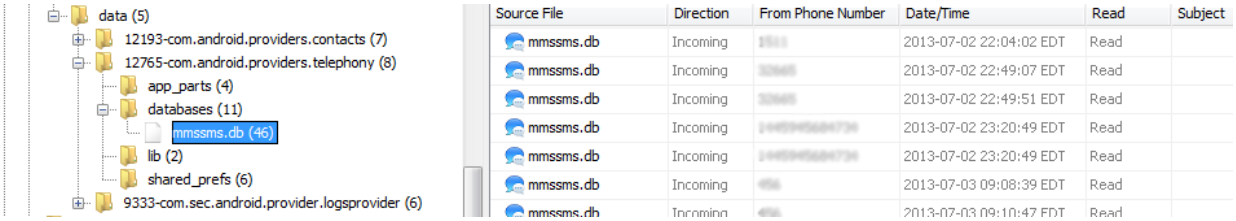
There is no runtime ingest settings required.

Seeing Results

The results show up in the tree under "Results", "Extracted Content".



Messages can also be seen by browsing to the source file in the Data Sources tree, which will display the messages in the Results Viewer to the right. Any messages with attachments will be shown under the source file in the tree, and the attachments can be seen in the Result Viewer.



Interesting Files Identifier Module

What Does It Do?

The Interesting Files module allows you to search for files or directories in a data source and generate alerts when they are found. You configure rules for the files that you want to find.

Use this to be notified when certain things are found. There are examples below that generate alerts when VMWare images are found or when iPhone backup files are found. This module is useful for file types that will frequently have a consistent name and that may not be part of the standard checklist that you look for, or if you simply want to automate your checklist.

Configuration

Add rules using "Tools", "Options", "Interesting Files".

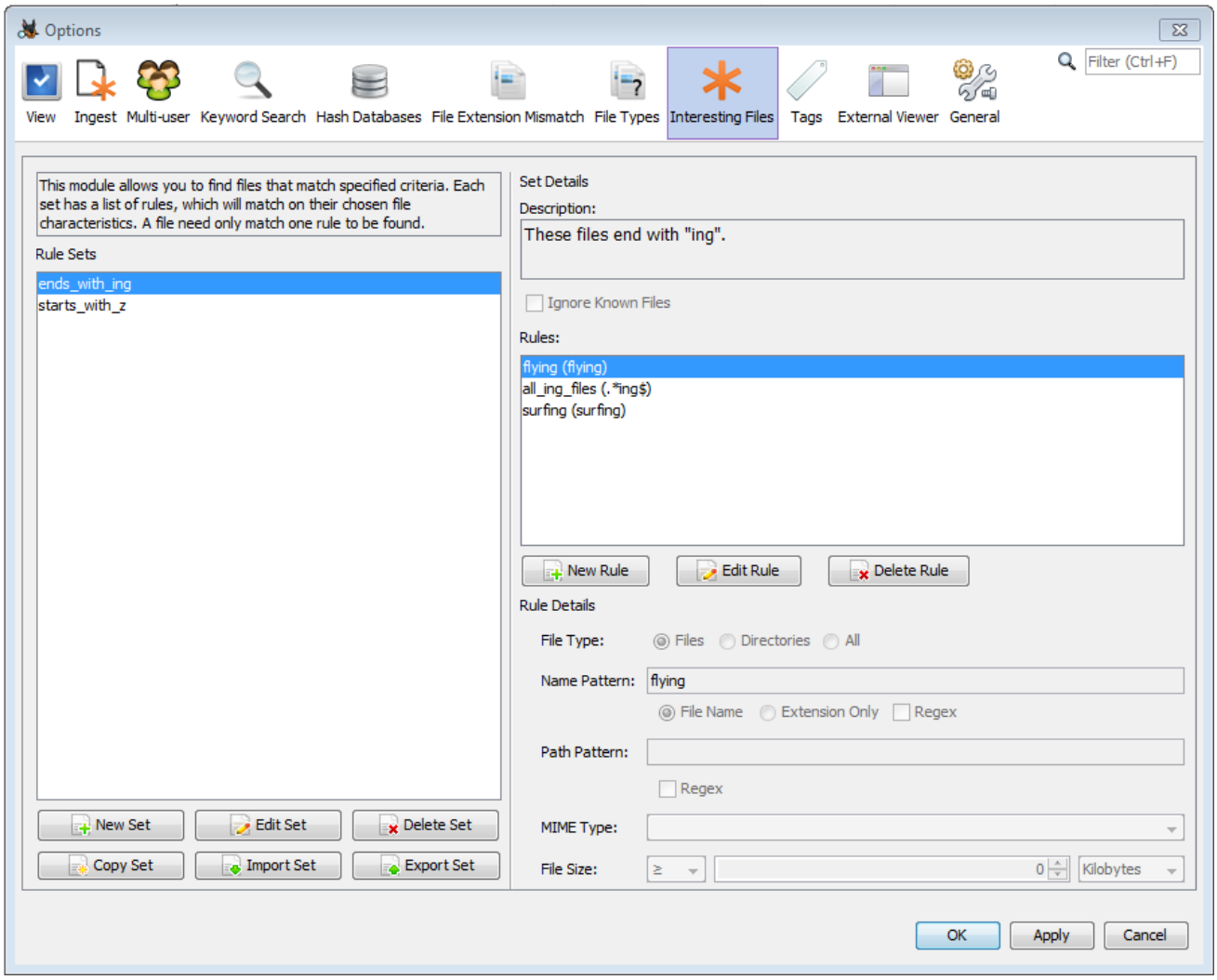
All rules need to be part of a set. Select "New set" on the left side panel to create a new set. Sets need to have the following defined:

- Set Name (required)
- Set Description (optional)

Sets can be renamed, edited, copied, and imported and exported from the left side panel.

Rules specify what to look for in a data source. Each rule specifies:

- Type: If the rule should be applied to only files, only directories, or both files and directories.
- Name Pattern: String to match the file name against. Note that you can enter multiple extensions in a comma-separated list.
- Name Pattern Type: Should the pattern be matched against the full file type or just the extension.
- Path Pattern: A substring of the parent path that must be matched. This allows you to restrict generic names to a specific structure (such as an application name). A substring match is performed.
- Rule Name: Additional details that are displayed in the UI when that rule is matched. This allows you to determine which rule in the set matched.



VMWare Example

This set of rules is to detect VMWare Player or vmdk files. This would help to make sure you investigate the virtual machines for additional evidence.

NOTE: This is not extensive and is simply a minimal example:

- Set Name: VMWare
- Rule 1:
    - Type: Files
    - Full Name: vmplayer.exe
    - Name: Program EXE
- Rule 2:
    - Type: Files
    - Extension: vmdk
    - Name: VMDK File

iPhone Backups Example

This set of rules is to detect a folder for iPhone Backups. These are typically in a folder such as "%AppData%\Roaming\Apple Computer\MobileSync\Backup" on Windows. Here is a rule that you could use for that.

- Set Name: iPhone Backups
- Rule 1:
    - Type: Directory
    - Name: Backup
    - Path: Apple Computer/MobileSync

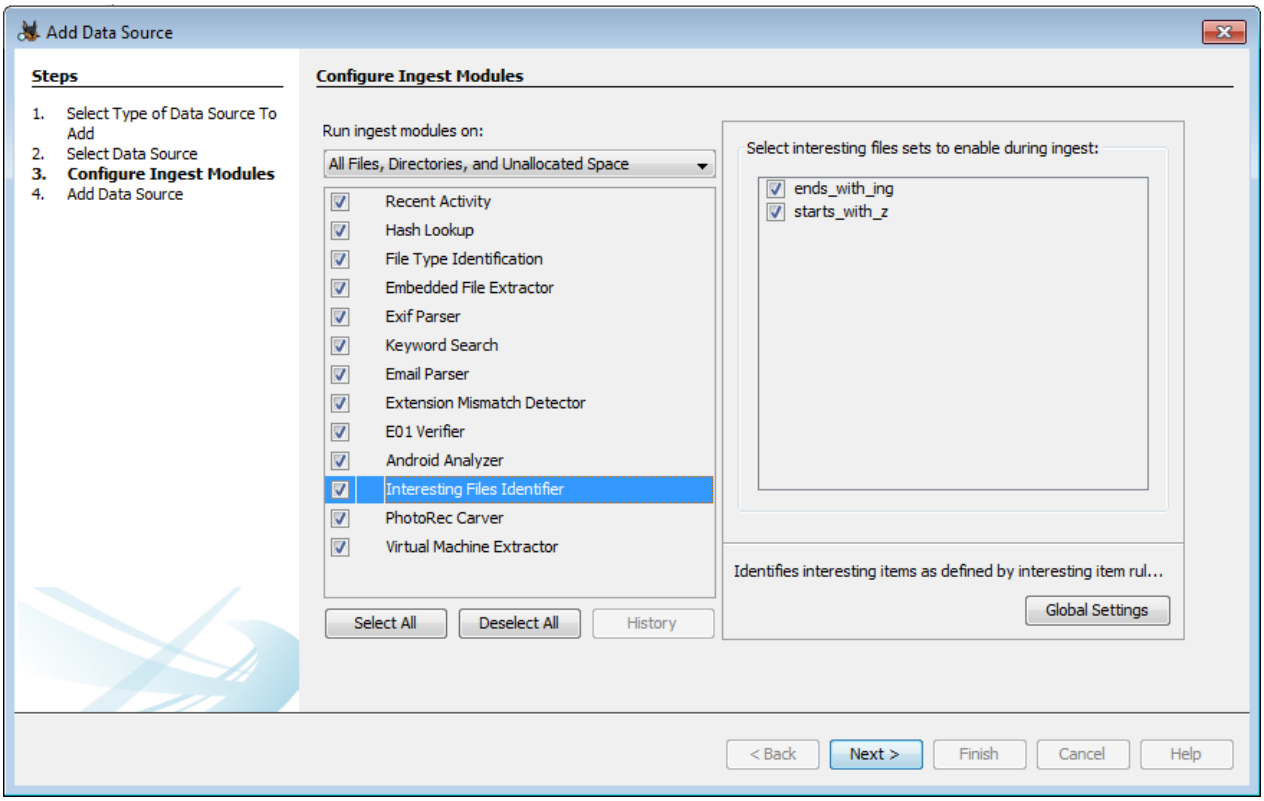
Using the Module

When you enable the Interesting Files module, you can choose what rule sets to enable. To add rules, use the "Advanced" button from the ingest module panel.

When files are found, they will be in the Interesting Files area of the tree. You should see the set and rule names with the match.

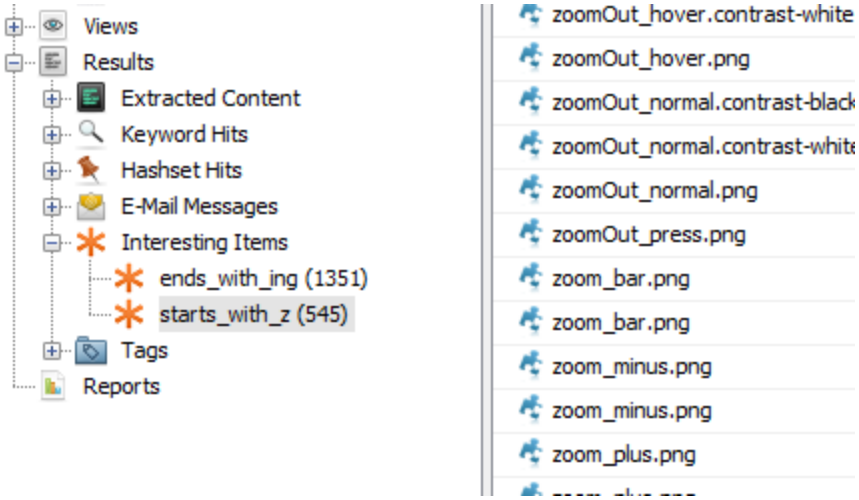
Ingest Settings

When running the ingest modules, the user can choose which interesting file rules to enable .



Seeing Results

The results show up in the tree under "Results", "Interesting Items".



PhotoRec Carver Module

What Does It Do?

The PhotoRec Carver module carves files from unallocated space in the data source and sends the files found through the ingest processing chain.

This can help a reviewer discover more information about files that used to be on the device and were subsequently deleted. These are simply extra files that were found in "empty" portions of the device storage.

Configuration

There is nothing to configure for this module.

Using the Module

Select the checkbox in the Ingest Modules settings screen to enable the PhotoRec Carver. Ensure that "Process Unallocated Space" is selected.

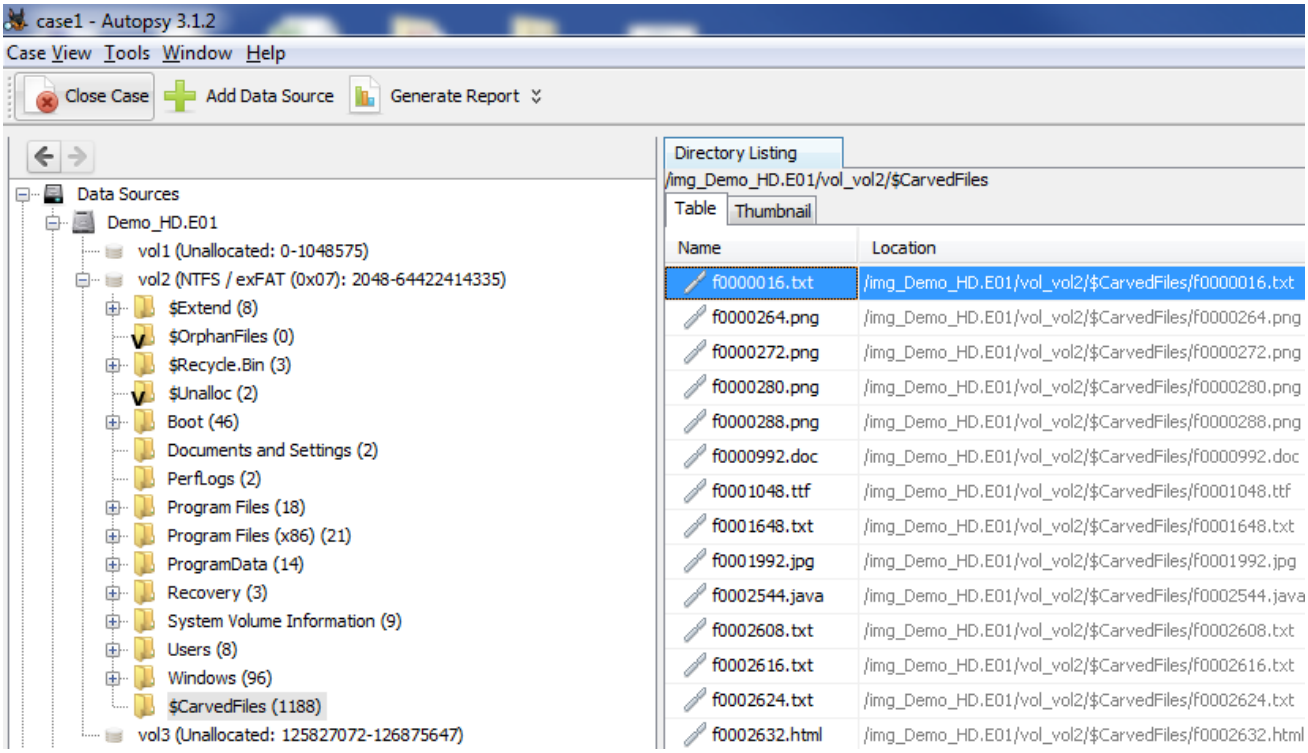
Ingest Settings

The run-time setting for this module allows you to choose whether to keep corrupted files.

Also note that the "Run ingest modules on" selection needs to include unallocated space for this module to run.

Seeing Results

The results of carving show up on the tree under the appropriate data source with the heading "$CarvedFiles".



Applicable types also show up in the "Views", "File Types" portion of the the tree, depending upon the file type.

Custom File Signatures

To add custom file signatures, create a file (if it does not exist) photorec.sig in the user home directory (for example - /home/john/photorec.sig, or C:\Users\john\photorec.sig). The photorec.sig file should contain one expression per line. For example, to detect a file foo.bar which has header signature - 0x4141414141414141, add an expression

```
bar 0 0x4141414141414141
```

in photorec.sig where *bar* is the file extension, *0* is the signature offset, and *0x4141414141414141* is the signature. Add another expression on a new line to detect another custom file based on its signature.

Central Repository

Overview

The central repository allows a user to find matching artifacts both across cases and across data sources in the same case. It is a combination of an ingest module that extracts, stores, and compares properties against lists of notable properties, a database that stores these properties, and an additional panel in Autopsy to display other instances of each property. The central repository database can either be SQLite or PostgreSQL.

The following are some use cases for the central repository:

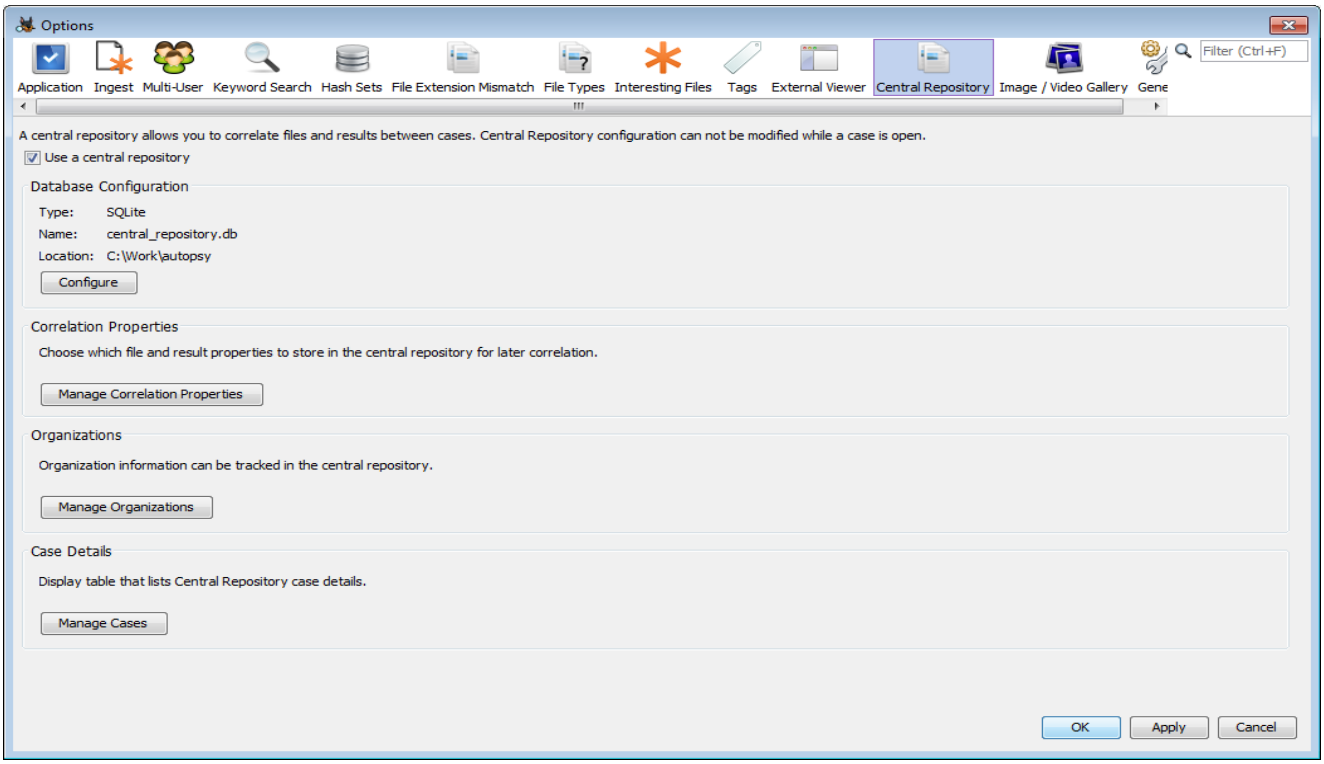
- **Finding Other Instances of a Property**
  - If you navigate to a file or Autopsy artifact (such as a Web History item), there is a content viewer in the bottom right that will show you other instances of this property across the data stored in the central repository.
- **Alerting When Previously Notable Properties Occur**
  - You can use the central repository to record which properties were associated with files and artifacts that were evidence (or notable). Once these properties have been tagged as notable they will be added to the Interesting Items section of the tree when seen again in any future cases.
- **Storing Hash Sets**
  - You can create and import hash sets into the central repository instead of using local copies in the **Hash Lookup module**. These hash sets are functionally equivalent to local hash sets but can be shared among multiple analysts (when using a PostgreSQL central repository).

Terms and Concepts

- **Central Repository** - The Autopsy feature containing the central repository database and Correlation Engine Ingest Module. Also responsible for displaying correlated properties to the user
- **Central Repository Database** - the SQLite or PostgreSQL database that holds all the data
- **Correlation Engine Ingest Module** - The ingest module responsible for adding new properties to the database and comparing these properties against existing notable properties
- **Property** - The data being stored/correlated. These can be file paths/MD5 hashes, email addresses, phone numbers, etc.

Setup

To start, open the main options panel and select the "Central Repository" icon.



Setting up the Database

On the central repository options panel, check the 'Use a Central Repository' option and then click the Configure button to set up a database. There are two options here:

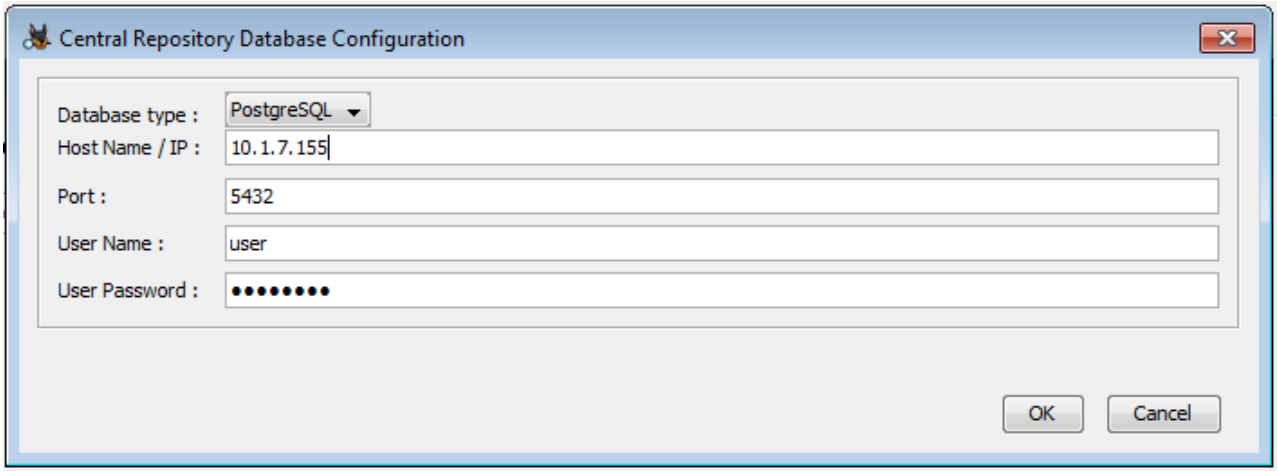
- **SQLite** - This option stores the database in a file. It should only be used when a single client will be accessing the database.
- **PostgreSQL** - This option uses a database server running either on the user's host or a remote server. This option must be used if multiple users will be using the same database.

Once a database has been configured, the lower two buttons on the main panel will be enabled, which will be described below.

Setting up PostgreSQL Deployment

If needed, see the **Install and Configure PostgreSQL** for help setting up your PostgreSQL server.

For PostgreSQL all values are required, but some defaults are provided for convenience.

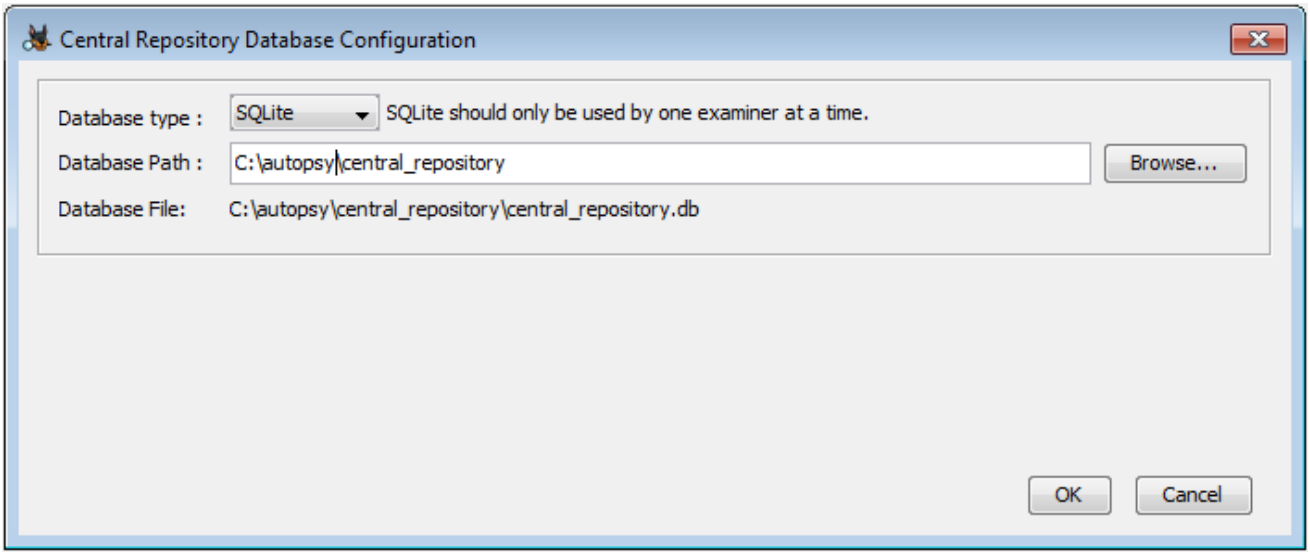


- Host Name/IP is the hostname or IP of your PostgreSQL server.
- Port is the port that the PostgreSQL server is listening on; default is 5432.
- User Name is a PostgreSQL user that can create and modify databases
- User Password is the password for the user.

If the database does not exist, you wll be prompted to create it.

Setting Up SQLite Deployment

Select SQLite in the Database Type to set up a SQLite database. SQLite databases should not be used if more than one client will be accessing the central repository.

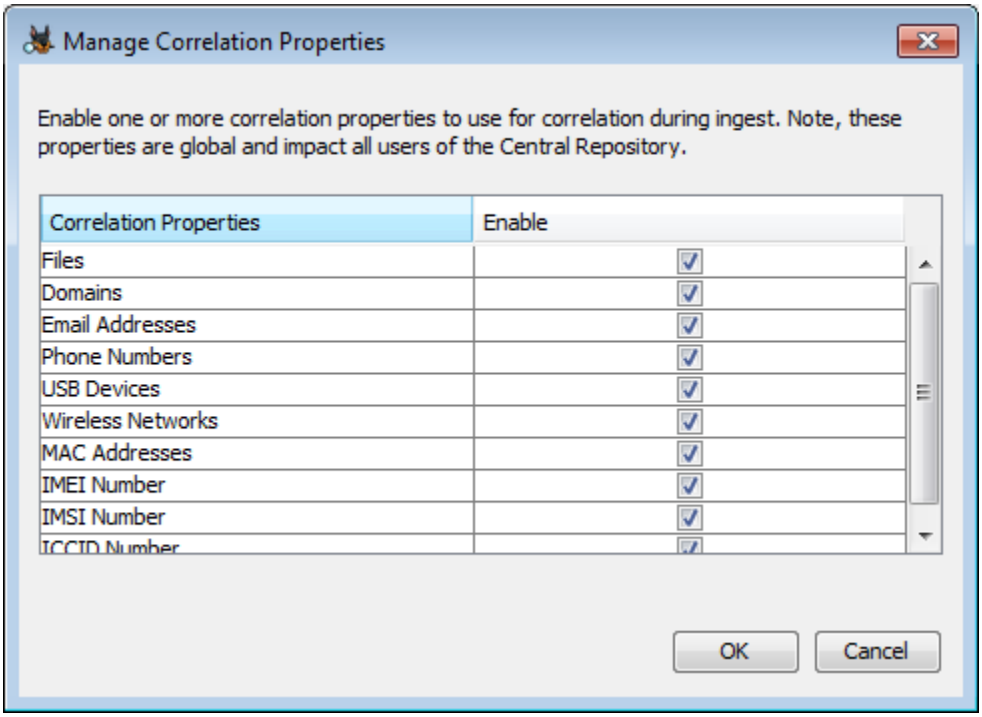


Enter or browse to a folder for the database. If the database file does not exist in that folder, you will be prompted to create it.

Manage Correlation Properties

The Correlation Engine ingest module can save different types of properties to the database. By default all properties are recorded, but this setting can be changed on the options panel through the

Manage Correlation Properties button. Note that these settings are saved to the database, so in a multi-user setting any changes will affect all users.



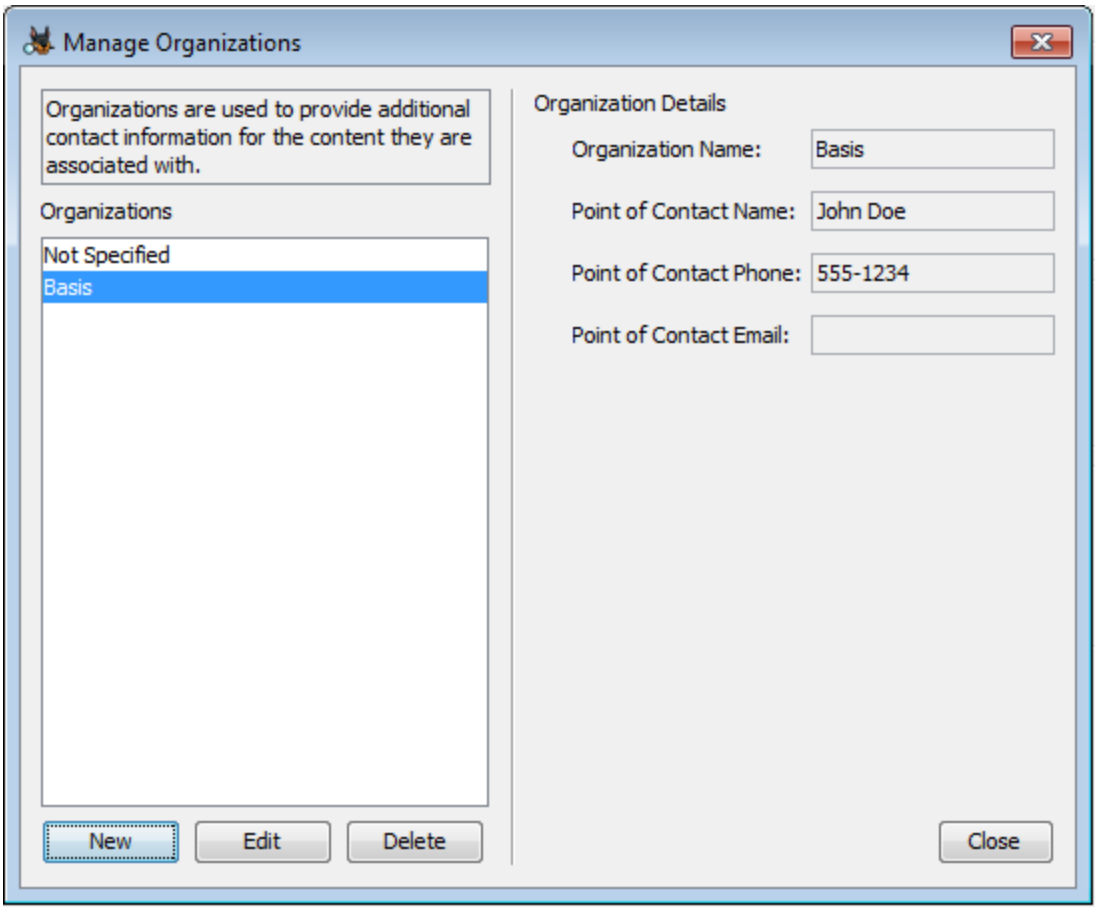
Descriptions of the property types:

- **Files**
  - Files are correlated based on MD5 hash and file path and name. The Hash Lookup ingest module must be enabled.
- **Domains**
  - Domains are extracted from the various web artifacts, which primarily come from the Recent Activity module
- **Email Addresses**
  - Email addresses are pulled from Email Address hits from the Keyword Search module.
- **Phone Numbers**
  - Phone numbers are currently only extracted from call logs, contact lists and message, which come from the Android Analyzer module.
- **USB Devices**
  - USB device properties come from the registry parsing in the Recent Activity Module.
- **Wireless Networks**
  - Wireless networks are correlated on SSIDs, and come from the registry parsing in the Recent Activity Module.
- **MAC Addresses**
  - MAC address properties are currently only created by custom Autopsy modules
- **IMEI Number**
  - IMEIs properties are currently only created by custom Autopsy modules

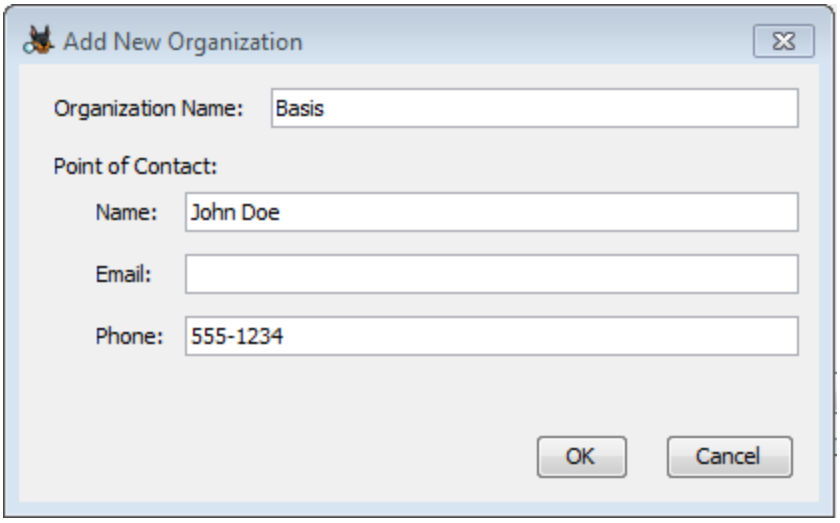
- **IMSI Number**
  - IMSI properties are currently only created by custom Autopsy modules
- **ICCID Number**
  - ICCID properties are currently only created by custom Autopsy modules

Manage Organizations

Organizations are stored in the central repository and contain contact information for the given organization. Organizations are used for Hash Sets saved in the central repository, and can also be associated with Autopsy cases.

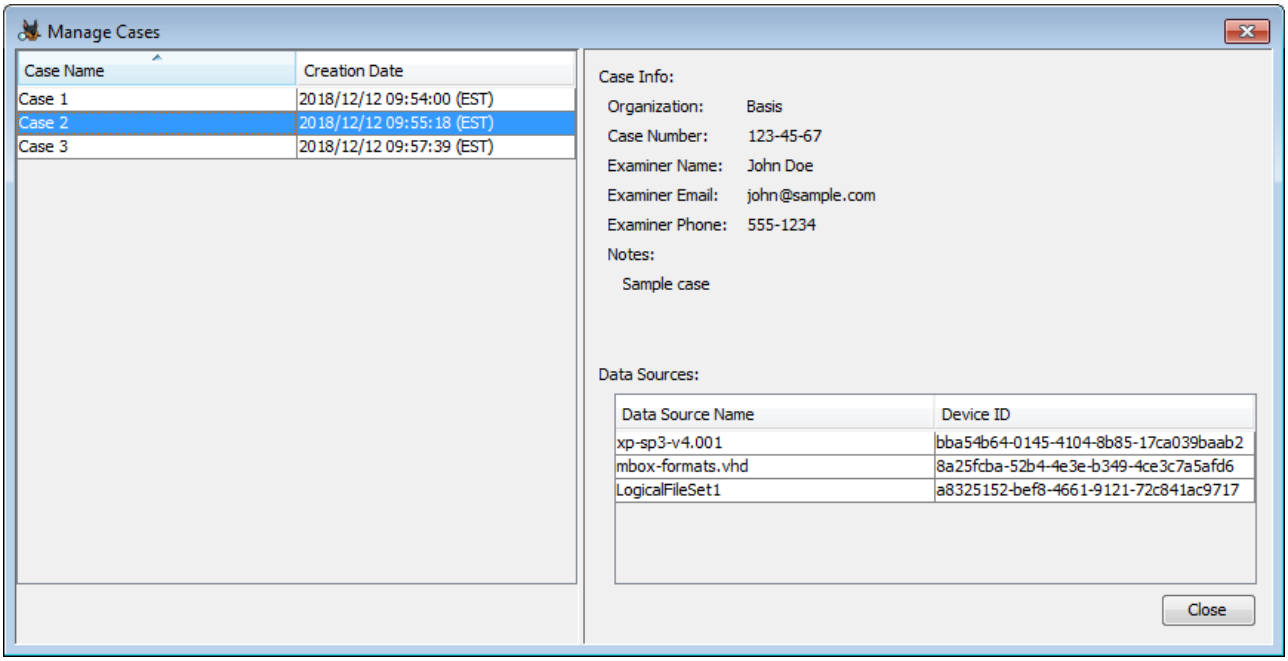


One default org, "Not Specified" will always be present in the list. New organizations can be created, edited, and deleted through the appropriate buttons. Note that any organization that is currently in use by a case or hash set can not be deleted. All fields apart from the organization name are optional.



Manage Cases

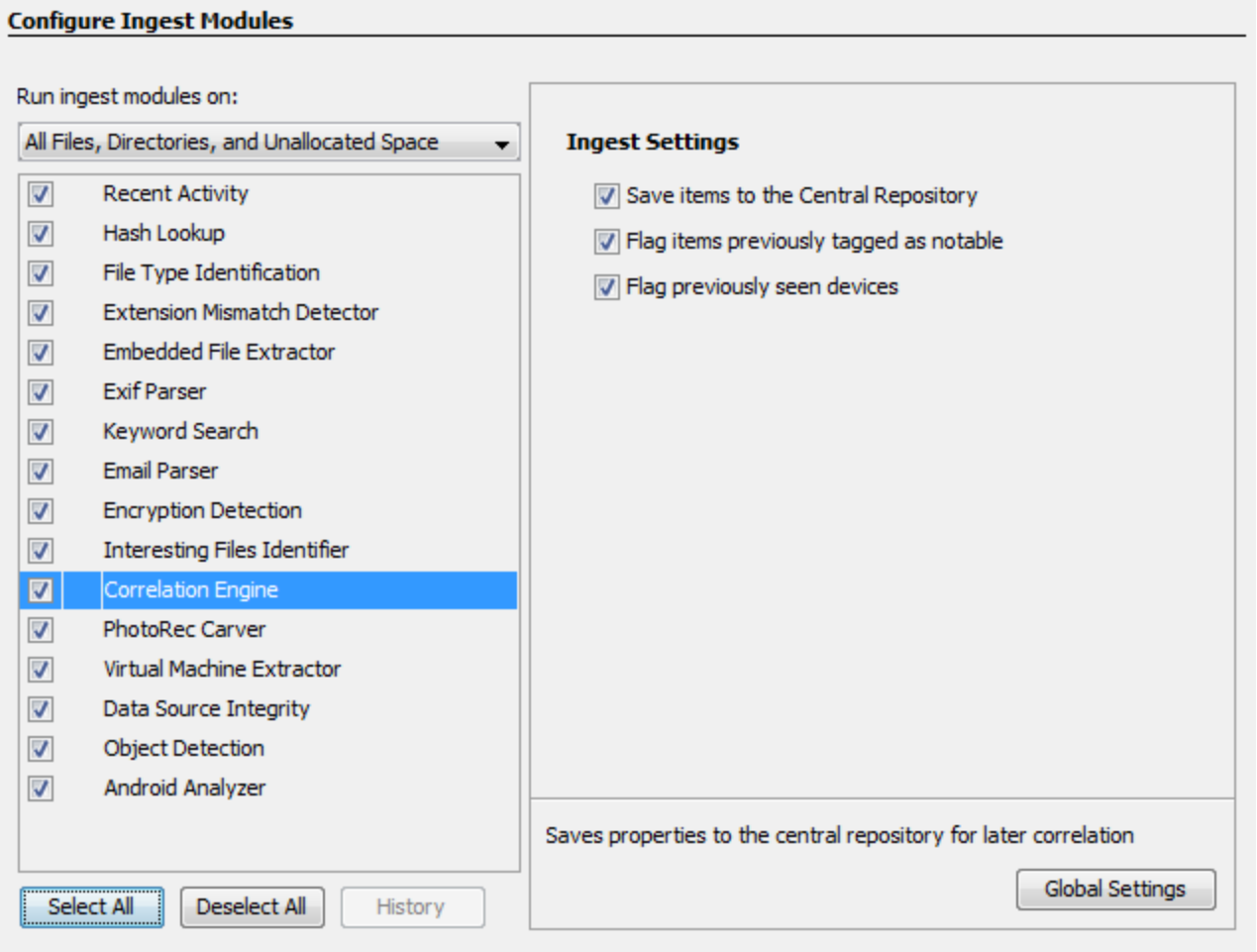
Displays a list of all cases that are in the central repository database and details about each case.



Using the Central Repository

Correlation Engine Module

The Correlation Engine ingest module is responsible for adding properties to the database and comparing each property against the list of notable properties. It is best to run all ingest modules to get the most out of the Correlation Engine. For example, if Hash Lookup is not run then the Correlation Engine module will not put any files into the database. If the Correlation Engine module is not run on a particular case but a central repository is enabled, there will still be some limited functionality. The Content Viewer will still display matching properties from other cases/data sources where the Correlation Engine was run.

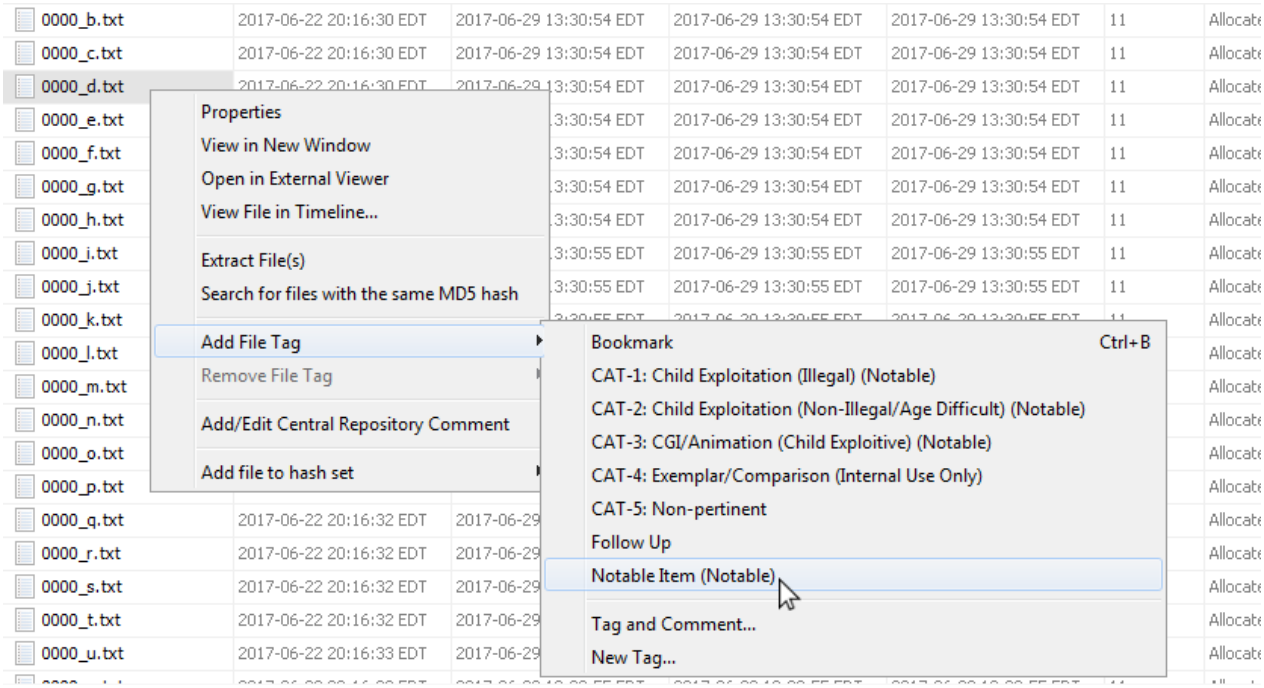


There are three settings for the Correlation Engine ingest module:

- **Save items to the Central Repository** - This should only be unselected in the rare case that you don't want to add any properties from the current data source to the central repository, but still want to flag past occurrences.
- **Flag items previously tagged as notable** - Enabling this causes Interesting Item/File artifacts to be created when properties matching those previously flagged are found. See the next section **Tagging Files and Artifacts** for details.
- **Flag previously seen devices** - When this is enabled, an Interesting Item artifact will be created if any device-related property (USB, MAC Address, IMSI, IMEI, ICCID) is found that is already in the central repository, regardless of whether they have been flagged.

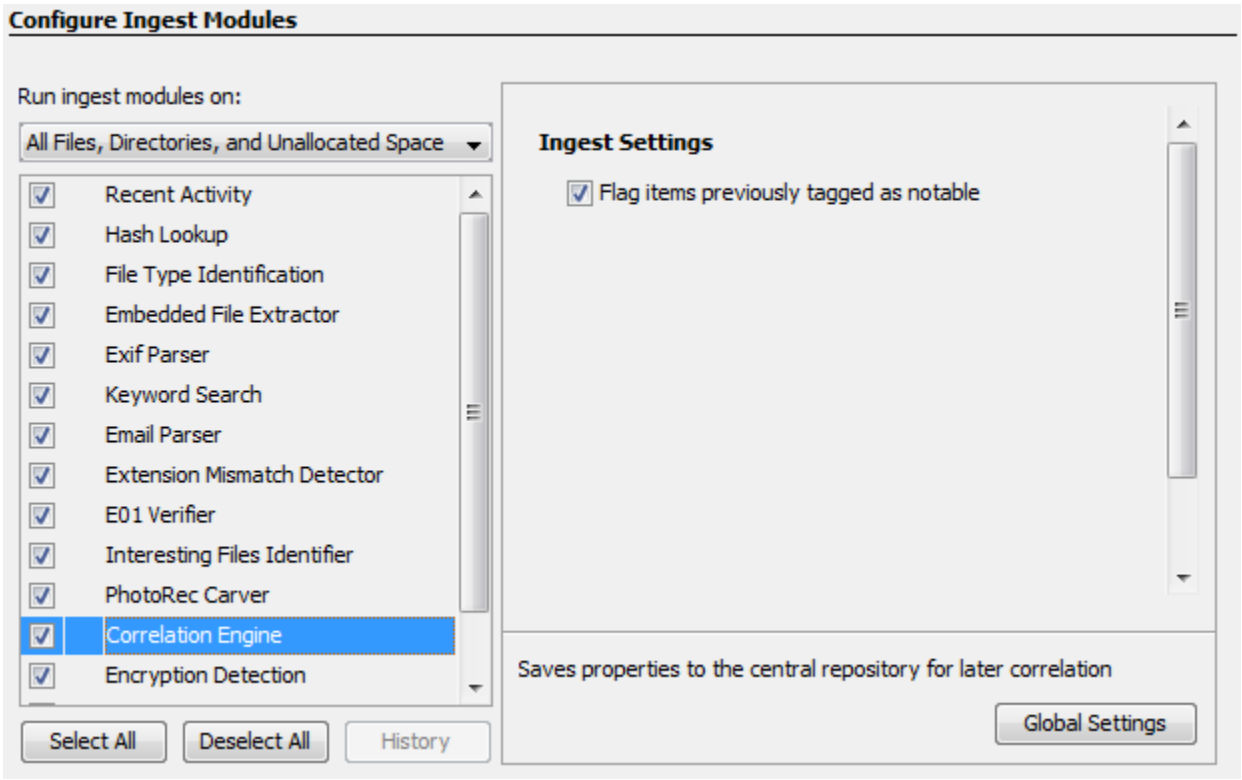
Tagging Files and Artifacts

Tagging a file or artifact with a "notable" tag will change its associated property in the central repository to notable as well. By default, there will be a tag named "Notable Item" that can be used for this purpose. See the **Tagging page** for more information on creating additional tags with notable status. Any future data source ingest (where this module is enabled) will use those notable properties in a similar manner as a Known Bad hash set, causing matching files and artifacts from that ingest to be added to the Interesting Items list in that currently open case.



If a tag is accidentally added to a file or artifact, it can be removed though the context menu. This will remove its property's notable status in the central repository.

If you would like to prevent the Interesting Items from being created in a particular case, you can disable the flagging through the run time ingest properties. Note that this only disables the Interesting Item results - all properties are still added to the central repository.



Viewing Results

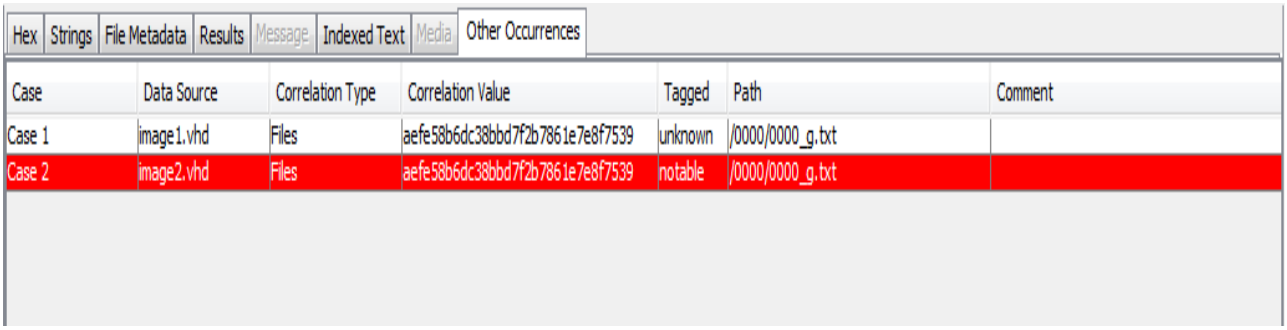
Results from enabling a central repository and running the Correlation Engine Ingest Module can be seen in two places:

- The Content Viewer for each file or artifact will display all matching properties from other cases/data sources
- The Interesting Files node of the result tree will contain any files or results that matched properties previously marked as notable

Content Viewer

The **Content Viewer** panel is where previous instances of properties are displayed. Without a central repository enabled, this "Other Occurrences" panel will show files with hashes matching the selected file within the current case. Enabling a central repository allows this panel to also display matching properties stored in the database, and adds some functionality to the row. Note that the Correlation Engine Ingest Module does not have to have been run on the current data source to see correlated properties from the central repository. If the selected file or artifact is associated by one of the supported Correlation Types, to one or more properties in the database, the associated properties will be displayed. Note: the Content Viewer will display ALL associated properties available in the database. It ignores the user's enabled/disabled Correlation Properties.

By default, the rows in the content viewer will have background colors to indicate if they are known to be of interest. Properties that are notable will have a Red background, all others will have a White background.



The user can click on any column heading to sort by the values in that column.

If the user right-clicks on a row, a menu will be displayed. This menu has several options.

1. Select All
2. Export Selected Rows to CSV
3. Show Case Details
4. Show Frequency
5. Add/Edit Comment

Select All

This option will select all rows in the Content Viewer table.

Export Selected Rows to CSV

This option will save ALL SELECTED rows in the Content Viewer table to a CSV file. By default, the CSV file is saved into the Export directory inside the currently open Autopsy case, but the user is free to select a different location.

Note: if you want to copy/paste rows, it is usually possible to use CTRL+C to copy the selected rows and then CTRL+V to paste them into a file, but it will not be CSV formatted.

Show Case Details

This option will open a dialog that displays all of the relevant details for the selected case. The details will include:

- Case UUID
- Case Name
- Case Creation Date
- Case Examiner contact information
- Case Examiner's notes

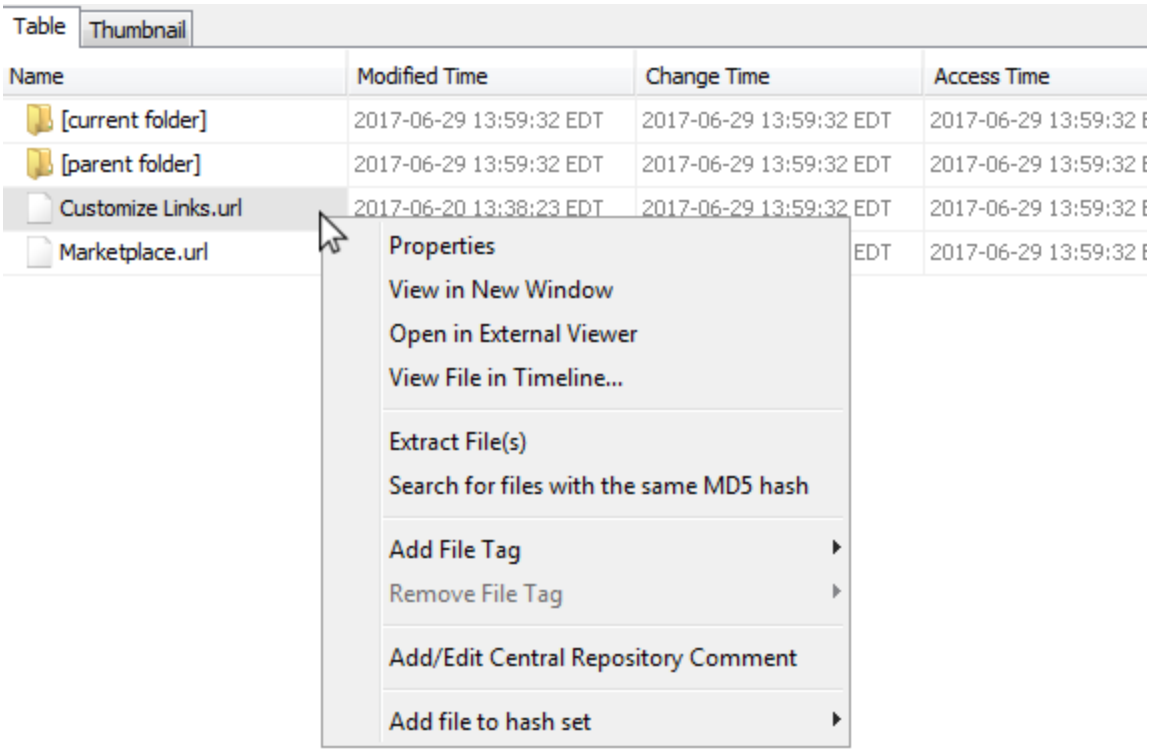
These details would have been entered by the examiner of the selected case, when creating the case or later by visiting the Case -> Case Properties menu.

Show Frequency

This shows how common the selected file is. The value is the percentage of case/data source tuples that have the selected property.

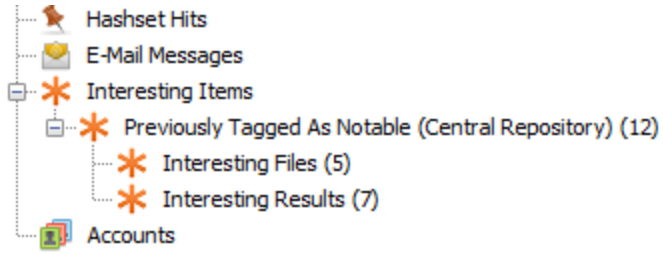
Add/Edit Comment

This allows you to add a comment for this entry or edit an existing comment. If you want instead to edit the comment of the originally selected node, it can be done by right clicking on the original item in the result viewer and selecting "Add/Edit Central Repository Comment".



Interesting Items

In the Results tree of an open case is an entry called Interesting Items. When this module is enabled, all of the enabled Correlatable Properties will cause matching files and artifacts to be added to this Interesting Items tree during ingest.



As an example, suppose the Files Correlatable Property is enabled and the ingest is currently processing a file "badfile.exe", and the MD5 hash for that file already exists in the database as a notable file property. In this case an entry in the Interesting Items tree will be added for the current instance of "badfile.exe" in the data source currently being ingested.

The same type of thing will happen for each enabled Correlatable Property.

In the case of the phone number correlatable type, the Interesting Items tree will start a sub-tree for each phone number. The sub-tree will then contain each instance of that notable phone number.

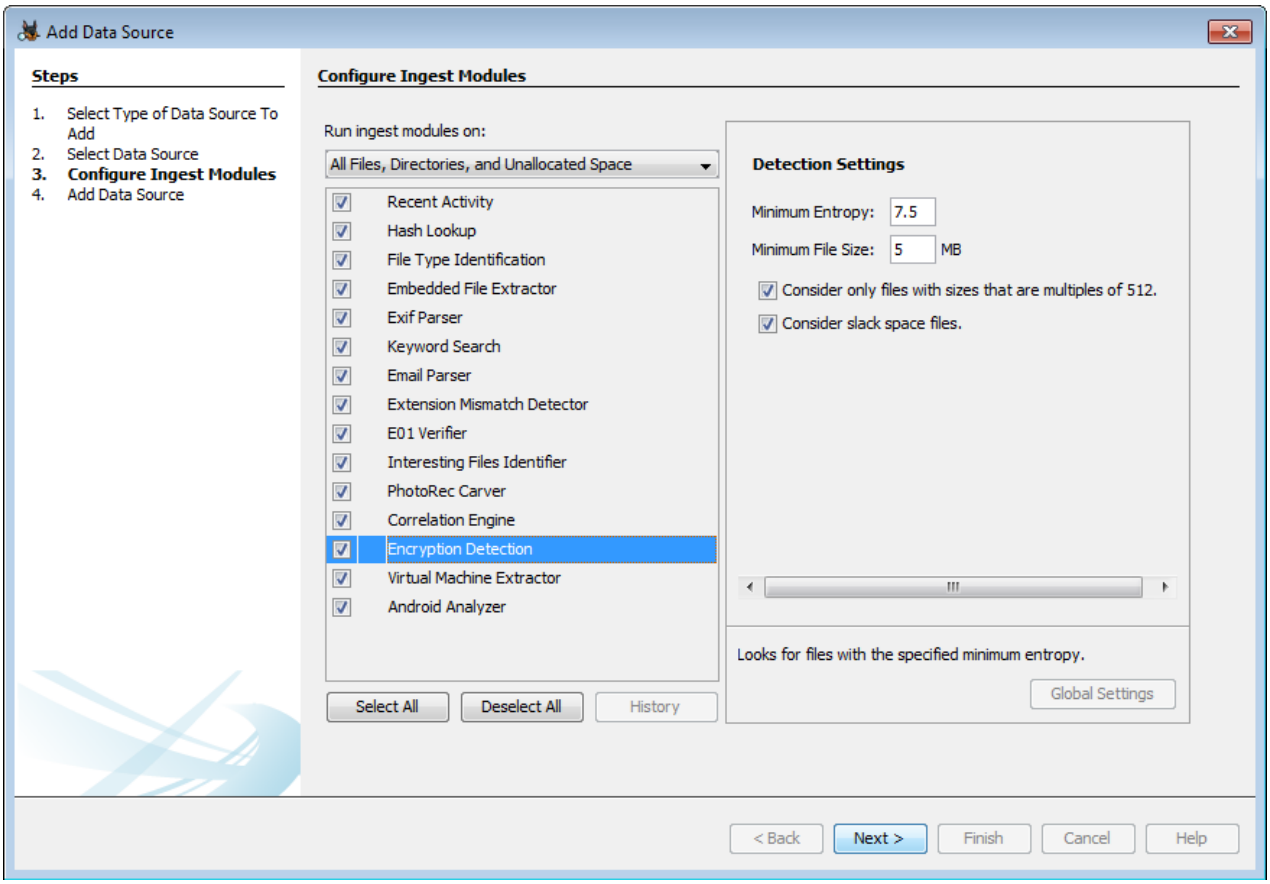
Encryption Detection Module

Overview

The Encryption Detection Module searches for files that could be encrypted using both a general entropy calculation and more specialized tests for certain file types.

Running the module

The module's settings can be configured at runtime. These settings only effect the tests that are based on entropy.



Minimum entropy can be set higher or lower, depending on how many false hits are being produced. There is also an option to only run the test on files whose size is a multiple of 512, which is useful for finding certain encryption algorithms.

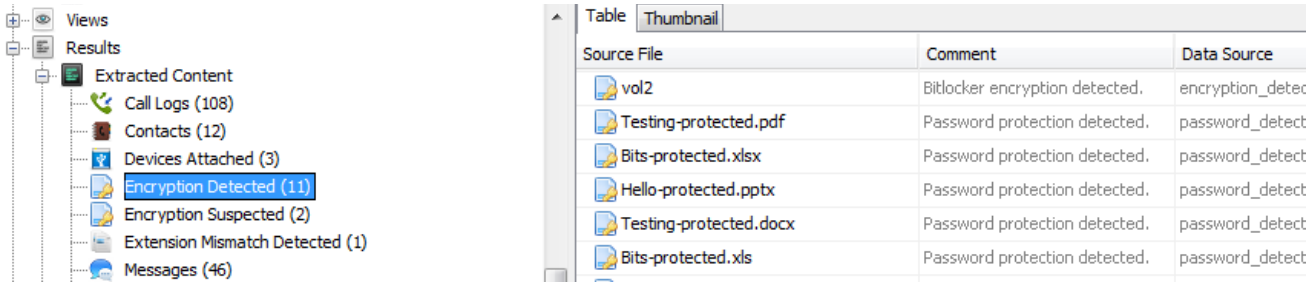
The module looks for the following types of encryption:

- Any file that has an entropy equal to or greater than the threshold in the module settings and that fits the file size constraints
- Password protected Office files, PDF files, and Access database files
- BitLocker volumes
- SQLCipher (uses the minimum entropy from the module settings)

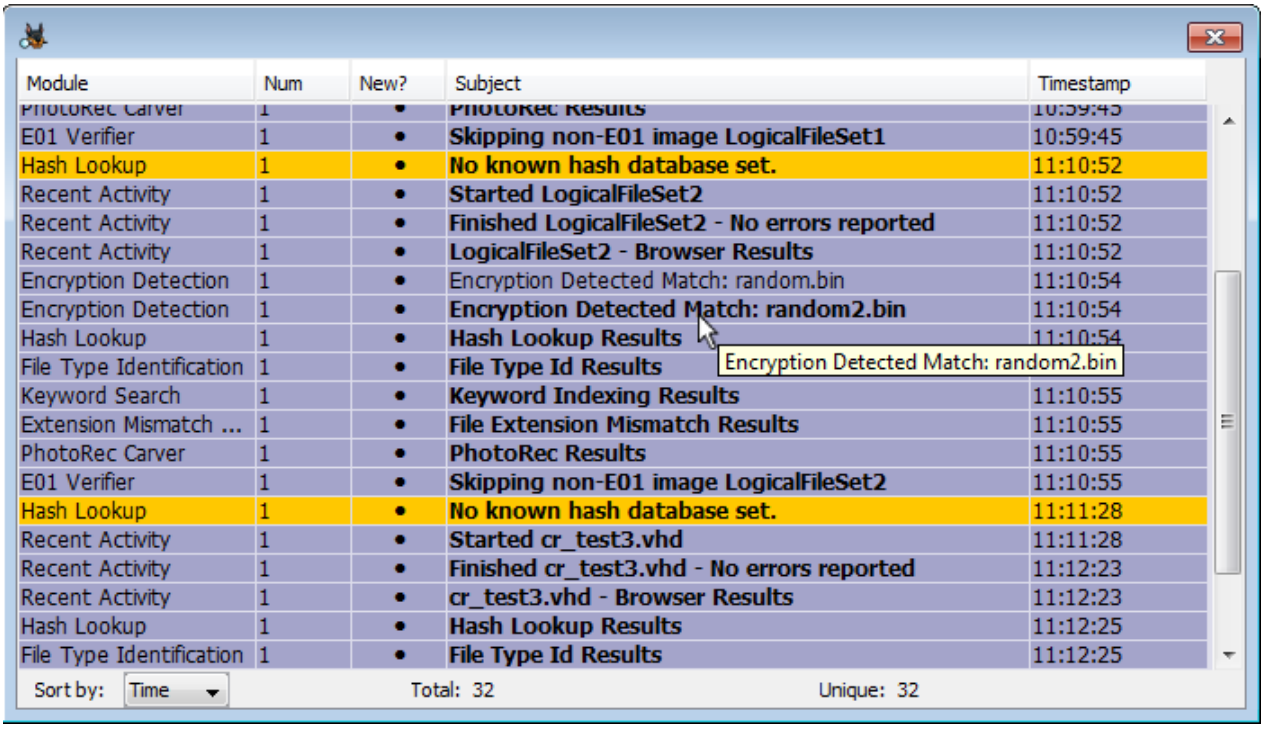
- VeraCrypt (uses the minimum entropy from the module settings)

Viewing results

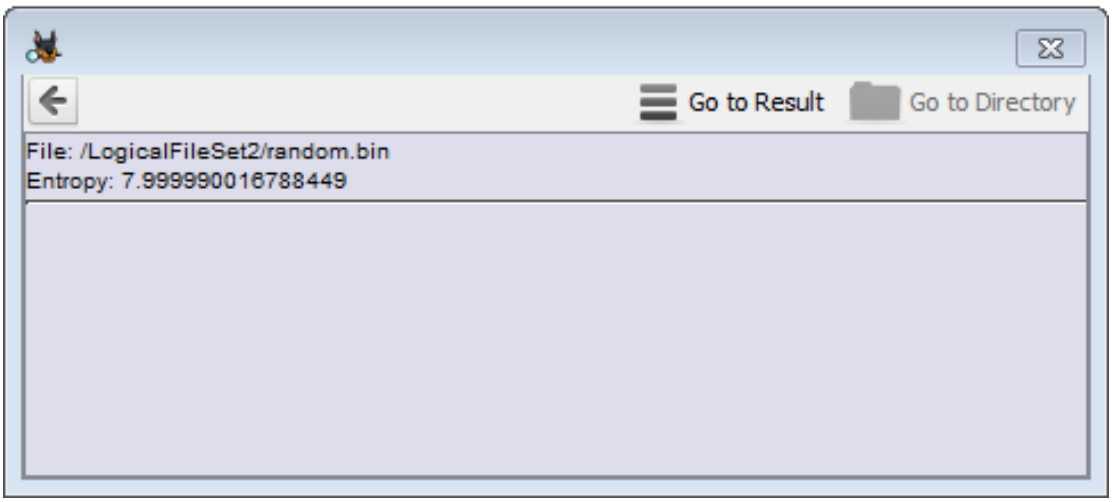
Files that pass the tests are shown in the Results tree under "Encryption Detected" or "Encryption Suspected". Generally, if the test used involved looking for a specific header/file structure, the result will be "Encryption Detected" and the type of encryption will be displayed in the Comment field. If the test was based on the entropy of the file, the result will be "Encryption Suspected" and the calculated entropy will be displayed in the Comment field.



Each hit also generates an inbox message. These are viewed through the warning triangle near the top of the screen.



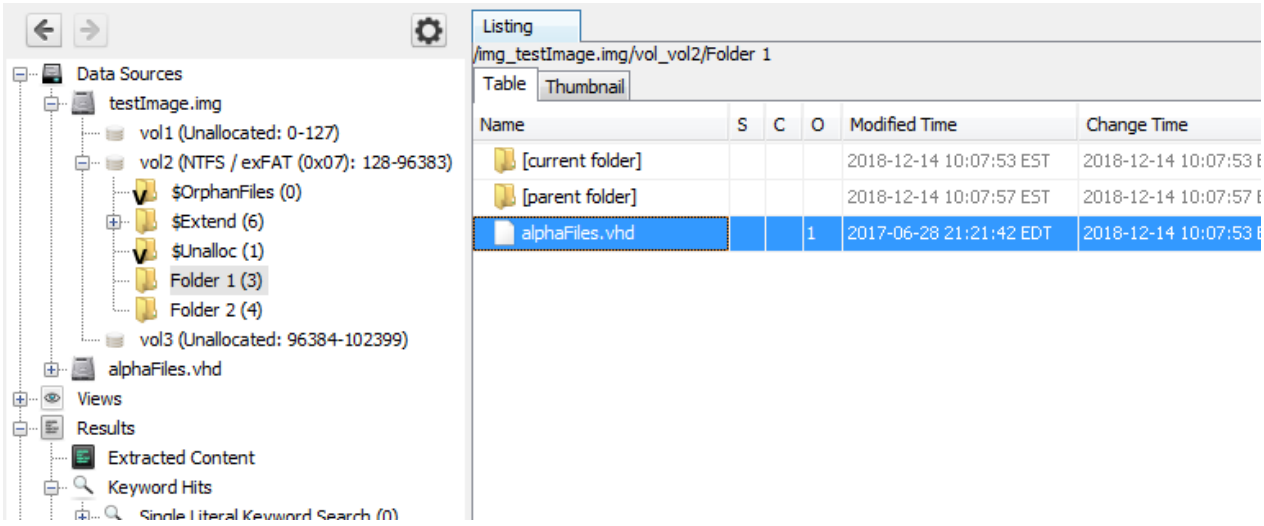
Selecting one of the encryption detection hits displays the calculated entropy of the file.



Virtual Machine Extractor Module

The Virtual Machine Extractor Module adds any virtual machines it finds in a data source to the case as new data sources. This includes virtual machine disk (.vmdk) files and virtual hard drive (.vhd) files. Note that each virtual disk will be extracted to the case folder.

In the example below, the original data source "testImage.img" contained a VHD file. This VHD "alphaFiles.vhd" was added to the case as a new data source, and it was processed by the same ingest modules that were run on the original image.

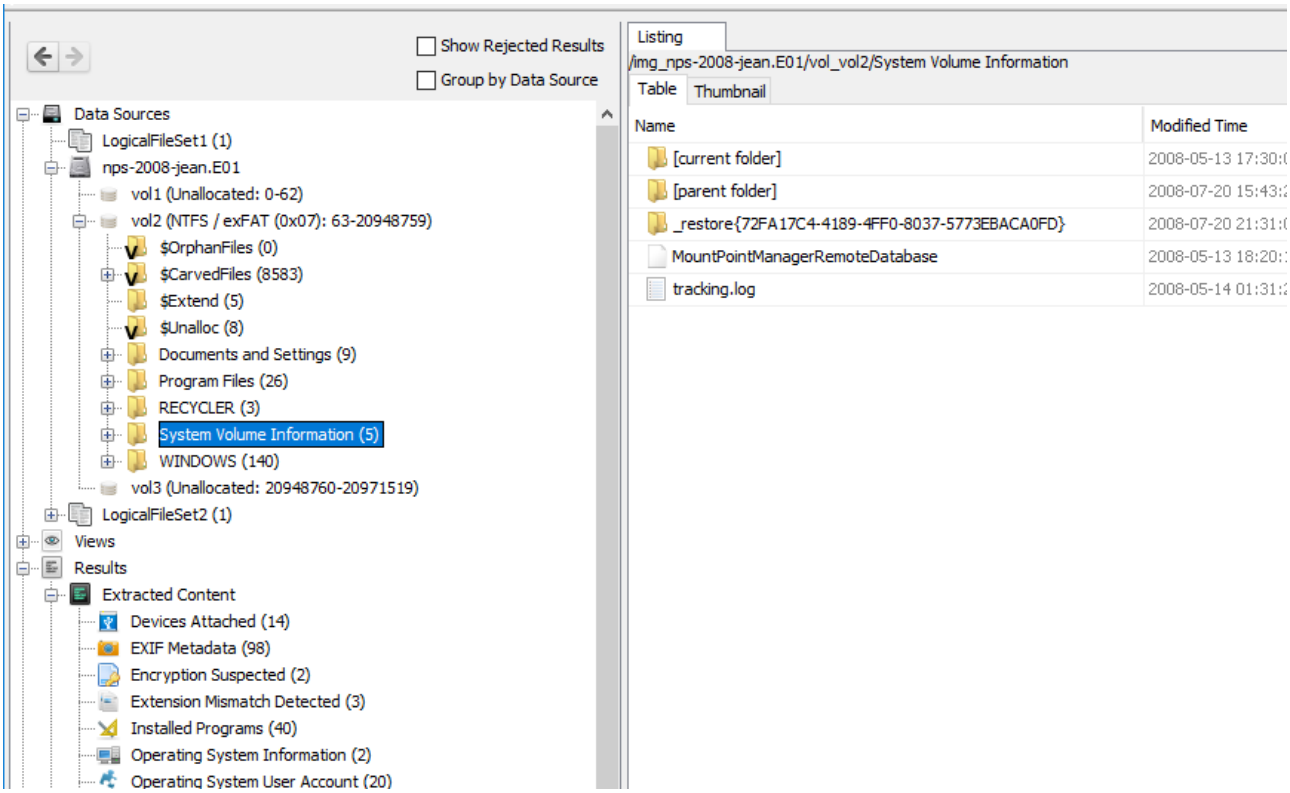


Manual Analysis

Tree Viewer

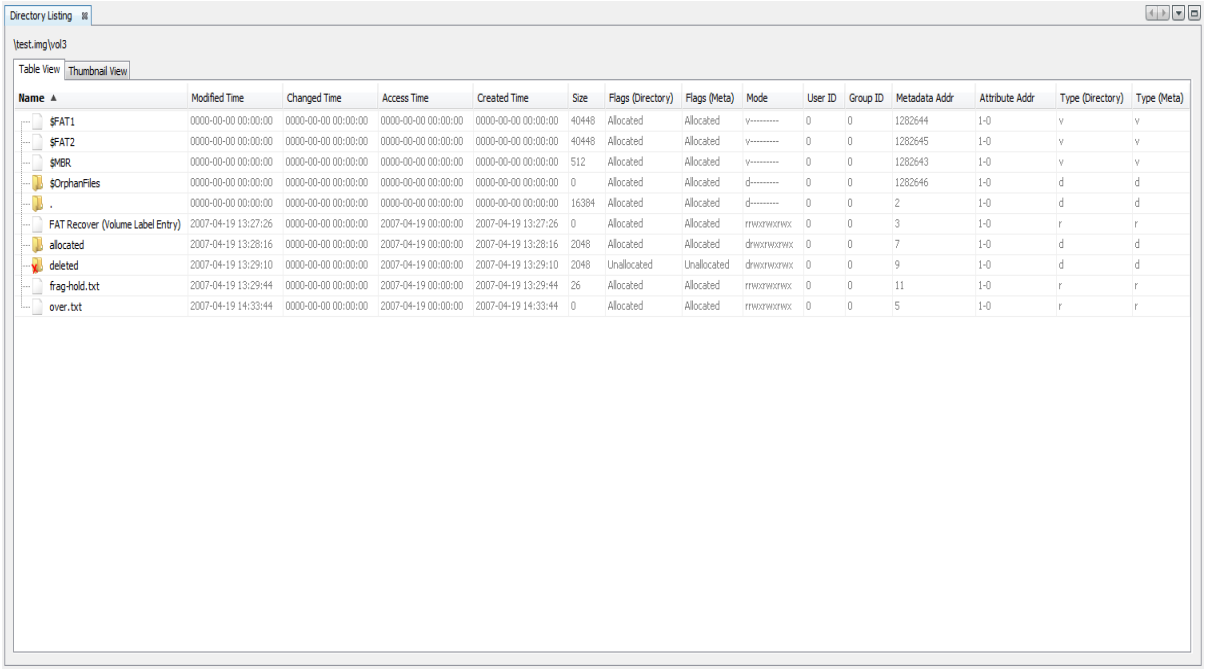
The Tree Viewer shows the discovered folders by the data sources they come from, as well as a list of files in the folders. It is located on the left side of the Autopsy screen. The "Group by Data Source" option on the top left moves all views, results, and tags under their corresponding data source.

Each folder in the tree on the left shows how many items are contained within it in parentheses after the directory name. See the picture below.

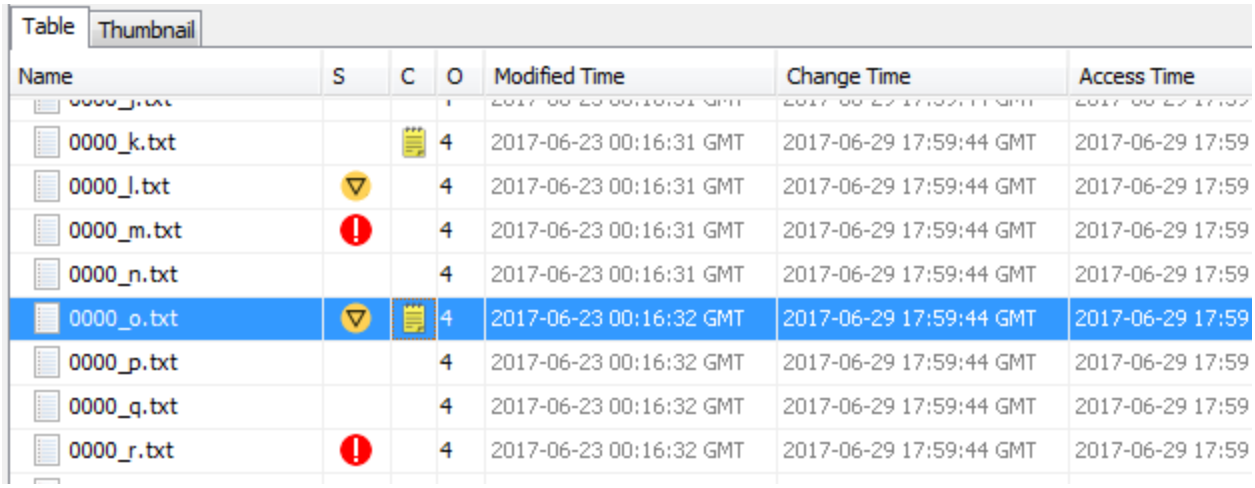


Result Viewer

The Result Viewer is located on the top right of the Autopsy screen. It shows lists of files and their corresponding attributes such as time, path, size, checksum, etc.



By default, the first three columns after the file name in the results viewer are named "S", "C" and "O".

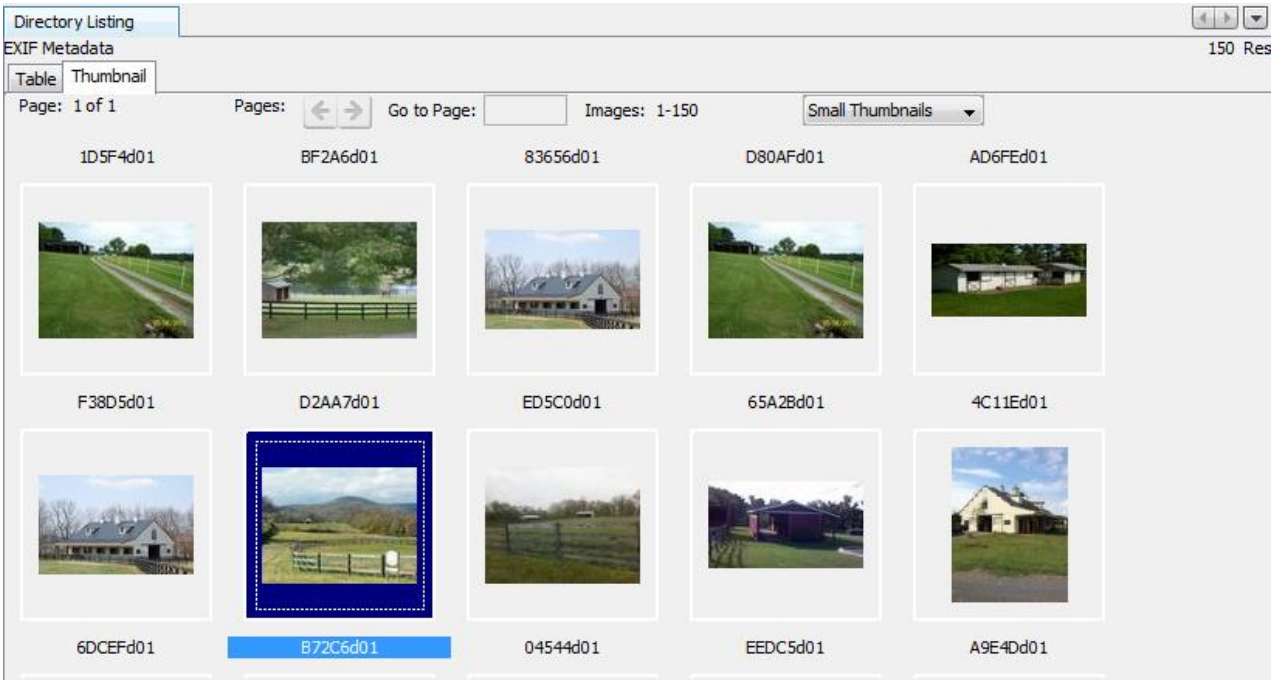


These columns display the following:

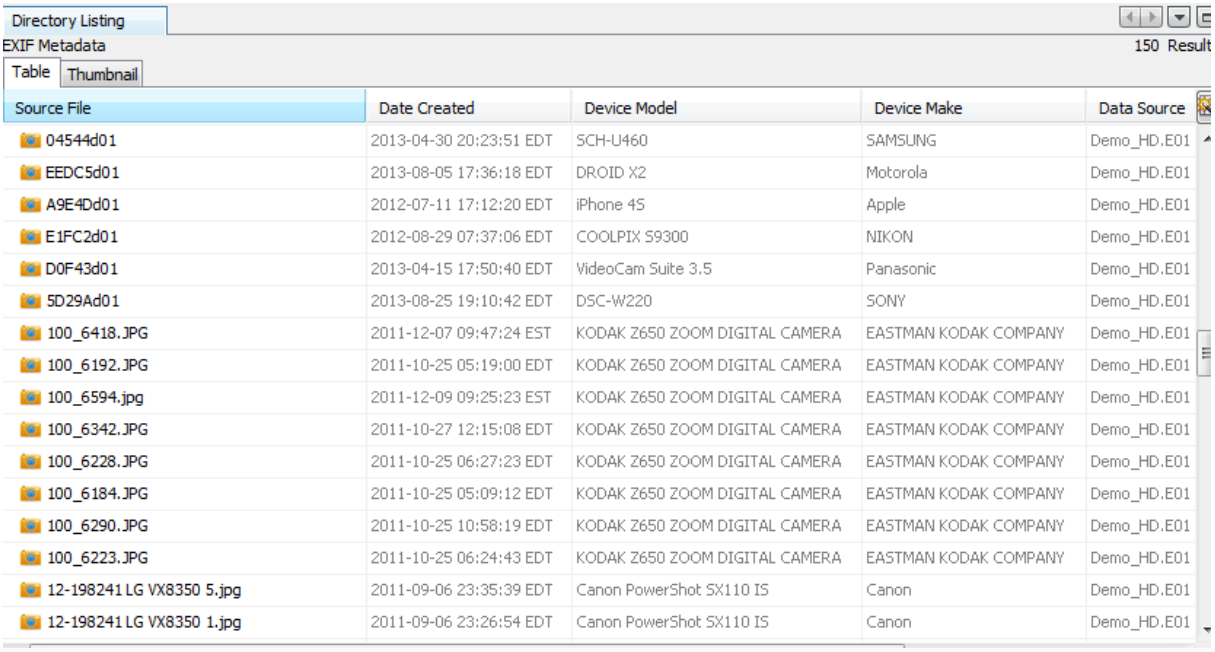
- (S)core column - indicates whether the item is interesting or notable
  - Displays a red icon if the file is a match for a notable hash set or has been tagged with a notable tag
  - Displays a yellow icon if the file has an interesting item match or has been tagged with a non-notable tag
- (C)omment column - indicates whether the item has a comment in the Central Repository or has a comment associated with a tag
- (O)ther occurrences column - indicates how many data sources in the Central Repository contain this item. The count will include the selected item.

To display more information about why an icon has appeared, you can hover over it. The Comment and Other occurrences columns query the Central Repository. If this seems to be having a performance impact, it can be disabled through the **View Options**. This will remove the Other occurrences column entirely and the Comment column will be based only on tags.

You can also switch it to Thumbnail view to see thumbnails of the content in the selected folder.



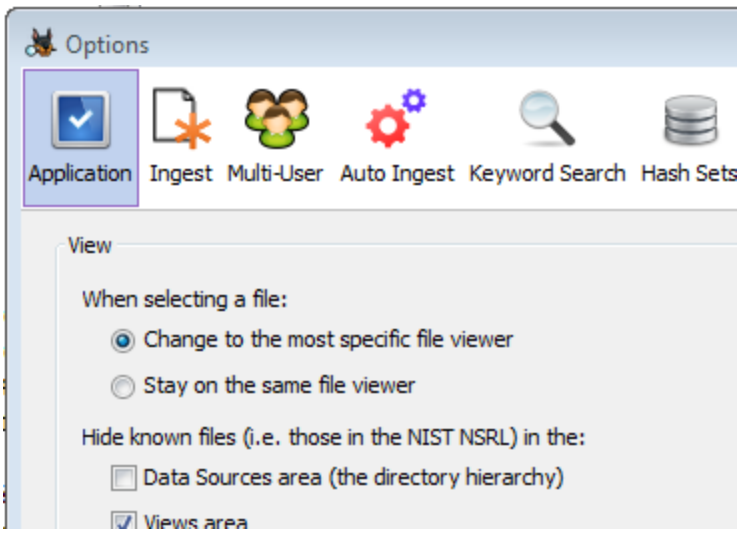
The Result Viewer is context-aware, meaning it will show applicable columns for the data type selected.



Content Viewer

The Content Viewer lives in the lower right-hand side of the Autopsy main screen and shows pictures, video, hex, text, extracted strings, metadata, etc. The Content Viewer is enabled when you select an entry in the **Result Viewer**.

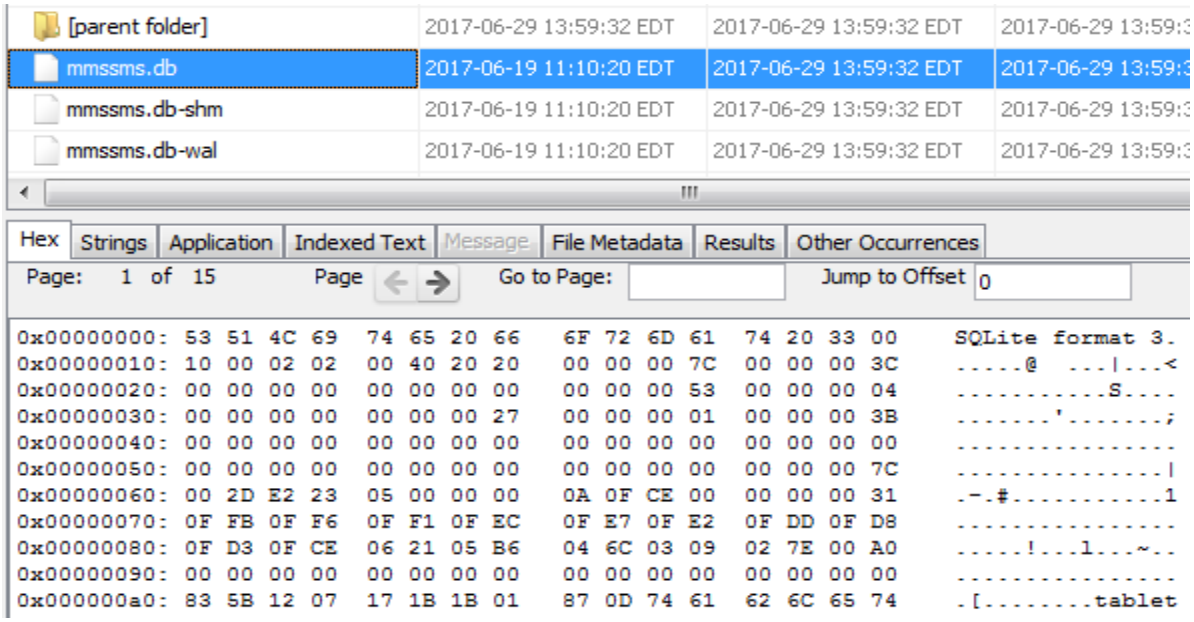
The Content Viewer is context-aware, meaning different tabs will be enabled depending on the type of content selected and which ingest modules have been run. It will default to what it considers the "most specific" tab. For example, selecting a JPG will cause the Content Viewer to automatically select the "Application" tab and will display the image there. If you instead would like the Content Viewer to stay on the previously selected tab when you change to a different content object, go to the **View Options** panel through Tools->Options->Application Tab and select the "Stay on the same file viewer" option.



When a Result type is selected in the Result Viewer (as opposed to a file), most of the tabs will correspond to the file associated with the result and not the result itself. For example, when selecting a Keyword Hit, the "Hex", "Strings", and "File Metadata" tabs will show data from the file where the keyword was found. The descriptions below will generally assume a file has been selected, but most also apply when we have a file associated with a selected result.

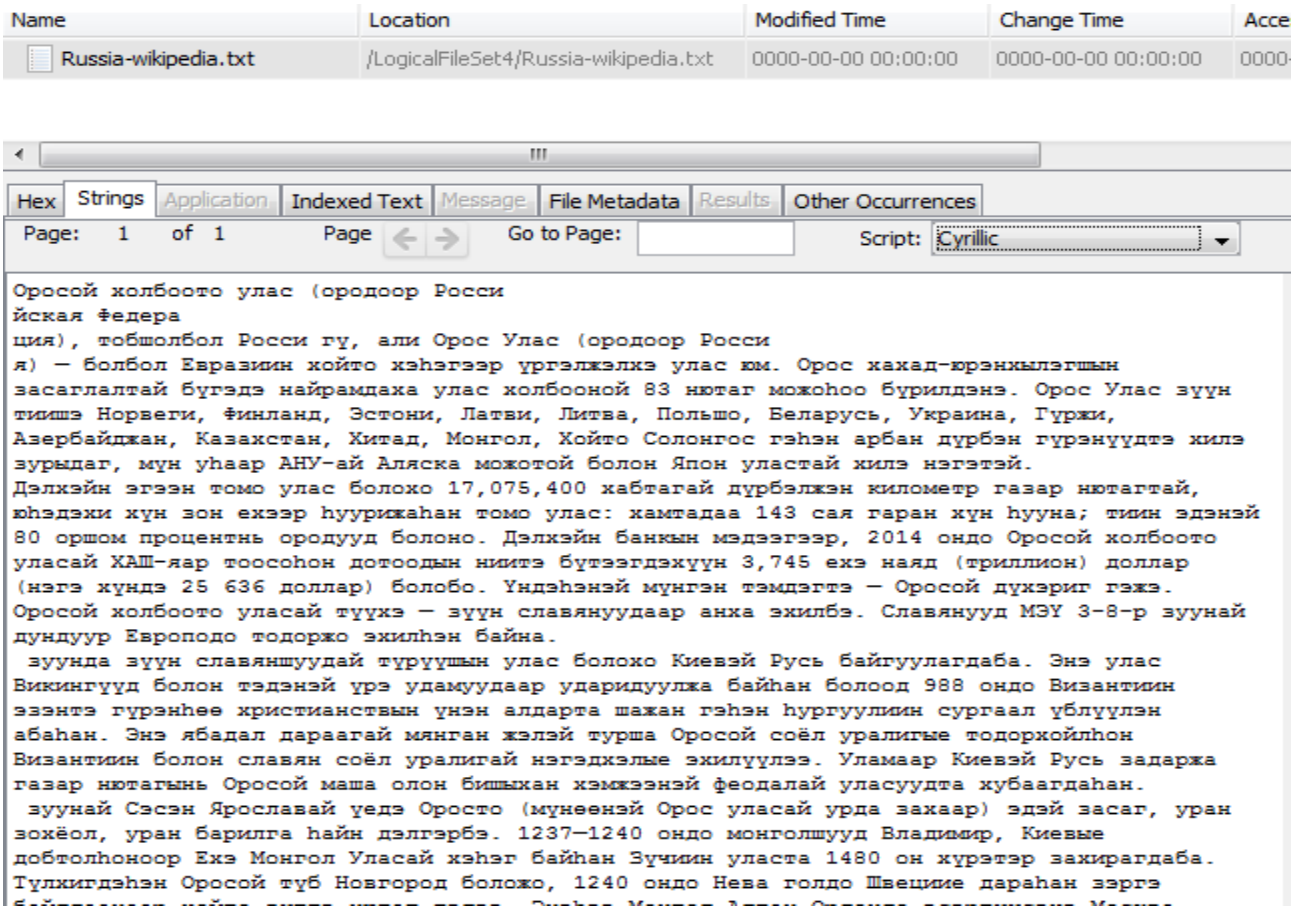
Hex

The Hex tab is nearly always available and shows the contents of the file.



Strings

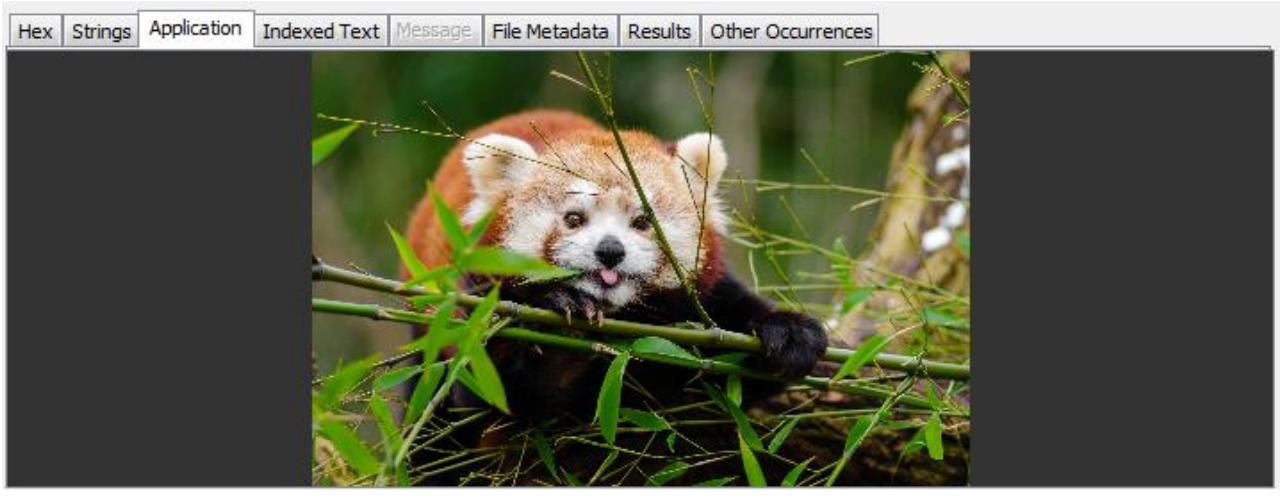
The Strings tab shows all text strings found in the file. Different scripts can be chosen from the drop-down menu to display results for non-Latin alphabets.



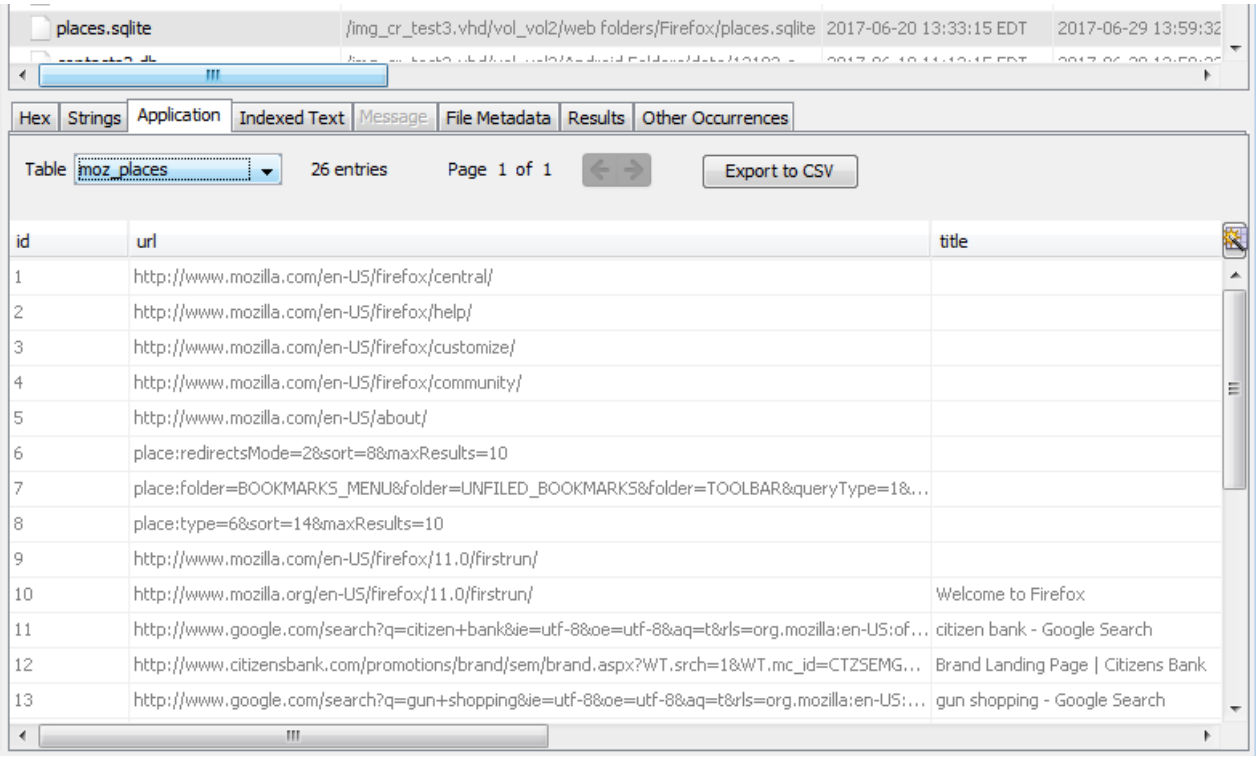
Application

For certain file types, the Application tab can display the contents in a user friendly format. The following screenshots show some examples of what the Application tab will display.

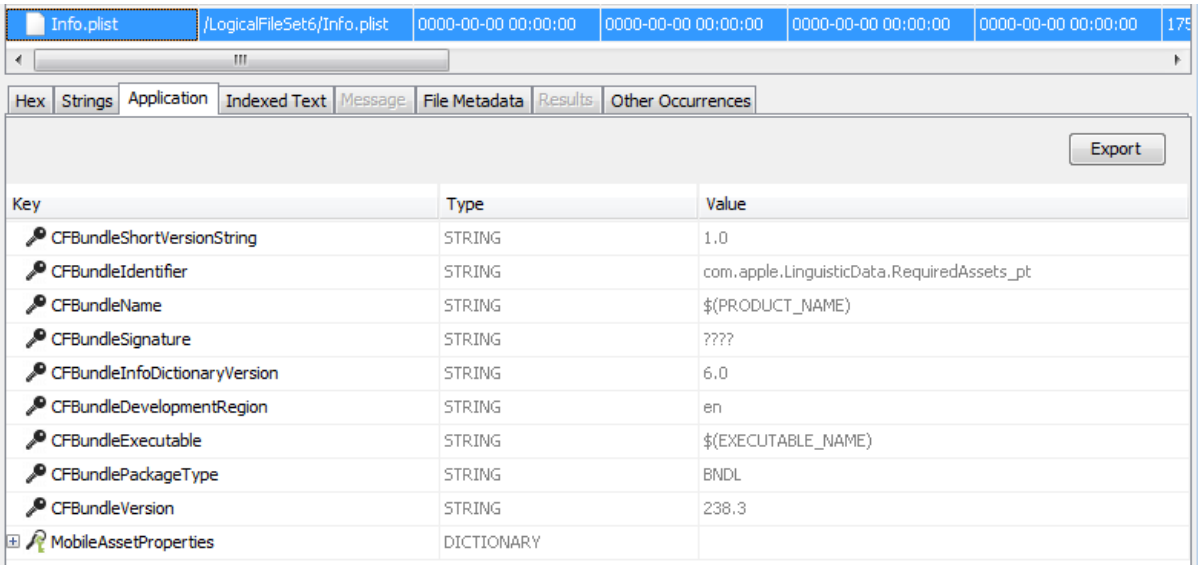
It will display most image types:



It also allows you to browse SQLite tables and export their contents as CSV:

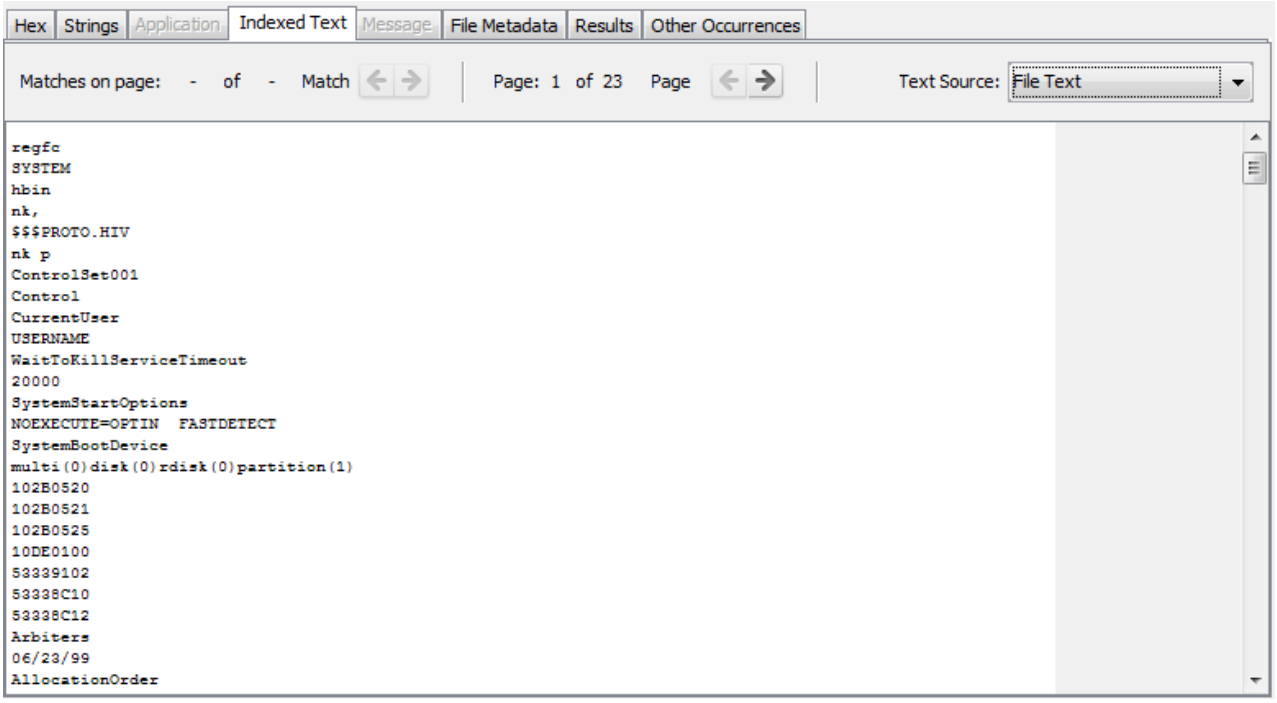


And plist file data will be shown and can be exported:



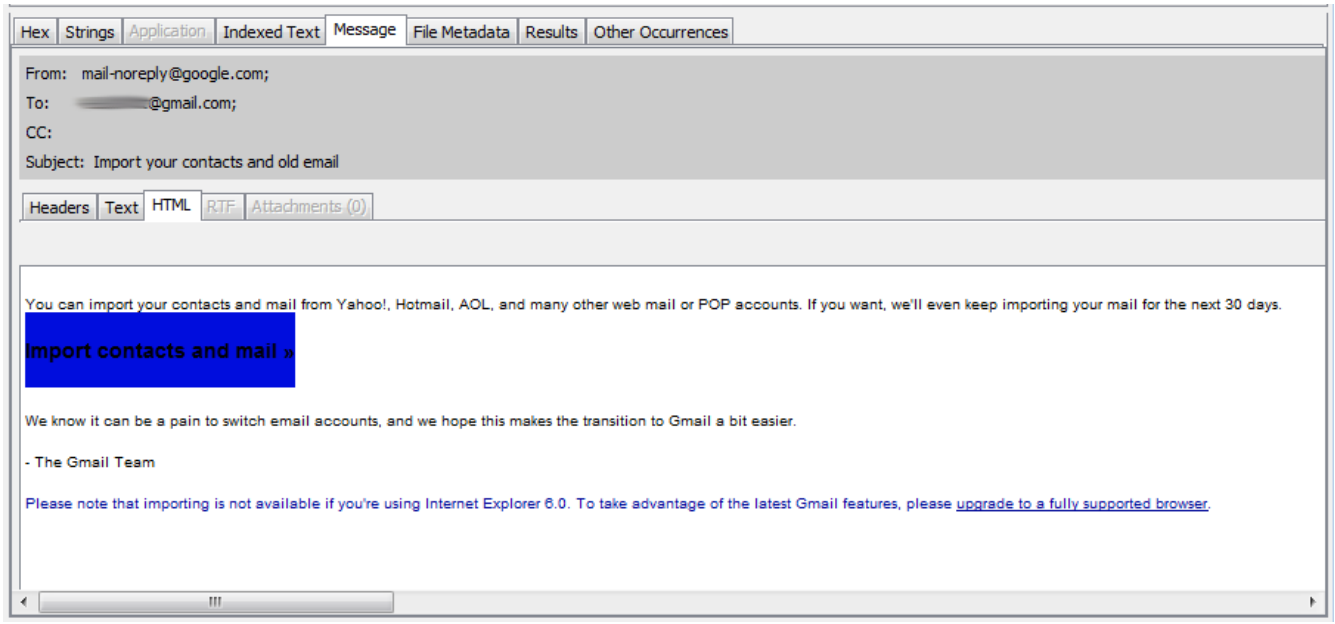
Indexed Text

The Indexed Text tab shows the text that has been indexed by the Keyword Search module. You can switch the "Text Source" Field to "Result Text" to see which text has been indexed for associated results.



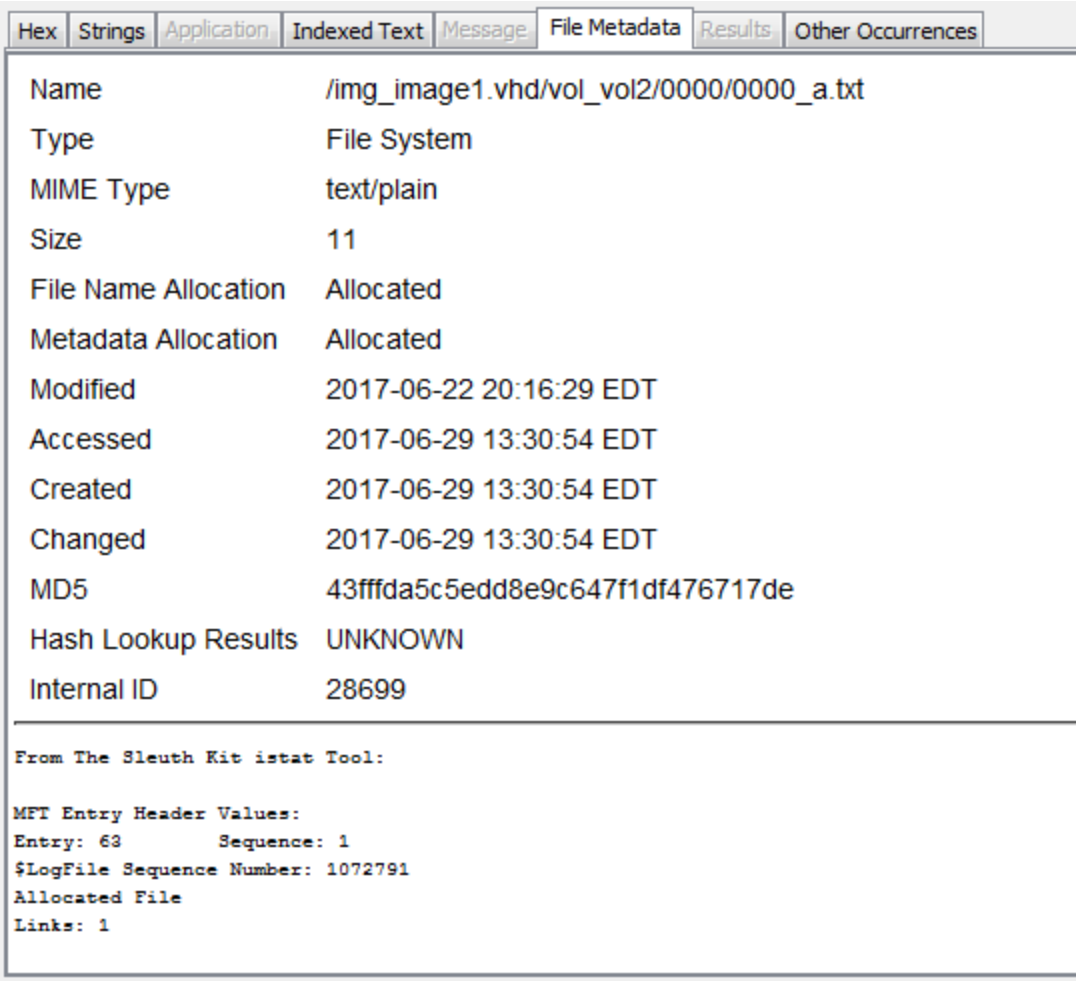
Message

The Message tab shows details of emails and SMS messages.



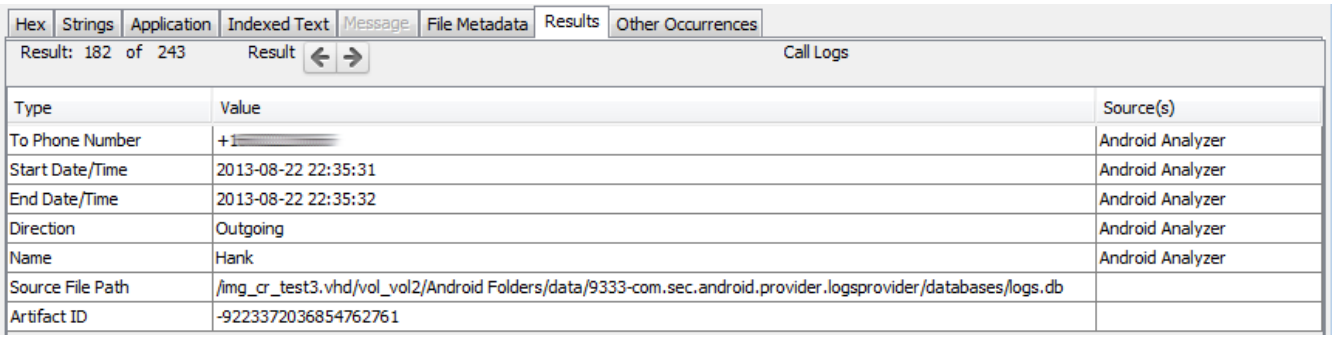
File Metadata

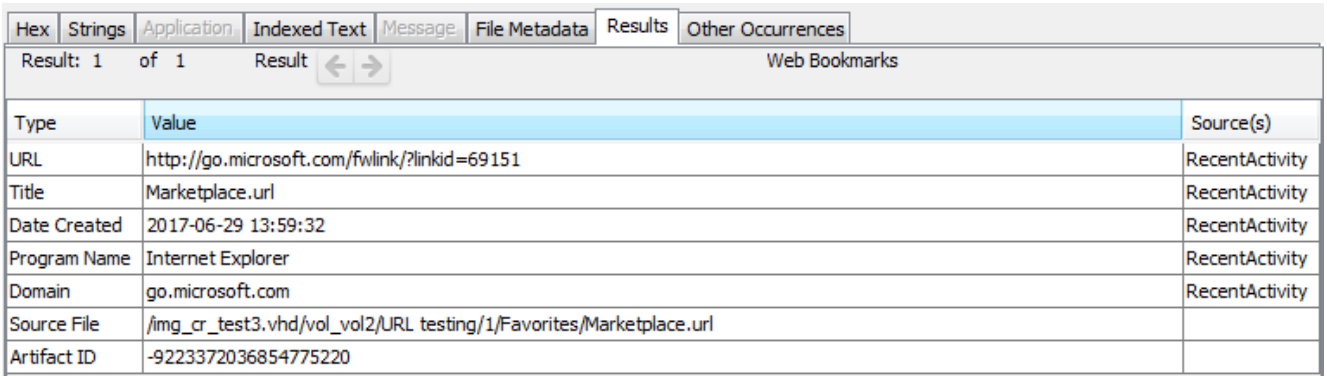
The File Metadata tab displays basic information about the file, such as type, size, and hash. It also displays the output of the Sleuth Kit istat tool.



Results

The Results tab is active when selecting entries that are part of the Results tree, such as keyword hits, call logs, and messages. It is also active when looking at a file that has results associated with it. The exact fields displayed depend on the type of entry. The two images below show the Results tab for a call log and a web bookmark.

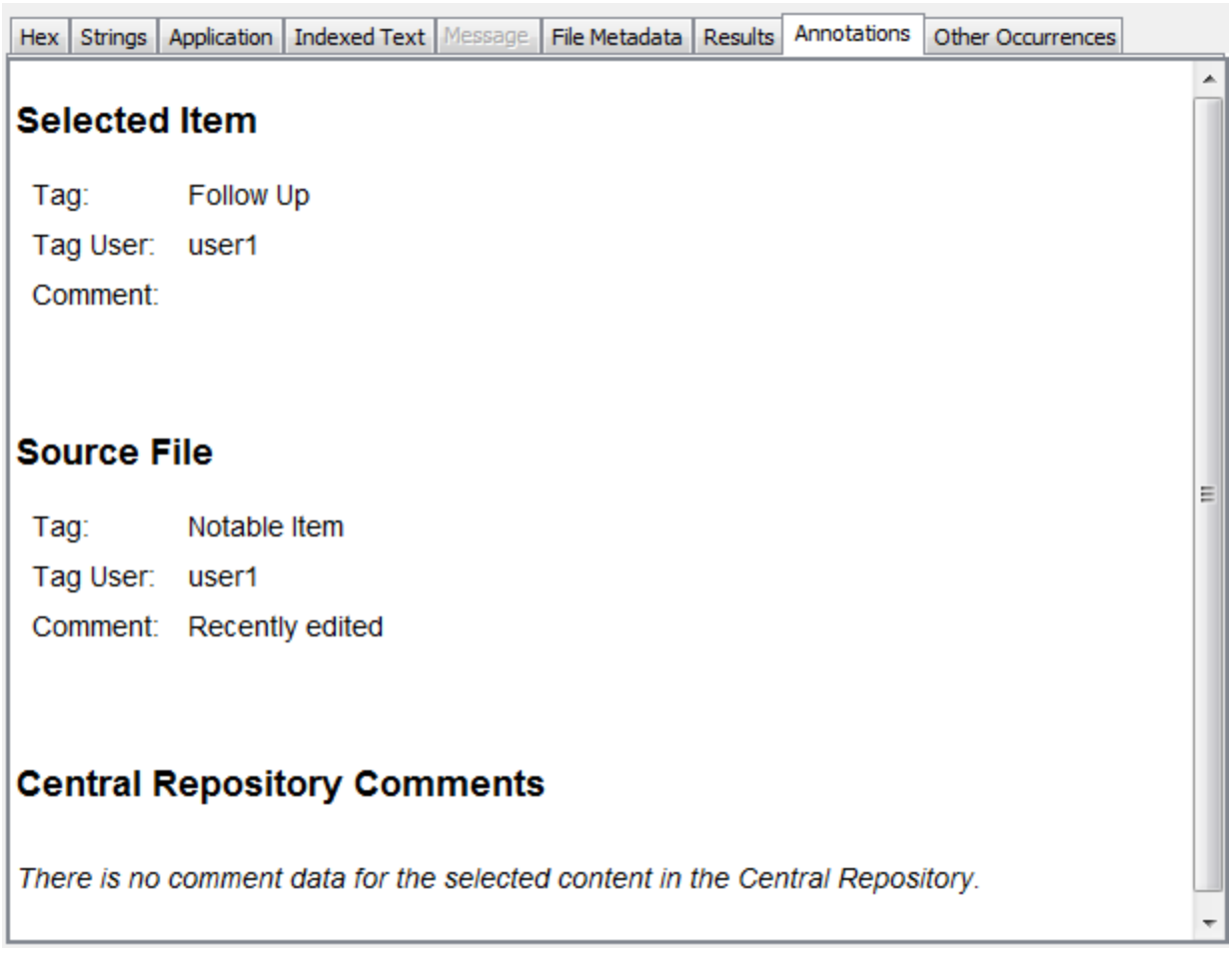




Type	Value	Source(s)
URL	http://go.microsoft.com/fwlink/?linkid=69151	RecentActivity
Title	Marketplace.url	RecentActivity
Date Created	2017-06-29 13:59:32	RecentActivity
Program Name	Internet Explorer	RecentActivity
Domain	go.microsoft.com	RecentActivity
Source File	/img_cr_test3.vhd/vol_vol2/URL testing/1/Favorites/Marketplace.url	
Artifact ID	-9223372036854775220	

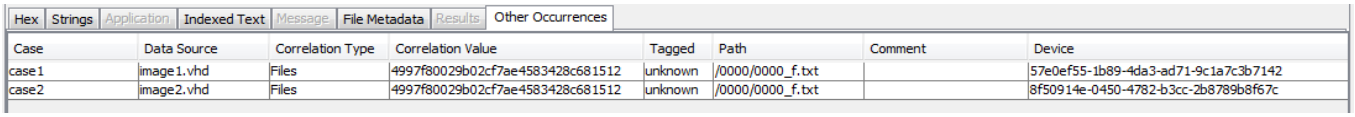
Annotations

The Annotations tab shows information added by an analyst about a file or result. It displays any tags and comments associated with the file or result, and if the **Central Repository** is enabled it will also display any comments saved to the Central Repository.



Other Occurrences

The Other Occurrences tab shows other instances of this file or result. Enabling the **Central Repository** adds additional functionality to this tab. See the **Content Viewer** section for more information.



Case	Data Source	Correlation Type	Correlation Value	Tagged	Path	Comment	Device
case1	image1.vhd	Files	4997f80029b02cf7ae4583428c681512	unknown	/0000/0000_f.txt		57e0ef55-1b89-4da3-ad71-9c1a7c3b7142
case2	image2.vhd	Files	4997f80029b02cf7ae4583428c681512	unknown	/0000/0000_f.txt		8f50914e-0450-4782-b3cc-2b8789b8f67c

UI Quick Search

The user interface quick search feature allows you to search within the data on a panel for a given string, it will not search data in hidden columns or collapsed nodes.

How to use it

In order to use the search, you need to select any item in the area you wish to search, and start typing. If user interface quick search is available in the area you have selected a search field will appear in the bottom left hand corner of the area. As you type the string you are searching for it will auto-update to select one of the results which matches your string. You can switch between the results which match the string you have typed with the up and down keys. The search does not support the use of regular expressions but will match against any sub-sting in the fields it searches, not just at the beginning of the field.

Configuration

By default, the search will match against the data in all fields which are in the currently selected area. The search will also ignore case by default. If you want to change either of these default behaviors, you can click the magnifying glass with the down arrow icon and configure which columns will be searched as well as if the search should ignore case.

Where it can be used

- The **tree viewer**
- The **table view**
- The **open multi-user case panel**
- The **Timeline** tool's table view
- The **Communication Visualization Tool's** browse panel
- The **Communication Visualization Tool's** message panel

Image Gallery Module

Overview

This document outlines the use of the Image Gallery feature of Autopsy. This feature was funded by DHS S&T to help provide free and open source digital forensics tools to law enforcement.

The Image Gallery feature has been designed specifically with child-exploitation cases in mind, but can be used for a variety of other investigation types that involve images and videos. It offers the following features beyond the traditional long list of thumbnails that Autopsy and other tools currently provide.

- Groups images by folder (and other attributes) to help examiner break the large set of images into smaller groups and to help focus on areas with images of interest.
- Allows examiner to start viewing images immediately upon adding them to the case. As images are hashed, they are updated in the interface. You do not need to wait until the entire image is ingested.

This document assumes basic familiarity with Autopsy.

Quick Start

1. The Image Gallery tool can be configured to collect data about images/videos as ingest runs or all at once after ingest. To change this setting go to "Tools", "Options", "Image /Video Gallery". This setting is saved per case, but cannot be changed during ingest. See the Options window for more details
2. Create a case as normal and add a disk image (or folder of files) as a data source. Ensure that you have the hash lookup module enabled with NSRL and known bad hashsets, the EXIF module enabled, and the File Type module enabled.
3. Click the "View Images/Videos" button or select "View Images/Videos" in the "Tools" menu. This will open the Autopsy Image/Video Analysis tool in a new window.
4. Groups of images will be presented as they are analyzed by the background ingest modules. You can later resort and regroup, but it is required to keep it grouped by folder while ingest is still ongoing.
5. As each group is reviewed, the next highest priority group is presented, according to a sorting criteria (the default is the density of hash set hits).
6. Images that were hits from hashsets, will have a dashed border around them.
7. You can use the menu bar on the top of the group to categorize the entire group.
8. You can right click on an image to categorize or tag the individual image.
9. Tag files with customizable tags. A ‘Follow Up’ tag is already built into the tool and integrated into the filter options. Tags can be applied in addition to categorization. An image can only have one categorization, but can have many tags to support your work-flow.
10. Create a report containing the details of every tagged and/or categorized file, via the standard Autopsy report generation feature.

Use Case Details

In addition to the basic ideas presented in the previous section, here are some hints on use cases that were designed into the tool.

- When you are viewing the groups, they are presented in an order based on density of hash hits(by default). If you find a group that has lots of interesting files and you want to see what is in the parent folder or nearby folders, use the navigation tree on the left.
- At any time, you can use the list on the left-hand side to see the groups with the largest hashset hits.
- To see which folders have the most images in them, sort the groups by group size (descending).
- Files that have hashset hits are not automatically tagged or categorized. You need to do that after reviewing them. The easiest way to do that is to wait until ingest is over and then group by hashsets. You can then review each group and categorize the entire group at a time using the group header.

Categories

The tool has been designed specifically with child-exploitation cases in mind and has a notion of categorizes. We will be changing this in the future to be more flexible with custom category names, but currently it is hard coded to use the names that Project Vic (and other international groups) use. We have assigned colors to each category to highlight each image.

Name	Description	Color
CAT-0	Uncategorized	**gray**
CAT-1	Child Abuse Material	**red**
CAT-2	Child Exploitative / Age Difficult	**orange**
CAT-3	CGI / Animation	**yellow**
CAT-4	Comparison Images	**bisque**
CAT-5	Non-pertinent	**green**

GUI controls

You can do your entire investigation using the mouse, but many examiners like to use keyboard shortcuts to quickly process large amounts of images.

Keyboard Shortcuts

shortcut	action
digits 0-5	assign the correspondingly numbered category to the selected file(s)
alt + 0-5	assign the correspondingly numbered category to all files in the focused group
arrows	select the next file in the direction pressed
page up/down	scroll the list of files

Additional Mouse Controls

mouse gesture	action
ctrl + left click	toggle selection of clicked file, select multiple files
right click on file	bring up context menu allowing per file actions (tag, categorize, extract to local file, view in external viewer, view in Autopsy content viewer, add file to HashDB)
right click empty space of group	bring up context menu allowing per group actions (tag, categorize, extract to local file(s), add file(s) to HashDB)
double click on file	open selected file in slide show mode

UI Details

Group Display Area

The central display area contains the list of files in the current group. Images in the group can be displayed in either thumbnail mode or slide show mode. Slide show mode provides larger images and playback of video files. At the right of the group header is a toggle for changing the viewing mode of the group (tiles vs slide-show).

Image/Video Tiles

Each file is represented in the main display area via a small tile. The tile shows:

- Thumbnail of the image/video
- Name of the file

- Indicators of other important details:

image	description	meaning
	solid colored border	file's assigned category.
	purple dashed border	file has a known bad hashset hit, but has not yet been categorized.
	pushpin	file has a known bad hashset hit
	clapboard on document	video file
	a red flag	file has been 'flagged' as with the follow up tag

Slide Show Mode

In slide show mode a group shows only one file at a time at an increased size. Per file tag/category controls above the top right corner of the image, and large left and right buttons allow cycling through the files in the group. If the active file is an Autopsy supported video format, video playback controls appear below the video.

Table/Tree of contents

The section in the top left with tabs labelled "Contents" and "Hash Hits" provides an overview of the groups of files in the case. It changes to reflect the current Group By setting: for hierarchical groupings (path) it shows a tree of folders (folders containing images/videos (groups) are marked with a distinctive icon), and for other groupings it shows only a flat list.

Each group shows the number of files that hit against configured Hash DBs during ingest (hash hits) and the total number of image/video files as a ratio (hash hits / total) after its name. By selecting groups in the tree/list you can navigate directly to them in the main display area. If the Hash Hits tab is selected only groups containing files that have hash hits are shown.

Listening for Changes

The Image Gallery maintains its own database, which needs to be updated as files are analyzed by Autopsy. For example, it needs to know when a file has been hashed or had EXIF data extracted. By default, the Image Gallery is always listening in single-user cases for these changes and keeps its database up to date. If this is causing a performance impact, you can disable this feature in the Options panel.

You can turn the listening off for the current case and you can change the default behavior for future cases.

Multi-User Cases

If a case was created in a multi-user environment, then it becomes much harder to keep the Image Gallery database in sync because many other examiners could be analyzing data from that case. Therefore, Image Gallery has different update behaviors in a multi-user case than it does for a single-user case. Notably:

- If your system is running ingest on the data source, then you will continue to get real-time updates just like in a single-user case. So, as soon as a folder of files has been hashed and had EXIF data extracted, it will be possible for you to view it.
- If another system in the cluster is running ingest on a data source, you may not see its results until the ingest has completed. You will not get real-time updates and instead you will get updates only after you have closed Image Gallery and opened it again.
- Each time you open Image Gallery, it will check the local database to see if it is in sync with the case database. If it is not, it will ask you to rebuild it. This is because additional data may have been added to the case database by another system and your Image Gallery database is no longer accurate.

You also have the option to see groups (or folders) that are new to you or new to everyone. When you press “Show Next Unseen Group”, the default behavior is to show you the highest priority group that you have not seen yet. But, you can also choose to see groups that no one else has seen. This choice can be made using the check box next to the “Show Next Unseen Group” button.

File Search

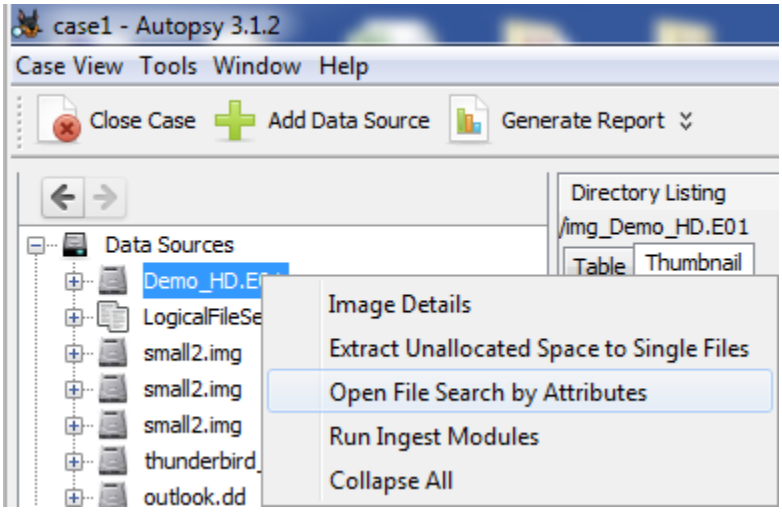
About File Search

The File Search tool can be accessed either from the Tools menu or by right-clicking on a data source node in the Data Explorer / Directory Tree. By using File Search, you can specify, filter, and show the directories and files that you want to see from the images in the currently opened case. The File Search results will be populated in a brand new Table Result viewer on the right-hand side.

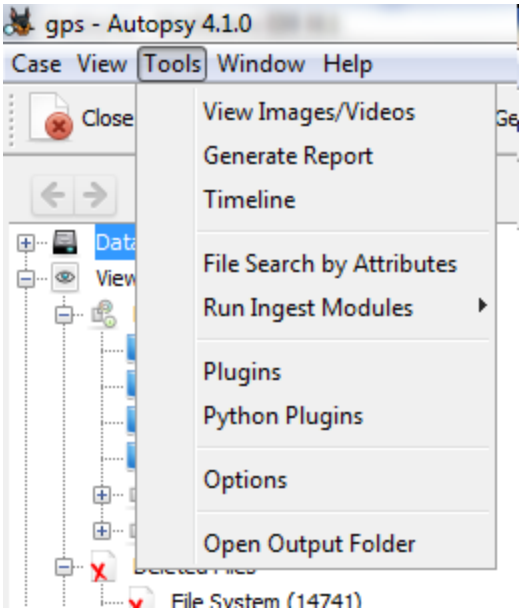
Note: Currently File Search doesn't support regular expressions. The Keyword Search feature of Autopsy does support regular expressions and can be used for to search for files and/or directories by name.

How To Open File Search

To open the File Search, you can do one of the following thing: Right-click a data source and choose "Open File Search by Attributes".



or select the "Tools", "File Search by Attributes".



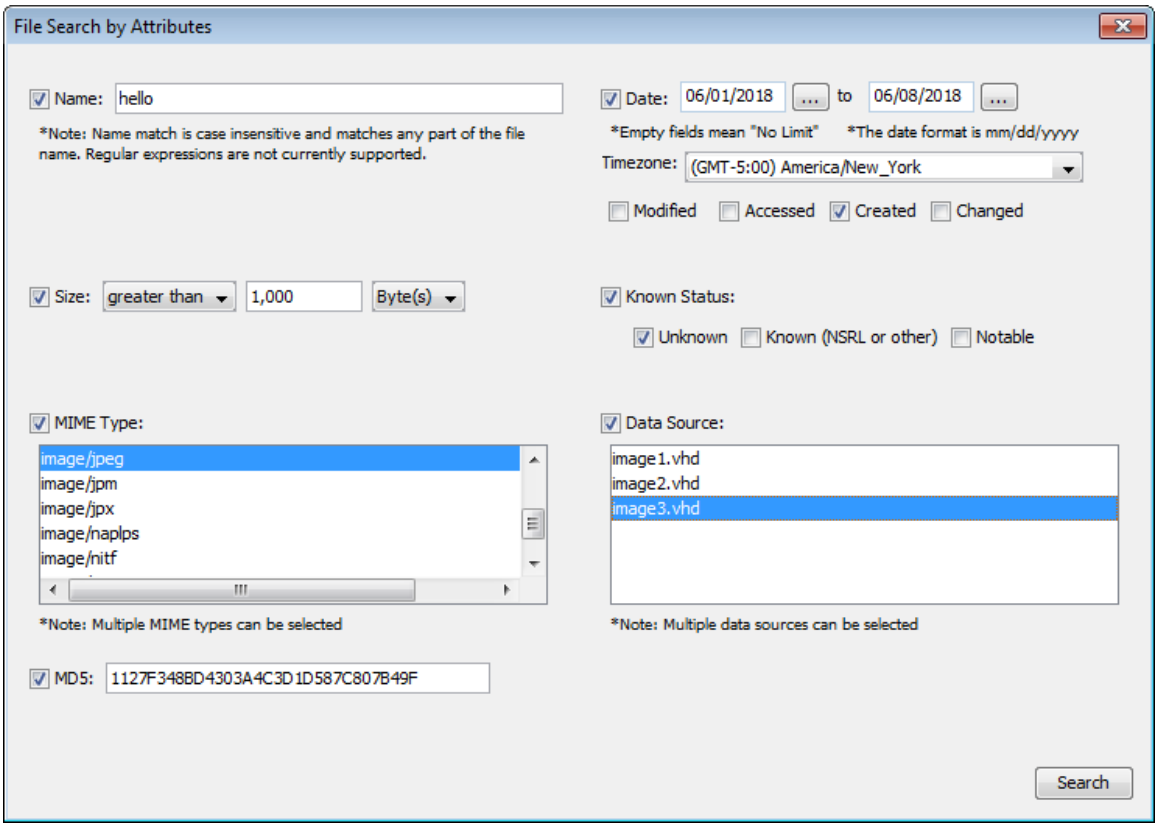
How To Use File Search

There are several categories that you can use to filter and show the directories and files within the images in the current opened case. The categories are:

- Name: Search for all files and directory whose name contains the pattern given. Note: it doesn't support regular expression and keyword matching.
- Size: Search for all files and directory whose size matches the pattern given. The pattern can be "equal to", "greater than", and "less than". The unit for the size can be "Byte(s)", "KB", "MB", "GB", and "TB".
- MIME Type: Search for all files with the selected MIME type. Multiple types can be used by holding SHIFT or CTRL while selecting.

- MD5: Search for all files with the given MD5 hash.
- Date: Search for all files and directory whose "date property" is within the date range given. The "date properties" are "Modified Date", "Accessed Date", "Changed Date", and "Created Date". You must also specify the timezone for the date given.
- Known Status: Search for all files and directory whose known status is recognized as either Unknown, Known, or Known Bad. For more on Known Status, see the **Hash Lookup Module**. To use any of these filters, check the box next to the category and click "Search" button to start the search process. The result will show up in the "Result Viewer".
- Data Source: Search only within the specified data source instead of the entire case. Note that multiple data sources can be selected by holding SHIFT or CTRL while selecting.

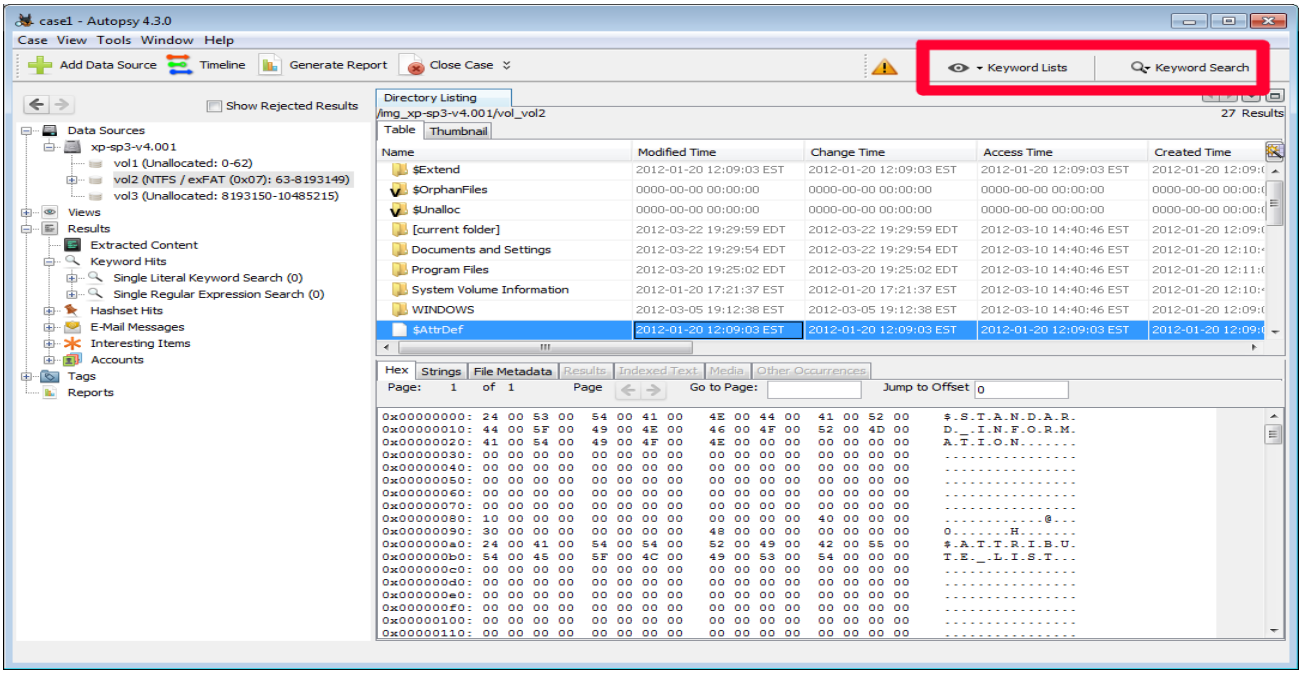
Here's a contrived example where we try to get all the directories and files whose name contains "hello", has a size greater than 1000 Bytes, is in JPEG format, was created between 06/01/2018 and 06/08/2017 (in GMT-5 timezone), is an unknown file, has a hash of 1127F348BD4303A4C3D1D587C807B49F, and appears in data source "image3.vhd":



Ad Hoc Keyword Search

Overview

The ad hoc keyword search features allows you to run single keyword terms or lists of keywords against all images in a case. Both options are located in the top right of the main Autopsy window.



The **Keyword Search Module** must be selected during ingest before doing an ad hoc keyword search. If you don't want to search for any of the existing keyword lists, you can deselect everything to just index the files for later searching.

Creating Keywords

The following sections will give a description of each keyword type, then will show some sample text and how various search terms would work against it.

Exact match

Exact match should be used in cases where the search term is expected to always be surrounded by non-word characters (typically whitespace or punctuation). Spaces/punctuation are allowed in the search term, and capitalization is ignored.

The quick reddish-brown fox jumps over the lazy dog.

- "quick", "brown", "dog" will match
- "FOX", "Fox", "fox" will all match
- "reddish-brown fox", "brown fox", "LAZY DOG" will match
- "rown" and "lazy do" will not match since they are not bounded by non-word characters in the text

Substring match

Substring match should be used where the search term is just part of a word, or to allow for different word endings. Capitalization is ignored but spaces and other punctuation can not appear in the search term.

The quick reddish-brown fox jumps over the lazy dog.

- "jump" will match "jumps", and would also match "jumping", "jumped", etc.
- "dog" will match
- "UMP", "oX" will match
- "y dog", "ish-brown" will not match

Regex match

Regex match can be used to search for a specific pattern. Regular expressions are supported using Lucene Regex Syntax which is documented here: https://www.elastic.co/guide/en/elasticsearch/reference/1.6/query-dsl-regexp-query.html#regexp-syntax. Wildcards are automatically added to the beginning and end of the regular expressions to ensure all matches are found. Additionally, the resulting hits are split on common token separator boundaries (e.g. space, newline, colon, exclamation point etc.) to make the resulting keyword hit more amenable to highlighting. As of Autopsy 4.9, regex searches are no longer case sensitive. This includes literal characters and character classes.

Note: Since Autopsy 4.4, boundary characters ('^' and '$') no longer work as word boundaries. Previously a search for "^[0-9]{5}$" would return all five digit strings surrounded by some type of non-word characters. For example, "The number 12345 is.." would contain a match, while "123456789 people" would not. This was because the regex was compared against each "word" in the document. In newer versions, the text is not split into words internally so this type of search no longer works. To get similar results, replace the boundary characters with the specific characters that should represent a word break. For example, "^[0-9]{5}$" could become "[\.\-\,][0-9]{5}[\.\-\,]".

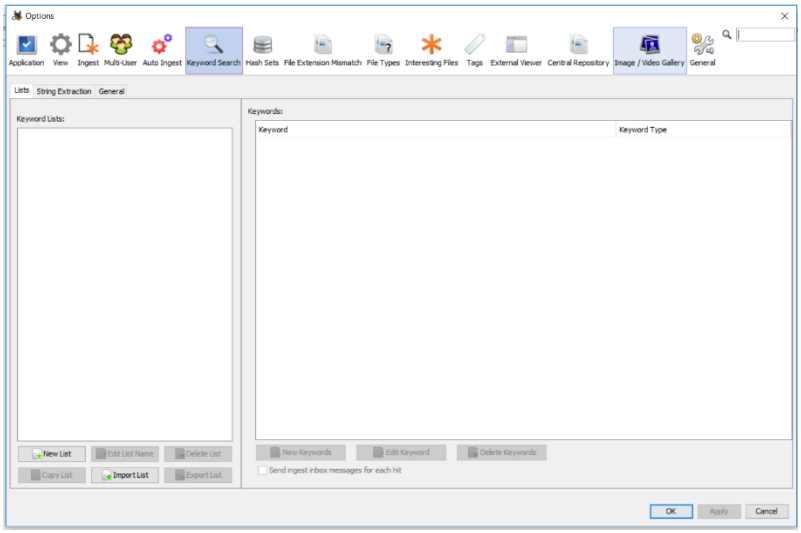
There is some validation on the regex but it's best to test on a sample image to make sure your regexes are correct and working as expected. One simple way to test is by creating a sample text file that your expression should match, ingesting it as a **Logical File Set** and then running the regex query.

In the year 1885 in an article titled Current Notes, the quick brown fox first jumped over the lazy dog.

- "fox" and "FOX" will both match since the search is case-insensitive
- "qu.ck", "cu.*es" will match
- "[JLK]umped" will match "jumped"
- "[0-9]{4}" will match 1885. Character classes like "\d" are not supported. Backreferences are also not supported (but will not generate an error), so "Cu(.)\1ent" would not work to find "Current"

Other notes

Built-in keywords



The **Keyword Search Module** has several built-in searches that can not be edited. The ones that are most prone to false hits (IP Address and Phone Number) require that the matching text is surrounded by boundary characters, such as spaces or certain punctuation. For example:

- "Address 10.1.5.127 is unavailable" - The built-in IP Address search would find "10.1.5.127" because it is surrounded by whitespace
- "abc10.1.7.99xyz" - The built-in IP Address search would not find it because it is surrounded by letters

If you want to override this default behavior:

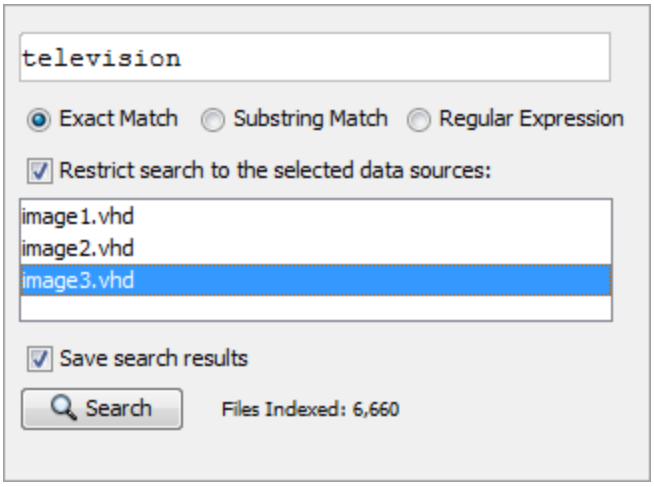
- Copy the existing regex. The easiest way to do this is to click on Keyword Lists, the list you want then the specific entry you want and hit control+c to copy. It will need a bit of cleanup afterward.
- Remove the boundary characters on the beginning and end of the regex
- Make a new keyword list containing the result and run it either during ingest or through the Keyword Lists button.

Non-Latin text

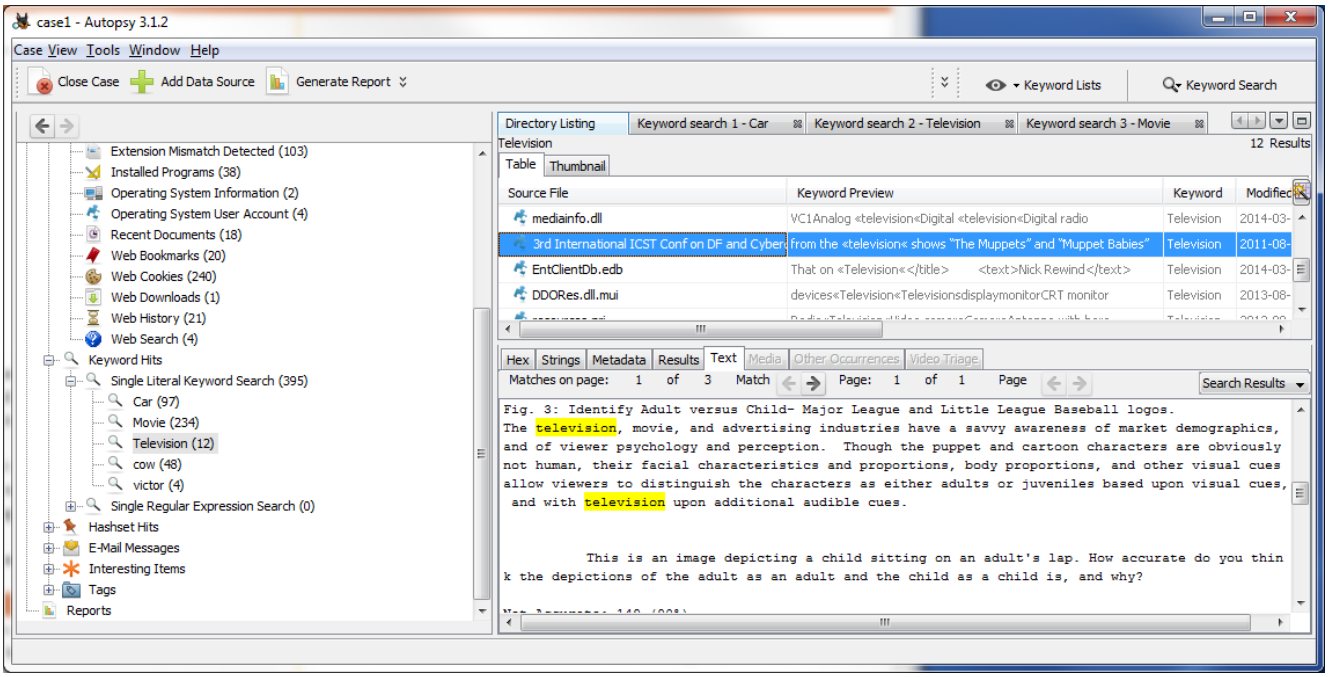
In general all three types of keyword searches will work as expected but the feature has not been thoroughly tested with all character sets. For example, the searches may no longer be case-insensitive. As with regex above, we suggest testing on a sample file.

Keyword Search

Individual keyword or regular expressions can quickly be searched using the search text box widget. You can select "Exact Match", "Substring Match" and "Regular Expression" match. See the earlier **Creating Keywords**section for information on each keyword type. The search can be restricted to only certain data sources by selecting the checkbox near the bottom and then highlighting the data sources to search within. Multiple data sources can be selected used shift+left click or control+left click. The "Save search results" checkbox determines whether the search results will be saved to the case database.



Results will be opened in a separate Results Viewer for every search executed. If the "Save search results" checkbox was enabled, the results will also be saved in the Directory Tree as shown in the screenshot below.

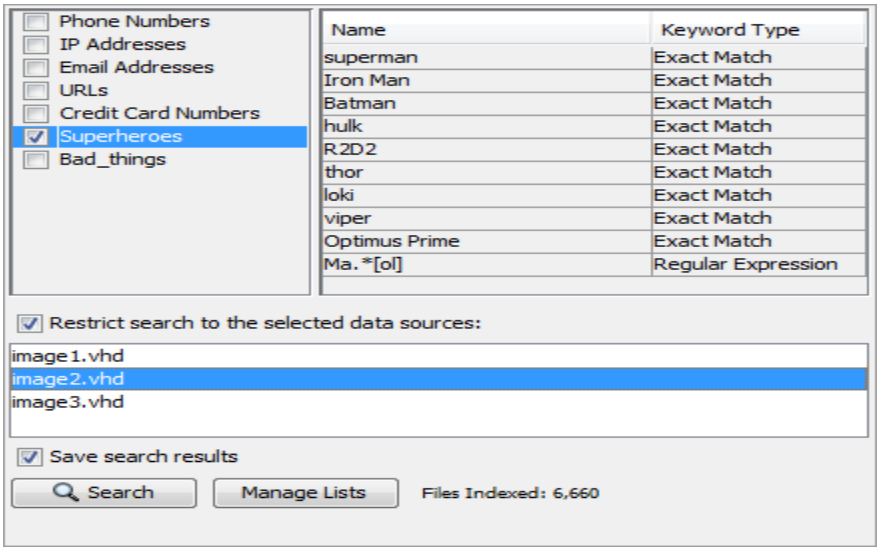


Keyword Lists

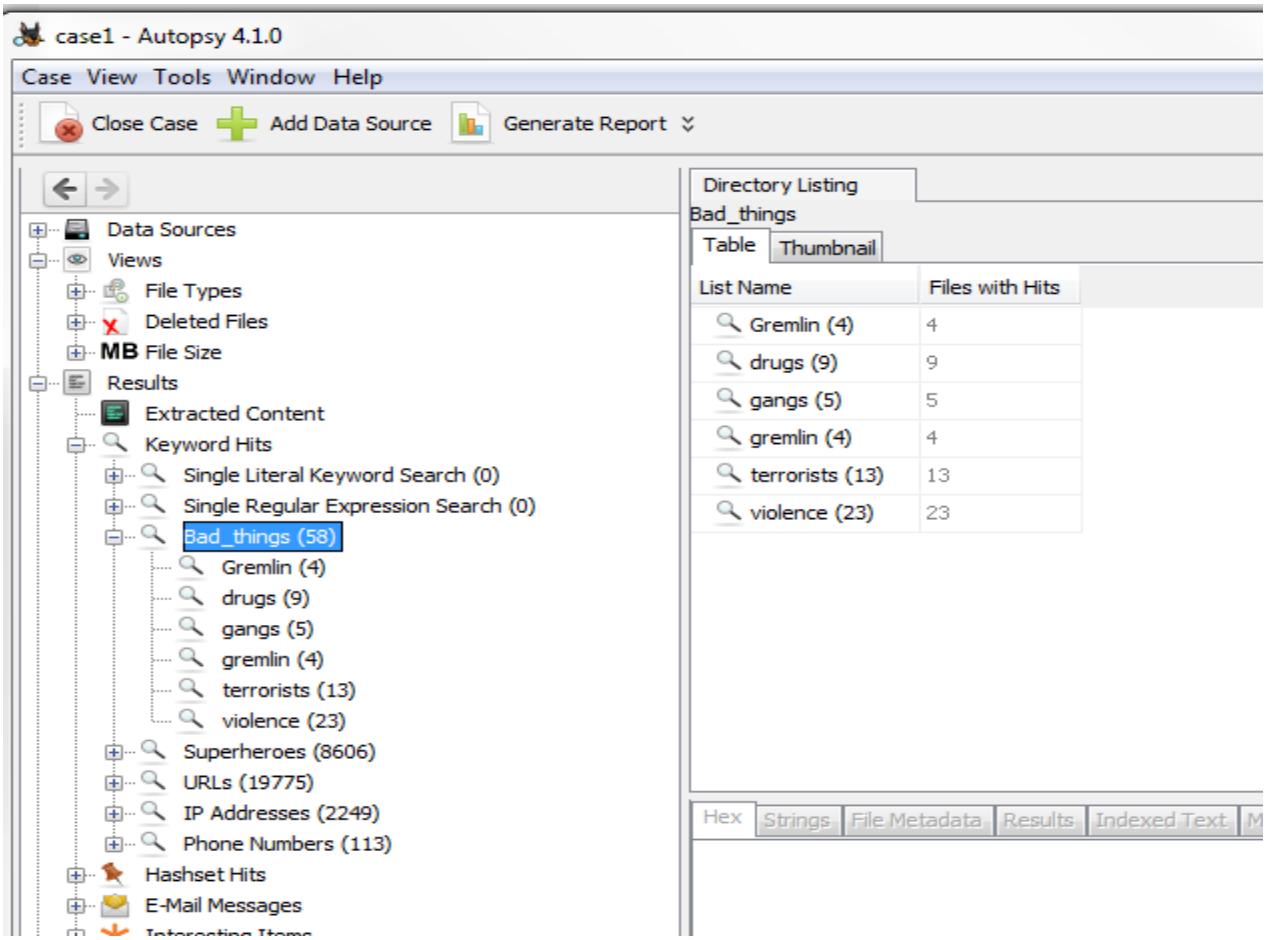
In addition to being selected during ingest, keyword lists can also be run through the Keyword Lists button. For information on setting up these keyword lists, see the **Lists tab** section of the ingest module documentation.

Lists created using the Keyword Search Configuration Dialog can be manually searched by the user by pressing on the 'Keyword Lists' button and selecting the check boxes corresponding to the lists to be searched. The search can be restricted to only certain data sources by selecting the checkbox near the bottom and then highlighting the data sources to search within. Multiple data sources can be selected used shift+left click or control+left click. Once everything has been

configured, press "Search" to begin the search. The "Save search results" checkbox determines whether the search results will be saved to the case database.



If the "Save search results" checkbox was enabled, the results of the keyword list search will be shown in the tree, as shown below.



Doing ad hoc searches during ingest

Ad hoc searches are intended to be used after ingest completes, but can be used in a limited capacity while ingest is ongoing.

Manual **Keyword Search** for individual keywords or regular expressions can be executed while ingest is ongoing, using the current index. Note however, that you may miss some results if the entire index has not yet been populated. Autopsy enables you to perform the search on an incomplete index in order to retrieve some preliminary results in real-time.

During the ingest, the normal manual search using **Keyword Lists** behaves differently than after ingest is complete. A selected list can instead be added to the ingest process and it will be searched in the background instead.

Most keyword management features are disabled during ingest. You can not edit keyword lists but can create new lists (but not add to them) and copy and export existing lists.

Timeline

Overview

This document outlines the use of the Timeline feature of Autopsy. This feature was funded by DHS S&T to help provide free and open source digital forensics tools to law enforcement. This document assumes basic familiarity with Autopsy.

Quick Start

1. Create a case as normal and add a disk image (or folder of files) as a data source. To get the most out of the timeline, ensure that you have the hash lookup module enabled with NSRL (to ignore known files) and have the EXIF and recent activity modules enabled to collect additional temporal data.
2. After the image has been added, click "Tools", "Timeline" in the menu. This will open the Timeline tool in a new window. You can do this while ingest is running, but you will not have access to the temporal data that will be found after you create the timeline, unless you re-open the timeline tool.

Use Case Details

- In addition to the basic ideas presented in the previous section, here are some hints on use cases that were designed into the tool.
- When did major web activity occur on a system?
- When were external devices plugged into the system?
- When were pictures with EXIF information added?
- What websites were accessed that resulted in file system modifications immediately after?

Basic Concepts

This section covers some basic concepts of the interface.

Events

The timeline tool is organized around events. An Event has a timestamp, a type, and a description. Note: all Events are discrete, but might be grouped together to form clusters with a duration in the Details View depending on the level of Description that is enabled in the UI.

The timeline collects data from multiple sources and organizes the events into the following taxonomy:

- File System
  - Modified
  - Access
  - Created
  - Changed
- Web Activity
  - Web Downloads
  - Web Cookies
  - Web Bookmarks (creation)
  - Web History
  - Web Searches
- Miscellaneous
  - Messages
  - GPS Routes
  - Location History
  - Calls
  - Email
  - Recent Documents
  - Installed Programs
  - Exif metadata
  - Devices Attached

Visualization Types

There are two different graph types that the Autopsy viewer provides. Each is better suited for a different type of question that the investigator is trying to answer. You can change between the two types in top part of the interface (see previous section for a screen shot).

The **Counts View** shows a stacked bar chart. Use this type of graph to show how much activity occurred in a given time frame. It won't show you specific events though. It can be helpful to determine when the computer was last used or how often it was used. When you open a timeline, it will open in this style of graph.

The **Details View** shows individual or groups of related events. Date/time is represented horizontally along the x-axis, but the vertical axis does not represent any specific units. You would use this interface to answer questions about what specific events happened in a given time frame or what events occurred before or after a given event. You would generally use this type of interface after using the Counts View to identify a period of time that you wanted details on. There can be a lot of details in this view and we have introduced zooming concepts, as described in the next section, to help with this.

The table on the bottom left hand side of the panel has a **UI Quick Search** feature which can be used to quickly find a node in the table.

Visualization settings

The toolbar above the visualization area shows settings specific to the active visualization. These settings affect the way events are displayed and/or the layout of the visualization.

Zooming

A common challenge with timeline analysis is information overload. To help with this, the Autopsy interface has three ways of zooming that will help you identify the correct data. These can be controlled from a single area in the upper left of the interface.

- **Time Units**: This level of zooming controls the temporal detail shown on the X-axis. It dictates if there will be markers at the scale of years or seconds. As you want more details about what happened in a given time range, you will zoom in more with this control.
- **Event Type**: This level of zooming controls what level of event type you see. As an example, there is a top-level type of "File System" event with sub-types for modified times, accessed times, and created times. If you want more details about a given type, then you will zoom in more with this control.
- **Description Detail**: This level of zooming is most unique to Autopsy and groups similar events together based on their description. As an example, it will group file system events together if they are in the same root folder when you are zoomed all of the way out. This allows you to generally see where there is activity without seeing each individual file.

For the quick start approach to things, you should keep this in mind: Double clicking on something will change only one of these levels of zooming. We have tried to choose what would be most intuitive for most use cases. If you want to choose a different zooming approach, use the sliders in the upper left or right click on the chart.

History

If at any time you want to back out to something you saw before, use the back and forward history buttons in the upper left , or the keyboard shortcut Alt + Left/Right.

Timeline Interaction and Configuration Details

Filters / Events

This area allows the user to apply filters to limit what events are shown in the visualization. When the Details View is active, a tab in this area also enables navigating the visualization by event descriptions (see the Details View section for more on this)

When the **Hide Known Files** filter is active, files with known hashes will not be included in any way in the rest of the timeline tool (except for the Histogram which shows all events). In order for this filter to work, the Hash Lookup ingest module must have been run with a Known hash set enabled.

When the **Text Filter** is active, only events with descriptions containing the supplied string as a substring will be shown. Note: this filter users the full description in its search even if not displayed.

The **Event Types** filter allows the user to select which event types should be shown. Right clicking an event type brings up a context menu with options to select different sets of types.

The Event Type hierarchy displayed in the filter tab also functions as the **legend** for the visualizations. Events are color-coded to match their type, and have the corresponding icon displayed in several places.

Time Range Selection

The time range selection area provides several means of adjusting the displayed time range. Date/Time fields show the exact date and time of the start(left) and end(right) of the displayed range. The user can type directly into these fields or use a graphical date/time chooser to modify the start or end time. The minus and plus hour glass buttons(/) zoom the visible time range out and in a set percentage. The drop down menu to the right allows selecting a preset time range. These methods will adjust the visible time range around its center. The last method to adjust the visible time range is via the range slider. The user can position each end independently to adjust the start and end time respectively or drag the highlighted blue section to move the visible range without changing its length. In both visualizations, the user can also right-drag (starting in empty space) a time span, represented by a pale blue box, and then double click it to zoom the visible time range. Right clicking the blue time span box clears it.

Histogram

Behind the time range slider is a histogram of all events in the case. The histogram can help to put the main visualization in perspective by showing a high level summary of all events in the case, with a representation of the visible time range superimposed via the time range slider. The histogram divides the entire time span of all events in the case into equal intervals and shows the number of events in each interval via the height of the corresponding bar. The histogram should only be used for relative comparison and context and not for determining exact numbers or times of events. Note: This histogram is not affected by filters or zooming.

Time Zone

The user can choose between viewing events in their local time zone or in Universal Coordinated Time.

Visualization Area: Counts View

The Counts View shows a stacked bar chart with time periods along the x-axis and event counts along the y-axis. The height of each bar represents the number of events that occurred in that time period. The different colored segments represent different event types. Right clicking the bars brings up a context menu with selection and zooming actions.

The only setting specific to the Counts View is what kind of vertical scale to use: The linear scale is good for many use cases. When this scale is selected, the height of the bars represents the counts in a linear, one-to-one fashion, and the y-axis is labeled with values. When the range of values is very large, time periods with low counts may have a bar that is too small to see. To help the user detect this, the labels for date ranges with events are bold. To see bars that are too small, there are three options: adjust the window size so that the visualization area has more vertical space, adjust the time range shown so that time periods with larger bars are excluded, or adjust the scale setting to logarithmic.

The logarithmic scale represents the number of events in a non-linear way that compresses the difference between large and small numbers. Note that even with the logarithmic scale, an extremely large difference in counts may still produce bars too small to see. In this case the only option may be to filter events to reduce the difference in counts. NOTE: Because the logarithmic scale is applied to each event type separately, the meaning of the height of the combined bar is not intuitive, and to emphasize this, no labels are shown on the y-axis with the logarithmic scale. The logarithmic scale should be used to quickly compare the counts *across time within a type, or across types for one time period, but not both.* The actual counts (available in tooltips or the result viewer) should be used for absolute comparisons. Use the logarithmic scale with care.

Visualization Area: Details View

The Details View shows events clustered by their description. Date/time is represented horizontally along the x-axis, but the vertical axis does not represent anything and is only used as a space to layout overlapping events. Events with the same type and description that occur close together in time may be clustered together. The Time Unit, Event Type and Description Detail sliders control how events are clustered. When the Description Detail level is at full, it is likely that very few events will be clustered, resulting in an enormous amount of detail being displayed. This can cause significant UI lag, and so **it is not recommended to use the full description unless the time range has been narrowed and/or filters applied to reduced the number of events shown**. Projections of the selected clusters are displayed on the x-axis to help visualize the temporal relationships between them.

The Details View has four settings that affect the visible information and the layout of the event clusters. The four settings are independent and can be combined to achieve a variety of effects with different densities of information and layout patterns.

Band by Type: If Band by type is not selected, all the event clusters of different types will be intermixed, in a compact layout. If Band by Type is selected, each event type will have a horizontal band reserved for it and events of different types will not be intermixed. Band by Type is useful when the user wants to compare events of the same type primarily.

One event per Row: If one event per row is selected no event clusters will ever overlap vertically, this will make the visualization more like a Gantt chart but uses much more vertical space.

Truncate Descriptions: The user can select 'truncate descriptions' and choose a length (in pixels) to truncate the text label shown with each cluster. This is useful if the descriptions are long and preventing a compact layout.

Description Visibility: The user may choose a description visibility level of 'show', 'counts only', or 'hide'. Show is the default. If Counts only is selected, only the count in parenthesis is shown, if hide is selected the entire text label is hidden. Counts only and hide are useful if the user wants to get a less cluttered view, focussed more on when event clusters occurred and their type, and is not interested in the descriptions.

Clicking the small green [+] button in a cluster will expand it with the next level of detail. The events in the cluster will be displayed clustered at a time scale appropriate for their extent and the detail level chosen. This can be repeated for the subclusters, to create a nested hierarchy of clusters. Clicking the red [-] button collapses a cluster to a lower level of detail. As with the global description level, care should be used when fully expanding large clusters, as this may cause an enormous amount of detail to be shown, slowing the tool down.

When the Detail View is active, the Events tab next to the Filters tab is enabled. This tab shows a list of all the descriptions presented in the visualization. Selecting a description in the list highlights all the event clusters with that description.

STIX

Overview

This document outlines the use of the STIX feature of Autopsy. This feature allows one or more Structured Threat Information Exchange (STIX) files to be run against a data source, reporting which indicators were found in the data source. More information about STIX can be found at https://stix.mitre.org/. This document assumes basic familiarity with Autopsy.

Quick Start

1. Create a case as normal and add a disk image (or folder of files) as a data source. To get the most out of the STIX module, ensure that the following ingest modules are selected:
    - Recent Activity
    - Hash Lookup (Check box to calculate MD5 hashes even with no database selected)
    - File Type Identification
    - Keyword Search (URL, IP, and Email addresses)
    - Email Parser
    - Extension Mismatch Detector
2. After the image has been added and ingest is complete, click the Report button then select STIX. Next choose either a single STIX file or a directory of STIX files to run against the image. It is possible to do this while ingest is running but the results will be incomplete.
3. Once the STIX report module is complete, there will be two sets of results:
    - Entries will be created under Interesting Items in the Autopsy tree, under a sub-heading for each indicator.
    - A log of which indicators/observables were found is generated by the report module (Follow the link on the Report Generation Progress window)

Supported CybOX Objects

- Address Object
    - Address_Value
- Domain Name Object
    - Value
- Email Message Object
    - To
    - CC
    - From
    - Subject
- File Object
    - Size_In_Bytes
    - File_Name
    - File_Path
    - File_Extension
    - Modified_Time
    - Accessed_Time
    - Created_Time
    - Hashes (MD5 only)
    - File_Format
    - is_masqueraded
- URI Object
    - Value
- URL History Object
    - Browser_Information (Name)

    - URL
    - Hostname
    - Referrer_URL
    - Page_Title
    - User_Profile_Name
- User Account Object
    - Home_Directory
    - Username
- Win Executable File Object
    - Time_Date_Stamp
- Windows Network Share Object
    - Local_Path
    - Netname
- Win Registry Key Object
    - Key (Required)
    - Hive
    - Values
- System Object
    - Hostname
    - Processor_Architecture
- Win System Object
    - Product_ID
    - Product_Name
    - Registered_Owner
    - Registered_Organization
    - Windows_System_Directory
    - Windows_Temp_Directory
- Win User Account Object
    - SID

See http://cybox.mitre.org for more information on CybOX Objects.

Limitations

- As shown in the list above, not all CybOX objects/fields are currently supported. When an unsupported object/field is found in an observable, its status is set to "indeterminate" instead of true or false. These indeterminate fields will not change the result of the observable composition (i.e., if the rest is true, the overall result will stay as true).
- Not all ConditionTypeEnum values are supported. It varies by field, but generally on String fields the following work: EQUALS, DOES_NOT_EQUAL, CONTAINS, DOES_NOT_CONTAIN, STARTS_WITH, ENDS_WITH. If a condition type is not supported there will be a warning in the log file.
- Related objects are not processed

Central Repository

Overview

The central repository allows a user to find matching artifacts both across cases and across data sources in the same case. It is a combination of an ingest module that extracts, stores, and compares properties against lists of notable properties, a database that stores these properties, and an additional panel in Autopsy to display other instances of each property. The central repository database can either be SQLite or PostgreSQL.

The following are some use cases for the central repository:

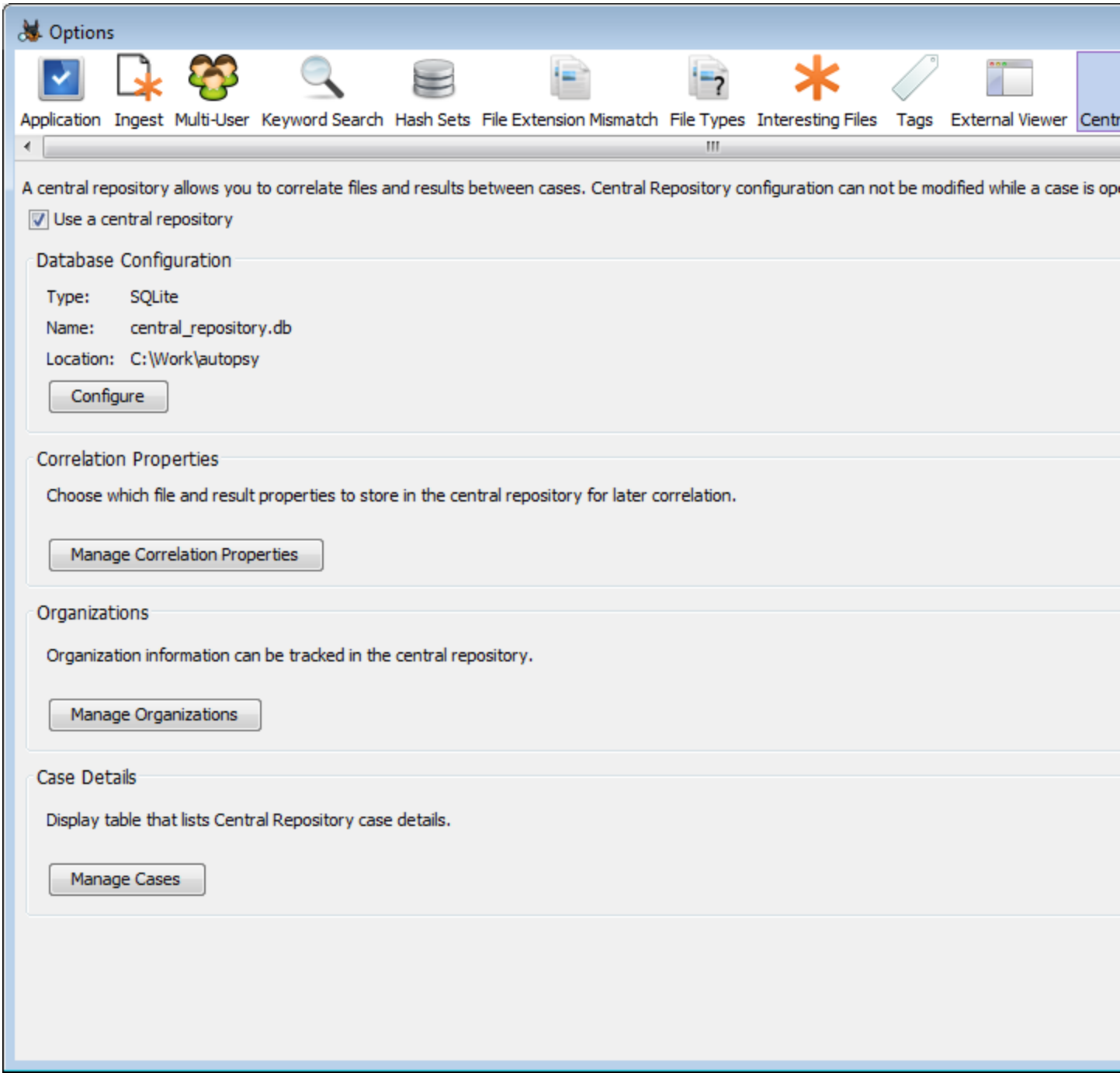
- **Finding Other Instances of a Property**
  - If you navigate to a file or Autopsy artifact (such as a Web History item), there is a content viewer in the bottom right that will show you other instances of this property across the data stored in the central repository.
- **Alerting When Previously Notable Properties Occur**
  - You can use the central repository to record which properties were associated with files and artifacts that were evidence (or notable). Once these properties have been tagged as notable they will be added to the Interesting Items section of the tree when seen again in any future cases.
- **Storing Hash Sets**
  - You can create and import hash sets into the central repository instead of using local copies in the **Hash Lookup module**. These hash sets are functionally equivalent to local hash sets but can be shared among multiple analysts (when using a PostgreSQL central repository).

Terms and Concepts

- **Central Repository** - The Autopsy feature containing the central repository database and Correlation Engine Ingest Module. Also responsible for displaying correlated properties to the user
- **Central Repository Database** - the SQLite or PostgreSQL database that holds all the data
- **Correlation Engine Ingest Module** - The ingest module responsible for adding new properties to the database and comparing these properties against existing notable properties
- **Property** - The data being stored/correlated. These can be file paths/MD5 hashes, email addresses, phone numbers, etc.

Setup

To start, open the main options panel and select the "Central Repository" icon.



Setting up the Database

On the central repository options panel, check the 'Use a Central Repository' option and then click the Configure button to set up a database. There are two options here:

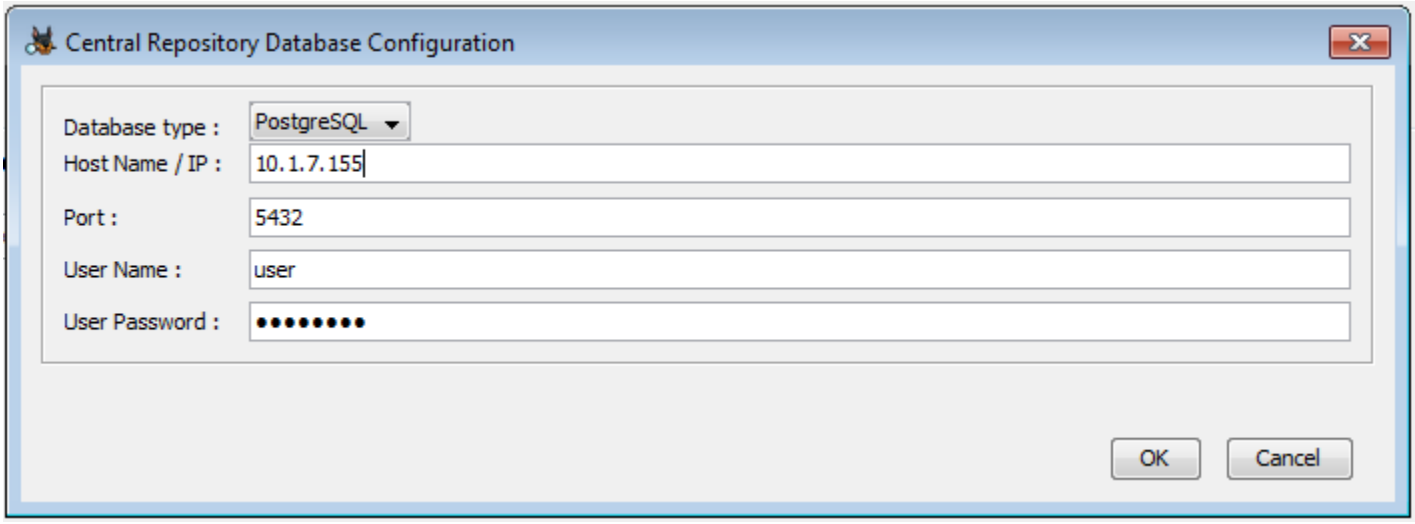
- **SQLite** - This option stores the database in a file. It should only be used when a single client will be accessing the database.
- **PostgreSQL** - This option uses a database server running either on the user's host or a remote server. This option must be used if multiple users will be using the same database.

Once a database has been configured, the lower two buttons on the main panel will be enabled, which will be described below.

Setting up PostgreSQL Deployment

If needed, see the **Install and Configure PostgreSQL** for help setting up your PostgreSQL server.

For PostgreSQL all values are required, but some defaults are provided for convenience.

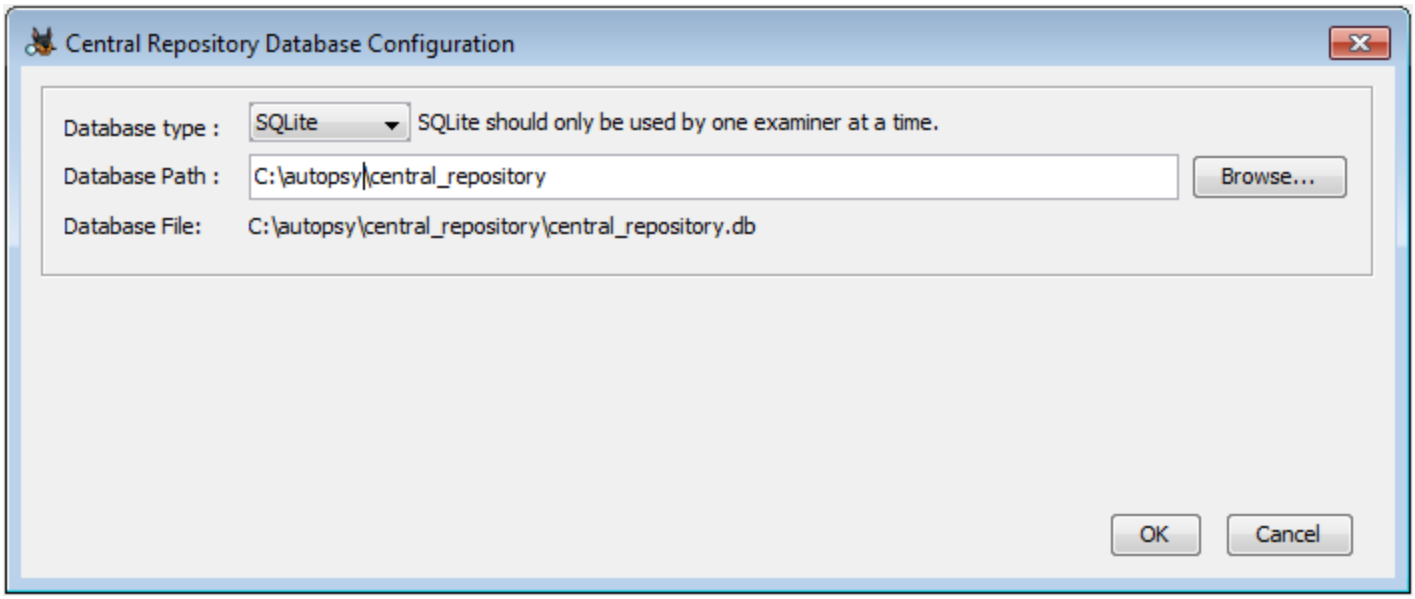


- Host Name/IP is the hostname or IP of your PostgreSQL server.
- Port is the port that the PostgreSQL server is listening on; default is 5432.
- User Name is a PostgreSQL user that can create and modify databases
- User Password is the password for the user.

If the database does not exist, you wll be prompted to create it.

Setting Up SQLite Deployment

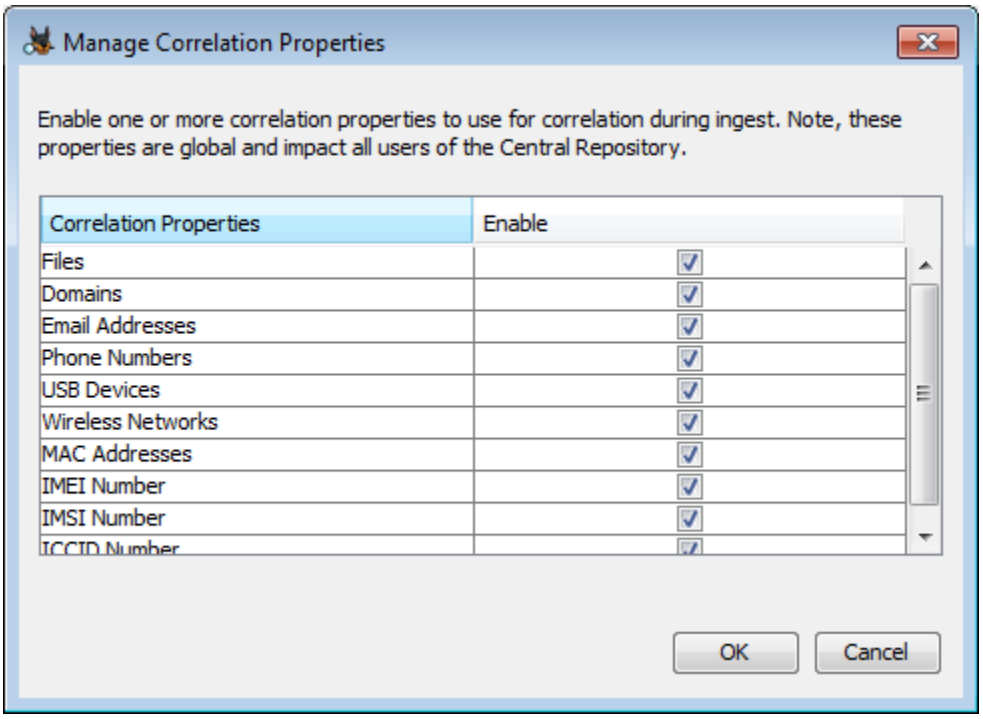
Select SQLite in the Database Type to set up a SQLite database. SQLite databases should not be used if more than one client will be accessing the central repository.



Enter or browse to a folder for the database. If the database file does not exist in that folder, you will be prompted to create it.

Manage Correlation Properties

The Correlation Engine ingest module can save different types of properties to the database. By default all properties are recorded, but this setting can be changed on the options panel through the Manage Correlation Properties button. Note that these settings are saved to the database, so in a multi-user setting any changes will affect all users.

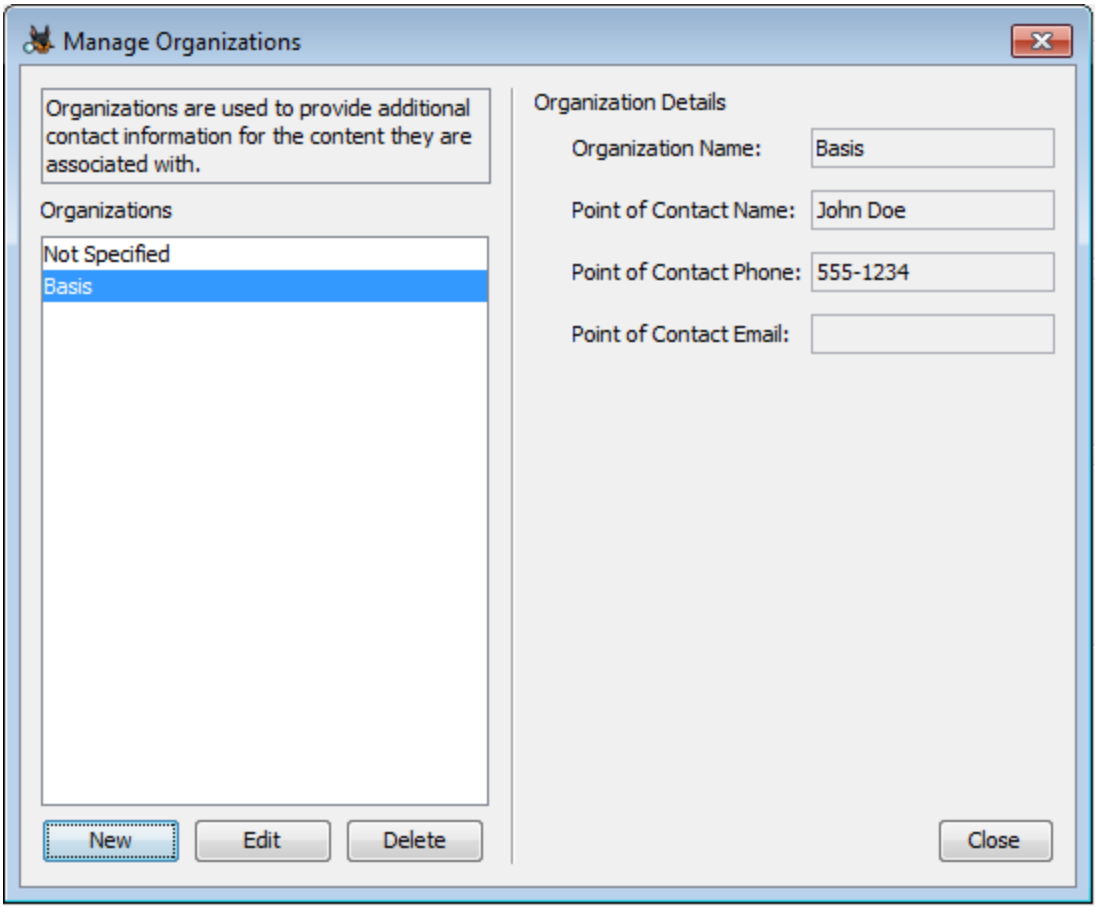


Descriptions of the property types:

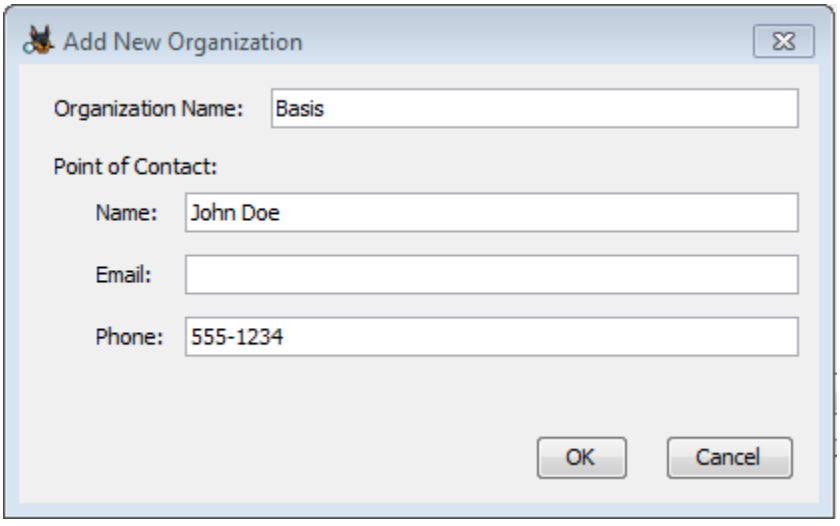
- **Files**
  - Files are correlated based on MD5 hash and file path and name. The Hash Lookup ingest module must be enabled.
- **Domains**
  - Domains are extracted from the various web artifacts, which primarily come from the Recent Activity module
- **Email Addresses**
  - Email addresses are pulled from Email Address hits from the Keyword Search module.
- **Phone Numbers**
  - Phone numbers are currently only extracted from call logs, contact lists and message, which come from the Android Analyzer module.
- **USB Devices**
  - USB device properties come from the registry parsing in the Recent Activity Module.
- **Wireless Networks**
  - Wireless networks are correlated on SSIDs, and come from the registry parsing in the Recent Activity Module.
- **MAC Addresses**
  - MAC address properties are currently only created by custom Autopsy modules
- **IMEI Number**
  - IMEIs properties are currently only created by custom Autopsy modules
- **IMSI Number**
  - IMSI properties are currently only created by custom Autopsy modules
- **ICCID Number**
  - ICCID properties are currently only created by custom Autopsy modules

Manage Organizations

Organizations are stored in the central repository and contain contact information for the given organization. Organizations are used for Hash Sets saved in the central repository, and can also be associated with Autopsy cases.

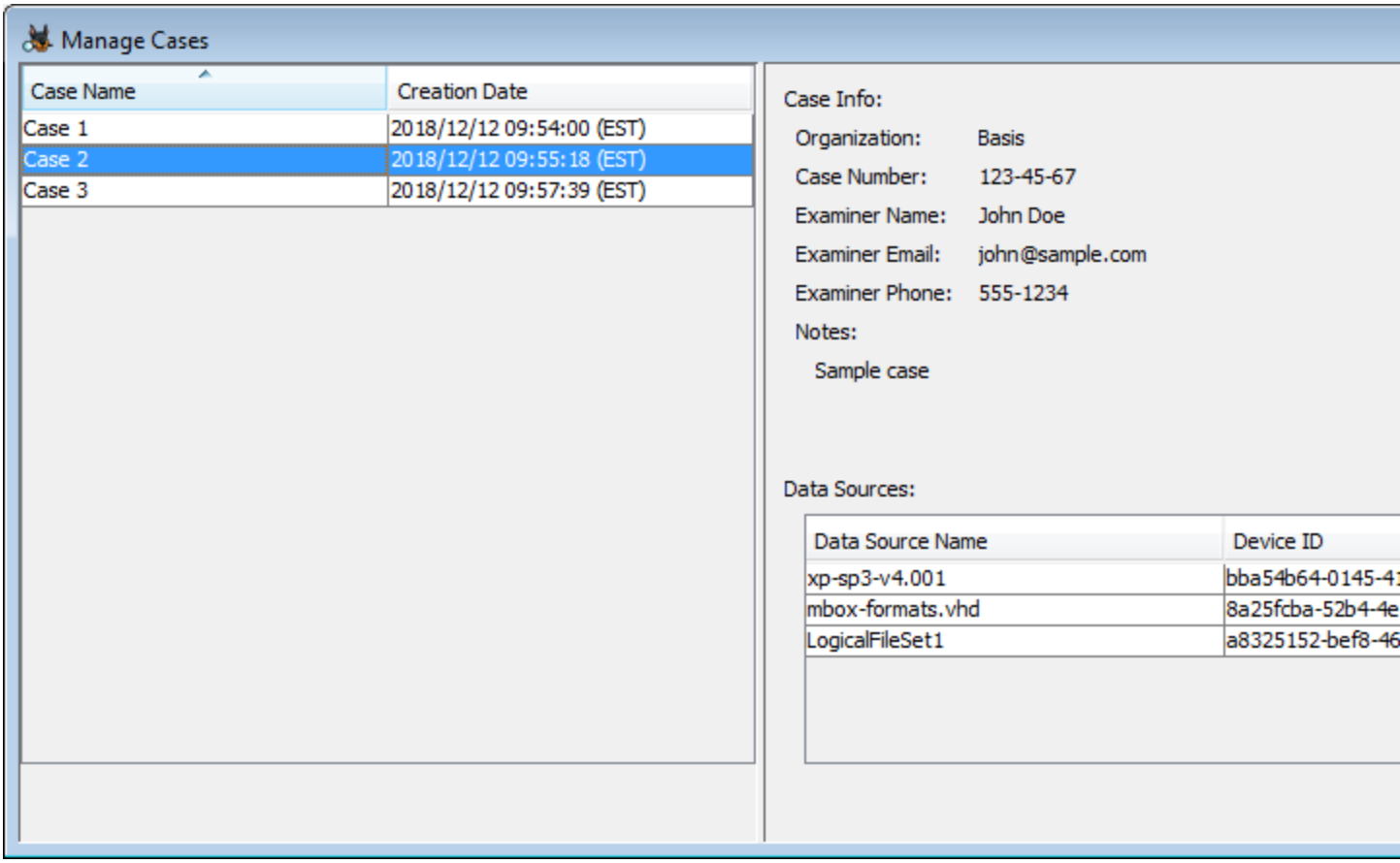


One default org, "Not Specified" will always be present in the list. New organizations can be created, edited, and deleted through the appropriate buttons. Note that any organization that is currently in use by a case or hash set can not be deleted. All fields apart from the organization name are optional.



Manage Cases

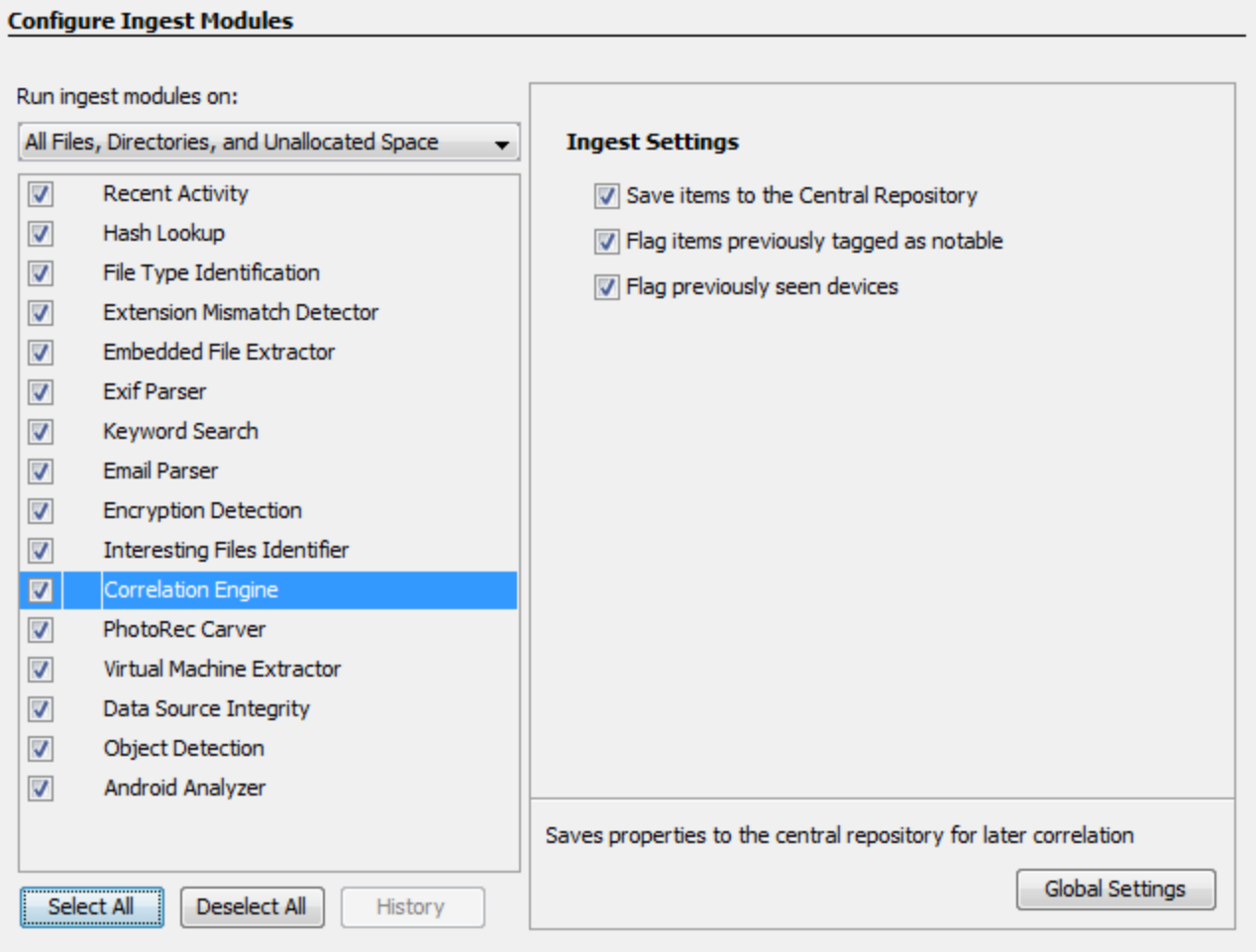
Displays a list of all cases that are in the central repository database and details about each case.



Using the Central Repository

Correlation Engine Module

The Correlation Engine ingest module is responsible for adding properties to the database and comparing each property against the list of notable properties. It is best to run all ingest modules to get the most out of the Correlation Engine. For example, if Hash Lookup is not run then the Correlation Engine module will not put any files into the database. If the Correlation Engine module is not run on a particular case but a central repository is enabled, there will still be some limited functionality. The Content Viewer will still display matching properties from other cases/data sources where the Correlation Engine was run.

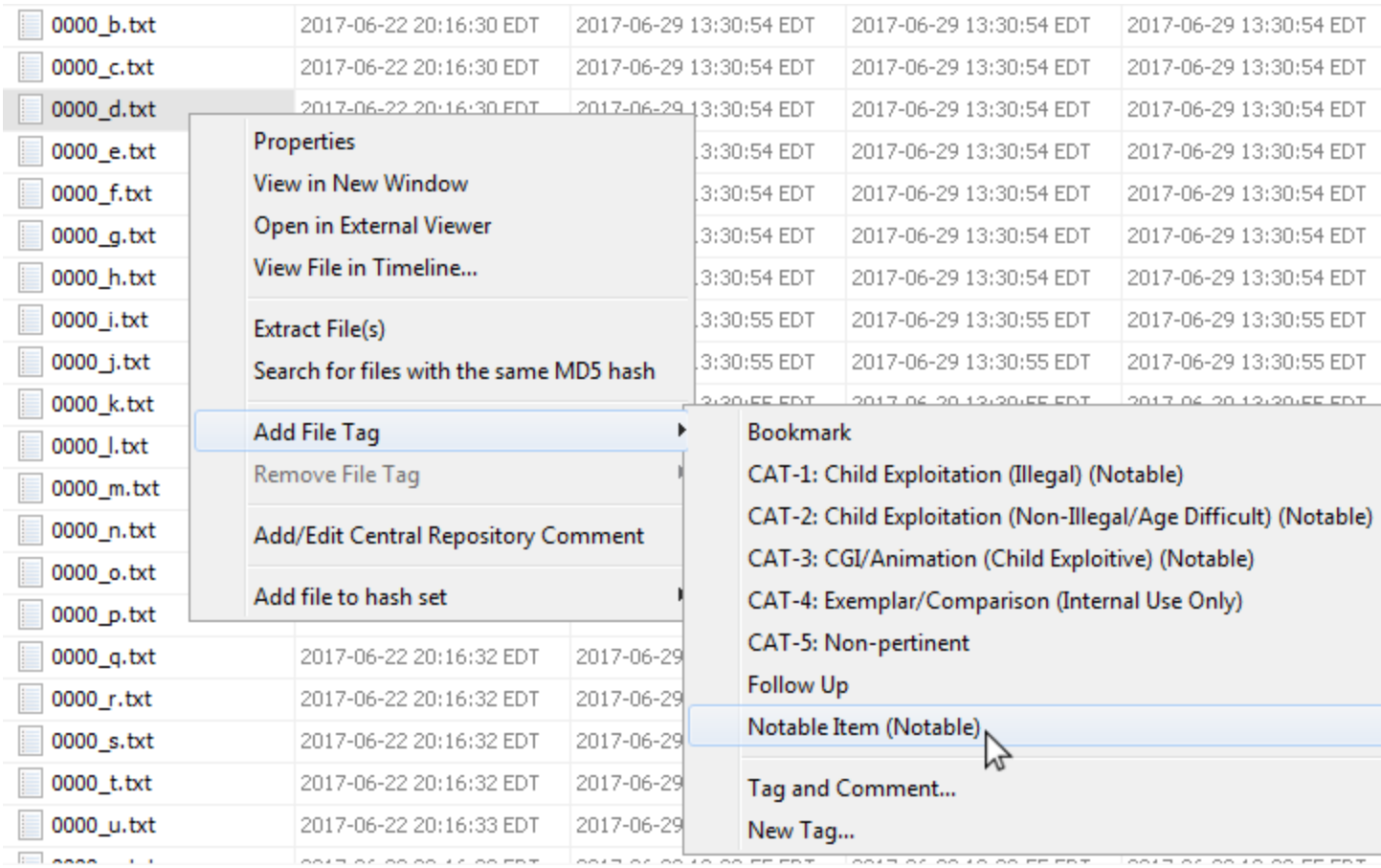


There are three settings for the Correlation Engine ingest module:

- **Save items to the Central Repository** - This should only be unselected in the rare case that you don't want to add any properties from the current data source to the central repository, but still want to flag past occurrences.
- **Flag items previously tagged as notable** - Enabling this causes Interesting Item/File artifacts to be created when properties matching those previously flagged are found. See the next section **Tagging Files and Artifacts** for details.
- **Flag previously seen devices** - When this is enabled, an Interesting Item artifact will be created if any device-related property (USB, MAC Address, IMSI, IMEI, ICCID) is found that is already in the central repository, regardless of whether they have been flagged.

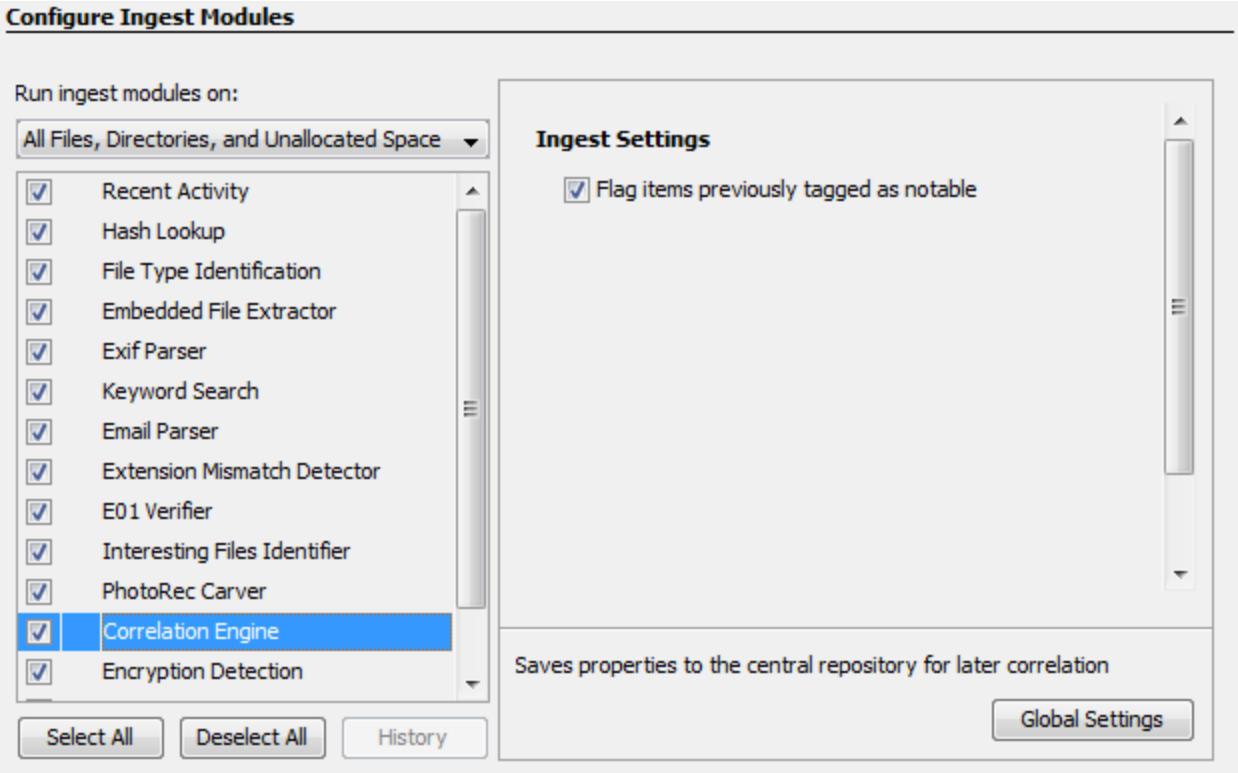
Tagging Files and Artifacts

Tagging a file or artifact with a "notable" tag will change its associated property in the central repository to notable as well. By default, there will be a tag named "Notable Item" that can be used for this purpose. See the **Tagging page** for more information on creating additional tags with notable status. Any future data source ingest (where this module is enabled) will use those notable properties in a similar manner as a Known Bad hash set, causing matching files and artifacts from that ingest to be added to the Interesting Items list in that currently open case.



If a tag is accidentally added to a file or artifact, it can be removed though the context menu. This will remove its property's notable status in the central repository.

If you would like to prevent the Interesting Items from being created in a particular case, you can disable the flagging through the run time ingest properties. Note that this only disables the Interesting Item results - all properties are still added to the central repository.



Viewing Results

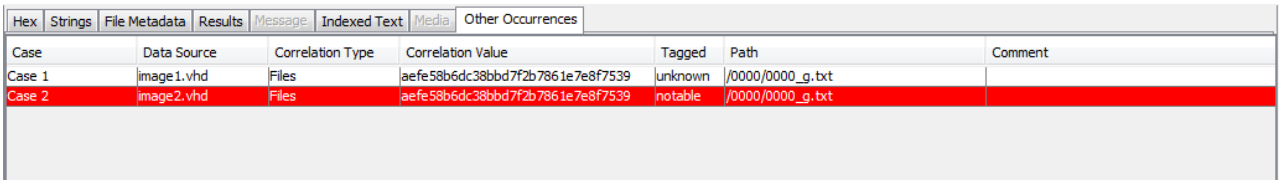
Results from enabling a central repository and running the Correlation Engine Ingest Module can be seen in two places:

- The Content Viewer for each file or artifact will display all matching properties from other cases/data sources
- The Interesting Files node of the result tree will contain any files or results that matched properties previously marked as notable

Content Viewer

The **Content Viewer** panel is where previous instances of properties are displayed. Without a central repository enabled, this "Other Occurrences" panel will show files with hashes matching the selected file within the current case. Enabling a central repository allows this panel to also display matching properties stored in the database, and adds some functionality to the row. Note that the Correlation Engine Ingest Module does not have to have been run on the current data source to see correlated properties from the central repository. If the selected file or artifact is associated by one of the supported Correlation Types, to one or more properties in the database, the associated properties will be displayed. Note: the Content Viewer will display ALL associated properties available in the database. It ignores the user's enabled/disabled Correlation Properties.

By default, the rows in the content viewer will have background colors to indicate if they are known to be of interest. Properties that are notable will have a Red background, all others will have a White background.



The user can click on any column heading to sort by the values in that column.

If the user right-clicks on a row, a menu will be displayed. This menu has several options.

1. Select All
2. Export Selected Rows to CSV
3. Show Case Details
4. Show Frequency
5. Add/Edit Comment

Select All

This option will select all rows in the Content Viewer table.

Export Selected Rows to CSV

This option will save ALL SELECTED rows in the Content Viewer table to a CSV file. By default, the CSV file is saved into the Export directory inside the currently open Autopsy case, but the user is free to select a different location.

Note: if you want to copy/paste rows, it is usually possible to use CTRL+C to copy the selected rows and then CTRL+V to paste them into a file, but it will not be CSV formatted.

Show Case Details

This option will open a dialog that displays all of the relevant details for the selected case. The details will include:

- Case UUID
- Case Name
- Case Creation Date
- Case Examiner contact information
- Case Examiner's notes

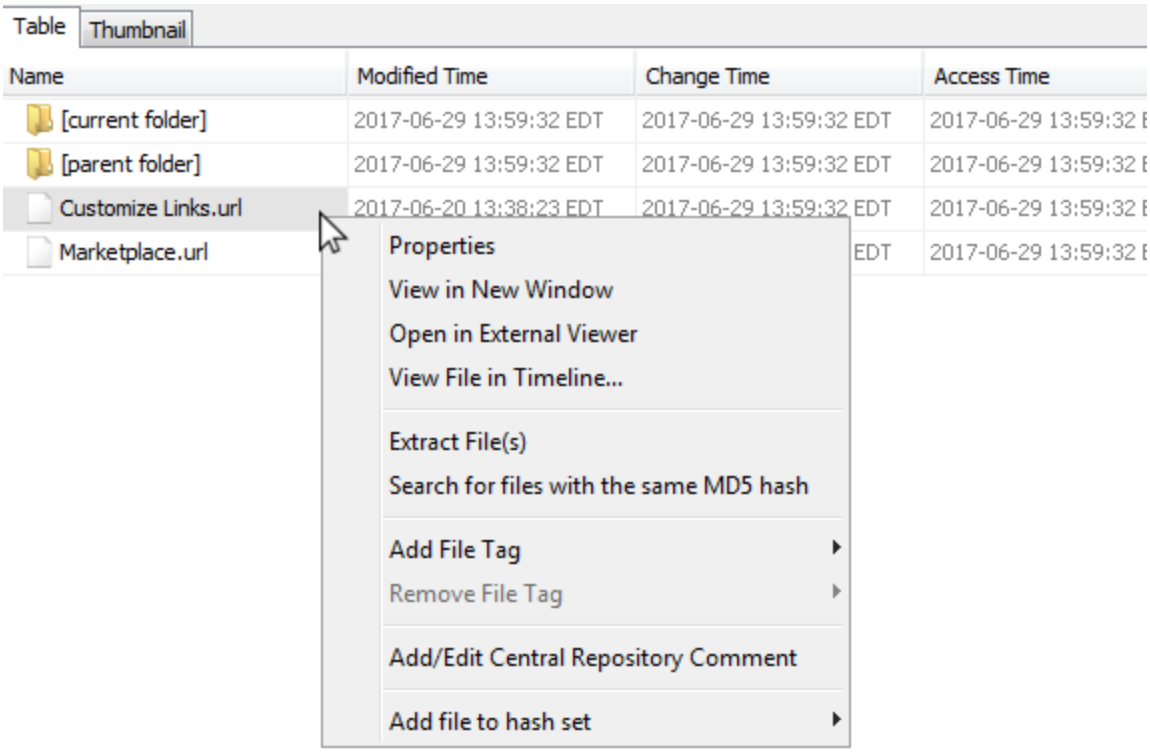
These details would have been entered by the examiner of the selected case, when creating the case or later by visiting the Case -> Case Properties menu.

Show Frequency

This shows how common the selected file is. The value is the percentage of case/data source tuples that have the selected property.

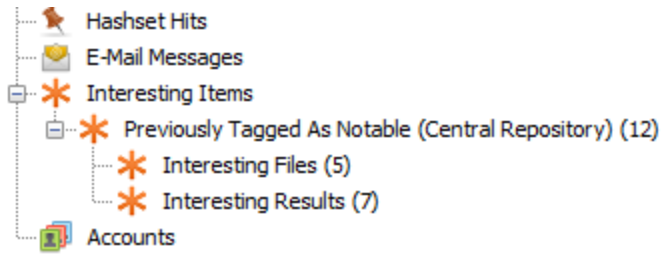
Add/Edit Comment

This allows you to add a comment for this entry or edit an existing comment. If you want instead to edit the comment of the originally selected node, it can be done by right clicking on the original item in the result viewer and selecting "Add/Edit Central Repository Comment".



Interesting Items

In the Results tree of an open case is an entry called Interesting Items. When this module is enabled, all of the enabled Correlatable Properties will cause matching files and artifacts to be added to this Interesting Items tree during ingest.



As an example, suppose the Files Correlatable Property is enabled and the ingest is currently processing a file "badfile.exe", and the MD5 hash for that file already exists in the database as a

notable file property. In this case an entry in the Interesting Items tree will be added for the current instance of "badfile.exe" in the data source currently being ingested.

The same type of thing will happen for each enabled Correlatable Property.

In the case of the phone number correlatable type, the Interesting Items tree will start a sub-tree for each phone number. The sub-tree will then contain each instance of that notable phone number.

Communications Visualization Tool

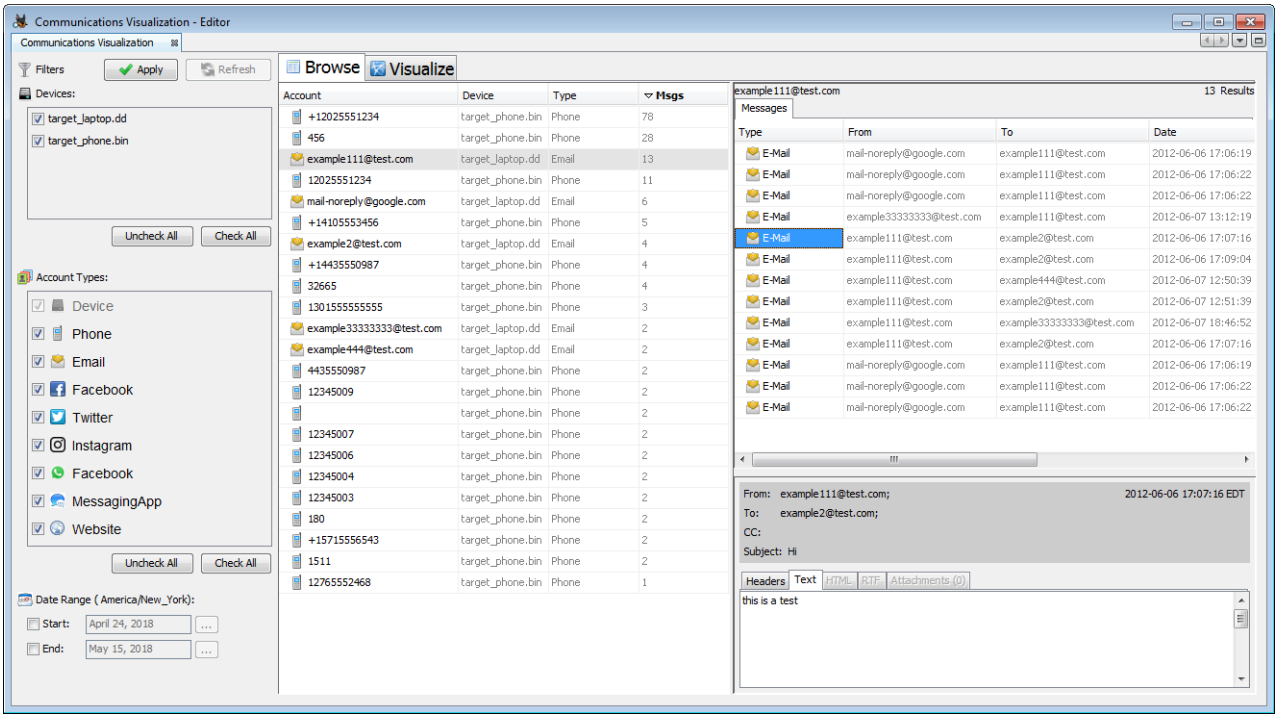
Overview

The Communications Visualization Tool gives a consolidated view of all communication events for the case. This allows an analyst to quickly view communications data such as:

- The most commonly used accounts
- Communications within a specific time frame

Usage

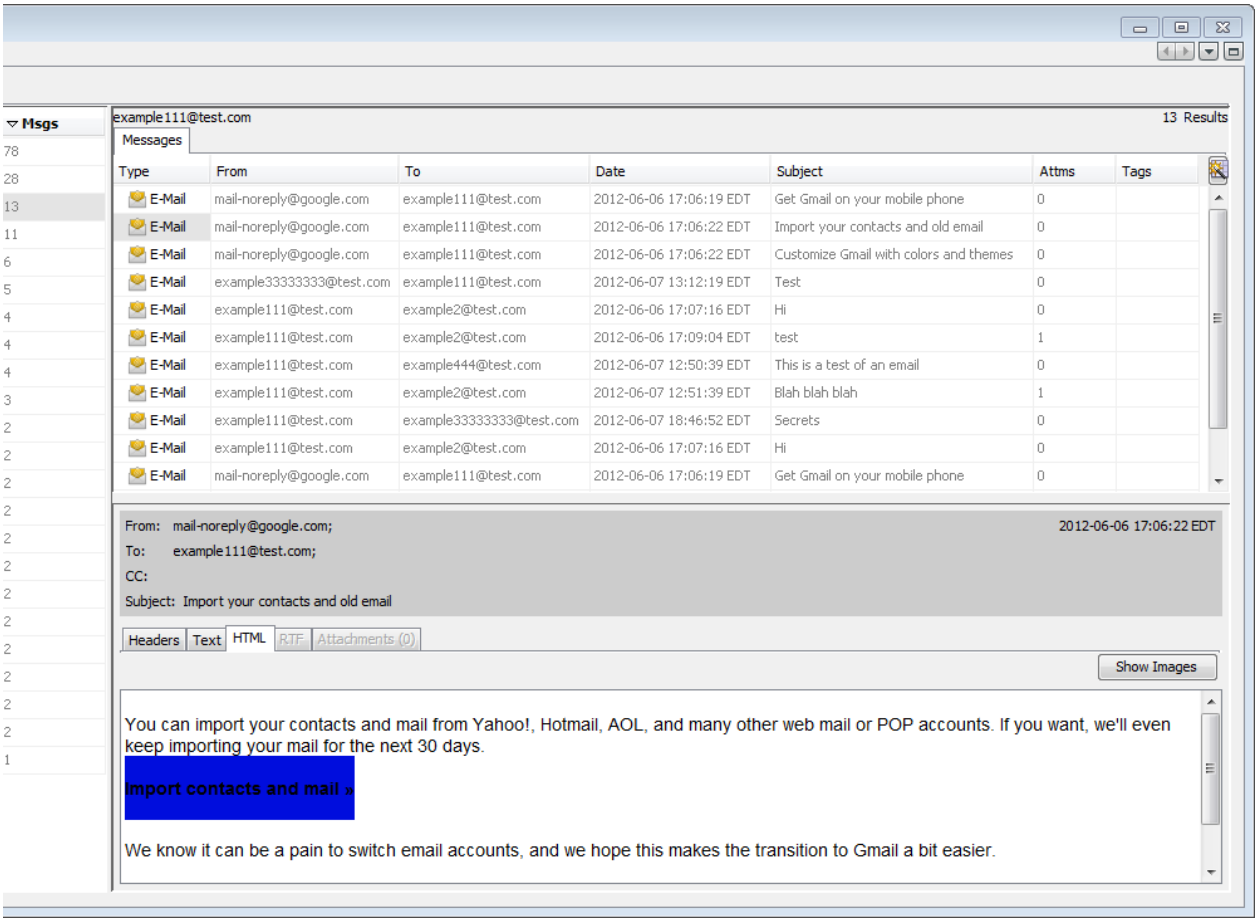
The Communications Visualization Tool is loaded through the Tools->Communications menu item.



From the left hand column, you can choose which devices to display, which types of data to display, and optionally select a time range. After any changes to the filters, use the Apply button to update the tables.

The middle column displays each account, its device and type, and the number of associated messages (emails, call logs, etc.). By default it will be sorted in descending order of frequency.

Selecting an account in the middle column will bring up the messages for that account in the right hand column. Here data about each message is displayed in the top section, and the messages itself can be seen in the bottom section (if applicable).

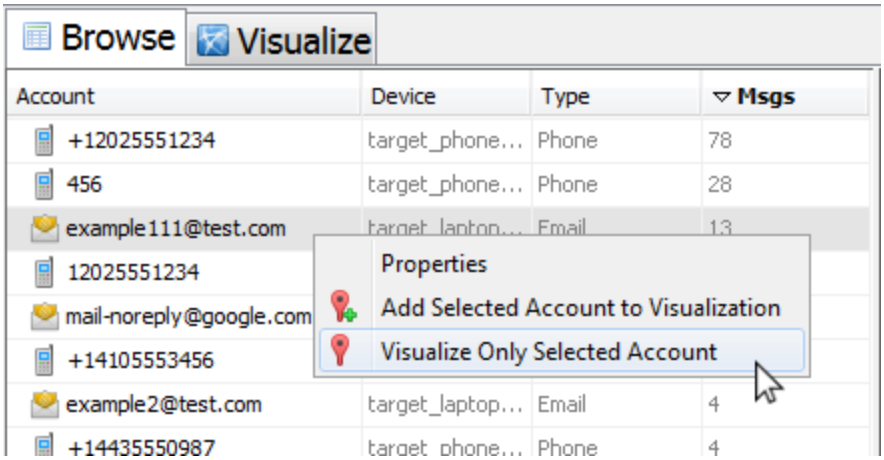


The middle column and the right hand column both have a **UI Quick Search** feature which can be used to quickly find a visible item in their section's table.

Visualization

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

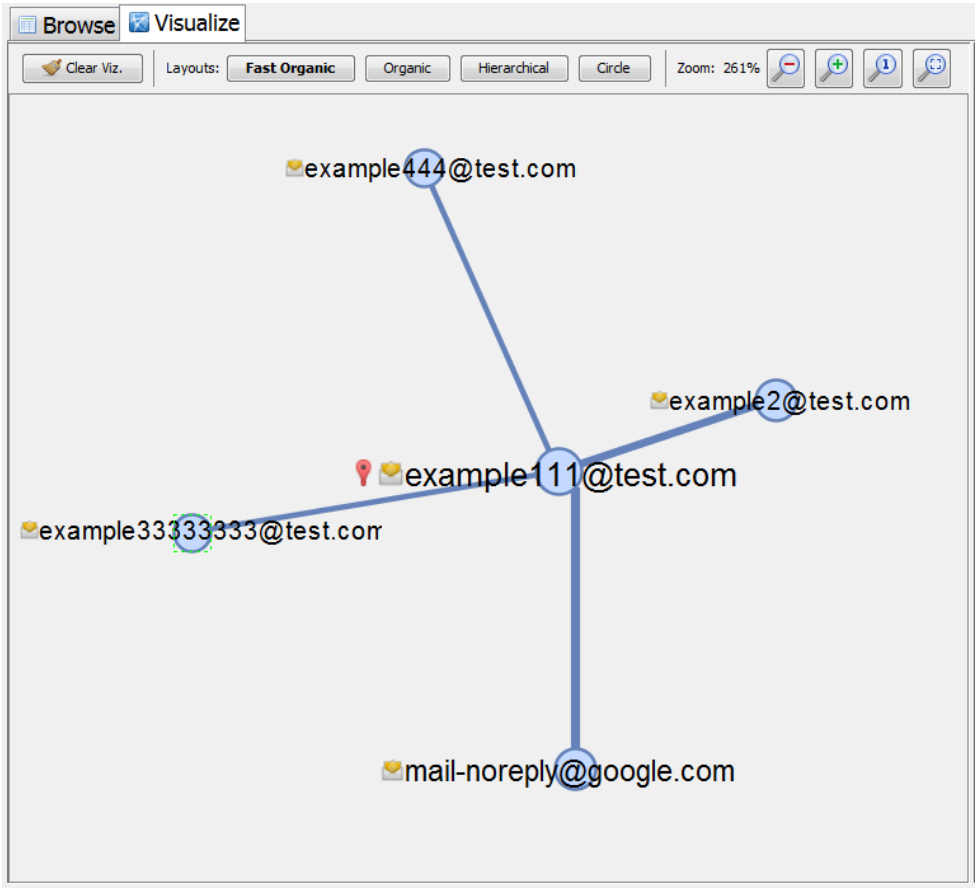
To start, right click the first account you want to view.



There are two options, which are equivalent when no accounts have previously been selected:

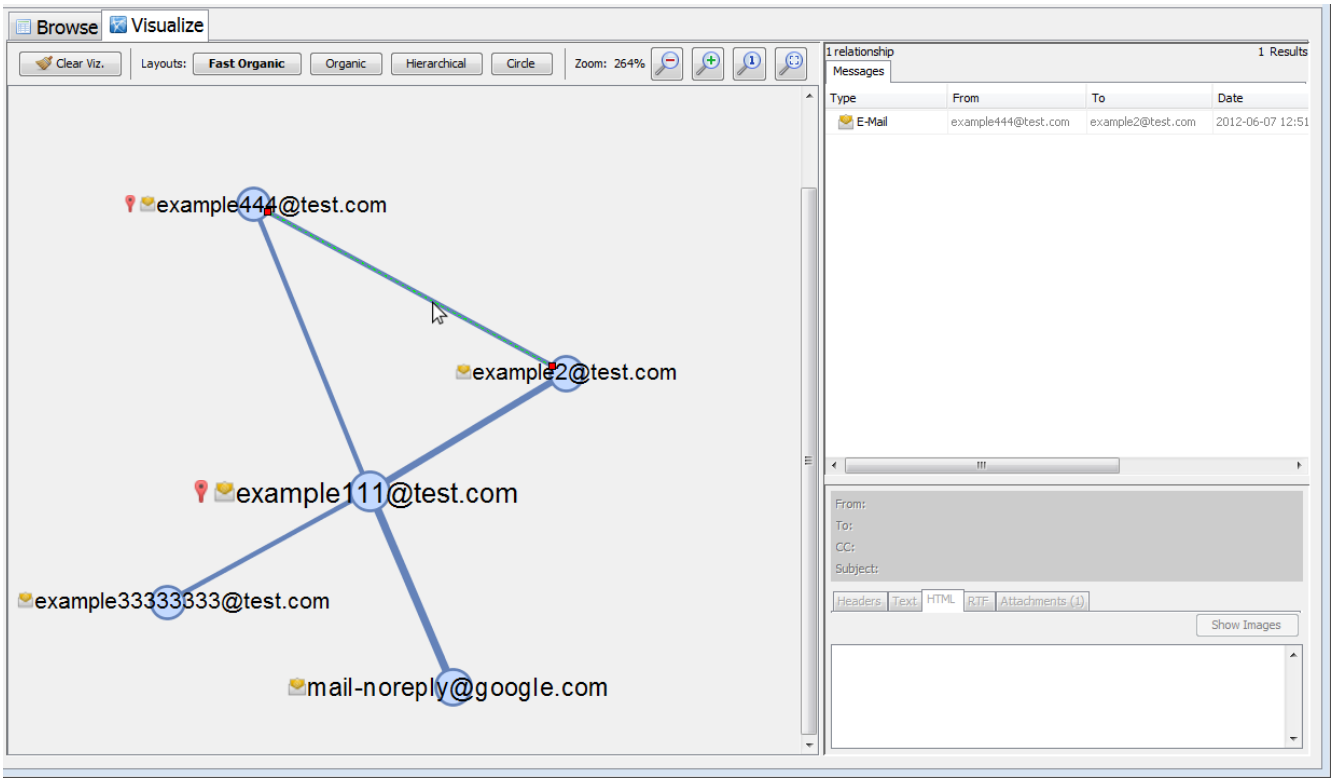
- Add Selected Account to Visualization - Adds this account and its connections to the graph
- Visualize Only Selected Account - Clears the graph and only displays the connections for this account

After selecting either option, the middle tab will switch to the Visualize view and the graph will be displayed.



The options at the top allow you to clear the graph, try different graph layouts, and resize the graph. The nodes in the graph can be dragged around and nodes and edges can be selected to display their messages or relationships in the right side tab. For example, in the image below the link between

two email addresses has been selected so the Messages viewer is displaying the single email between those two email addresses.



Common Properties Search

Overview

The Common Properties Search feature allows you to search for multiple copies of a property within the current case or within the **Central Repository**.

To start a search, go to Tools->Find Common Properties to bring up the main dialog. Searching requires at least one of the following to be true:

- The current case has more than one data source
- The Central Repository contains at least two cases

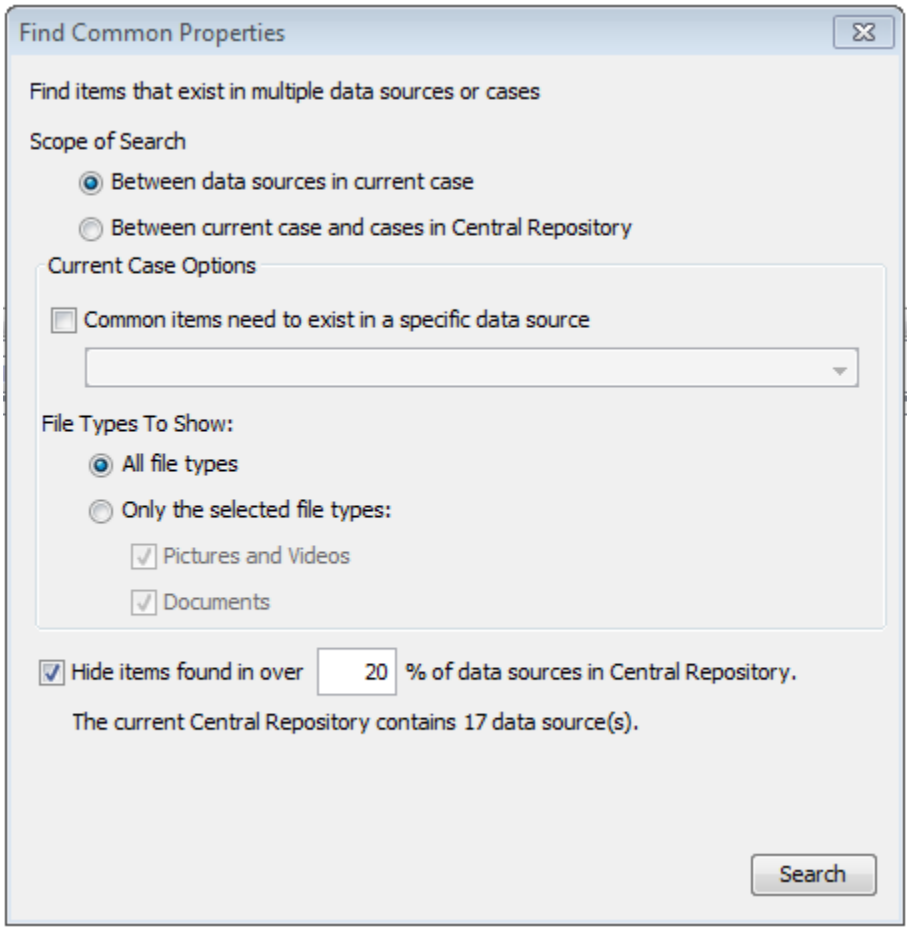
If both conditions are false, then the menu item will be disabled. If only one is false then part of the search dialog will be disabled.

Common Properties Search Scope

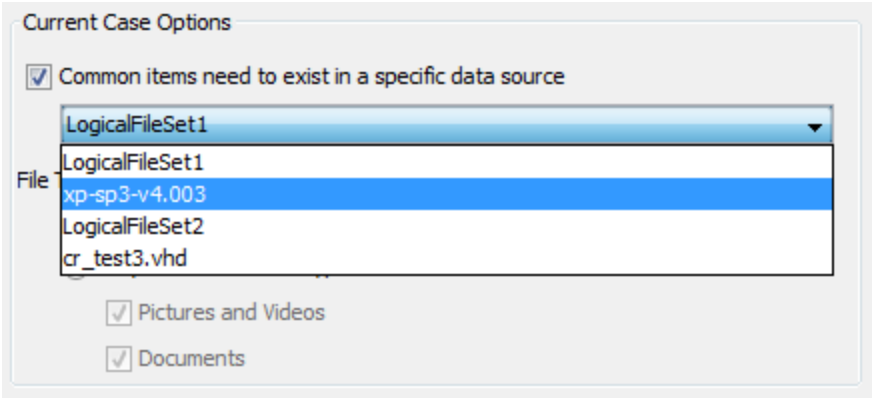
Different parameters are needed for setting up the two types of searches. These will be described below.

Scope - between data sources in the current case

This type of search looks for files that are in multiple data sources within the current case. It does not require the Central Repository to be enabled, and currently only searches for common files. You must run the **Hash Lookup Module** to compute MD5 hashes on each data source prior to performing the search. The search results will not include any files that have been marked as "known" by the hash module (ex: files that are in the NSRL).



By default, the search will find matching files in any data sources. If desired, you can change the search to only show matches where one of the files is in a certain data source by selecting it from the list:

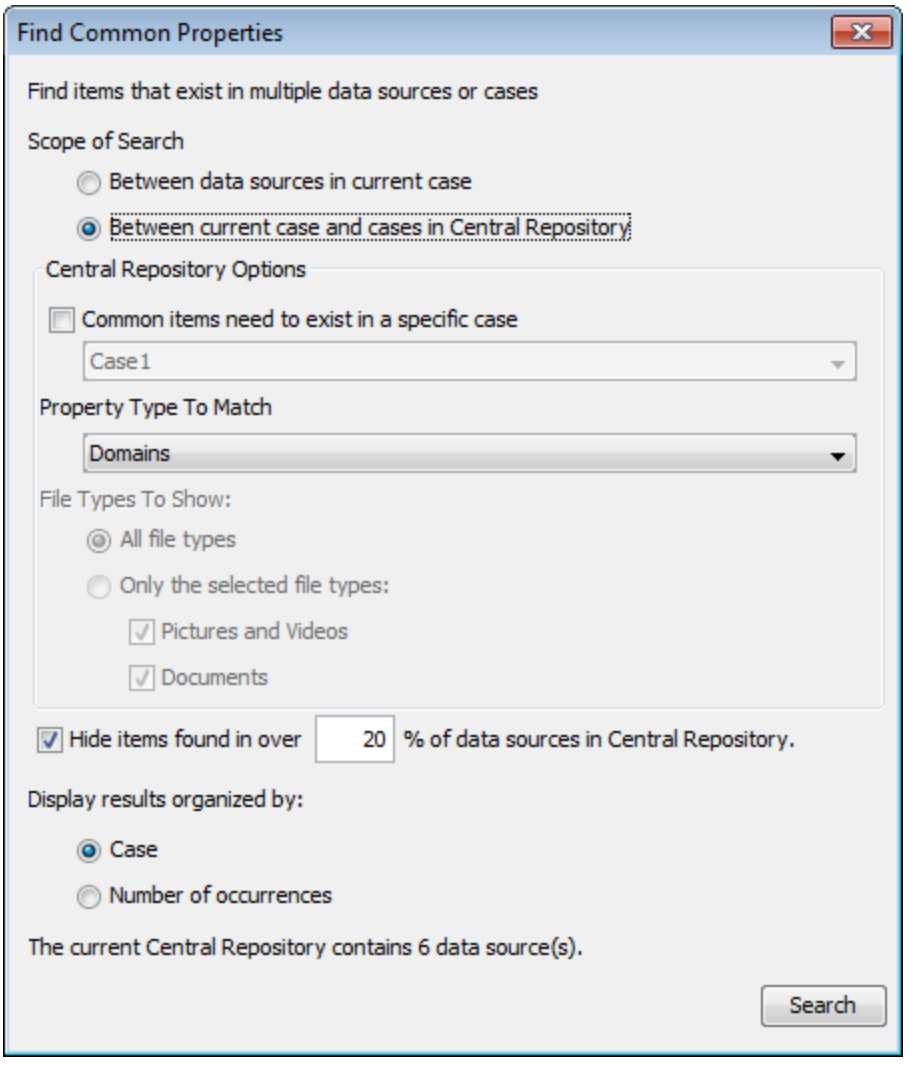


You can also choose to show any type of matching files or restrict the search to pictures and videos and/or documents.

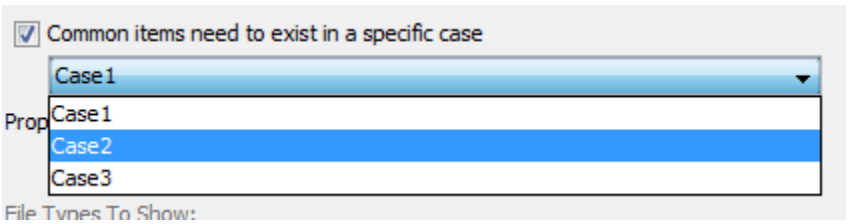
Finally, if you have the Central Repository enabled you can choose to hide matches that appear with a high frequency in the Central Repository.

Scope - between current case and cases in the Central Repository

This type of search looks for files that contain common properties between the current case and other cases in the Central Repository. You must run the Correlation Engine ingest module on each case with the property you want to search for enabled, along with the ingest modules that produce that property type (see **Manage Correlation Properties**).

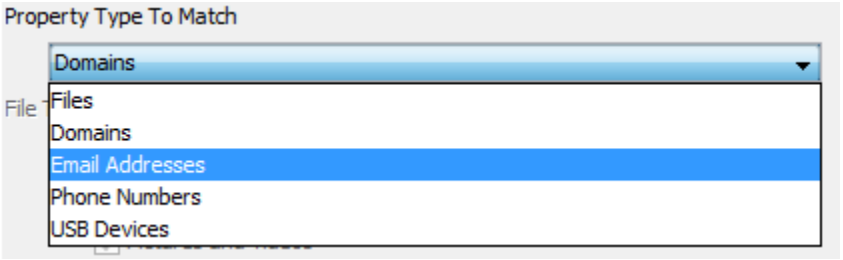


You can restrict the search to only include results where at least one of the matches was in a specific case.



In the example above, any matching properties would have to exist in the current case and in Case 2. Note that matches in other cases will also be included in the results, as long as the property exists in the current case and selected case.

You can select the type of property to search for in the menu below:



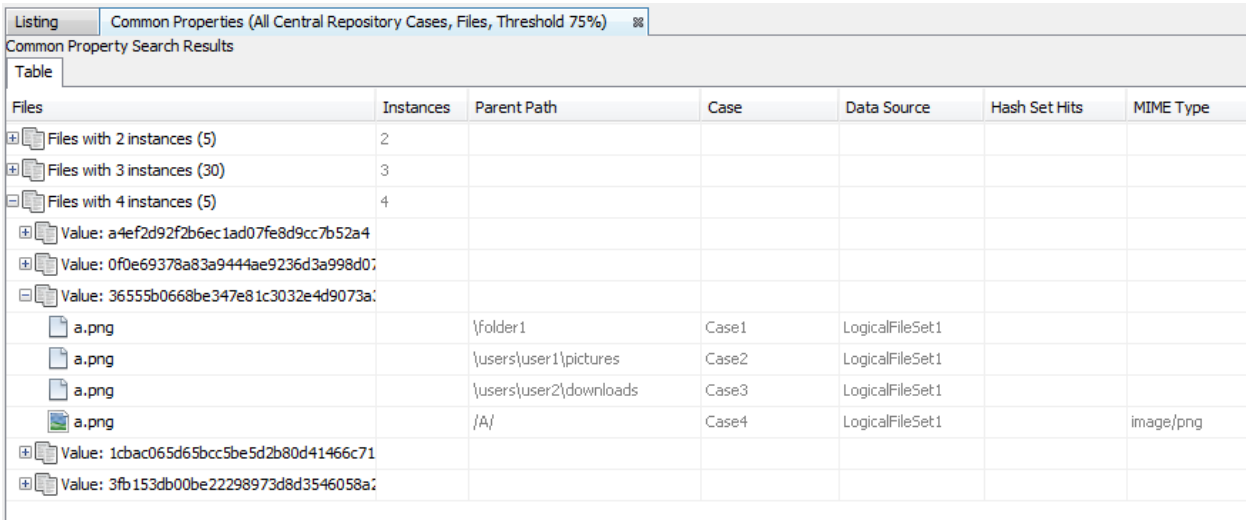
Restricting a file search to only return images or documents is currently disabled.

You can choose to hide matches that appear with a high frequency in the Central Repository. Finally you can choose how to display the results, which will be described below.

Search Results

Each search displays its results in a new tab. The title of the tab will include the search parameters.

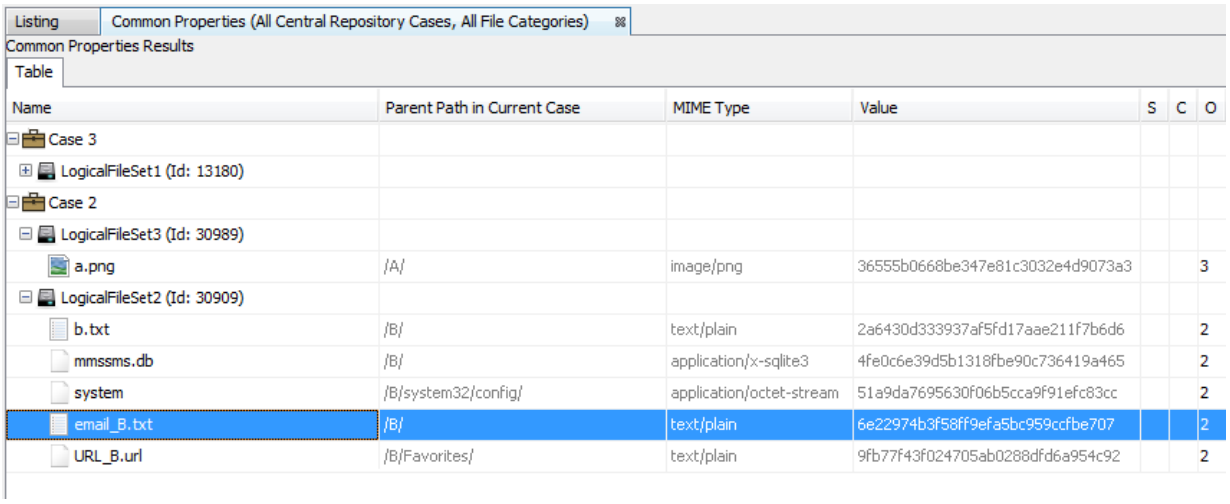
Sort by number of occurrences



This is how all results from searches within the current case are displayed, and an option for displaying the results of a search between the current case and the Central Repository. The top tree level of the results shows the number of matching properties. The results are grouped by how many matching properties were found and then grouped by the property itself.

Sort by case

This option is only available when searching between the current case and the Central Repository. The top level shows each case with matching properties, then you can select which data source to view. Every matching property will be displayed under the data source.



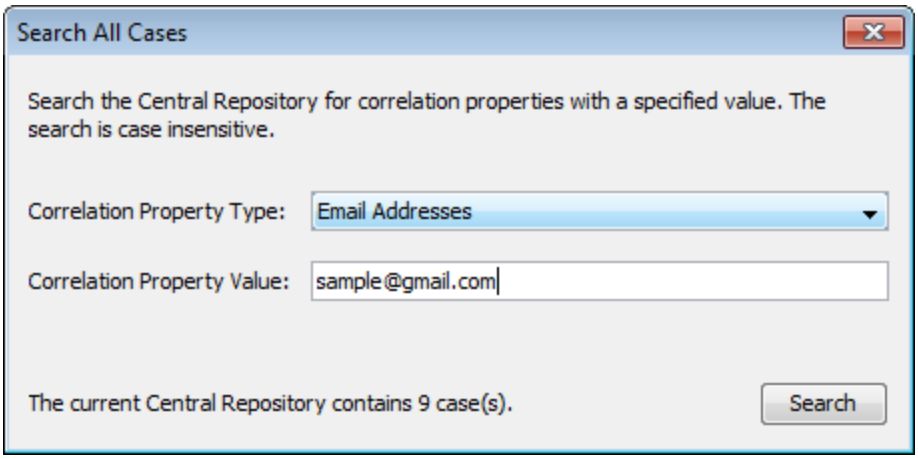
Search All Cases

Overview

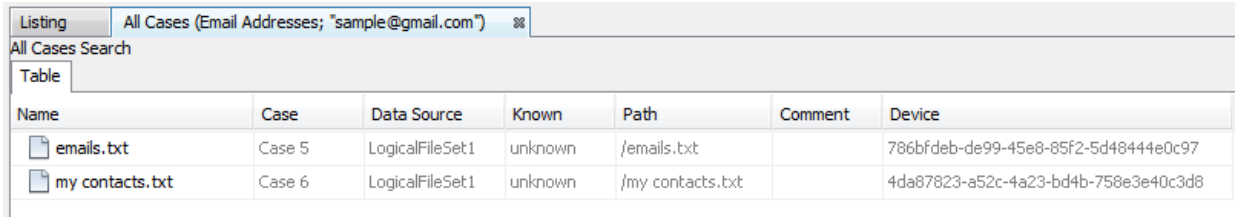
The Search All Cases feature allows you to search the **Central Repository** for arbitrary properties. You must have the Central Repository enabled to run this search, and you must have a case open (though the open case has no effect on the search results).

Usage

Go to Tools->Search Other Cases to open the search dialog. Here you can select the property type and value to search for. An example of what the value should look like will be displayed in light grey in the Correlation Property Value box. If the entered value is invalid for that property type a red error message will be displayed.



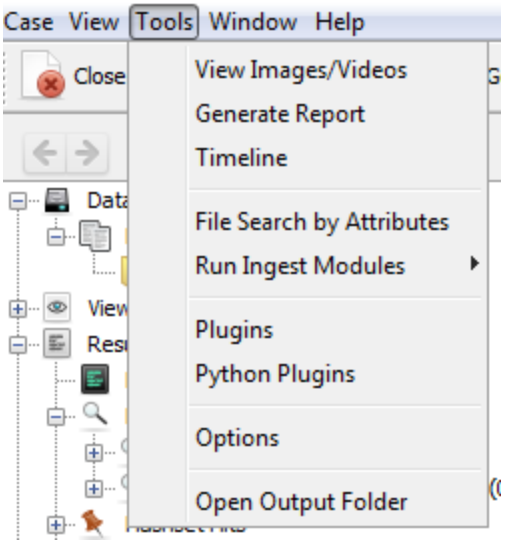
Once you hit the Search button, any results will be displayed in the Result Viewer. The tab title will display what was searched for ("Email Addresses" and "sample@gmail.com" in the example).



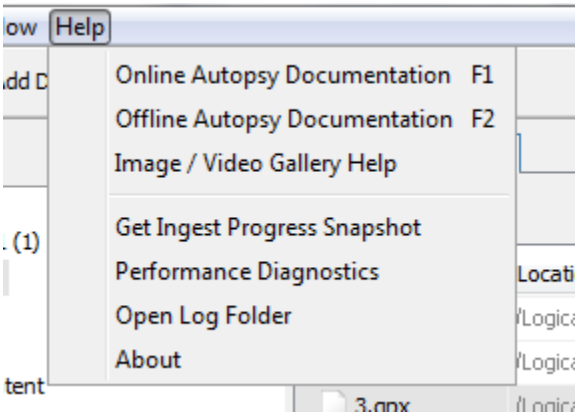
Logs, Output, and Progress

There are several shortcuts for getting to the output folder, log folder, and progress shapshot shown below.

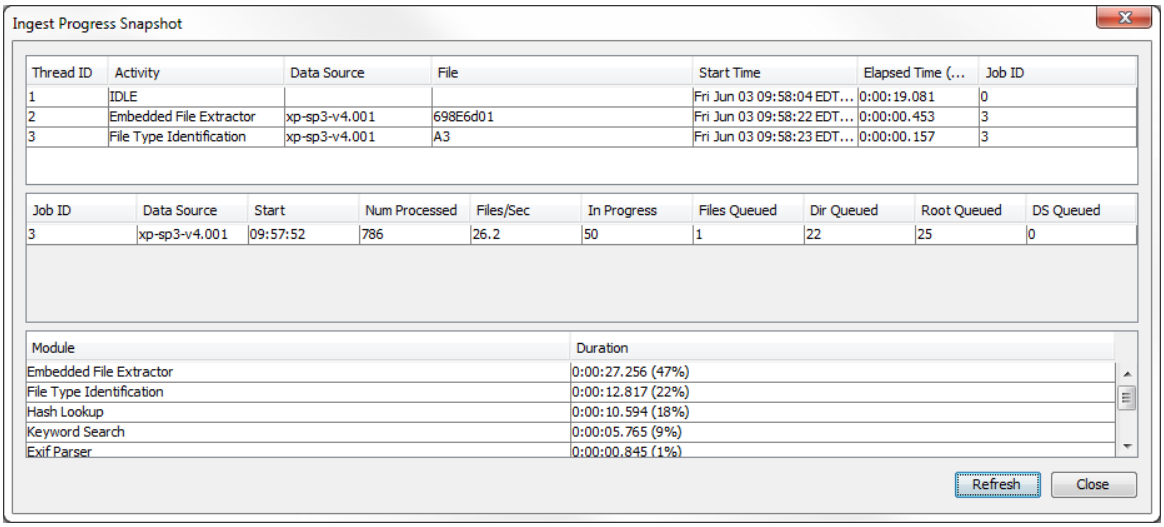
To open the Case output folder, use "Tools", "Open Output Folder" as shown below:



To open the Case log folder, use "Help", "Help" as shown below:



While Ingest is running, one can use the "Ingest Progress Snapshot" tool to see what activity is going on at the moment. Click on "Help", "Get Ingest Progress Snapshot" to view the dialog shown in the screenshot below.



To refresh the view, use the "Refresh" button.

Reporting

Tagging

Tagging (or Bookmarking) allows you to create a reference to a file or object and easily find it later. Tagging is also used by the **central repository** to mark items as notable.

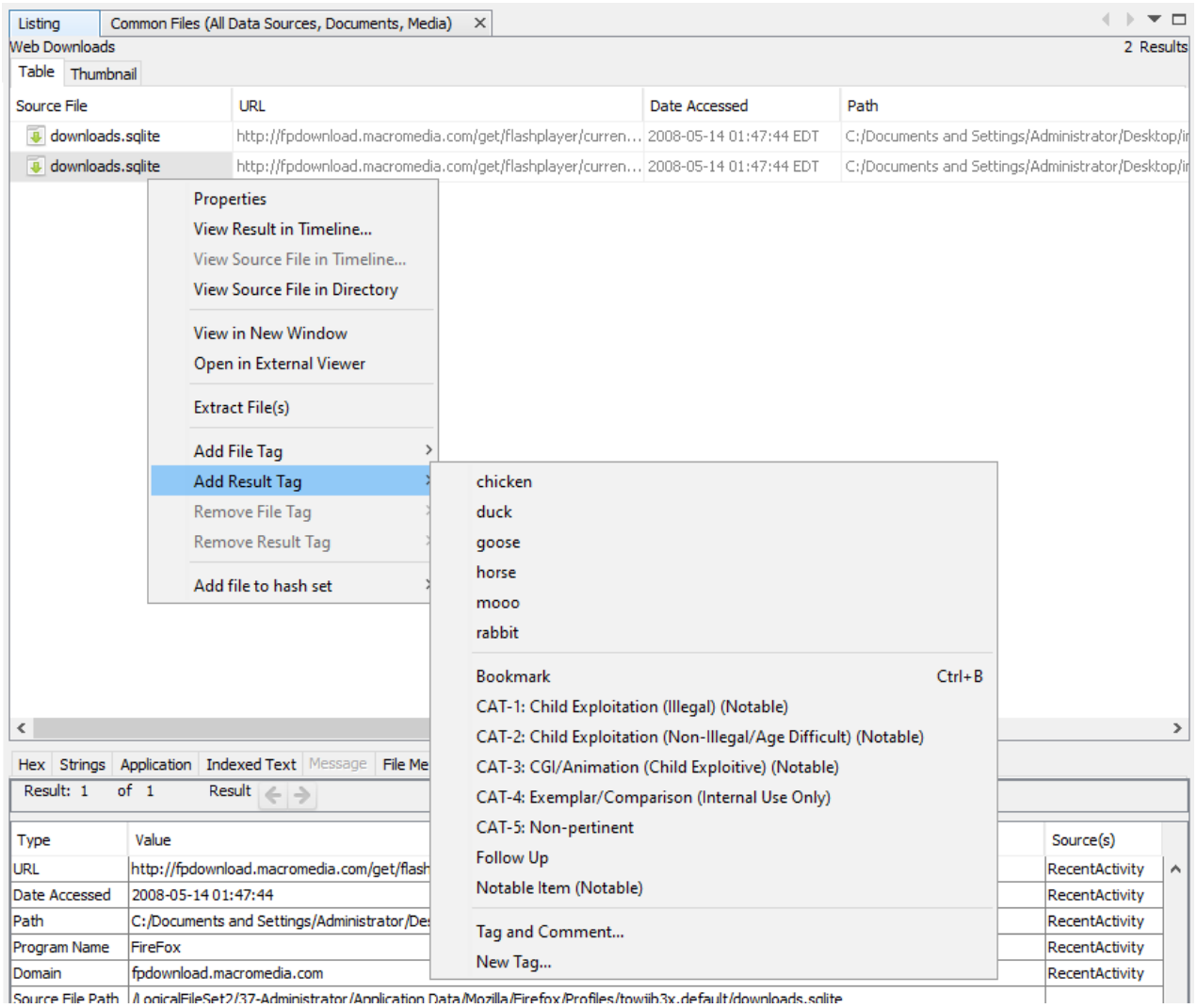
Tagging items

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 a Blackboard artifact result, you have the choice to either:

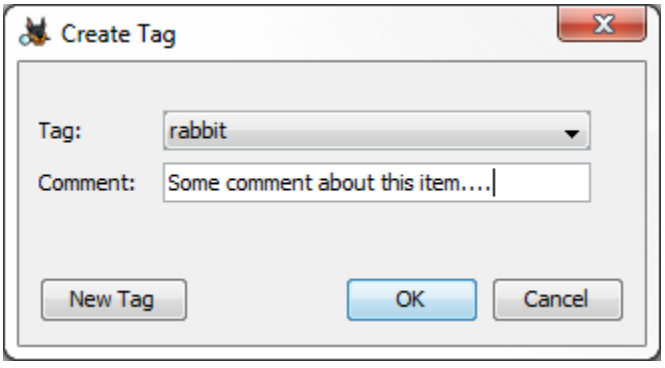
- Tag File – use this when the file itself is of interest
- Tag Result – use this when the result is of interest

Which to choose depends upon the context and what you desire in the final report.



At this point there are three options:

- Use one of the existing tags to add it to the file/result without a comment
- Tag and Comment – use this if you need to add a comment about this tag



- New tag – Create a new tag and add it to the file/result

There are several default tag names:

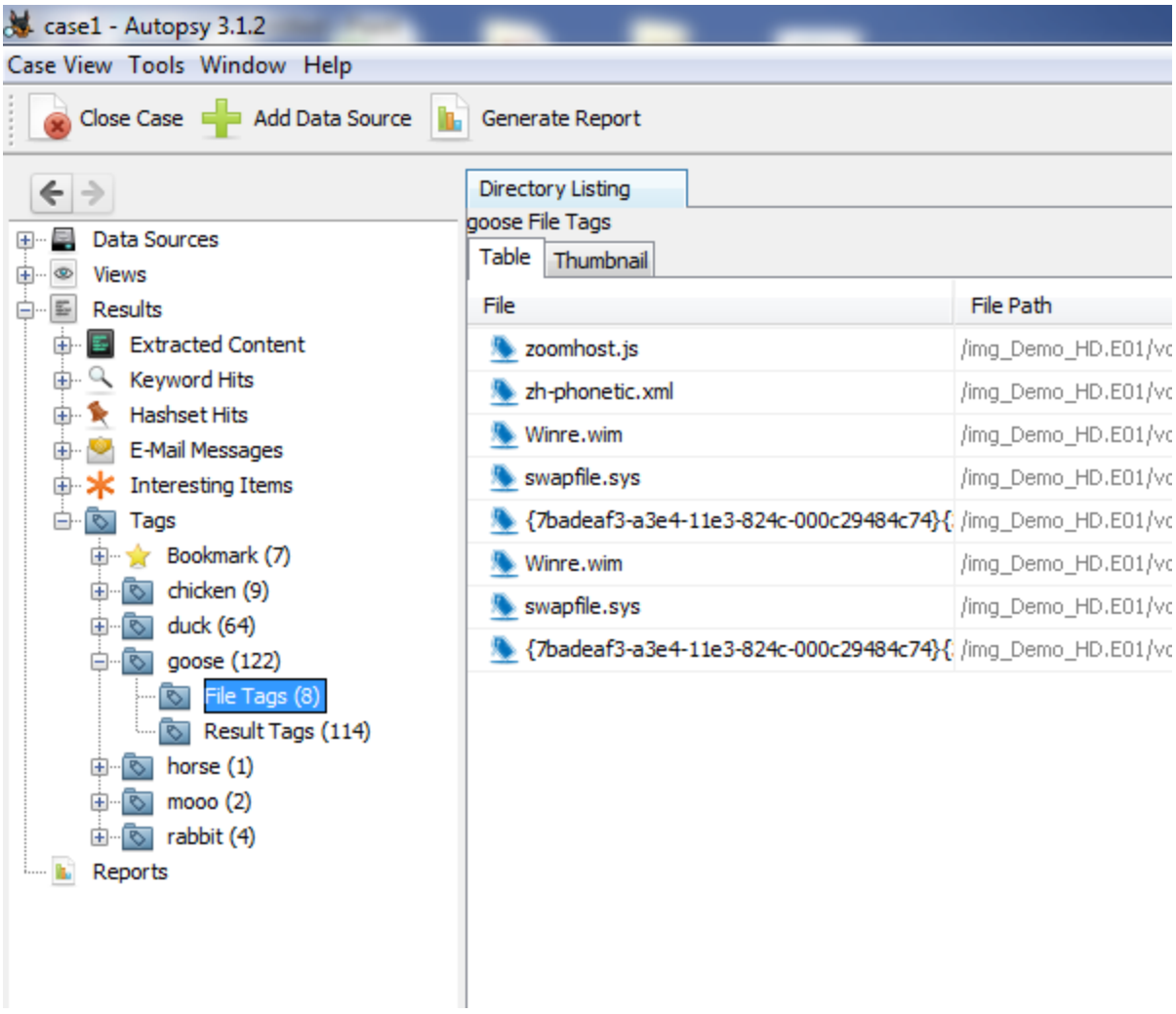
- Bookmark - Default tag for marking files of interest
- CAT-1 through CAT-5 - For law enforcement use
- Follow Up - Default tag for marking files to follow up on
- Notable item - Default tag for indicating that an item should be marked as notable in the central repository

You can also create custom tag names. These tag names will be automatically saved for future use and will be displayed above the default tag names.

If you just want to tag the item with the default "Bookmark" tag, you can also use the keyboard shortcut control+B instead of going through the menus.

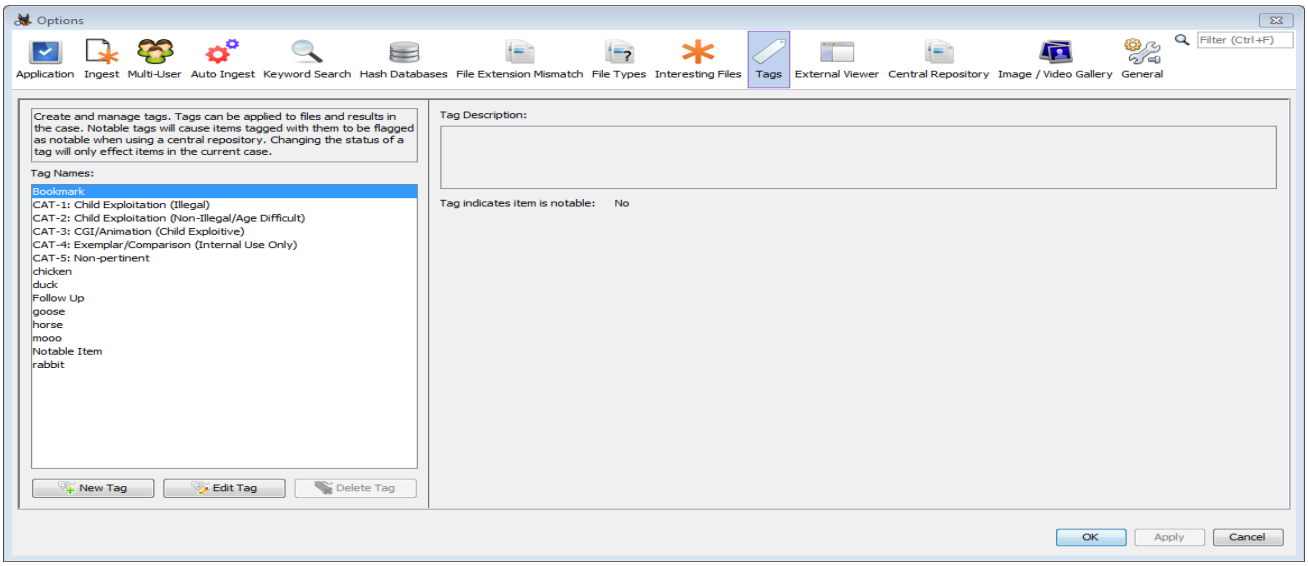
You can also apply tags to groups of items at once. Select multiple items in the Blackboard, right click, and add the appropriate tag. Items may have more than one tag.

Tagged results are shown in the "Results" portion of the tree under "Tags". Tagged items are also highlighted in the Results Viewer.

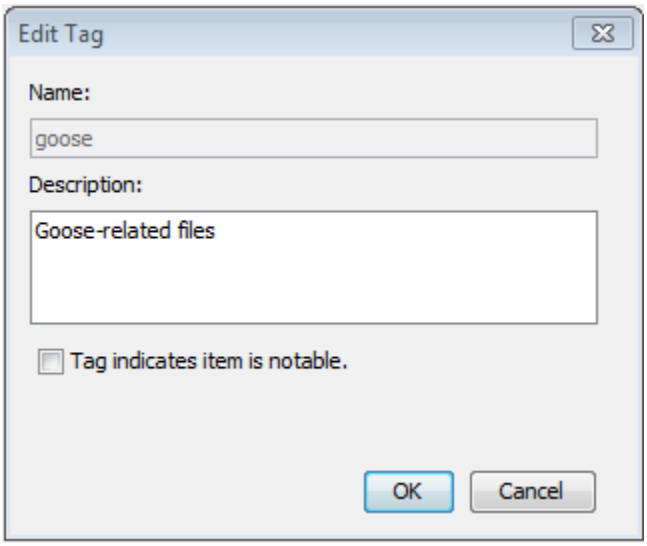


Managing tags

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



From here, new tags can be added, existing tags can be edited, and user-created tags can be deleted. Note that deleting a tag does not remove it from any tagged items, and that tag will still be usable in any case where it has been used to tag an item.

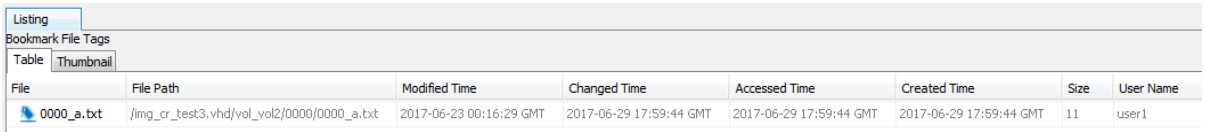


If using the central repository, changing the notable status will effect tagged items in the current case only in the following way:

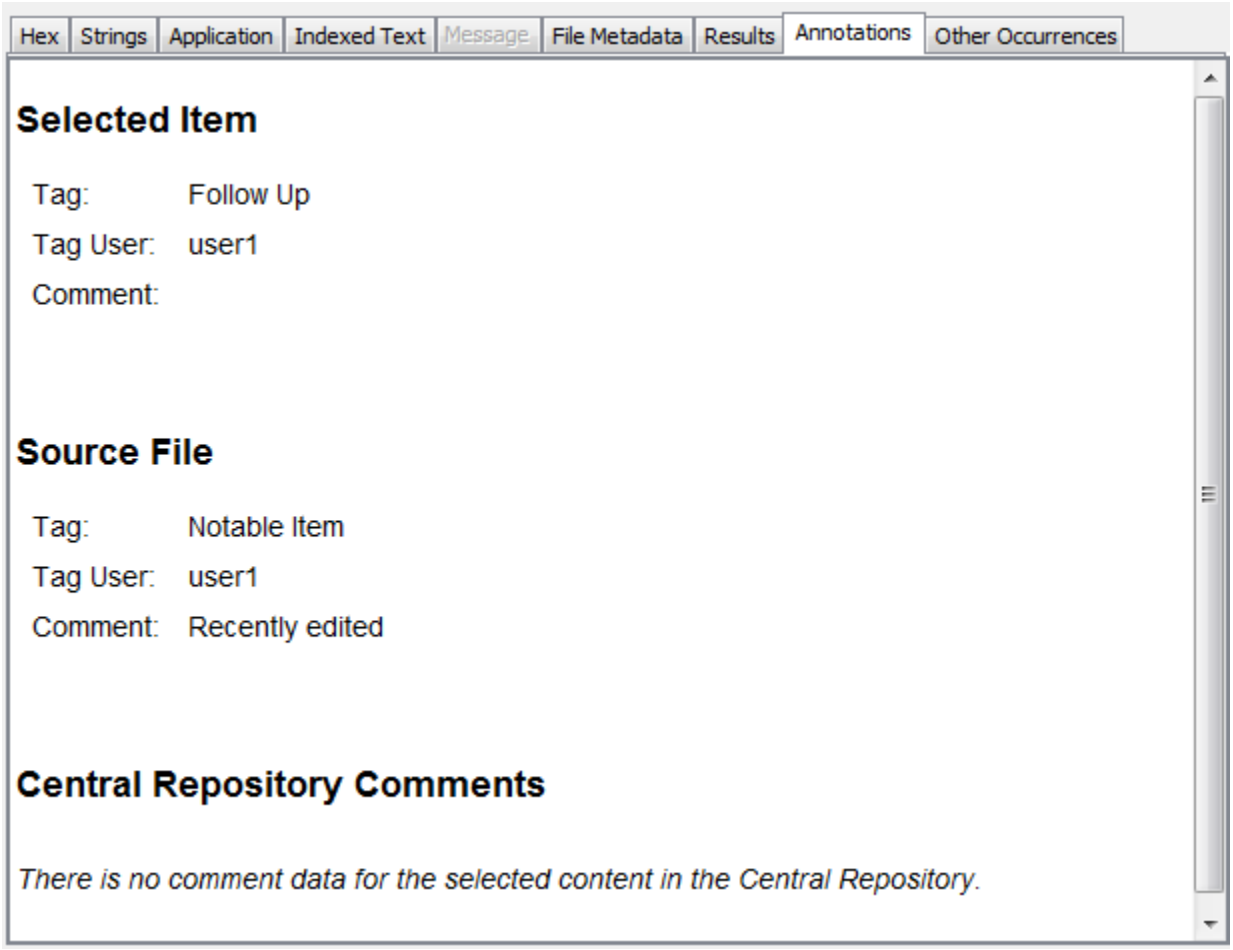
- If "File A" is tagged with "Tag A", which is not notable, and then "Tag A" is switched to notable, "File A" will be marked as notable in the central repository
- If "File B" is tagged with "Tag B", which is notable, and then "Tag B" is switched to non-notable, if there are no other notable tags on "File B" then its notable status in the central repository will be removed.

Hiding tags from other users

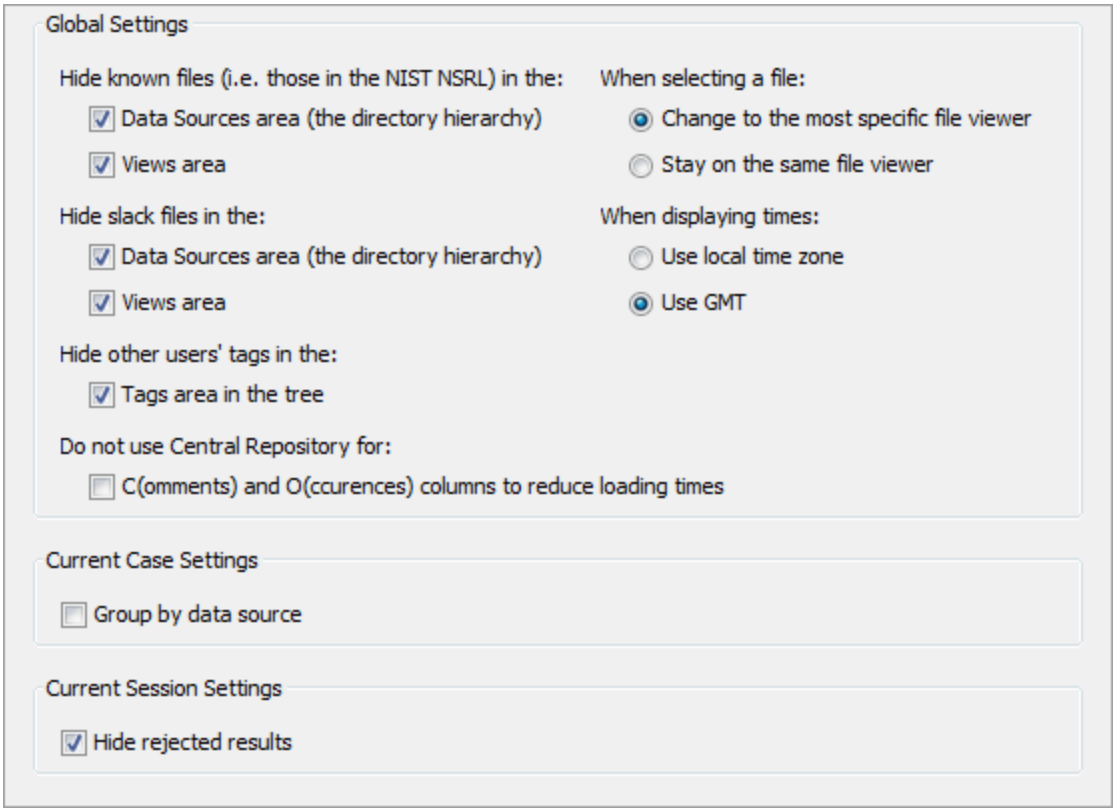
Tags are associated with the account name of the user that tagged them. This information is visible through selecting items under the "Tags" section of the directory tree:



or through the **Annotations** content viewer:



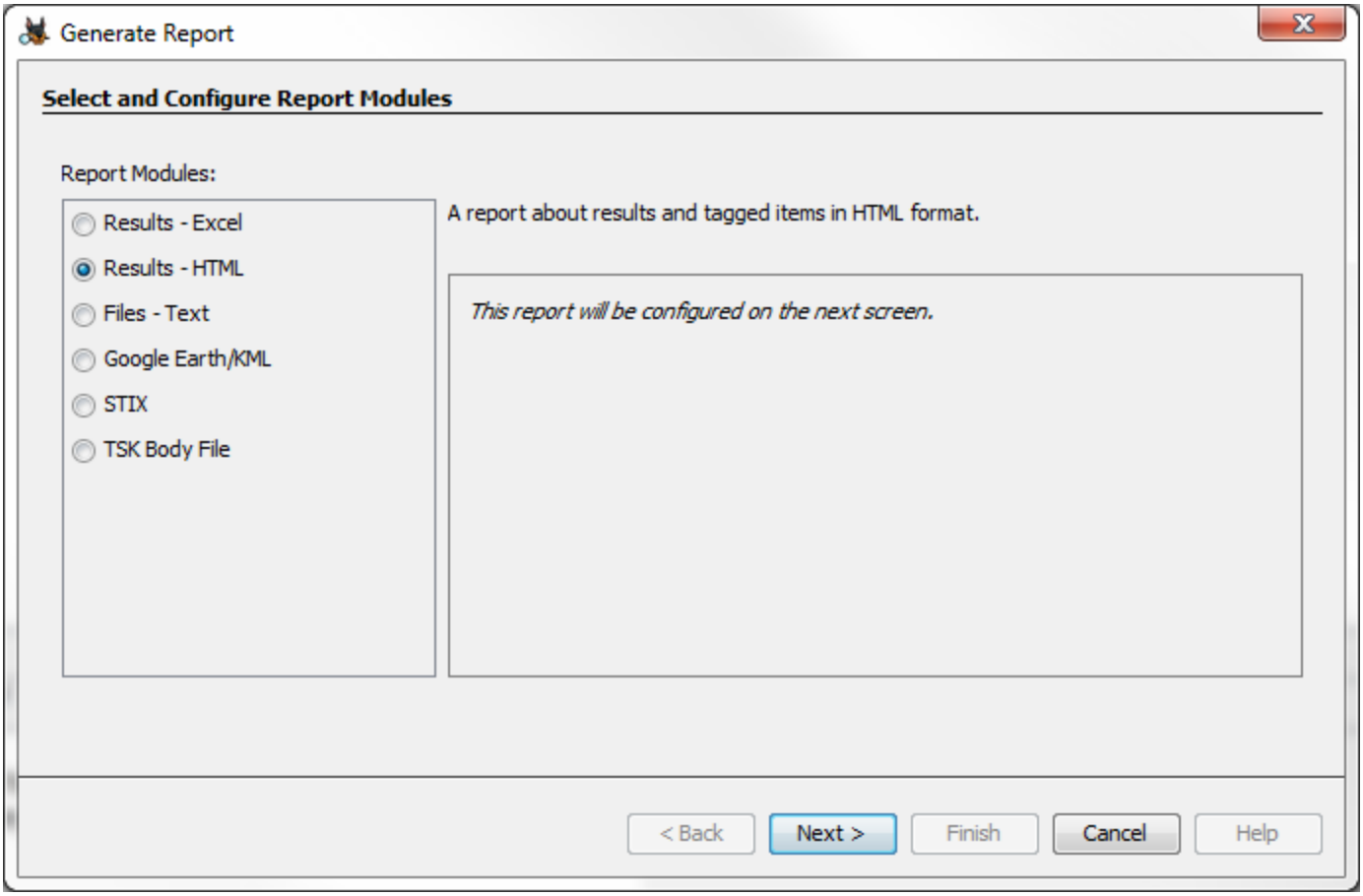
It is possible to hide all tagged files and results in the "Tags" area of the tree that were tagged by other users. Open the **View Options** menu either through the gear icon above the directory tree or through Tools->Options, and then select the checkbox to hide other users' tags in the tags area of the tree.



Reporting

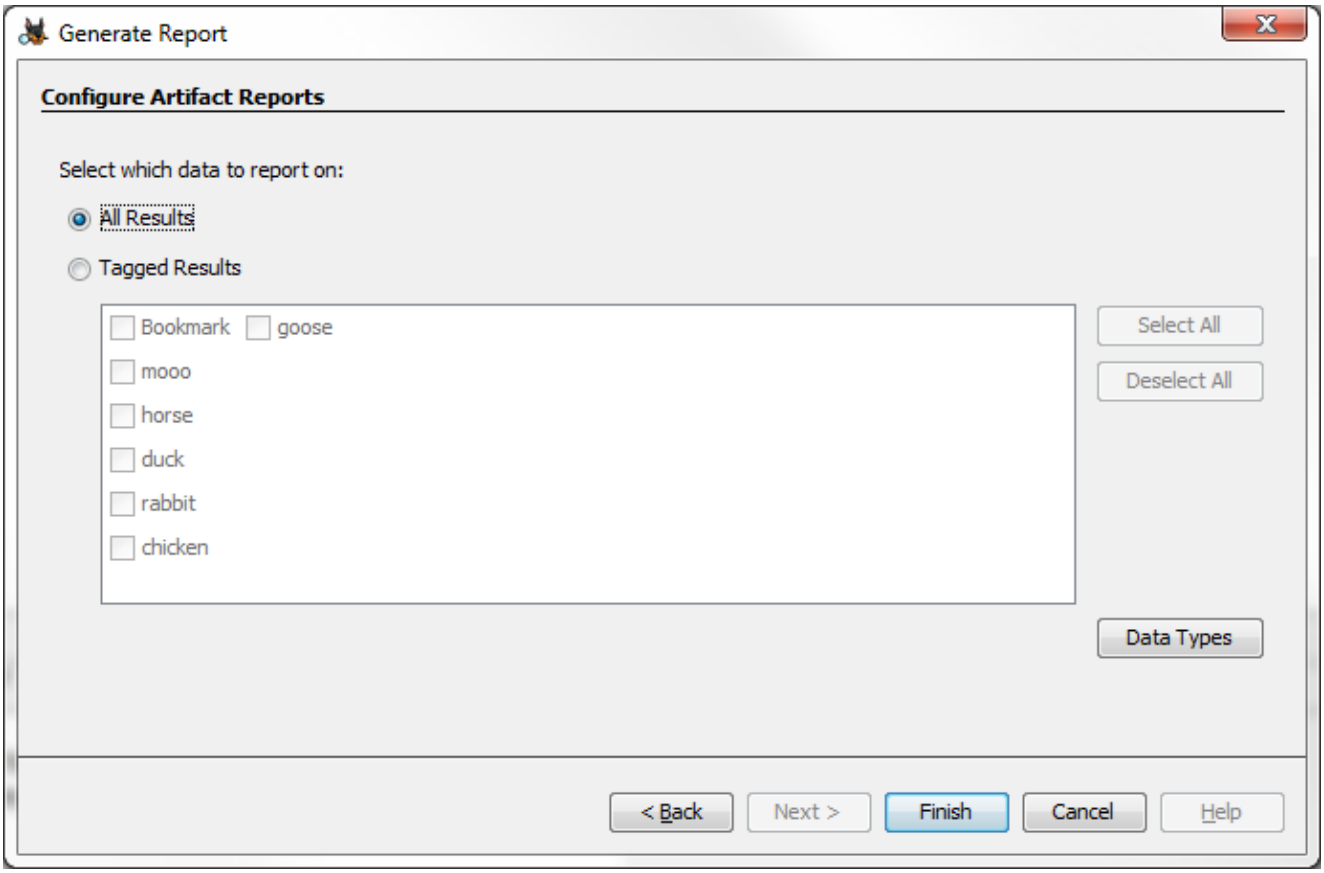
Reporting

To create a report, go to "Tools", "Generate Report". You can choose several different types of reports. We will go through the HTML report here.

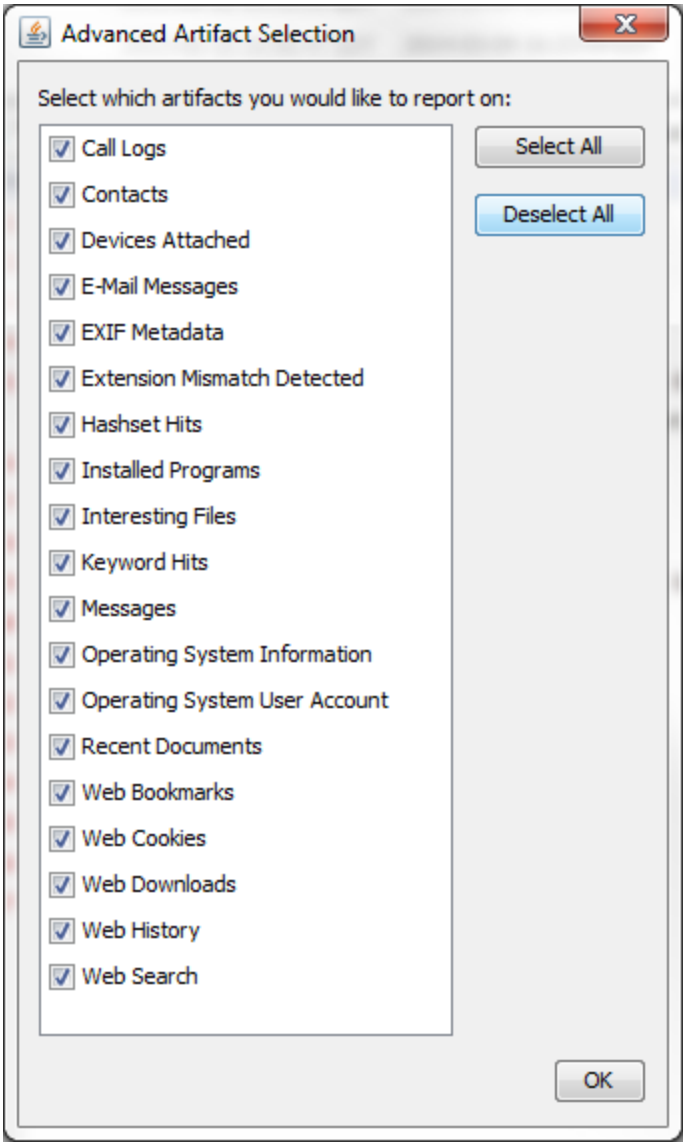


When you have selected a report type, choose between

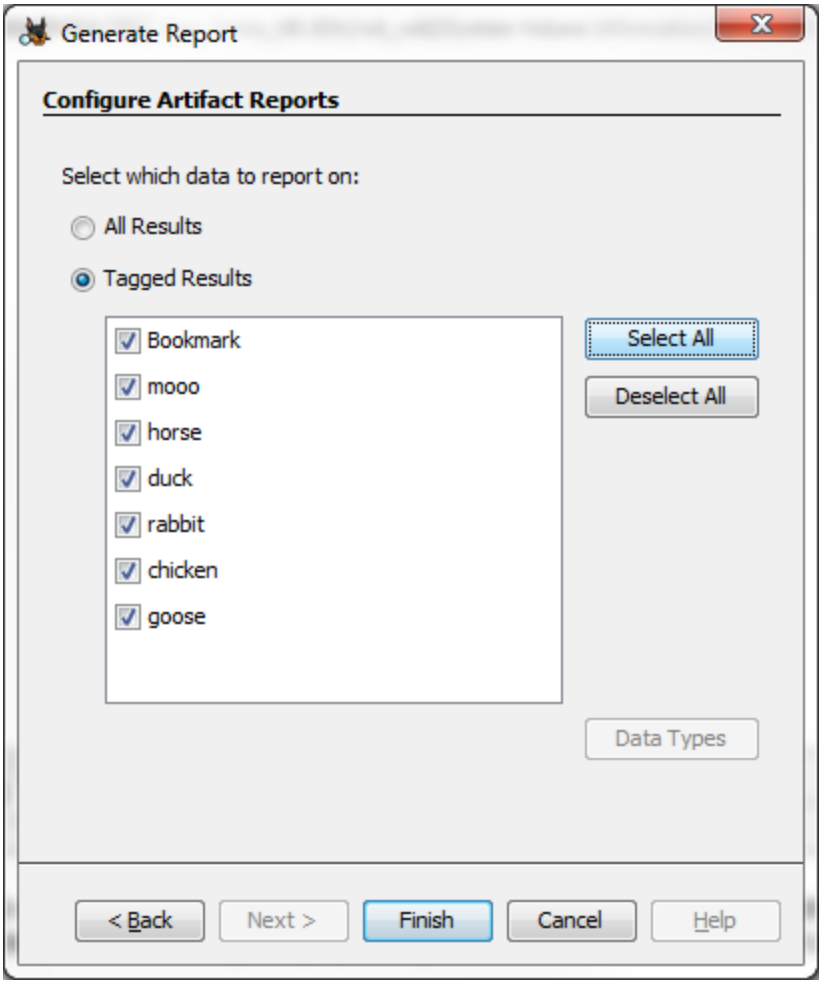
- All Results
- Tagged Results



If you select All Results, you can choose the Data Types (Artifact Types) you would like included.

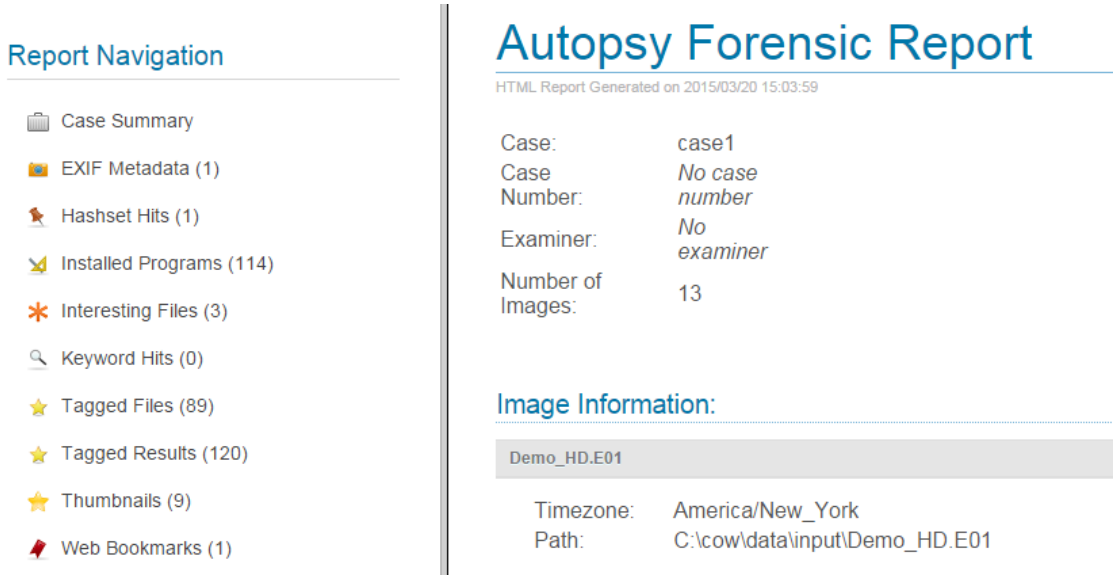


If you select Tagged Results, you can choose the tags you would like included.

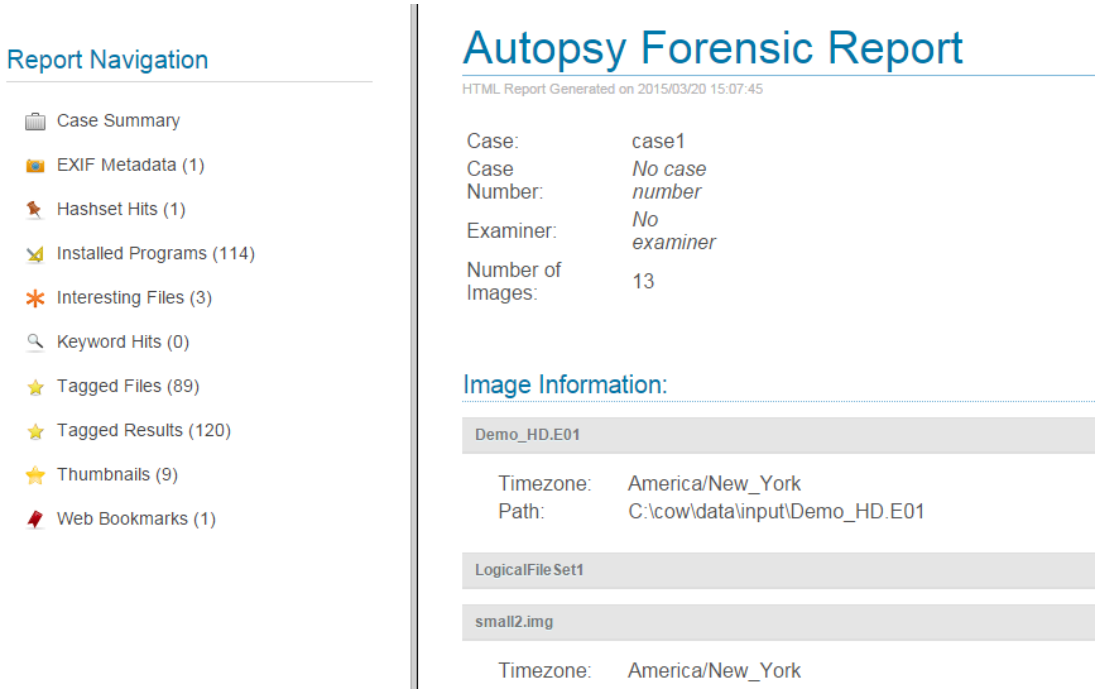


In our case, an HTML report is generated.

All Results HTML Report:



Tagged Results HTML Report:



There are other types of reports to choose, but they operate on the same principle. Select either All Results or Tagged results to include.

Installing 3rd-Party Modules

There are various places in Autopsy that developers can write custom plug-in modules. This page covers how to install them.

There are two types of modules:

- Modules written in Java that are shipped in NBM (NetBeans Module) files.
- Modules written in Python that are shipped as a folder in a ZIP file.

Installing NetBeans Modules

If you have an NBM file, then it may contain one or more Autopsy modules. To install it, use the plugin manager at "Tools", "Plugins".

Choose the "Downloaded" tab and then choose "Add Plugins". Browse to the NBM file. It may require you to restart Autopsy.

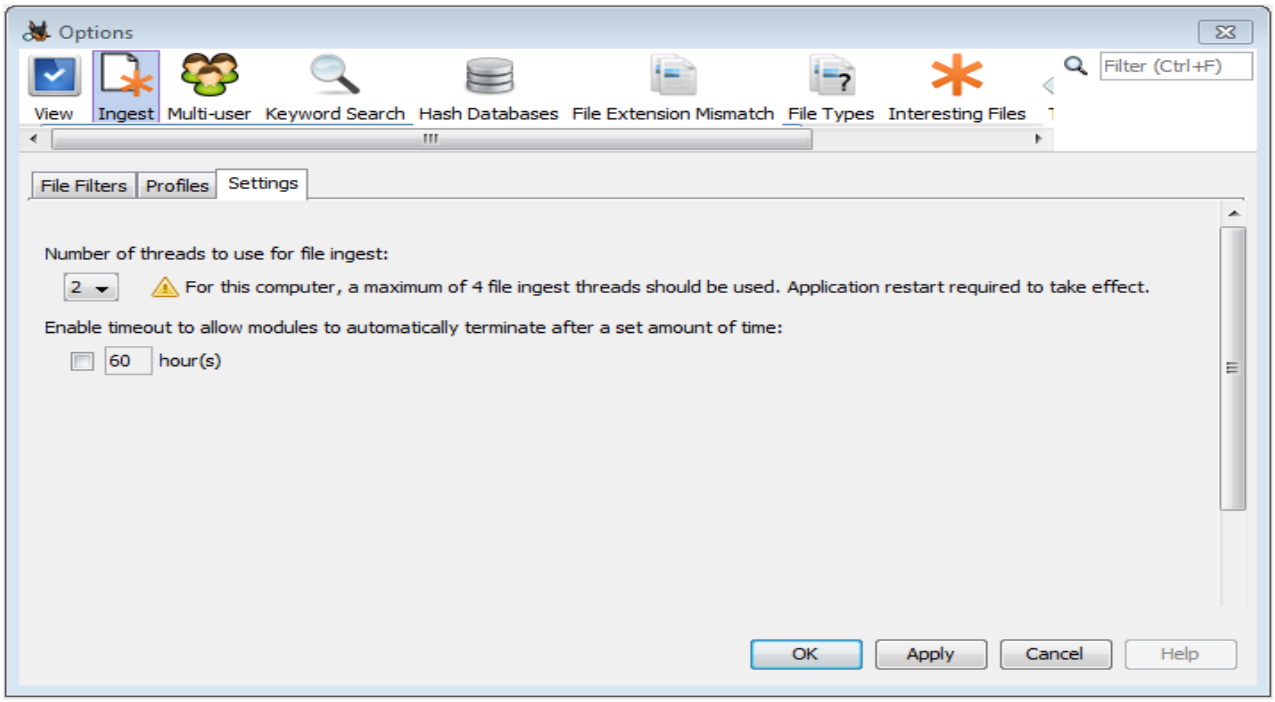
Installing Python Modules

If you have a ZIP file with a Python module in it, then unzip the file and you should get a folder. Open the Python module library folder using "Tools", "Python Plugins". Copy the module folder into there and Autopsy should identify and use it next time it loads modules.

Optimizing Performance

After installing Autopsy, there are several hardware-based things that we suggest you do to optimize performance:

1. Number of Threads: Change the number of parallel pipelines used at run time. The default is two pipelines, but this can be increased if you are running on a system with several cores. To do this:
    - Run Autopsy from the Start Menu or desktop
    - When presented with the case creation splash screen, cancel/close the window
    - Select "Tools", "Options"
    - On the "Ingest" panel on the "Settings" tab, there is a drop down for *Number of threads to use for file ingest*. The maximum value is the same as number of processors on your system (up to four). The number of ingest threads can not be set above four. Testing has revealed that for most systems and setups, after four threads, the machine is I/O bound anyway, and increasing this number beyond four may actually reduce performance.
    - After each change, restart Autopsy to let this setting take effect.



1. When making a case, use different drives to store the case and the images. This allows the maximum amount of data to be read and written at the same time.
2. We have had best performance using either solid state drives or fibre channel-attached SAN storage.

Multi-user Collaborative Deployments

Setting Up Multi-user Environment

Multi-user Installation

Autopsy can be setup to work in an environment where multiple users on different computers can have the same case open at the same time. To set up this type of environment, you will need to configure additional (free and open source) network-based services.

Network-based Services

You will need the following that all Autopsy clients can access:

- Centralized storage that all clients running Autopsy have access to. The central storage should be either mounted at the same Windows drive letter or UNC paths should be used everywhere. All clients need to be able to access data using the same path.

- A central PostgreSQL database. A database will be created for each case and will be stored on the local drive of the database server. Installation and configuration is explained in **Install and Configure PostgreSQL**.
- A central Solr text index. A Solr core will be created for each case and will be stored in the case folder (not on the local drive of the Solr server). We recommend using Bitnami Solr. This is explained in **Install and Configure Solr**.
- An ActiveMQ messaging server to allow the various clients to communicate with each other. This service has minimal storage requirements. This is explained in **Install and Configure ActiveMQ**.

When you setup the above services, write down the addresses, user names, and passwords or each so that you can configure each of the client systems afterwards.

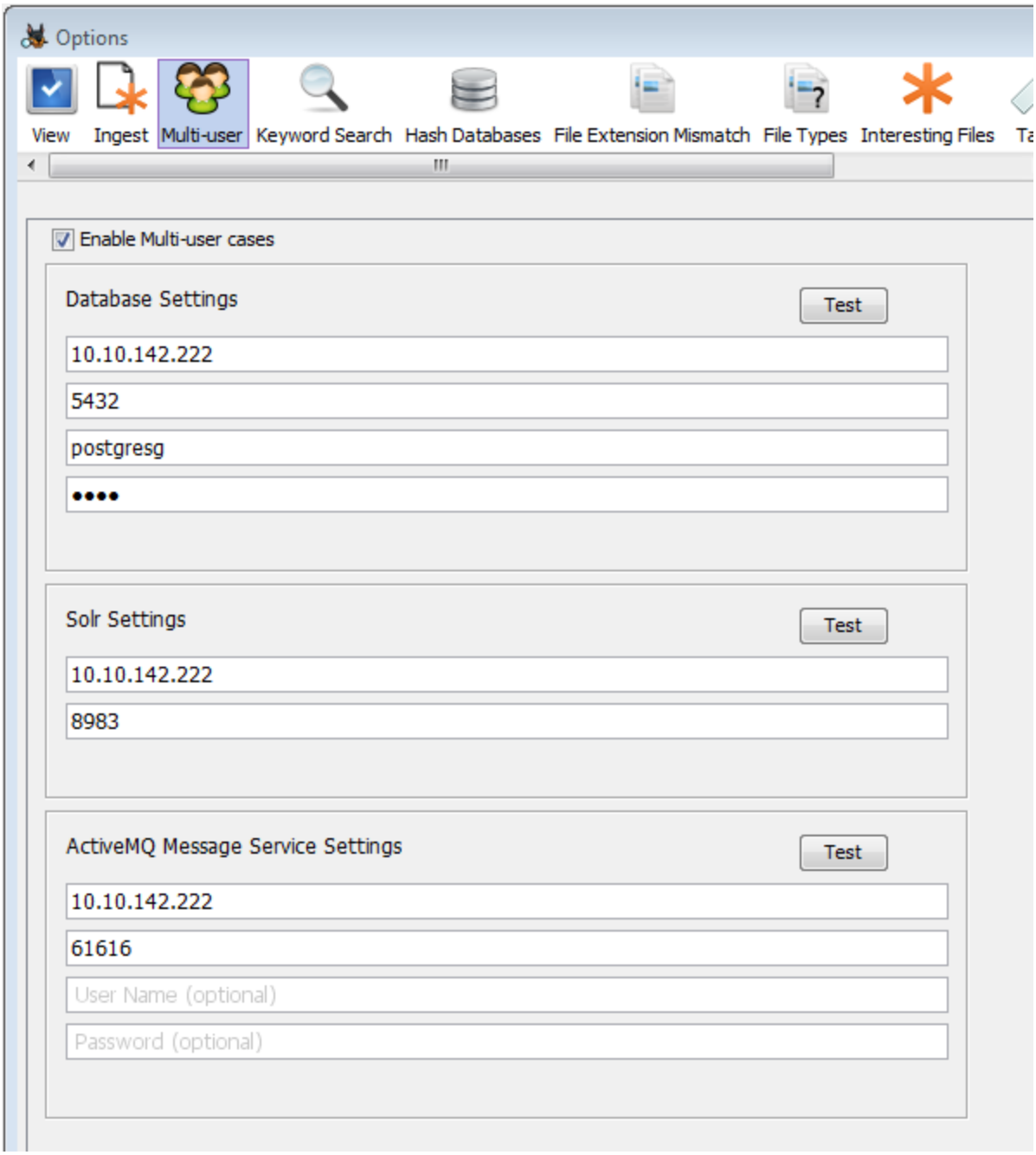
We recommend using at least 2 dedicated computers for this additional infrastructure. Spreading the services out across several machines can improve throughput. If possible, place Solr on a machine by itself, as it is the largest RAM and CPU utilizer among the servers.

Ensure that the central storage and PostgreSQL servers are regularly backed up.

Autopsy Clients

Once the infrastructure is in place, you will need to configure Autopsy to use them.

- Install Autopsy on each client system as normal using the steps from **Installing Autopsy**.
- Start Autopsy and open the multi-user settings panel from "Tools", "Options", "Multi-user". As shown in the screenshot below, you can then enter all of the address and authentication information for the network-based services. Note that in order to create or open Multi-user cases, "Enable Multi-user cases" must be checked and the settings below must be correct.



Install and Configure ActiveMQ

To install ActiveMQ, perform the following steps:

Prerequisites

You will need:

- 64-bit version of the Java Runtime Environment (JRE) from http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html.
- Download ActiveMQ from: http://activemq.apache.org/download.html . Autopsy has been tested with ActiveMQ version 5.14.0.

Installation

JRE Installation

Install the Java JRE if needed. You can test this by running *where java* from the command line. If you see output like the yellow results below, you have a JRE.

```
C:\Program Files\Java\jre1.8.0_111\bin>
```

If you need the JRE, install it with the default settings.

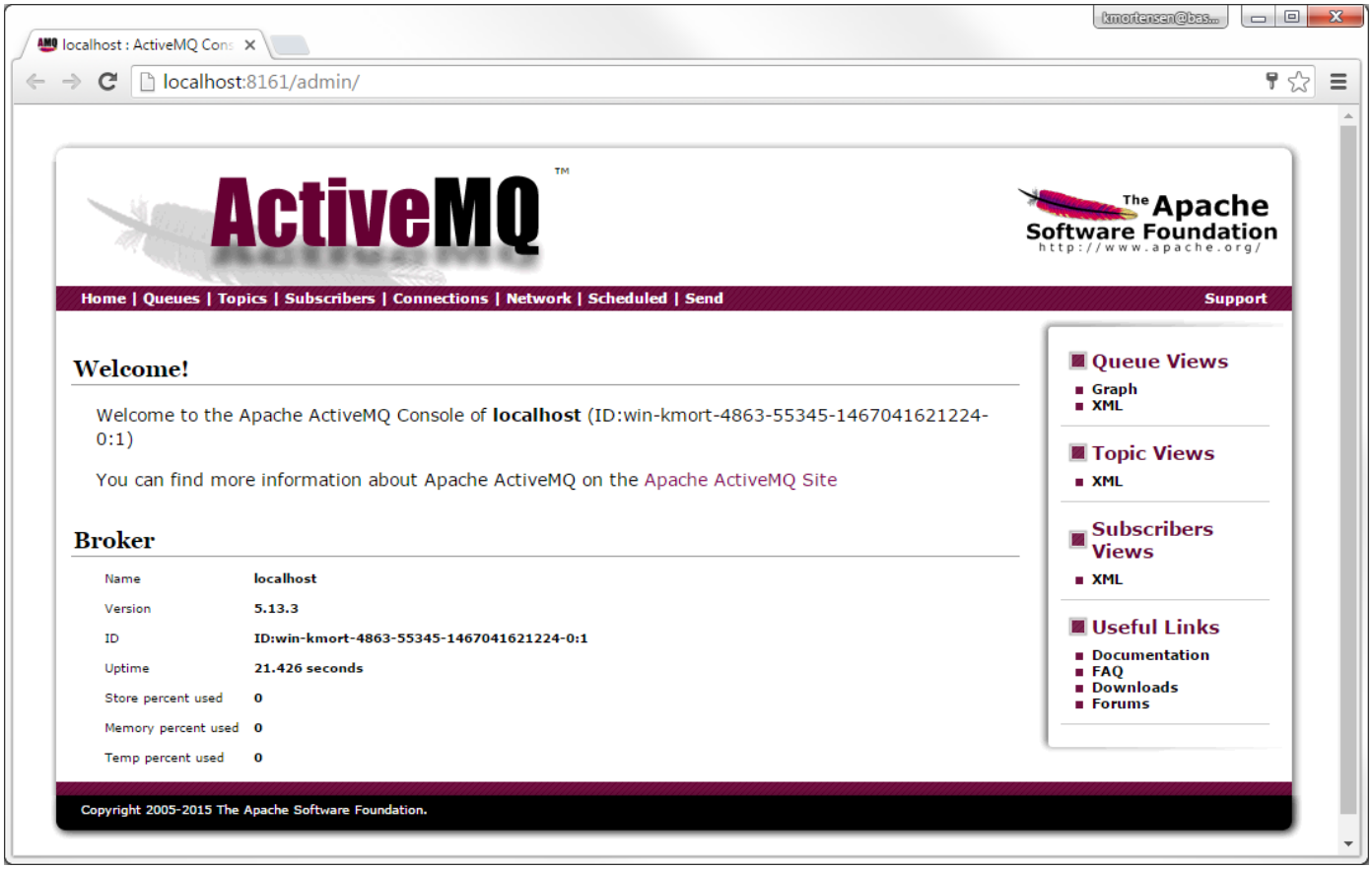
ActiveMQ Installation

1. Extract the contents of the ActiveMQ archive folder to a location of your choice, bearing in mind that the files should be in a location that the running process will have write permissions to the folder. A typical folder choice would be similar to *C:\Program Files\apache-activemq-5.13.3*. Typically, it will ask for administrator permission to move the folder. Allow it if required.
2. Edit the *conf\activemq.xml* in the extracted folder to add *"&wireFormat.maxInactivityDuration=0"* to the URI for the *transportConnector* named *openwire*. Add the text highlighted in yellow below:

```
109         http://activemq.apache.org/configuring-transports.html
110     -->
111     <transportConnectors>
112         <!-- DOS protection, limit concurrent connections to 1000 and frame size to 100MB -->
113         <transportConnector name="openwire" uri="tcp://0.0.0.0:61616?maximumConnections=1000&amp;amp;wireFormat.maxFrameSize=104857600&amp;amp;wireFormat.maxInactivityDuration=0"/>
114         <transportConnector name="amqp" uri="amqp://0.0.0.0:5672?maximumConnections=1000&amp;amp;wireFormat.maxFrameSize=104857600"/>
115         <transportConnector name="stomp" uri="stomp://0.0.0.0:61613?maximumConnections=1000&amp;amp;wireFormat.maxFrameSize=104857600"/>
```

3. Install ActiveMQ as a service by navigating to the folder *bin\win64*, right-clicking *InstallService.bat*, clicking *Run as administrator*, then click *Yes*.
4. Start the ActiveMQ service by pressing *Start*, type *services.msc*, and press *Enter*. Find *ActiveMQ* in the list and press the *Start the service* link.
5. ActiveMQ should now be installed and configured using the default credentials. You should go to the next section to change the default passwords. To test your installation, you can access the admin pages in your web browser via a URL like this (set your

host): http://localhost:8161/admin. The default administrator username is *admin* with a password of *admin* and the default regular username is *user* with a default password of *password*. You can change these passwords by following the instructions below. If you can see a page



that looks like the following, it is ready to function.

If you do not see a screen like the above screenshot and you have double checked that the ActiveMQ service is running, contact your network administrator. For the ActiveMQ service to be accessible by network clients you may need to configure your Windows firewall (and any other 3rd party firewall in use) to allow communication.

Configuring Authentication

You can optionally add authentication to your ActiveMQ server. The ActiveMQ communications are not encrypted and contain basic messages between the systems about when new data has been found.

The following directions allow you to set up credentials:

1. Copy and paste the following text to the file *"conf\groups.properties"*, overwriting the text highlighted in yellow in the screenshot below:

```
admins=system,sslclient,client,broker1,broker2
tempDestinationAdmins=system,user,sslclient,client,broker1,broker2
users=system,user,sslclient,client,broker1,broker2
guests=guest
```

```
10  ##
11  ## Unless required by applicable law or agreed to in writing, software
12  ## distributed under the License is distributed on an "AS IS" BASIS,
13  ## WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
14  ## See the License for the specific language governing permissions and
15  ## limitations under the License.
16  ## -------------------------------------------------------------------------
17
18  admins=admin
```

When complete, the file should look like this:

```
1   ## -------------------------------------------------------------------------
2   ## Licensed to the Apache Software Foundation (ASF) under one or more
3   ## contributor license agreements.  See the NOTICE file distributed with
4   ## this work for additional information regarding copyright ownership.
5   ## The ASF licenses this file to You under the Apache License, Version 2.0
6   ## (the "License"); you may not use this file except in compliance with
7   ## the License.  You may obtain a copy of the License at
8   ##
9   ## http://www.apache.org/licenses/LICENSE-2.0
10  ##
11  ## Unless required by applicable law or agreed to in writing, software
12  ## distributed under the License is distributed on an "AS IS" BASIS,
13  ## WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
14  ## See the License for the specific language governing permissions and
15  ## limitations under the License.
16  ## -------------------------------------------------------------------------
17
18  admins=system,sslclient,client,broker1,broker2
19  tempDestinationAdmins=system,user,sslclient,client,broker1,broker2
20  users=system,user,sslclient,client,broker1,broker2
21  guests=guest

Ln 1 / 21   Col 1 / 80   Sel 0   Sel Ln 0   1.12 KB   ANSI   CR+LF   INS   Configuration Files
```

2. Copy and paste the following text to the file *"conf\users.properties"*, overwriting the text highlighted in yellow in the screenshot below:

```
system=manager
        user=password
        guest=password
        sslclient=CN=localhost, OU=activemq.org, O=activemq.org, L=LA, ST=CA, C=US
```

When complete, the file should look like this:

```
## distributed under the License is distributed on an "AS IS" BASIS,
## WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implie
## See the License for the specific language governing permissions and
## limitations under the License.
## ----------------------------------------------------------------------

admins=system,sslclient,client,broker1,broker2
tempDestinationAdmins=system,user,sslclient,client,broker1,broker2
users=system,user,sslclient,client,broker1,broker2
guests=guest
```

3. Copy and paste the following text to the file *"conf\activemq.xml"*, inserting the text at the line shown in yellow in the screenshot below.

```
4.          <plugins>
5.          <jaasAuthenticationPlugin configuration="activemq-domain" />
6.            <simpleAuthenticationPlugin>
7.              <users>
8.                <authenticationUser username="system" password="manager"
groups="users,admins"/>
9.                <authenticationUser username="user" password="password"
groups="users"/>
10.               <authenticationUser username="guest" password="password"
groups="guests"/>
11.             </users>
```

```
12.              </simpleAuthenticationPlugin>
13.          </plugins>
```

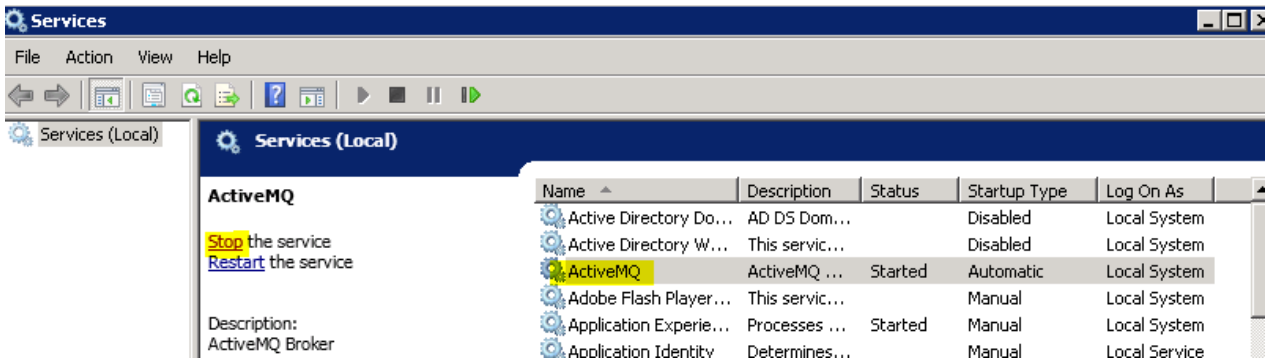
```
<!-- START SNIPPET: example -->
<beans
  xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans
  http://activemq.apache.org/schema/core http://activemq.apache.org/schema/core/activemq-core.xsd">

    <!-- Allows us to use system properties as variables in this configuration file -->
    <bean class="org.springframework.beans.factory.config.PropertyPlaceholderConfigurer">
        <property name="locations">
            <value>file:${activemq.conf}/credentials.properties</value>
        </property>
    </bean>

   <!-- Allows accessing the server log -->
    <bean id="logQuery" class="io.fabric8.insight.log.log4j.Log4jLogQuery"
          lazy-init="false" scope="singleton"
          init-method="start" destroy-method="stop">
    </bean>

    <!--
        The <broker> element is used to configure the ActiveMQ broker.
    -->
    <broker xmlns="http://activemq.apache.org/schema/core" brokerName="localhost" dataDirectory="${activemq.data}">

        <destinationPolicy>
            <policyMap>
              <policyEntries>
```

After insertion, the file should look like the screenshot below, with the inserted portion highlighted in yellow. This is where you can change the username and password for your ActiveMQ setup.

```
<!-- START SNIPPET: example -->
<beans
  xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-bea
  http://activemq.apache.org/schema/core http://activemq.apache.org/schema/core/activemq-core.xsd">

    <!-- Allows us to use system properties as variables in this configuration file -->
    <bean class="org.springframework.beans.factory.config.PropertyPlaceholderConfigurer">
        <property name="locations">
            <value>file:${activemq.conf}/credentials.properties</value>
        </property>
    </bean>

   <!-- Allows accessing the server log -->
    <bean id="logQuery" class="io.fabric8.insight.log.log4j.Log4jLogQuery"
          lazy-init="false" scope="singleton"
          init-method="start" destroy-method="stop">
    </bean>

    <!--
        The <broker> element is used to configure the ActiveMQ broker.
    -->
    <broker xmlns="http://activemq.apache.org/schema/core" brokerName="localhost" dataDirectory="${activemq.data}">
      <plugins>
      <jaasAuthenticationPlugin configuration="activemq" />
        <simpleAuthenticationPlugin>
            <users>
                <authenticationUser username="system" password="manager" groups="users,admins"/>
                <authenticationUser username="user" password="password" groups="users"/>
                <authenticationUser username="guest" password="password" groups="guests"/>
            </users>
        </simpleAuthenticationPlugin>
      </plugins>

        <destinationPolicy>
            <policyMap>
```

To add a new user or change the password:

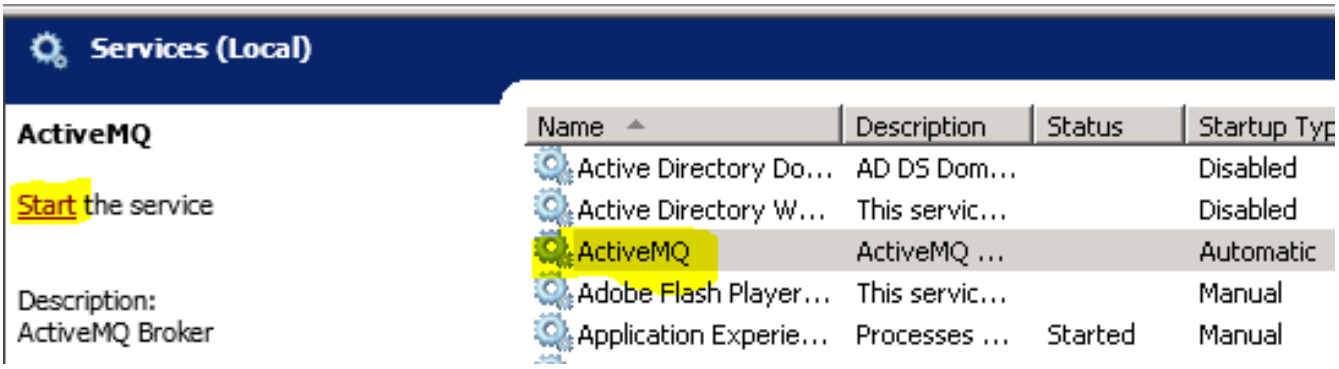
1. Stop the ActiveMQ service by pressing *Start*, type *services.msc*, and press *Enter*. Find *ActiveMQ* in the list and press the *Stop the service* link.



2. Edit *"conf\activemq.xml"* adding the desired line. Both *username* and *password* are case sensitive. You will very likely want to keep your new users in the *users* group.

```
<broker xmlns="http://activemq.apache.org/schema/core" brokerName="localhost" dataDirectory="${activemq.data}"
    <plugins>
    <jaasAuthenticationPlugin configuration="activemq" />
        <simpleAuthenticationPlugin>
            <users>
                <authenticationUser username="system" password="manager" groups="users,admins"/>
                <authenticationUser username="user" password="password" groups="users"/>
                <authenticationUser username="Autopsy" password="yspotuA" groups="users"/>
                <authenticationUser username="guest" password="password" groups="guests"/>
            </users>
        </simpleAuthenticationPlugin>
    </plugins>
```

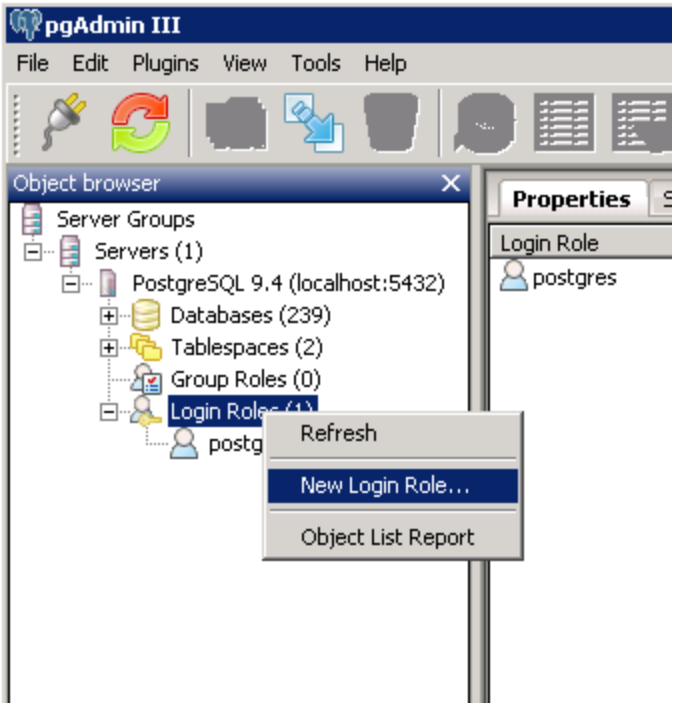
3. Start the ActiveMQ service by pressing *Start*, type *services.msc*, and press *Enter*. Find *ActiveMQ* in the list and press the *Start the service* link.



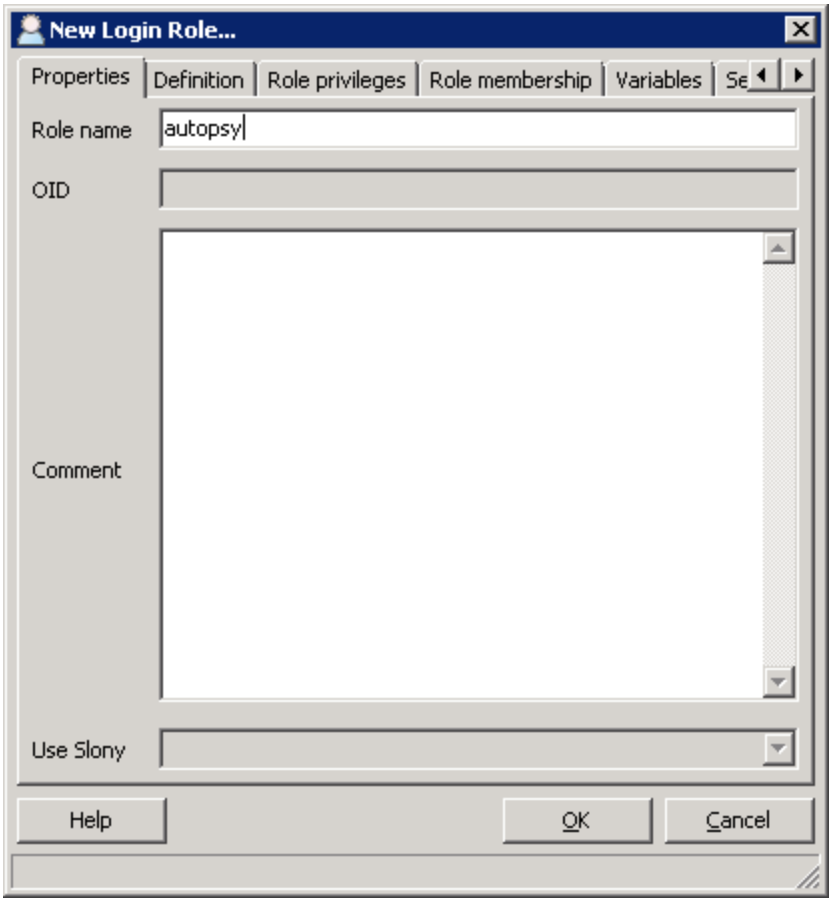
Install and Configure PostgreSQL

To install PostgreSQL, perform the following steps:

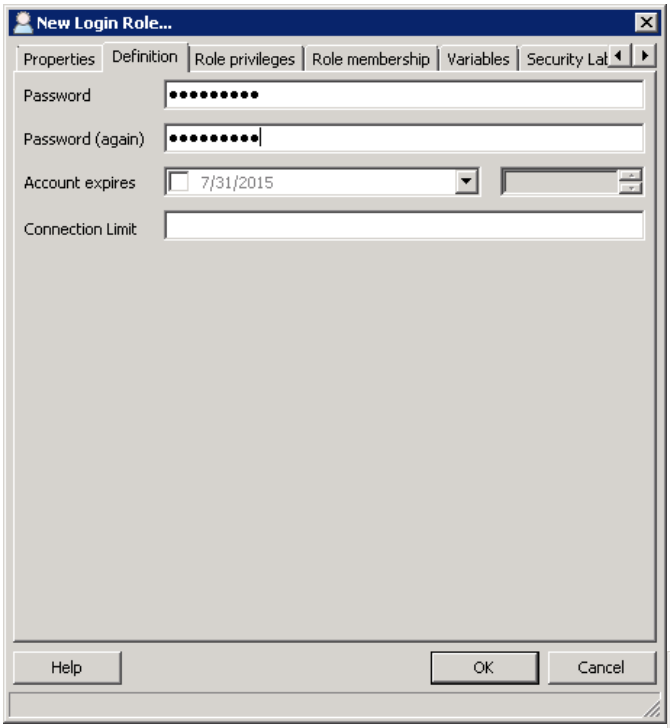
1. Download a 64-bit PostgreSQL installer from http://www.enterprisedb.com/products-services-training/pgdownload#windows Choose the one that says *Win X86-64*. Autopsy has been tested with PostgreSQL version 9.5.
2. Run the installer. The name will be similar to *postgresql-9.5.3-1-windows-x64.exe*.
3. You may accept defaults for all items except for the password as you work through the wizard. Do not lose the password you enter in. This is the PostgreSQL administrator login password.
4. You do not need to launch the StackBuilder nor acquire any more software from it. Uncheck the option to use StackBuilder and press *Finish*.



5. Create a regular user account to use while running Autopsy. You can do this with either of two methods, graphically, or command line. We cover graphically first.
   - Graphically:
     - Using the PostgreSQL administrator login and the pgAdmin III tool, create a regular user account to use while running Autopsy.
     - Right click on *"Login Roles"* and select *"New Login Role..."* as shown below:



     - Enter the user name you would like to use in the *"Role name"* field.
     - Enter the password on the *"Definition"* tab.

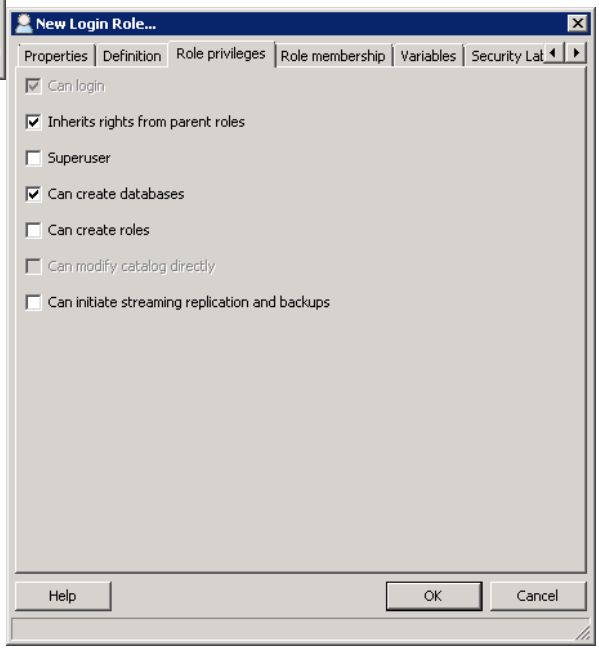


- Check *"Can create databases"* on the *"Role Privileges"* tab.

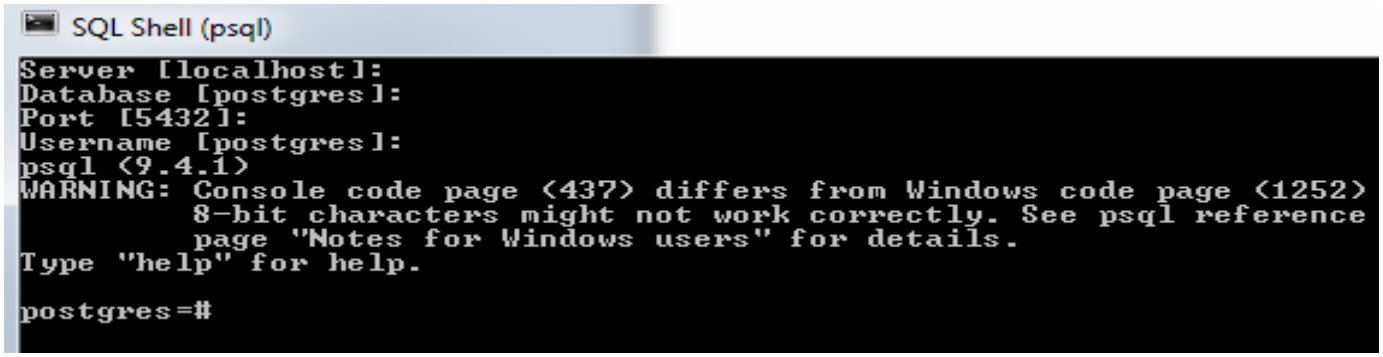
- Click *"OK"*.

- Command line:

Use the *psql* tool. To start *psql*, press *Start*, type *psql*, and press *Enter* a few times until it prompts you for a password. Type in the password you gave it when installing PostgreSQL. You should see a prompt that looks like the screenshot below.



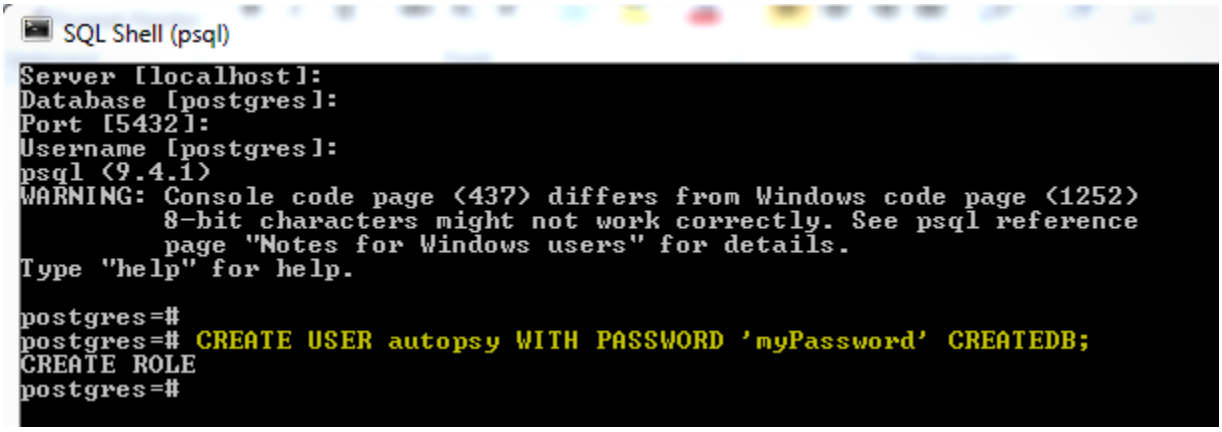
If you want your user account name to be *"Autopsy"* and your password to be *"myPassword"*, use the following command to create a new user, noting that the password is enclosed in single quotes, **not backticks nor double quotes**. Also note that it is important to type this command in from the keyboard directly, as copying and pasting can sometimes yield different characters for single quotes that can confuse *psql*.



The command is:

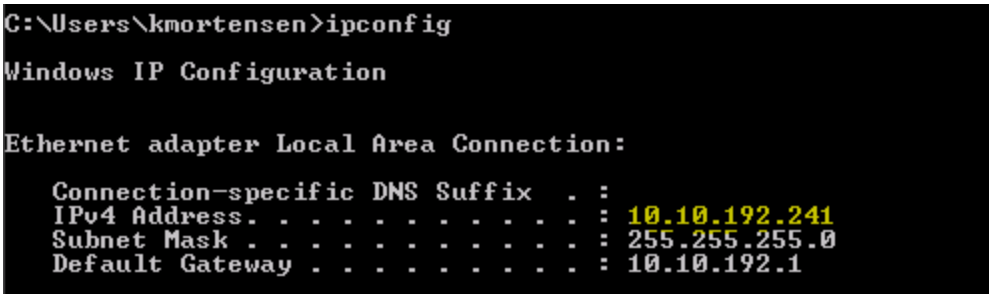
```
CREATE USER Autopsy WITH PASSWORD 'myPassword' CREATEDB;
```

When you see the *CREATE ROLE* output as shown in the screenshot below, the new user has been created. You can close the *psql* window now.



6.Edit *C:\Program Files\PostgreSQL\9.5\data\pg_hba.conf* to add an entry to allow external computers to connect via the network.

First, find your machine's IPv4 address and Subnet Mask (Press *Start*, type *cmd*, type *ipconfig* and parse the results. The IP address is shown in yellow below.



The following is an example rule that allows all clients on the 10.10.192.x subnet to connect using md5 authentication.

```
host    all    all    10.10.192.0/24    md5
```

Subnet Mask Rules of thumb:

- If your Subnet Mask is 255.255.0.0, your rule should look like this: A.B.0.0/16, where A is the first octet in your IP address and B is the second octet.

- If your Subnet Mask is 255.255.255.0, your rule should look like this: A.B.C.0/24, where A is the first octet in your IP address, B is the second octet, and C is the third octet.

Add the line highlighted in yellow below, formatted with spaces between the entries, adjusting the IP address to an appropriate value as described above.

```
77  # TYPE  DATABASE        USER            ADDRESS                 METHOD
78
79  # IPv4 local connections:
80  host    all             all             127.0.0.1/32            md5
81  # IPv6 local connections:
82  host    all             all             ::1/128                 md5
83  # Allow replication connections from localhost, by a user with the
84  # replication privilege.
85  #host    replication     postgres        127.0.0.1/32            md5
86  #host    replication     postgres        ::1/128                 md5
87  host     all             all             10.10.192.0/24          md5
```

If you intend to use PostgreSQL from machines on a different subnet, you need an entry in the *pg_hba.conf* file for each subnet.

7. Uncomment the following entires in the configuration file located at *C:\Program Files\PostgreSQL\9.5\data\postgresql.conf* by removing the leading "#", and change their values *"off"* as shown below.

```
fsync                           =               off
synchronous_commit                      =       off
full_page_writes = off
```

Pictorially, change the following, from this:

```
#fsync = on              # turns forced synchronization on or off
#synchronous_commit = on        # synchronization level;
                        # off, local, remote_write, or on
#wal_sync_method = fsync        # the default is the first option
                        # supported by the operating system:
                        #   open_datasync
                        #   fdatasync (default on Linux)
                        #   fsync
                        #   fsync_writethrough
                        #   open_sync
#full_page_writes = on          # recover from partial page writes
```

To this:

```
fsync = off             # turns forced synchronization on or off
synchronous_commit = off        # synchronization level;
                    # off, local, remote_write, or on
#wal_sync_method = fsync        # the default is the first option
                    # supported by the operating system:
                    #   open_datasync
                    #   fdatasync (default on Linux)
                    #   fsync
                    #   fsync_writethrough
                    #   open_sync
full_page_writes = off          # recover from partial page writes
```

Note the removal of the leading number symbol-this uncomments that entry.

8. Still in *"C:\Program Files\PostgreSQL\9.5\data\postgresql.conf"*, find the entry named *max_connections*and set it to the number of suggested connections for your configuration. A rule of thumb is add 100 connections for each Automated Ingest Node and 100 connections for each Reviewer node you plan to have in the network. More information is available at 5.1.1. See the screenshot below.

Install and Configure Solr

A central Solr server is needed to store keyword indexes, and its embedded Zookeeper is used as a coordination service for Autopsy. To install Solr, perform the following steps:

Prerequisites

You will need:

- 64-bit version of the Java Runtime Environment (JRE) from http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html.
- Download the Apache Solr 4.10.3-0 installation package from https://sourceforge.net/projects/autopsy/files/CollaborativeServices/Solr or Direct Download Link
- Access to an installed version of Autopsy so that you can copy files from it.
- A network-accessible machine to install Solr upon. Note that the Solr process will need to write data out to the main shared storage drive, and needs adequate permissions to write to this location, which may be across a network.

Installation

JRE Installation

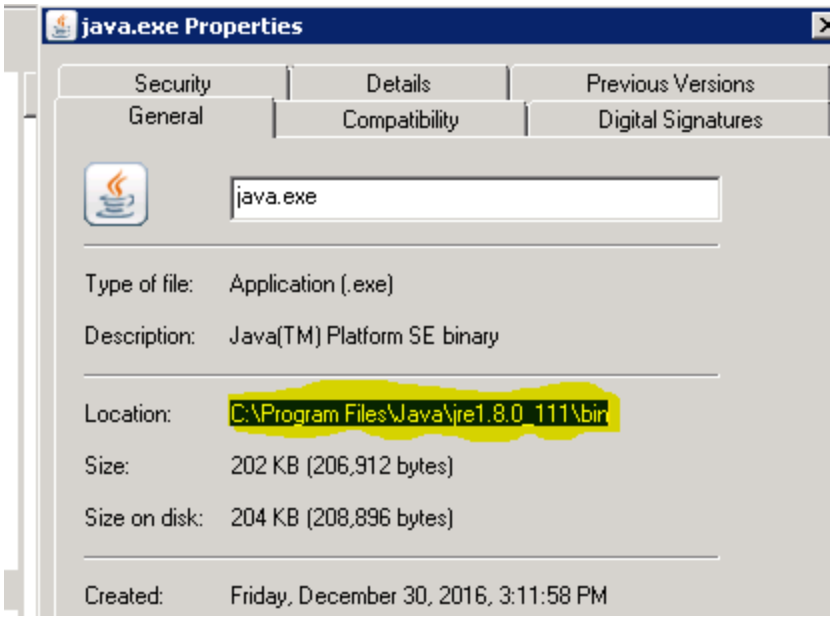
1. Install the Java JRE if needed. You can test this by running *where java* from the command line. If you see output like the yellow results below, you have a JRE.

If you need the JRE, install it with the default settings.

2. Create a Windows environment variable for your *JavaHome* with the path to your 64-bit version of the JRE. If you do not know the path, the correct *JavaHome* path can be obtained by running the command *where java* from the Windows command line. An example is shown below. Do not include the *"bin"* folder in the path you place into the *JavaHome* variable. A correct example of the final result will look something like this: *JavaHome="C:\Program Files\Java\jre1.8.0_111"*

Note that if you get something like the following when running the *"where java"* command, it is a symbolic link to the Java installation and you need to trace it to the proper folder as explained below.

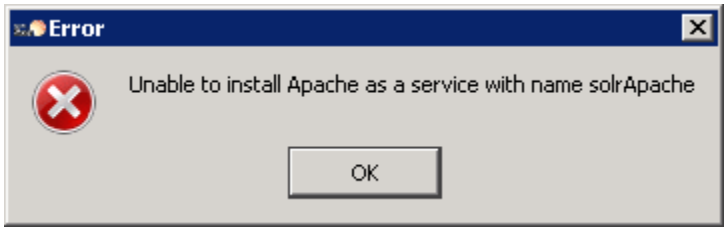
To trace a symbolic link to the proper folder, use Windows Explorer to navigate to the path shown (*C:\ProgramData\Oracle\Java\javapath* for the example above), then right click on *java.exe* and Click on *Properties*. You will see the path you should use in the *Location* field, shown in the screenshot below. Do not include the *"bin"* folder in the path you place into the *JavaHome* variable.



Solr Installation

The following steps will configure Solr to run using an account that will have access to the network storage.

1. Run the Bitnami installer, *"bitnami-solr-4.10.3-0-windows-installer.exe"*
2. If Windows prompts with User Account Control, click *Yes*
3. Follow the prompts through to completion. You do not need to *"Learn more about Bitnami cloud hosting"*so you can clear the check box.
4. If you see an error dialog like the following, you may safely ignore it.



5. When the installation completes, clear the *"Launch Bitnami Apache Solr Stack Now?"* checkbox and click *Finish*.

Solr Configuration

1. Stop the *solrJetty* service by pressing *Start*, typing *services.msc*, pressing *Enter*, and locating the *solrJetty* Windows service. Select the service and press *Stop the service*. If the service is already stopped and there is no *Stop the service* available, this is okay.

2. Edit the *"C:\Bitnami\solr-4.10.3-0\apache-solr\scripts\serviceinstall.bat"* script. You need administrator permission to change this file. The easiest way around this is to save a copy on the Desktop, edit the Desktop version, and copy the new one back over the top of the old. Windows will ask for permission to overwrite the old file; allow it. You should make the following changes to this file:

    - Add the following options in the line that begins with *"C:\Bitnami\solr-4.10.3-0/apache-solr\scripts\prunsrv.exe"* :
    - *++JvmOptions=-Dcollection.configName=AutopsyConfig*
    - *++JvmOptions=-Dbootstrap_confdir="C:\Bitnami\solr-4.10.3-0\apache-solr\solr\configsets\AutopsyConfig\conf"*
    - *++JvmOptions=-DzkRun*
    - Replace the path to JavaHome with the path to your 64-bit version of the JRE. If you do not know the path, the correct JavaHome path can be obtained by running the command "where java" from the Windows command line. An example is shown below.

```
"C:\Bitnami\solr-4.10.3-0/apache-solr\scripts\prunsrv.exe" //IS//solrJetty --DisplayName="solrJetty" --Install=
"C:\Bitnami\solr-4.10.3-0/apache-solr\scripts\prunsrv.exe" --LogPath="C:\Bitnami\solr-4.10.3-0/apache-solr\logs" --LogLevel=
Debug --StdOutput=auto --StdError=auto --StartMode=Java --StopMode=Java --Jvm=auto ++JvmOptions=-DSTOP.PORT=8079 ++JvmOptions=
-DSTOP.KEY=s3crEt ++JvmOptions=-Djetty.home="C:\Bitnami\solr-4.10.3-0/apache-solr" ++JvmOptions=-Dsolr.solr.home=
"C:\Bitnami\solr-4.10.3-0/apache-solr/solr" --Jvm=auto ++JvmOptions=-Djetty.logs="C:\Bitnami\solr-4.10.3-0/apache-solr\logs"
--JavaHome="C:\Program Files\Java\jre1.8.0_111" ++JvmOptions=-DzkRun ++JvmOptions=-Dcollection.configName=AutopsyConfig ++
JvmOptions=-Dbootstrap_confdir="C:\Bitnami\solr-4.10.3-0\apache-solr\solr\configsets\AutopsyConfig\conf" ++JvmOptions=
-XX:MaxPermSize=128M --Classpath="C:\Bitnami\solr-4.10.3-0/apache-solr\lib\*";"C:\Bitnami\solr-4.10.3-0/apache-solr\start.jar"
--StartClass=org.eclipse.jetty.start.Main ++StartParams="C:\Bitnami\solr-4.10.3-0/apache-solr\etc\jetty.xml" --StopClass=
org.eclipse.jetty.start.Main ++StopParams=--stop ++StopParams=-DSTOP.PORT=8079 ++StopParams=-DSTOP.KEY=s3crEt --Startup=auto

net start solrJetty >NUL
```

    The text in yellow is what we are interested in. Do not include the "bin" folder in the path you place into the JavaHome variable. A correct example of the final result will look something like this: *–-JavaHome="C:\Program Files\Java\jre1.8.0_111"*

    A portion of an updated *serviceinstall.bat* is shown below, with the changes marked in yellow.

3. Edit *"C:\Bitnami\solr-4.10.3-0\apache-solr\solr\solr.xml"* to set the *transientCacheSize* to the maximum number of cases expected to be open concurrently. If you expect ten concurrent cases, the text to add is *<int name="transientCacheSize">10</int>*

    The added part is highlighted in yellow below. Ensure that it is inside the *<solr>* tag as follows:

```
28
29 <solr>
30 <int name="transientCacheSize">10</int>
31   <solrcloud>
32     <str name="host">${host:}</str>
33     <int name="hostPort">${jetty.port:8983}</int>
34     <str name="hostContext">${hostContext:solr}</str>
35     <int name="zkClientTimeout">${zkClientTimeout:30000}</int>
36     <bool name="genericCoreNodeNames">${genericCoreNodeNames:true}</bool>
37   </solrcloud>
```

4. Edit *"C:\Bitnami\solr-4.10.3-0\apache-solr\resources/log4j.properties"* to configure Solr log settings:
   - Increase the log rotation size threshold (*log4j.appender.file.MaxFileSize*) from 4MB to 100MB.
   - Remove the *CONSOLE* appender from the *log4j.rootLogger* line.

   The log file should end up looking like this (modified lines are highlighted in yellow

```
# Logging level
solr.log=logs/
log4j.rootLogger=INFO, file

log4j.appender.CONSOLE=org.apache.log4j.ConsoleAppender

log4j.appender.CONSOLE.layout=org.apache.log4j.PatternLayout
log4j.appender.CONSOLE.layout.ConversionPattern=%-4r [%t] %-5p %c %x \u2013 %m%n

#- size rotation with log cleanup.
log4j.appender.file=org.apache.log4j.RollingFileAppender
log4j.appender.file.MaxFileSize=100MB
log4j.appender.file.MaxBackupIndex=9

#- File to log to and log format
log4j.appender.file.File=${solr.log}/solr.log
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%-5p - %d{yyyy-MM-dd HH:mm:ss.SSS}; %C; %m\n

log4j.logger.org.apache.zookeeper=WARN
log4j.logger.org.apache.hadoop=WARN

# set to INFO to enable infostream log messages
log4j.logger.org.apache.solr.update.LoggingInfoStream=OFF
```

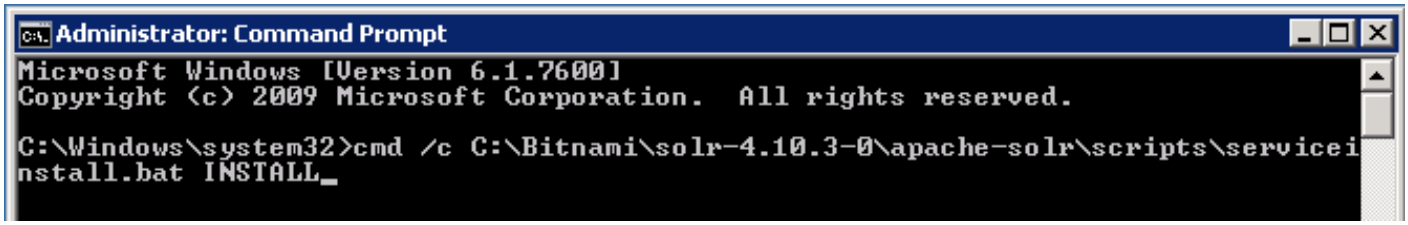
5. From an Autopsy installation, copy the folder *"C:\Program Files\Autopsy-XXX(current version)\autopsy\solr\solr\configsets"* to *"C:\Bitnami\solr-4.10.3-0\apache-solr\solr"*.
6. From an Autopsy installation, copy the folder *"C:\Program Files\Autopsy-XXX(current version)\autopsy\solr\solr\lib"* to *"C:\Bitnami\solr-4.10.3-0\apache-solr\solr"*.
7. From an Autopsy installation, copy the file *"C:\Program Files\Autopsy-XXX(current version)\autopsy\solr\solr\zoo.cfg"* to *"C:\Bitnami\solr-4.10.3-0\apache-solr\solr"*.
8. Stop the *solrJetty* service by pressing *Start*, typing *services.msc*, pressing Enter, and locating the *solrJetty* Windows service. Select the service and press *Stop the service*. If the service is already stopped and there is no *Stop the service* available, this is okay.
9. Start a Windows command prompt as administrator by pressing Start, typing *command*, right clicking on *Command Prompt*, and clicking on *Run as administrator*. Then run the following command to uninstall the solrJetty service:

10. cmd /c C:\Bitnami\solr-4.10.3-0\apache-solr\scripts\serviceinstall.bat UNINSTALL
11.
12. You will very likely see a result that says "The solrJetty service is not started." This is okay.

13. Start a Windows command prompt as administrator by pressing Start, typing *command*, right clicking on *Command Prompt*, and clicking on *Run as administrator*. Then run the following command to install the solrJetty service:

14. cmd /c C:\Bitnami\solr-4.10.3-0\apache-solr\scripts\serviceinstall.bat INSTALL

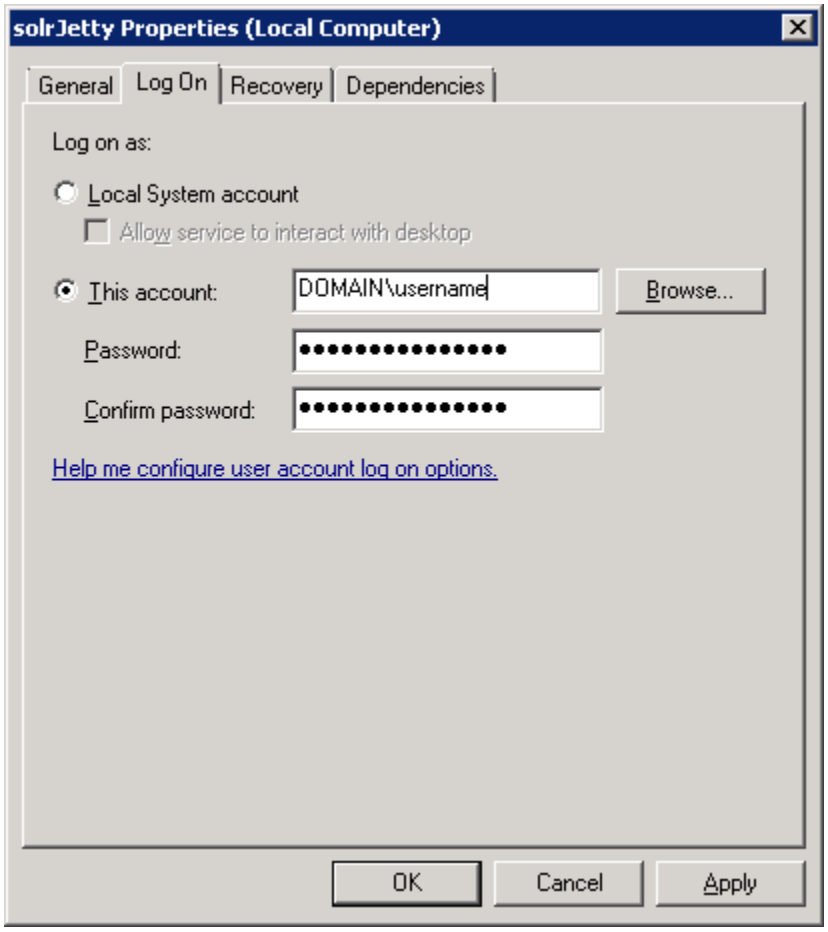
Note the argument "INSTALL" is case sensitive. Your command prompt should look like the screenshot below. Very likely your command prompt will say "The solrJetty service could not be started." This is okay.



Start Solr

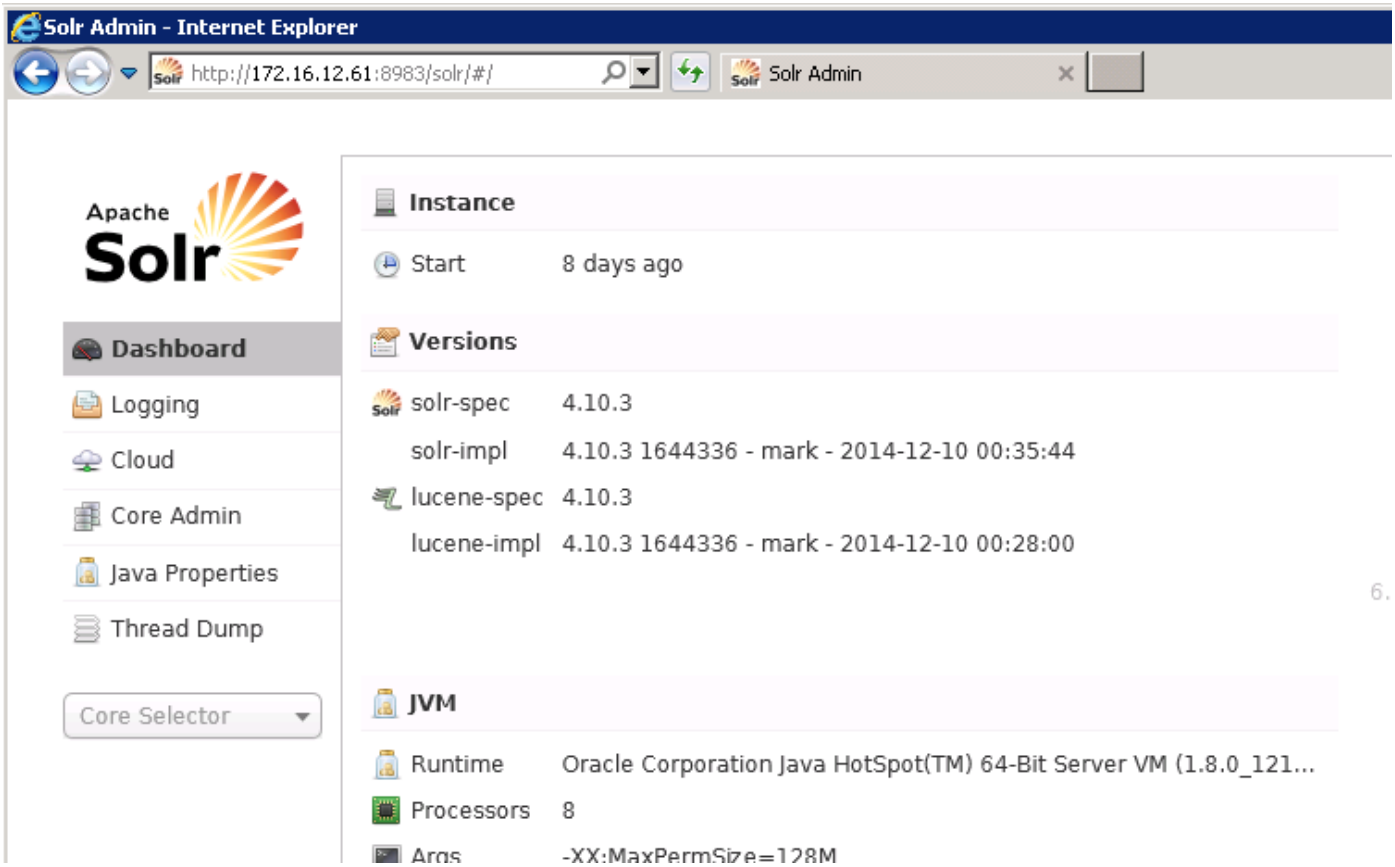
1. You should be able to see the Solr service in a web browser via the URL http://localhost:8983/solr/#/ as shown in the screenshot below. If you can, you should skip the next step. If you cannot, proceed to the next step.
2. Press *Start*, type *services.msc*, and press *Enter*. Find *solrJetty*. If the service is running, press *Stop the service*, then double click it, and switch to the *Log On* tab to change the logon credentials to a user who will have access to read and write the primary shared drive. Note that

selecting "Local System account" will work only if Solr service and case output folders are on the same machine. Using "Local System account" to run Solr service and having case output folders on a different machine will result in Solr being unable to create index files. If the machine is on a domain, the Account Name will be in the form of *DOMAIN-NAME\username* as shown in the example below. Note that in the screenshot below, the domain name is *DOMAIN* and the user name is *username*. These are just examples, not real values.



If the machine is on a domain, **make sure** to select the domain with the mouse by going to the *Log On*tab, clicking *Browse*, then clicking *Locations* and selecting the domain of interest. Then enter the user name desired and press *Check Names*. When that completes, press *OK*, type in the password once for each box and press *OK*. You may see "The user has been granted the log on as a service right."

3. You should be able to see the Solr service in a web browser via the URL *http://localhost:8983/solr/#/* as shown in the screenshot below.



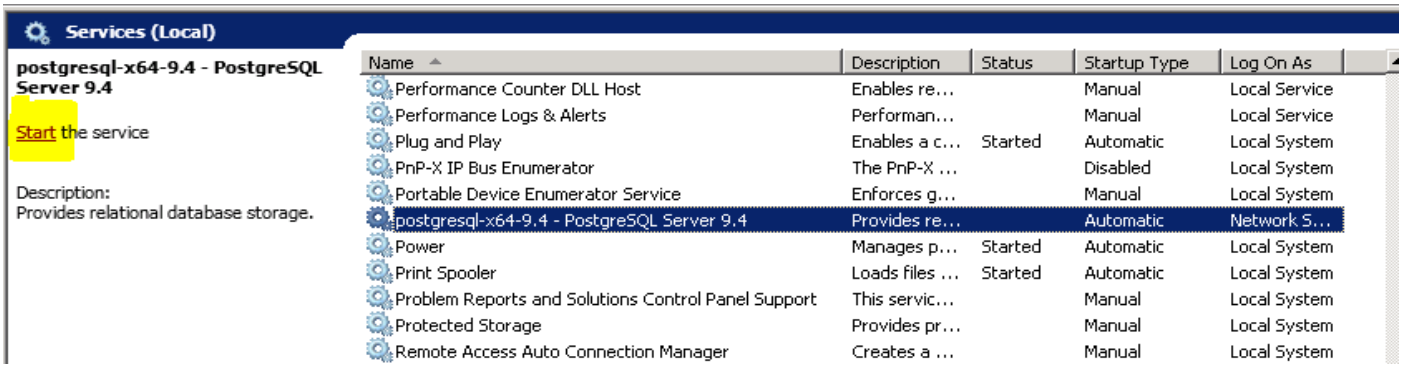
6.

```
53  #------------------------------------------------------------------------------
54  # CONNECTIONS AND AUTHENTICATION
55  #------------------------------------------------------------------------------
56
57  # - Connection Settings -
58
59  listen_addresses = '*'      # what IP address(es) to listen on;
60                      # comma-separated list of addresses;
61                      # defaults to 'localhost'; use '*' for all
62                      # (change requires restart)
63  port = 5432             # (change requires restart)
64  max_connections = 100           # (change requires restart)
65  # Note:  Increasing max_connections costs ~400 bytes of shared memory per
66  # connection slot, plus lock space (see max_locks_per_transaction).
67  #superuser_reserved_connections = 3 # (change requires restart)
```

If the service is appropriately started and you are unable to see the screenshot above, contact your network administrator to open ports in the firewall.

Warning: The Solr process must have adequate permissions to write data to the main shared storage drive where case output will be stored.

9. Press *Start*, type *services.msc*, and press *Enter*. Select *postgresql-x64-9.5* in the services list and click the link that says *Stop the service* then click the link that says *Start the service* as shown in the screenshot below.



PostgreSQL should now be up and running. You can verify by using either the *pgAdmin* tool or the *psql*tool to connect to the database server from another machine on the network .

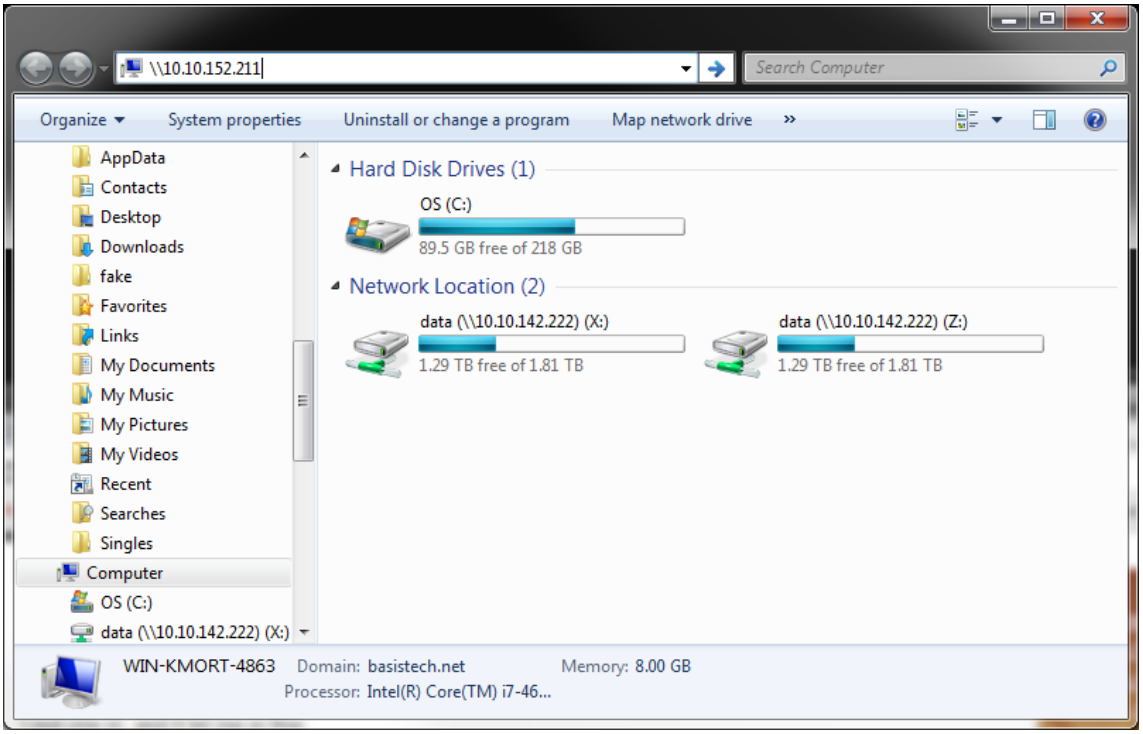
Shared Drive Authentication

If your shared drive is a Windows-hosted shared drive, you will likely need to provide authentication for each machine that connects to the shared drive. This guide only covers Windows-hosted shared drives.

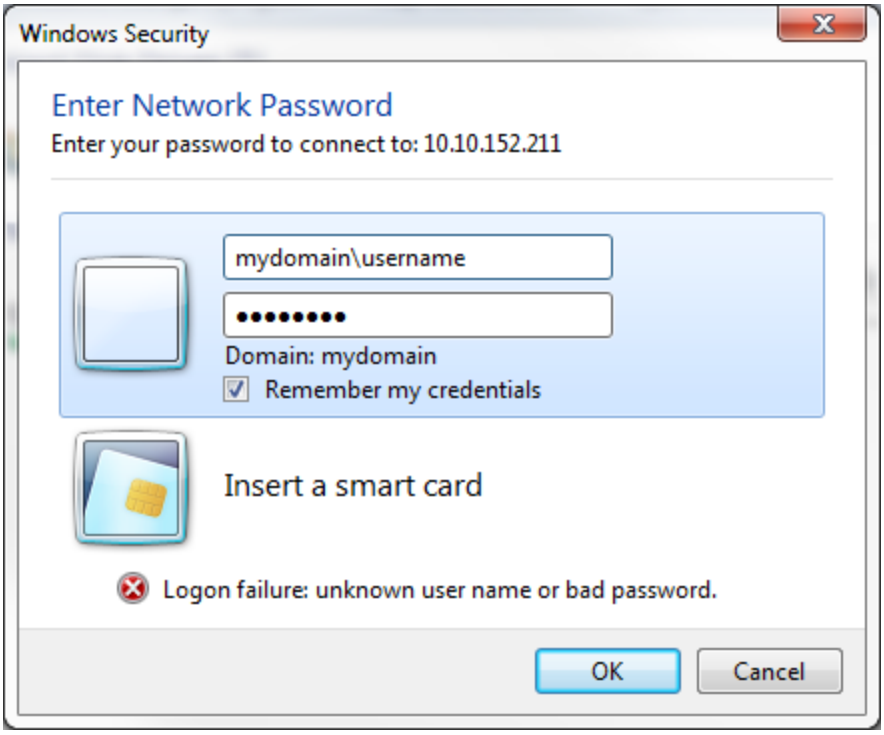
To authenticate with Windows and allow access to a shared drive, you will need:

- A username
- A password
- The domain name (if the machine hosting the shared drive is on a domain)
- The IP address of the machine hosting the shared drive
- The hostname of the machine hosting the shared drive

Using Windows Explorer, in the address bar enter two slashes "\\" followed by the storage machine's IP address and press *Enter*. An example is shown below with the text "\\10.10.152.211" entered.

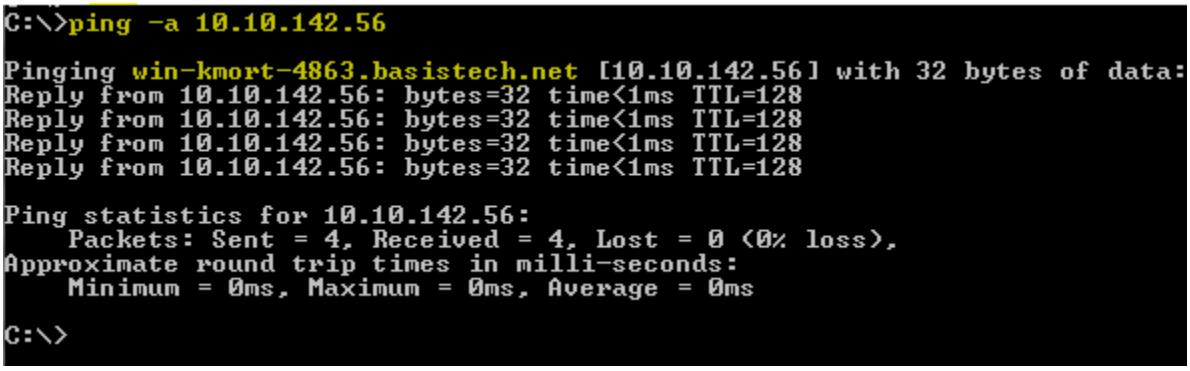


You will see a dialog similar to the following, asking for your credentials.

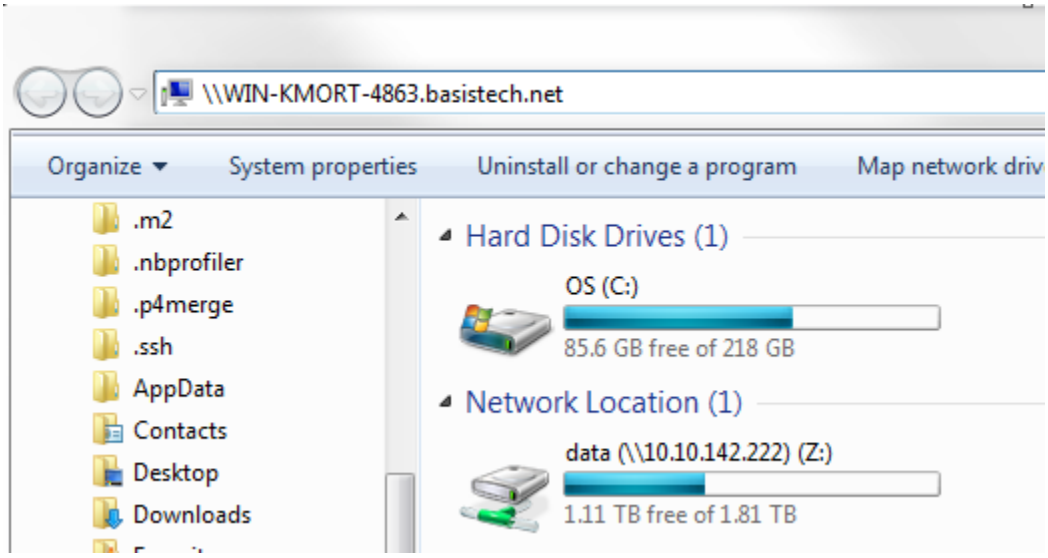


If you have a domain name, add it in the top box before the "\". Follow the slash with your username. If you have no domain name, just use your username with no slashes. Add your password in the next box down and place a check mark in *"Remember my credentials"*, then click *"OK"*.

Next, we will do the same steps over again, using the hostname of the machine. This is necessary to authenticate with both IP address access and hostname access. If you do not know the hostname, you may find it by pinging the IP address with the *"-a"* flag set. It will look something like the screenshot below, where we find the hostname associated with the IP address *10.10.142.56* is *win-kmort-4863.basistech.net*.



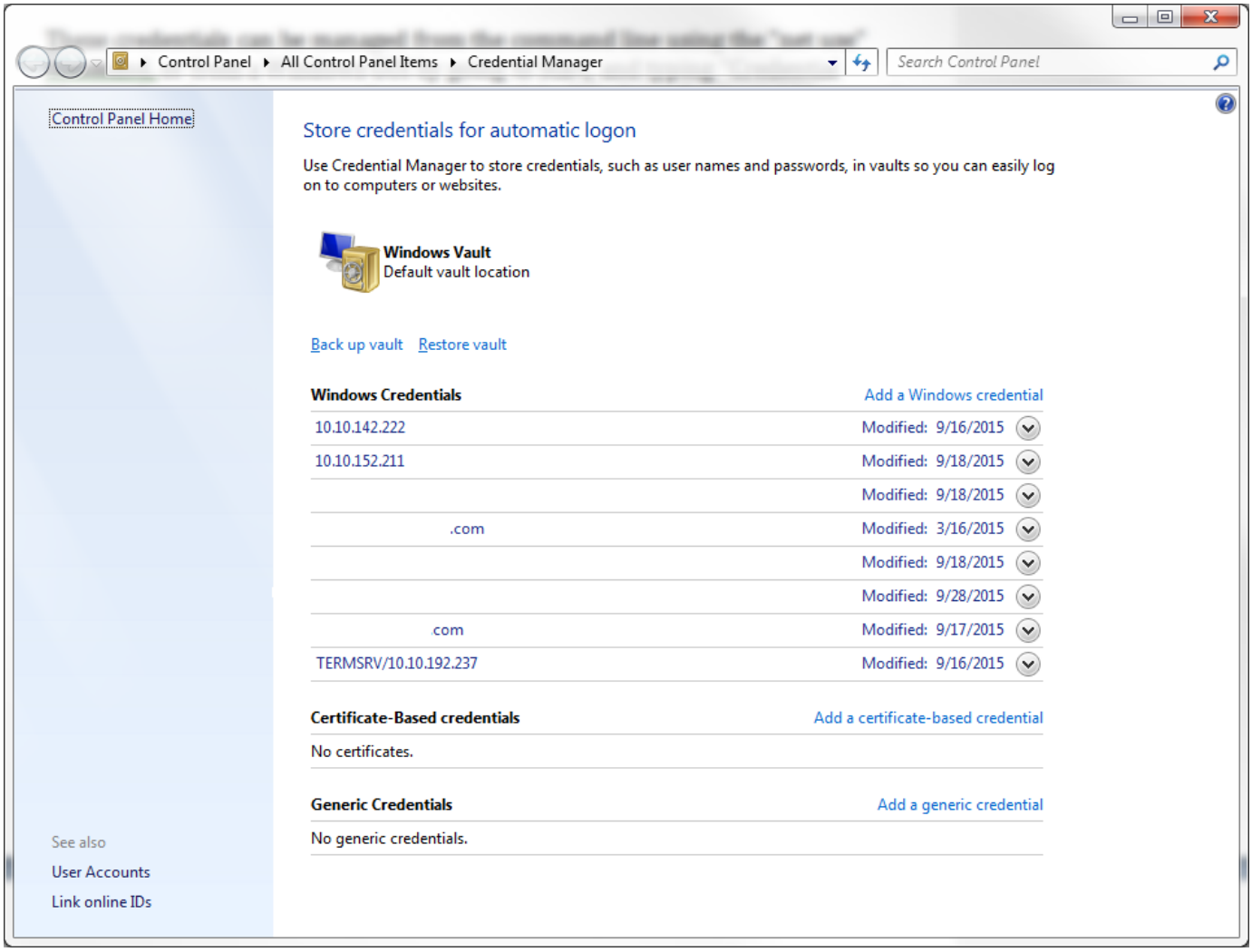
In Windows Explorer, use this hostname preceded by two slashes, "\\", in the address bar as shown below and press enter.



You will see a screen similar to the screenshot below. Do the same steps with domain, username, and password as you did above.

Do these steps for **each machine** that will be accessing the shared drive.

Note that if you are familiar with the Windows Credential Manager, you may use this tool to manage credentials. These credentials can also be managed from the command line using the "net use" command. To get to Credential Manager click on to *Start*, and typing *"Credential Manager"* and pressing enter. A screenshot of the Windows Credential Manager with some domain names intentionally blanked out is shown below.



Also note that authentication and access can be an issue when passwords change. When passwords change, for every computer using a credential that is no longer valid, you will need to redo the above steps. One indicator this is a problem is seeing the text: *"The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you."* Do not forget to re-authenticate with both the IP address and the hostname.

Multi-user Case Security

Overview

This page outlines the security protections that exist in a multi-user case deployment so that you can protect sensitive data. A multi-user deployment must be in a private network to ensure that only authorized users can access data. Remote sites should connect to central services via a VPN.

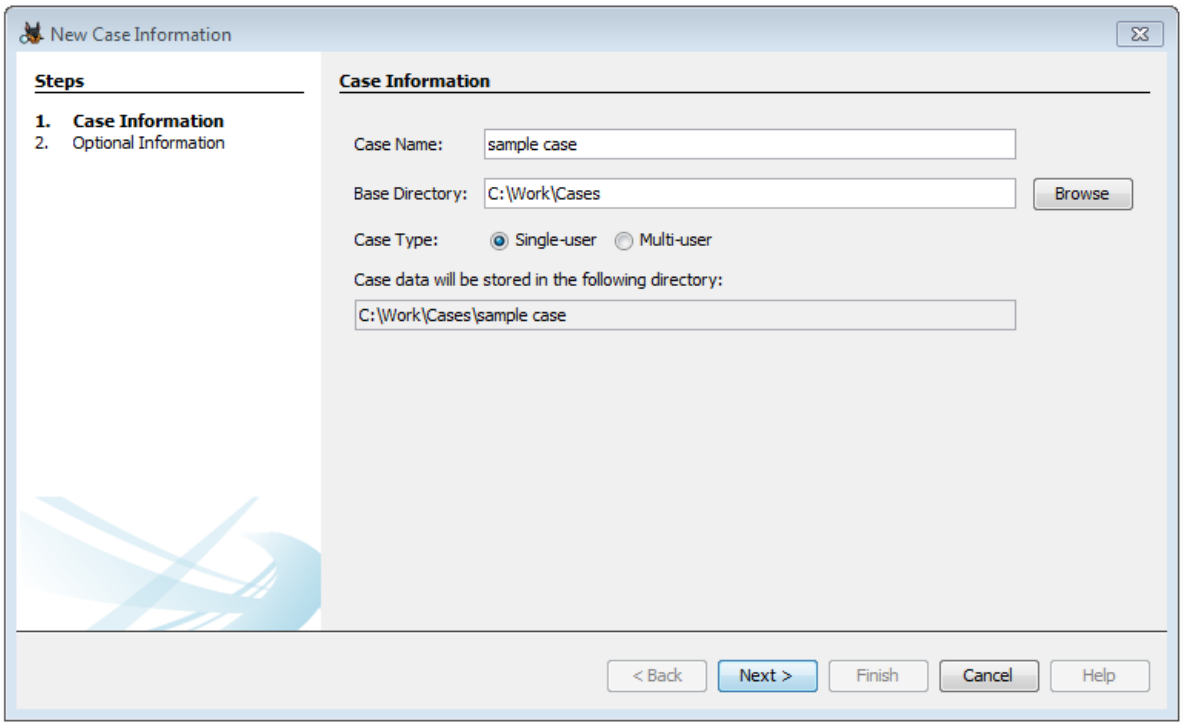
- Central Storage: It is your responsibility to use folder-based permissions to restrict access to the case folder. A user must be able to read and write into the case folder to open a case via Autopsy. It contains the Solr index, module output, logs, and reports.
- Central Database: PostgreSQL supports authentication via a login and password. Each Autopsy client must be configured with a PostgreSQL username and password. It is up to you to decide if there is a single username and password for the entire lab or if you will configure a new one for each client.
- Central Solr: Solr does not require a username or password to connect to it and query it. There is an optional way to configure Solr to require them, but we have not tried that yet.
- Messaging Service: ActiveMQ can be configured to require a username and password. Like the central database, it is up to you to decide on if there is a single username and password or one for each client.

Because the Solr server does not restrict access to the indexed content, you should deploy these services in a network that only authorized users have access to. Future versions will allow for additional protection of sensitive data.

Using Multi-user Cases

Creating Multi-user cases

Multi-user cases allow multiple instances of Autopsy to have the same case open at the same time. When creating a case, users are now presented with a choice of Single-user or Multi-user as shown in the screenshot below.



Single-user functions the same as always, with a back end SQLite database and a machine-local version of Solr.

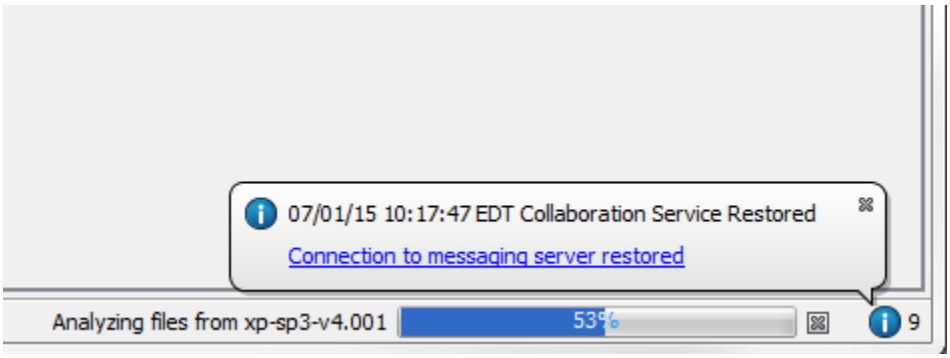
To create a multi-user case, the following must occur:

- The network services must be installed, configured, and running. See **Network-based Services**.
- The Case folder needs to be in a shared folder that all other clients can also access at the same path (UNC or drive letter).
- The data sources that are added with the Add Data Source wizard must be in a shared folder that all clients can access at the same path.

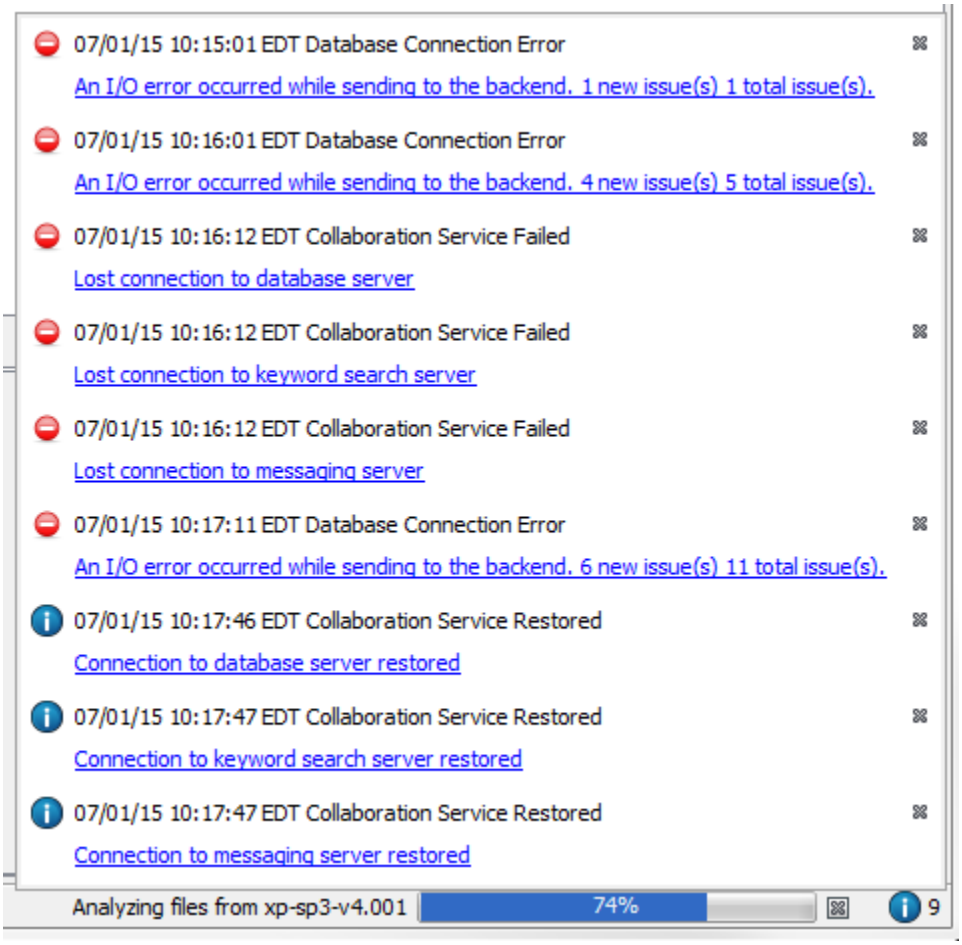
Other Multi-user Information

- When using a multi-user case, other nodes could be running data ingest on the same case. While this is happening, you will see a progress bar labelled with the hostname of the machine performing the ingest on the bottom right of Autopsy. The progress bar will continue to move back and forth until ingest has been completed or cancelled. You can still run ingest on your local machine while this is ongoing. This is shown in the screenshot below.

- When issues occur, there is an information "bubble" on the bottom right of the screen. It has an "i" inside a circle, with the color of the circle changed based upon the message. It uses red for bad and blue for good. See the screenshot below.



- Clicking on the information "bubble" brings up the list of prior notifications that have not been dismissed by clicking on the "x". As you can see in the screenshot below, the network cable was unplugged from the machine and it lost all connection to the three services. When the cable was reconnected, it found the services again.



- When creating multi-user cases, we recommend using UNC paths to specify drive names. Drive mapping will work, but it is sometimes difficult to get all the machines participating in a case to map to the same drive letters for the same resources. It is much simpler to use fully-specified UNC paths in the form of *\\hostname\sharename\folder*.

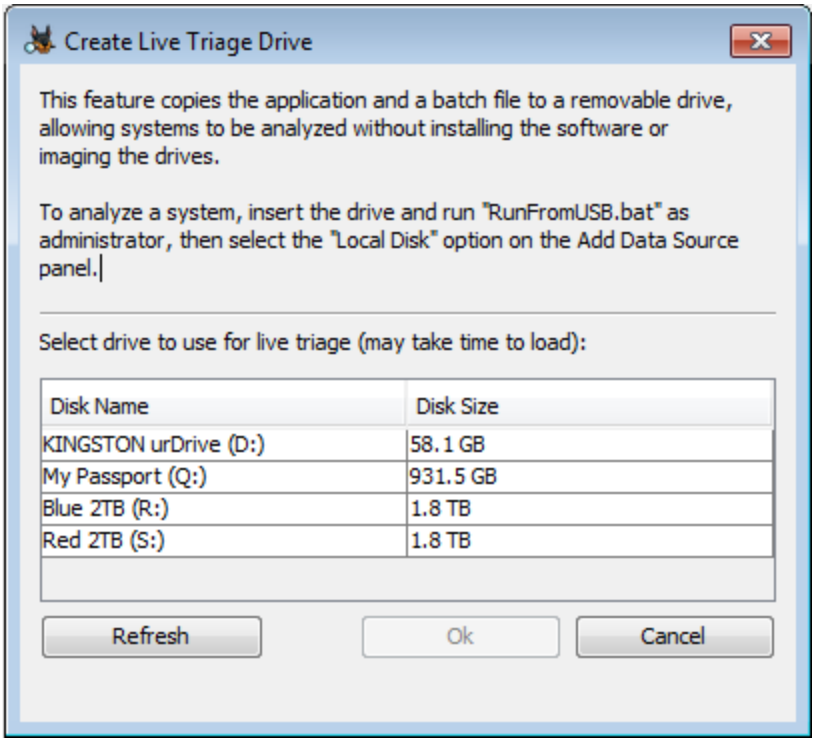
Live Triage

Overview

The Live Triage feature allows you to load Autopsy onto a removable drive to run on target systems while making minimal changes to that target system. This will currently only work on Windows systems.

Creating a live triage drive

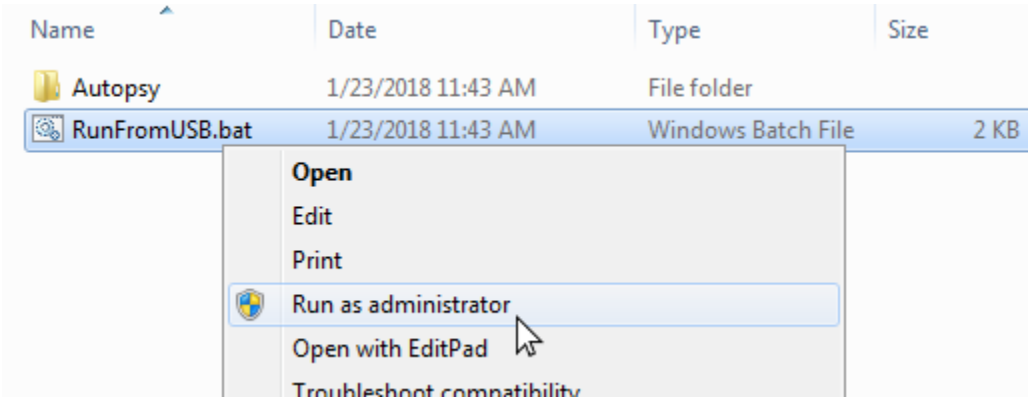
To create a live triage drive, go to Tools->Make Live Triage Drive to bring up the main dialog.



Select the drive you want to use - any type of USB storage device will work. For best results use the fastest drive available. Once the process is complete the root folder will contain an Autopsy folder and a RunFromUSB.bat file.

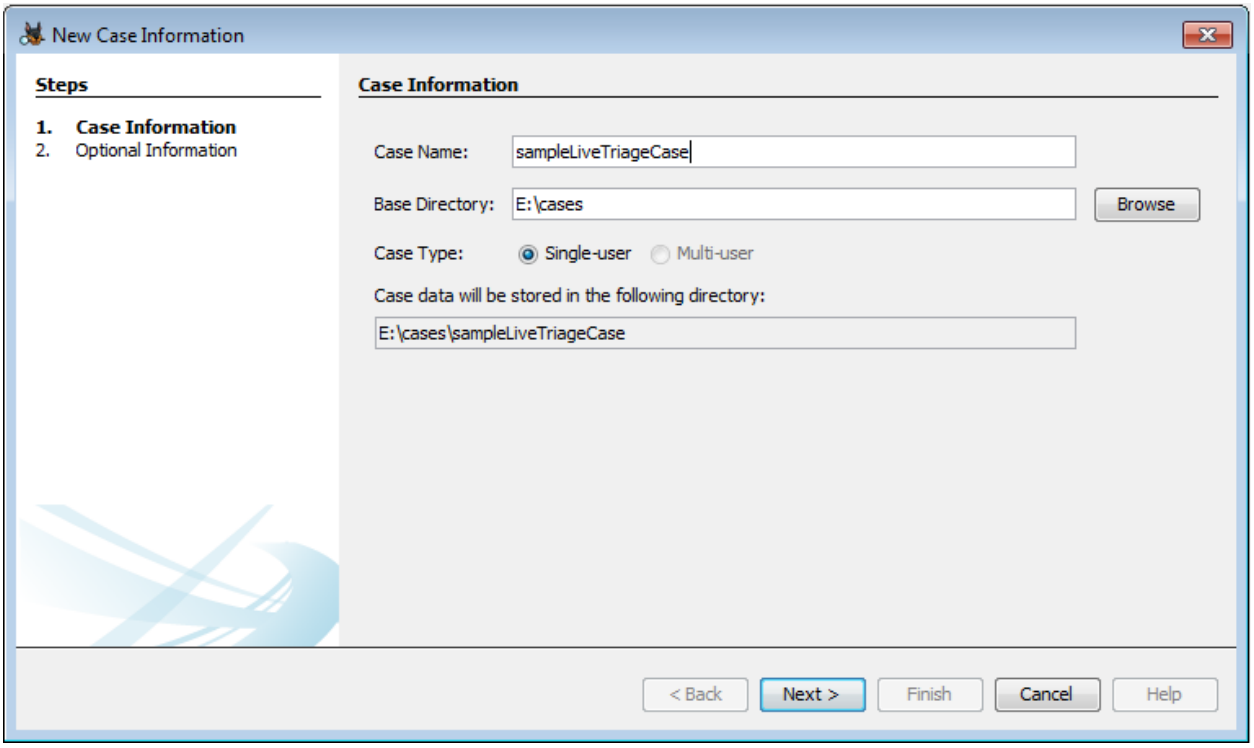
Running Autopsy from the live triage drive

Insert the drive into the target machine and browse to it in Windows Explorer. Right click on RunFromUSB.bat and select "Run as administrator". This is necessary to analyze the local drives.

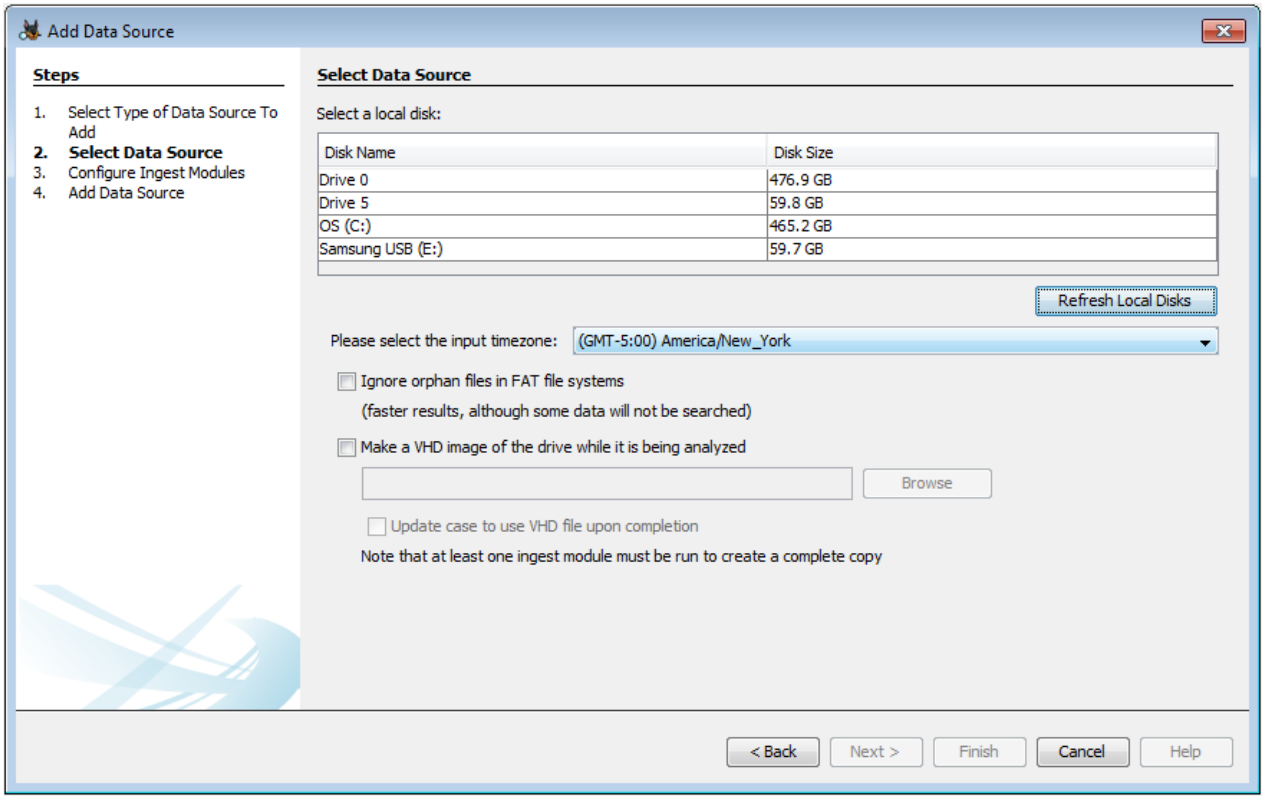


Running the script will generate a few more directories on the USB drive. The configData directory stores all the data used by Autopsy - primarily configuration files and temporary files. You can make changes to the Autopsy settings and they will persist between runs. The cases directory is created as a recommended place to save your case data. You will need to browse to it when creating a case in Autopsy.

Once Autopsy is running, proceed to create a case as normal, making sure to save it on the USB drive.



Then choose the Local Disk data source and select the desired drive.

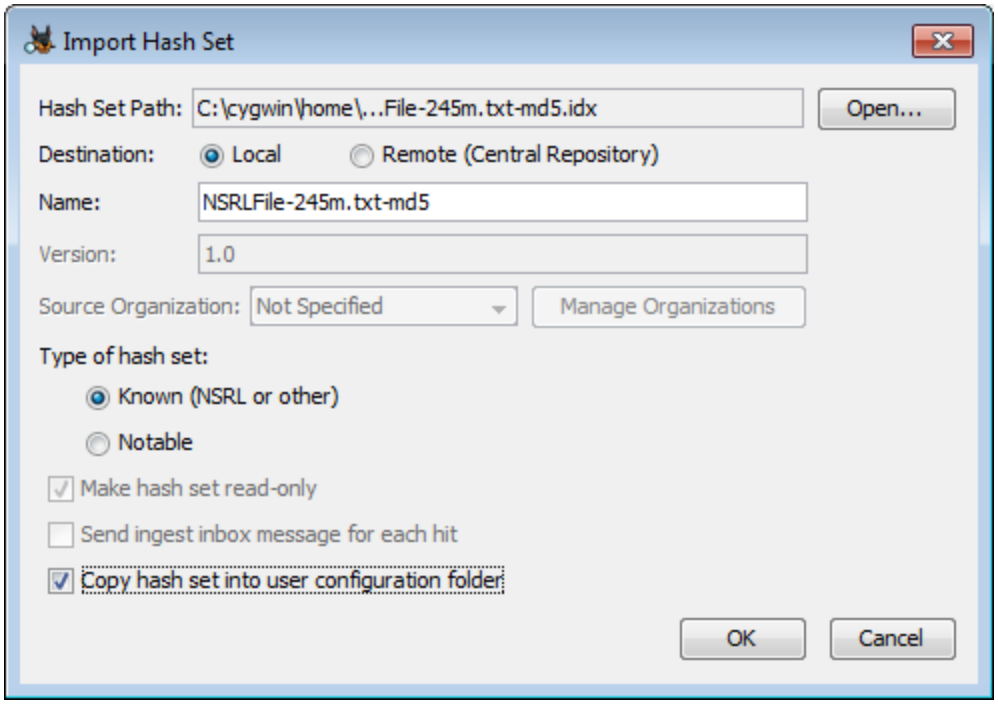


See the **Adding a Local Disk** page for more information on local disk data sources.

Using hash sets

Follow these steps to import a hash set to use with the **Hash Lookup Module** :

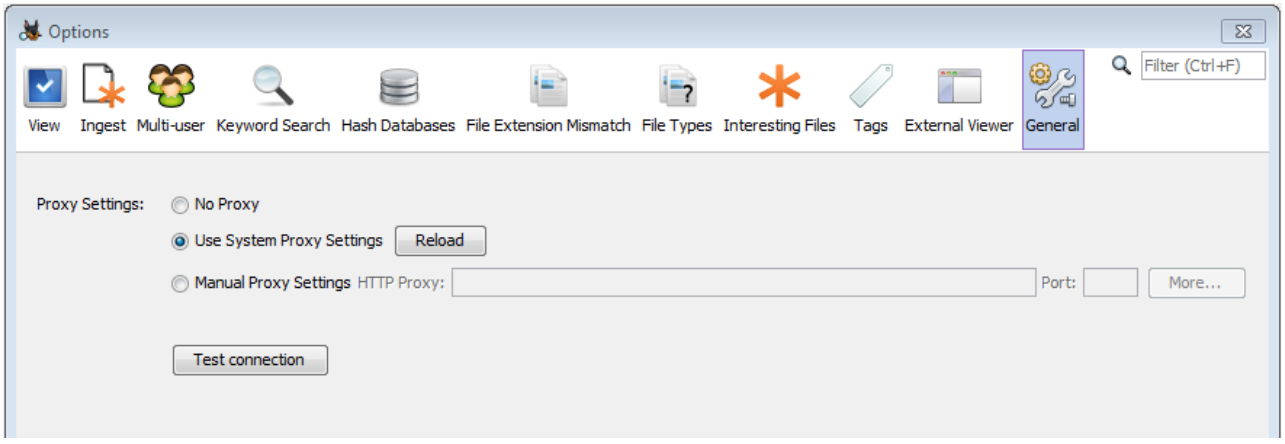
1. Run Autopsy from the live triage drive, as described earlier
2. Go to Tools->Options and then the "Hash Set" tab
3. Import the hash set as normal (using a "Local" destination) but check the "Copy hash set into user configuration folder" option at the bottom



This will allow the hash set to be used regardless of the drive letter assigned to the live triage drive.

Advanced Settings

If you are behind a proxy and need access to a network with Autopsy or one of the modules, you may set your proxy information in the *Tools*, *Options*, *General* tab as shown in the screenshot below.



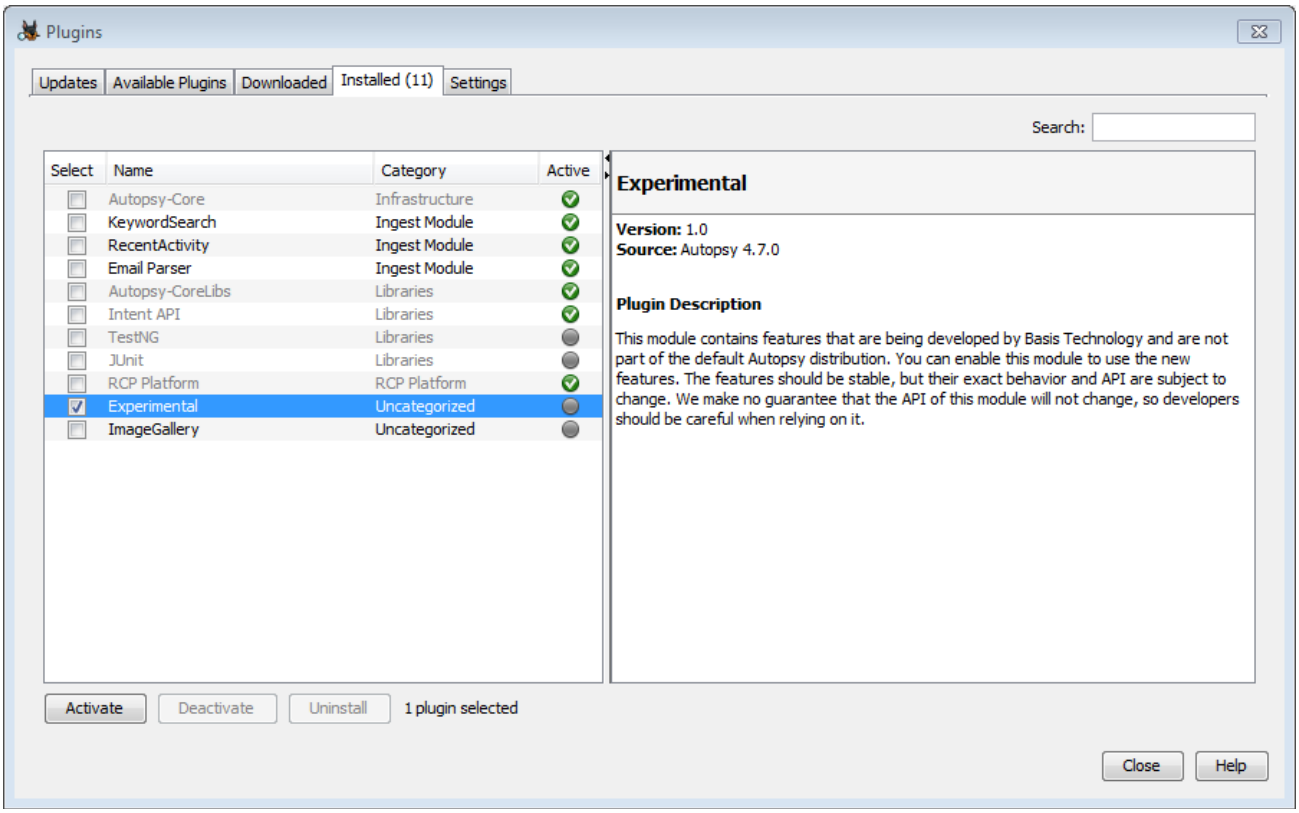
Experimental Module

Overview

The Experimental module, as the name implies, contains code that is not yet part of the official Autopsy release. These experimental features can be used but may be less polished than other features and will have less documentation. These modules may be changed at any time.

Enabling the Experimental Module

To start, go to Tools->Plugins and select the "Installed" tab, then check the box next to "Experimental" and click "Activate" and go throught the next couple of screens. A reset should not be required.



Current Experimental Features

- Auto Ingest
- **Object Detection**
- **Volatility Data Source Processor**