

4/15/2013



Autopsy

<http://www.sleuthkit.org>

AUTOPSY FORENSIC BROWSER USER GUIDE

Julia Keffer

Copyright

Copyright © 2013 Basis Technology Corp. All rights reserved.

License

This document is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported license. Refer to <http://creativecommons.org/licenses/by-nc-sa/3.0/>. Autopsy 3 is licensed under Apache License, Version 2.

Disclaimer

This document is provided to you for informational purposes only and is believed to be accurate as of the date of its publication, and is subject to change without notice. Basis Technologies Corp. assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

Version Information

Autopsy version 3.0.5

Document version 1.0

Table of Contents

Figures	iii
Chapter 1 – Introduction	1
Organization	1
Before you Begin	2
Overview of Digital Forensics	2
Chapter 2 – Getting Started Using the Wizard	4
Creating a Case	4
Adding a Disk Image	6
Configuring Disk Analysis	8
Adding a Hash Database	13
Chapter 3 – Exploring Analyzed Data	17
Using the Data Explorer	18
Using the Result Viewer	19
Viewing File Contents	21
Chapter 4 – Searching File Contents	24
Searching Using Built-in Keywords	24
Creating and Managing Keyword Lists	26
Saving File Locations	29
Chapter 5 – Generating Reports	33
Creating a Basic Report	34
Creating a Custom Report	36
Chapter 6 – Creating a Timeline	40
Creating a Graphical Timeline	41
Creating a Timeline Report	42
Chapter 7 – Collecting Files for Later Analysis	45
Extracting File and Directory Contents	45
Extracting Unallocated Disk Space	47
Appendix A: Toolbar Reference	50
Appendix B: Troubleshooting	51
Appendix C: FAQ	52
Glossary	53
Index	54

Table of Contents

Figures

Figure 1: Autopsy Process Flow	4
Figure 2: Autopsy Interface Window	17
Figure 3: The Data Explorer Panel	18
Figure 4: Result Viewer Directory View	19
Figure 5: Result Viewer Thumbnail View.....	20
Figure 6: Result Viewer Keyword Search	20
Figure 7: The Content Viewer	22

Chapter 1 – Introduction

The Autopsy Forensic Browser enables you to conduct a digital forensic investigation. It is a graphical interface to The Sleuth Kit and other tools. This guide covers information about using Autopsy version 3 on Windows.

This manual is for users with above average computer skills who have a basic understanding of digital forensics concepts. Users who are unfamiliar with the concepts may want to start with the section “Overview of Digital Forensics” on page 2.

Organization

The manual is organized as follows

- Description of digital forensics concepts (page 2)
- Chapter 2 – Getting Started Using the Wizard (page 4)
 - Getting started section to help you import your disk image into Autopsy and perform the initial automated analysis
- Chapter 3 – Exploring Analyzed Data (page 17)
 - Overview of the user interface regions and explanation of the results of the initial automated analysis
- Procedures to help you perform the following tasks
 - Search for keywords in the files in the disk image (page 24)
 - Generate reports (page 33)
 - Create timeline views (page 40)
 - Extract data from the disk image to analyze with other digital forensics tools (on page 45)
- Appendix A: Toolbar Reference (page 50)
- Appendix B: Troubleshooting to help you resolve errors (page 51)
- Appendix C: FAQ (page 52)
- Glossary (page 53)
- Index (page 54)

The following symbols are used in this document.



Additional information that is not necessary to perform the procedure, but that may be important to know later.



Reminders and shortcuts to help you perform tasks.

Before you Begin

You need the following items to begin using Autopsy.

- Computer running Windows XP, Vista or 7
- One or more disk images that contain the information you want to analyze in raw (single or split) or E01 format. The file system on the disk must be one of the following formats
 - NTFS
 - FAT12, FAT16, FAT32
 - HFS+
 - ISO9660
 - Ext2, Ext3
 - UFS
- Hash database if you want to compare MD5 file sums or identify known and unknown files. The following hash database formats are supported
 - NIST NSRL
 - EnCase
 - MD5
 - HashKeeper

Overview of Digital Forensics

Digital forensics refers to the process of recovering data from digital devices, from computer hard drives to mobile devices. This activity is often associated with criminal or civil investigations.

Digital devices can provide many different types of information that are not obvious to the casual user.

Internet data, such as cookies, browsing history, downloads, and cached web pages can provide a timeline of user activity, even when the user clears their cache or other Internet data.

Metadata is information assigned to a file by the program that creates or modifies it. It can include when the file was created, the user who created it, and the file size.

System files and logs provide information about various types of system activity, such as what programs are installed, what devices are attached to the system, and the history of users who logged on to the system.

Deleted files can yield information that the user thought was no longer available. Operating systems do not actually remove files when the user deletes them; the space is marked as available for use. Until the operating system reuses the space, the deleted data can be accessed with tools such as Autopsy.

Autopsy provides a graphical user interface to the tools, including The Sleuth Kit that can automate much of the forensic analysis. Autopsy provides additional features to continue analyzing the data after the automated analysis completes.



Autopsy has been completely rewritten since version 2; however, the following features you may have used in version 2 are not yet available.

- Viewing arbitrary sectors
- Notes and Event Sequencer

For further information and support, please visit the Autopsy Wiki at wiki.sleuthkit.org/index.php?title=Autopsy.

Chapter 2 – Getting Started Using the Wizard

The first time you start Autopsy, the wizard will guide you through the process of creating your first case, adding a disk image to the case, and configuring and starting the automated disk analysis, which Autopsy calls ingest. The following diagram shows the process.

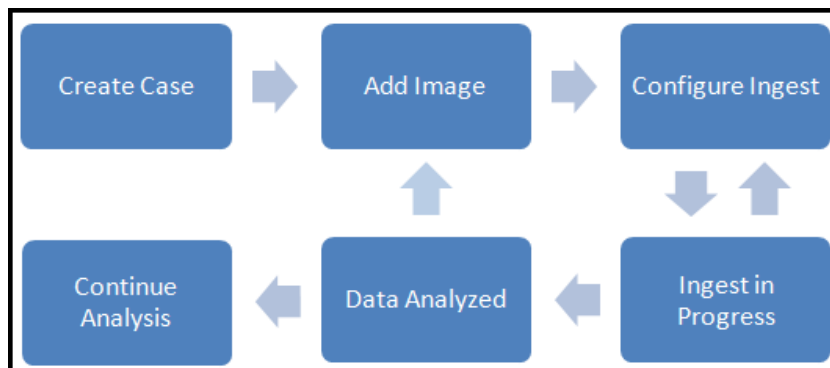


Figure 1: Autopsy Process Flow

At any time after you create the case, you can add additional images. You can also reconfigure ingest and restart the automated disk analysis.

In this section you will learn how to

- Create a case
- Add a disk image to a case
- Configure ingest to analyze the contents of the disk image
- Cancel and restart ingest
- Add a hash database to enhance data analysis

After this section, you will be prepared to continue further analysis of the image contents.

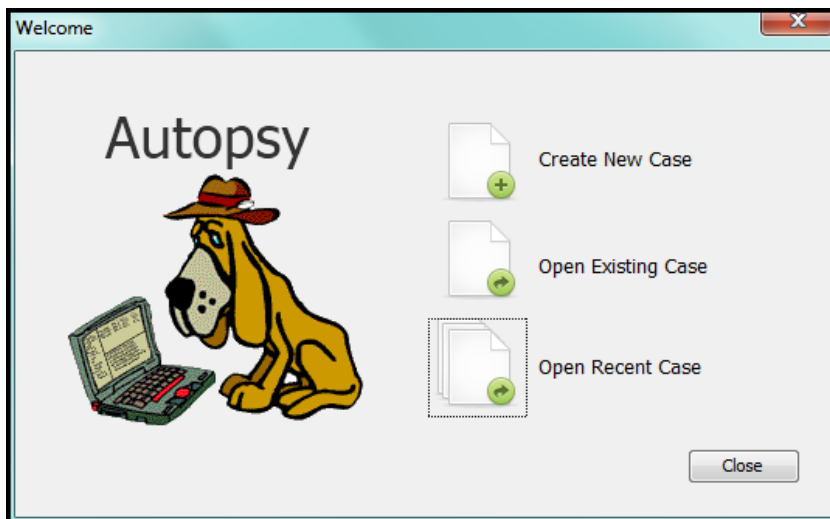
Creating a Case

A case is a container of information that groups data related to the same investigation. A case must contain at least one disk image, but you can add additional images to each case. For example, you may receive disk images from multiple hard drives on the same computer that you could analyze as a single case. We recommend that you group only related images in a single case.

When you start Autopsy, the **Welcome** window appears.



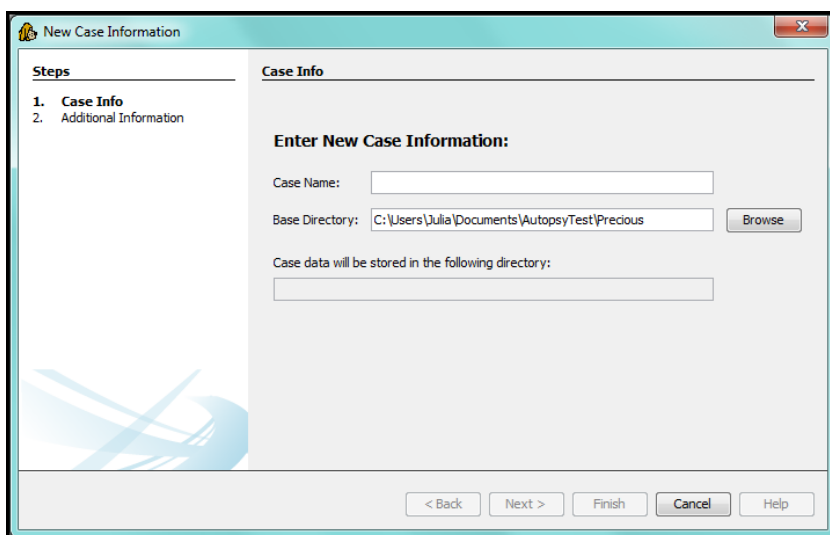
If you already created a case, to open it again, click **Open Existing Case** or **Open Recent Case** (shows a list of previously opened cases).



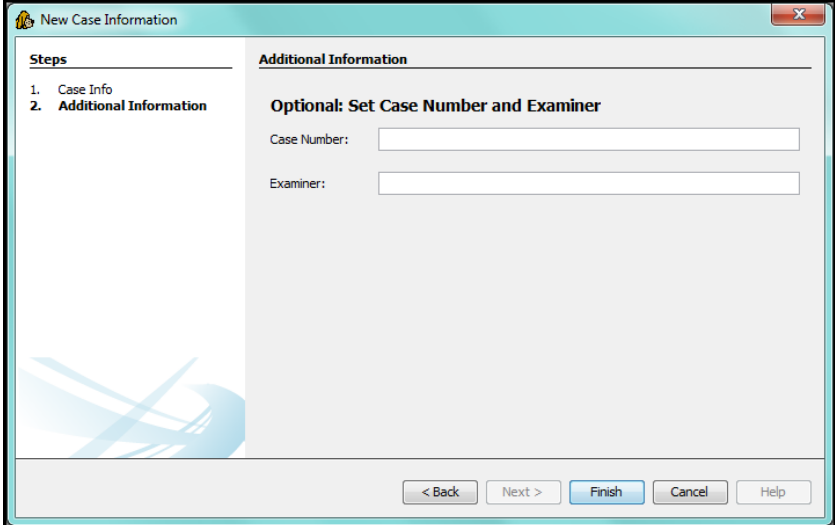
If this is your first time using Autopsy, you need to create a case.

To create a case

1. In the **Welcome** window, click **Create New Case**. The **New Case Information** window appears.



2. In the **Case Name** box, type a descriptive name for the case.
3. Click **Browse** and navigate to the directory where you want to store the case files and click **Select**.
4. In the **New Case Information** window, click **Next**. The **New Case Information** window updates to show **Additional Information**.



5. Optionally, in the **Case Number** box, type the number of the associated case, and in the **Examiner** box, type the name of the person responsible for the analysis.



If you do not add the case number and examiner when you create the case, you cannot add it to the case later.

6. Click **Finish**. The wizard displays the **Add Image** window and takes you to the next step automatically.

You are now ready to add an image to the case.

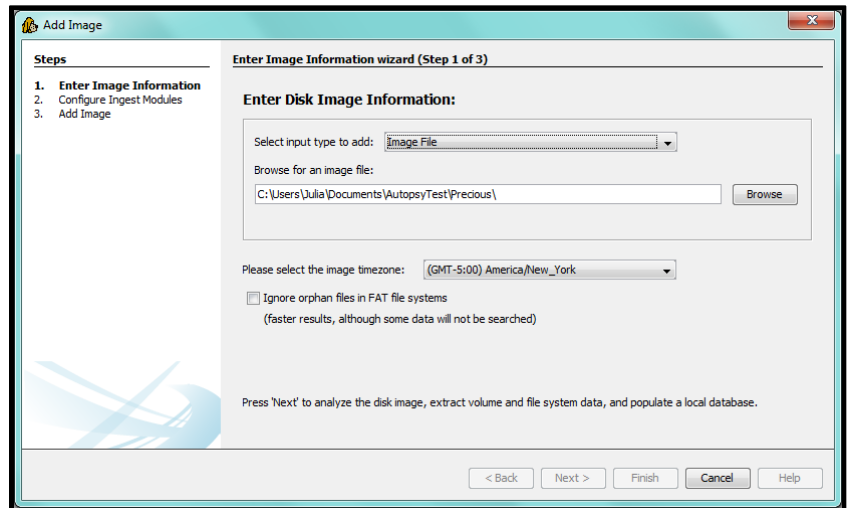
Adding a Disk Image

The first time you create a case, you will automatically see the **Add Image** window, which will take you through the steps to add an image to the case.



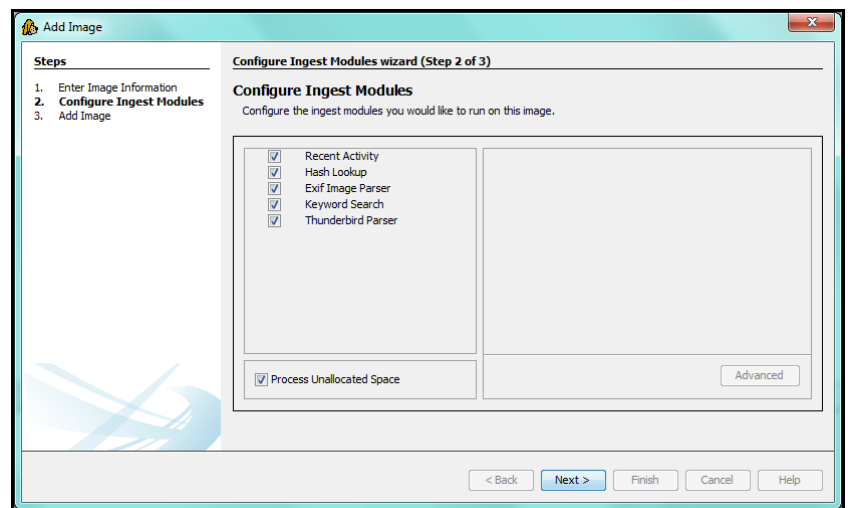
Once you add an image to a case, you cannot remove it.

The **Add Image** window enables you to select the image.



To add an image

1. Click **Browse** and navigate to the directory where the image is stored. Click the name of the image file and click **Open**.
2. If the investigator collected the image in a different time zone, in the time zone list, click the appropriate time zone.
3. Click **Next**. The **Add Image** window updates to show the **Configure Ingest Modules wizard**.



You are now ready to configure disk analysis, which Autopsy calls ingest. The wizard takes you to the next step automatically.

Configuring Disk Analysis

Autopsy refers to the process of automatically analyzing the disk contents as ingest. Ingest extracts the most common types of information used in digital forensic analysis from a disk image, which avoids the need to perform the tasks manually. Autopsy processes the user-related files first, to find the most likely sources of interesting information. The process runs in the background, which enables you to begin browsing the data while the process continues.

In this section you will learn about

- The types of ingest modules
- How to configure ingest
- How to cancel and start ingest

At the end of this section, you will know how to customize ingest to analyze the type of information you want to know about in the disk image.

The ingest process uses modules that analyze specific types of data. There are five default modules that you can select to find the type of data you need for your investigation.

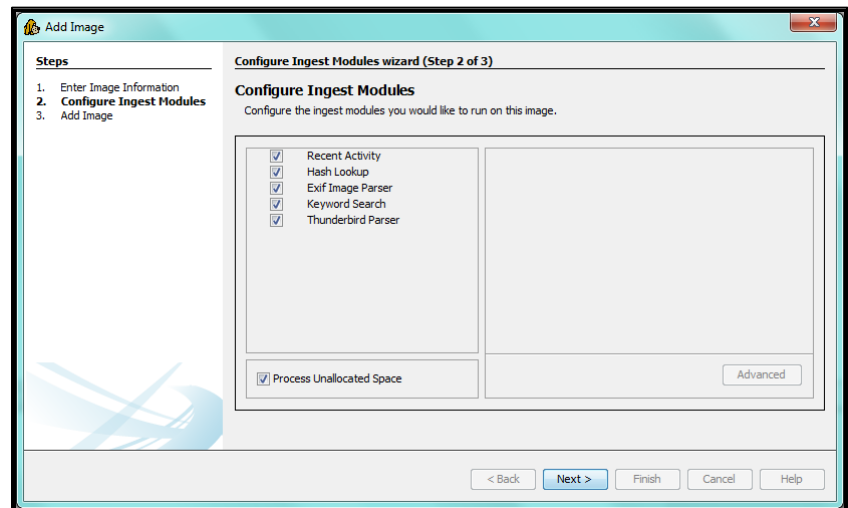
Module Name	Purpose
Keyword Search	Creates an index of keywords using the Apache SOLR search server. You can search the index for keywords and define keyword lists that ingest uses to produce search results.
Hash Database	Calculates the MD5 hash of each file. If you supply one or more hash databases, the module can look up the MD5 sum in databases to categorize the file type as known, unknown, or bad.
Thunderbird Parser	Extracts the contents of email folders from Outlook and Thunderbird email clients.
Exif Parser	Analyzes the metadata for graphic image files (location, date, and device used to capture the image). Can detect file formats JPG, GIF, and PNG.

Module Name	Purpose
Recent Activity	<p>Extracts recent user activity by focusing on web artifacts and system settings.</p> <ul style="list-style-type: none">• Extracts information about the last seven days of disk activity• Categorizes files based on the file metadata• Extracts Internet artifacts, such as downloads, browsing history, bookmarks, cookies, and search engine queries• Determines the device IDs of any devices connected to the computer at the time the disk image was captured <p>The module only supports Windows file systems.</p>

You can also select whether to analyze the unallocated disk space. This is the area that the operating system has marked as available for use, but which it has not yet overwritten with new data. If you choose not process it, ingest will finish more quickly, but you may miss some information.

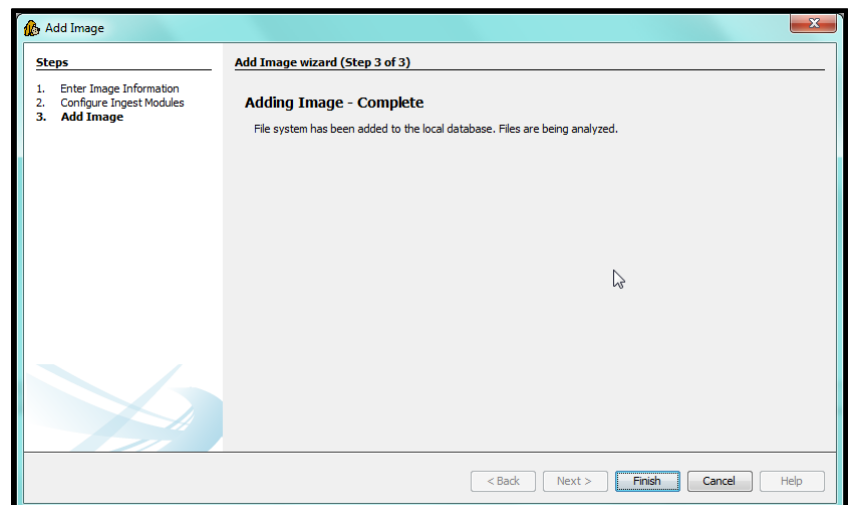
The size of the image and the ingest modules you use determine how long it will take to analyze the image contents. If you are not sure what data you need, you should select all the available modules. If the process takes too long, you can cancel it and clear some modules in the configuration window. Alternatively, if you think you only need certain types of information, you can limit the modules you select, and if you need more information, you can restart ingest later. For example, if you think you only need Internet artifacts, you may not need to select the **Hash Database** module.

In the previous step, you added the image and the **Add Image** window showed the **Configure Ingest Modules wizard**.



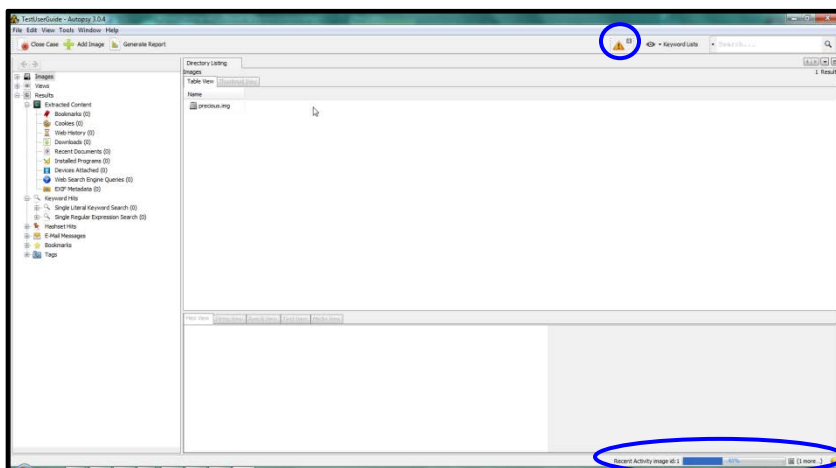
To configure ingest


1. Select the module name check boxes for the modules you want to use to analyze the disk image contents.
2. Click **Next**. The **Add Image** window updates to show **Adding Image – Complete**. The image is part of the case and the ingest process begins.



3. Click **Finish** to close the wizard.

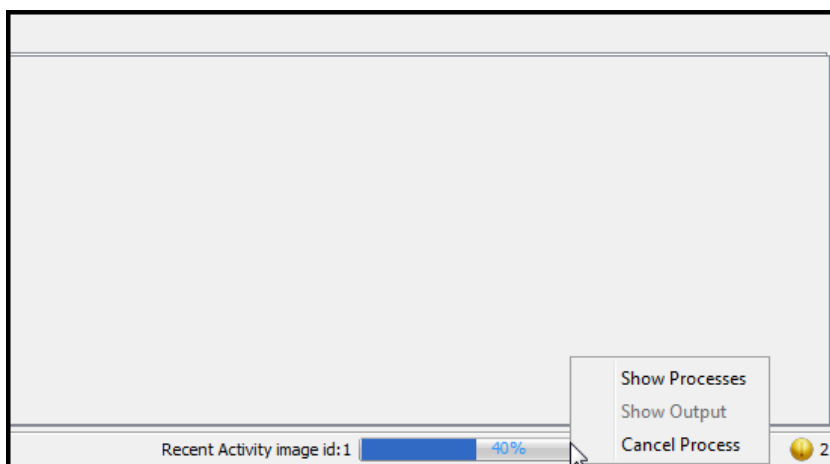
You can monitor the progress in the bottom right corner of the main window.



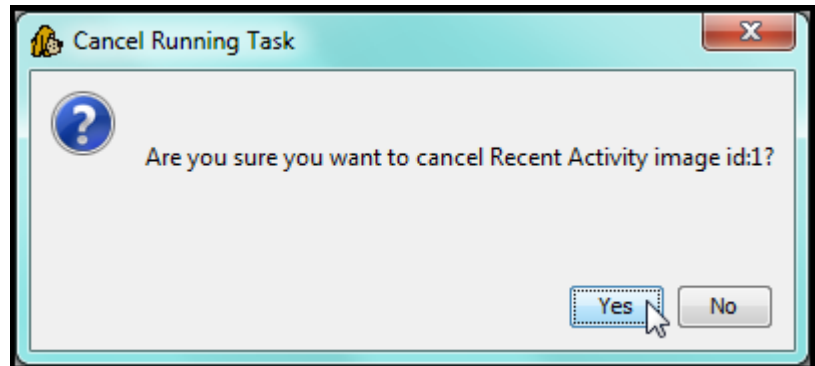
To view progress messages, click the  icon on the toolbar at the top of the window. If ingest takes too long, cancel it and reduce the set of data to analyze.

To cancel ingest

1. In the bottom right corner of the main window, right-click the blue progress bar and then click **Cancel Process**.



The **Cancel Running Task** box appears.



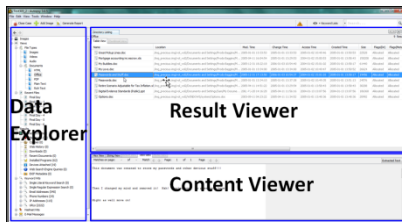
2. Click **Yes** to cancel ingest. Ingest stops and the blue progress bar at the bottom of the window disappears.

You can change the set of ingest modules to use and start ingest again.

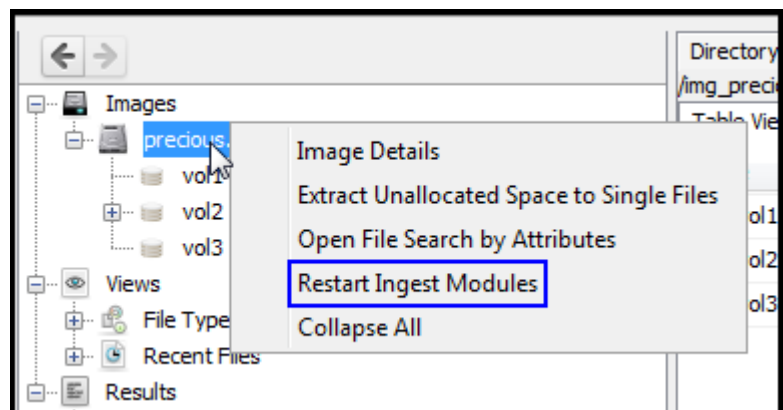
To restart ingest



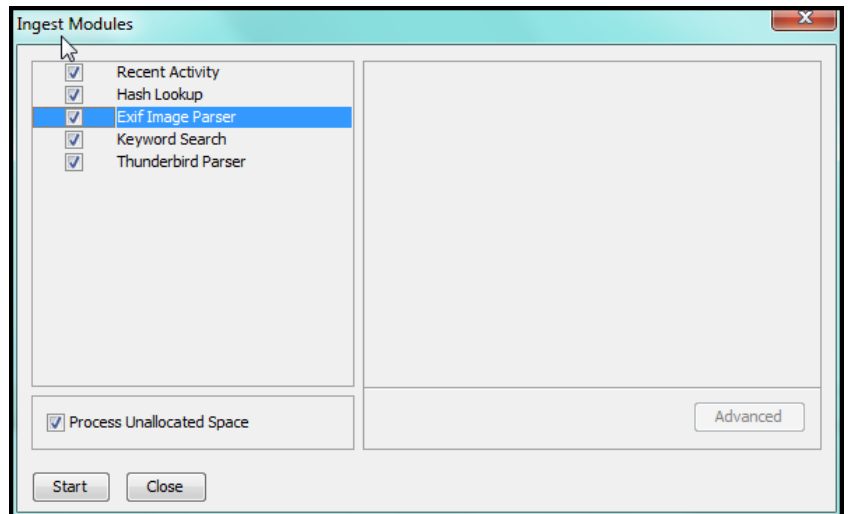
See the picture below if you need to locate the **Data Explorer**.



1. Click the **Images** section of the **Data Explorer** (see "Using the Data Explorer" on page 18). Right-click the image you want to process and then click **Restart Ingest Modules**.



The **Ingest Modules** window appears.



2. Select the module name check boxes for the modules you want to use and click **Start**. Ingest starts and you can monitor the progress in the bottom right corner of the window.

Adding a Hash Database

A hash database contains a list of MD5 sum values that Autopsy can use to identify files that are “known”. Known good files are those that can be safely ignored during disk analysis. This set of files frequently includes standard operating system and application files. By ignoring these files, you can greatly reduce disk image analysis time.

Known bad (also called notable) files are those that deserve special attention. This set will vary depending on the type of investigation, but common examples include contraband images and malware.

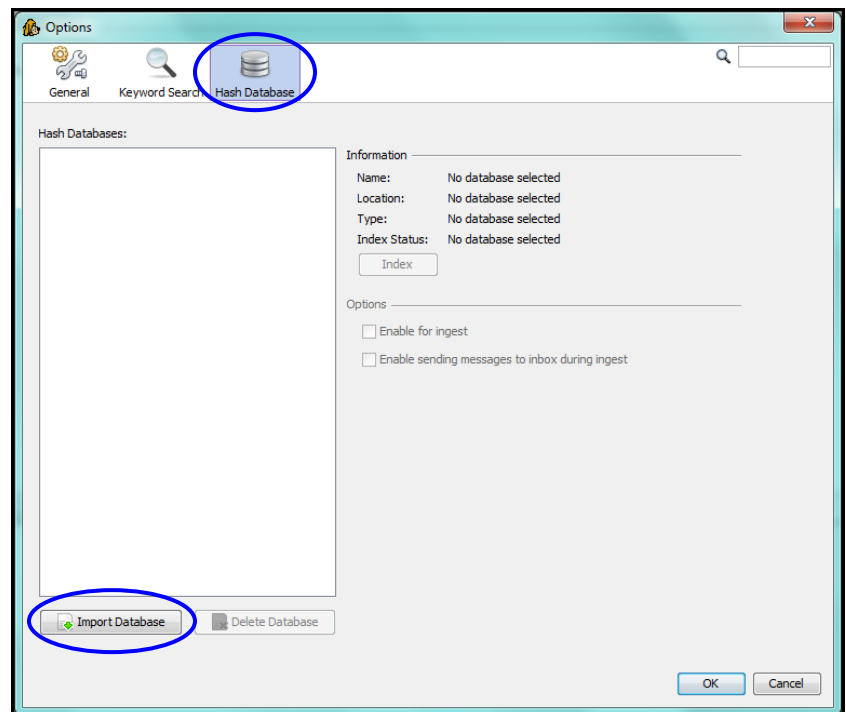
You can use hash databases with the following formats

- NIST NSRL
- EnCase
- MD5
- HashKeeper

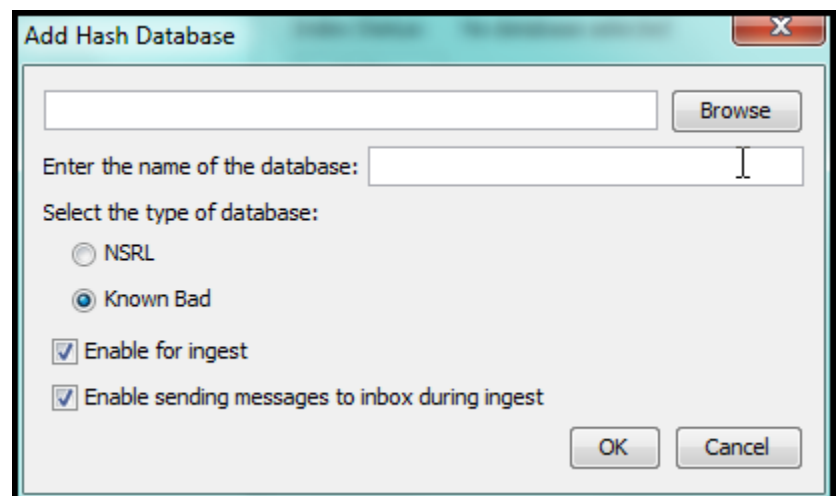
To use a hash database, ensure that you enable the **Hash Lookup** ingest module.

To add a hash database

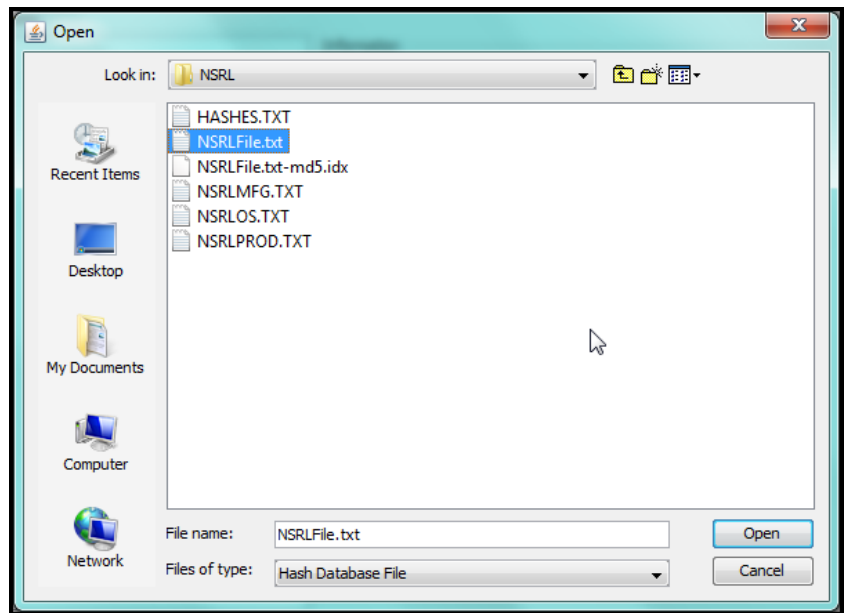
1. On the **Tools** menu, click **Options**. The **Options** window appears.



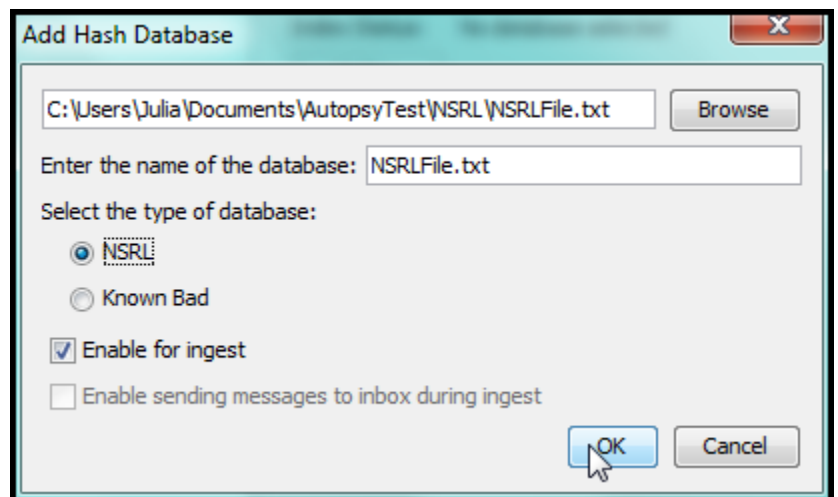
2. If it is not already active, click **Hash Database**. Click **Import Database**. The **Add Hash Database** dialog box appears.



3. Click **Browse** and navigate to the location of the hash database on your computer. The **Open** dialog box appears.



4. Click the database file name and click open.

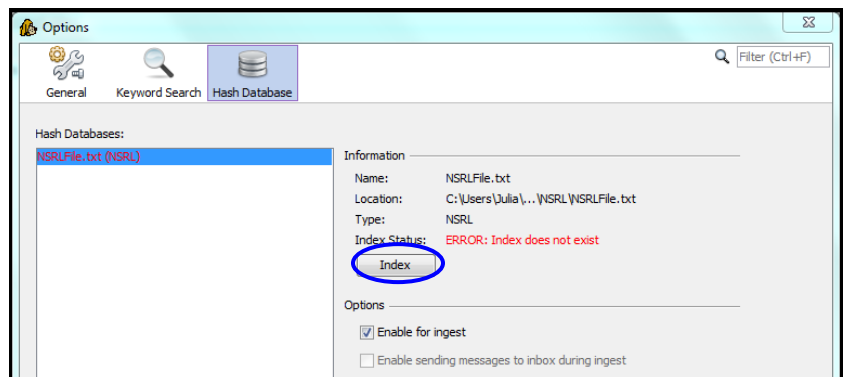


5. If you want to designate the database as a list of known good files, click **NSRL**. Otherwise, click **Known Bad**. Click **OK**.

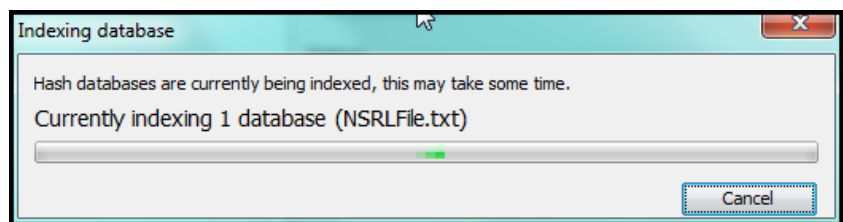


You can use multiple hash databases; however, you cannot use the same database for both good and bad files.

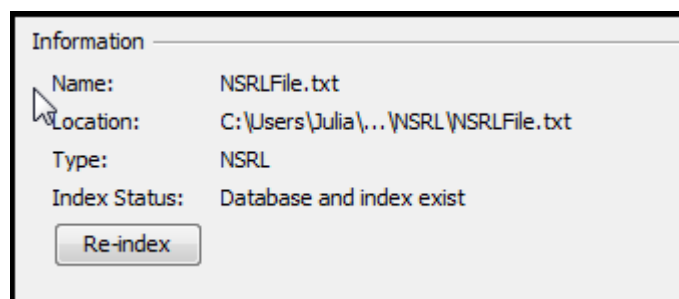
The **Options** window reappears and shows the database in the list.



6. If this is the first time you added the database, the **Index Status** shows **ERROR: Index does not exist**. Click **Index**. The **Index database** dialog box appears.



When it finishes, the **Index Status** changes to **Database and Index exist**.



7. To close the **Options** window, click **OK**. You have successfully added a hash database.

To use the database with your image, you need to restart ingest. See "To restart ingest" on page 12.

Chapter 3 – Exploring Analyzed Data

After ingest starts, you use the Autopsy interface window to begin exploring the data it analyzed. It has three regions:

- the **Data Explorer**
- the **Result Viewer**
- the **Content Viewer**

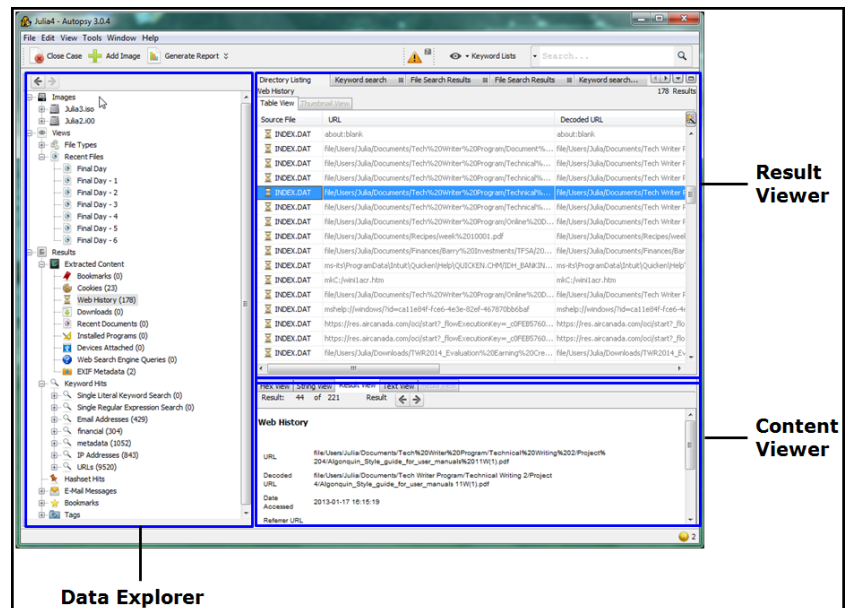
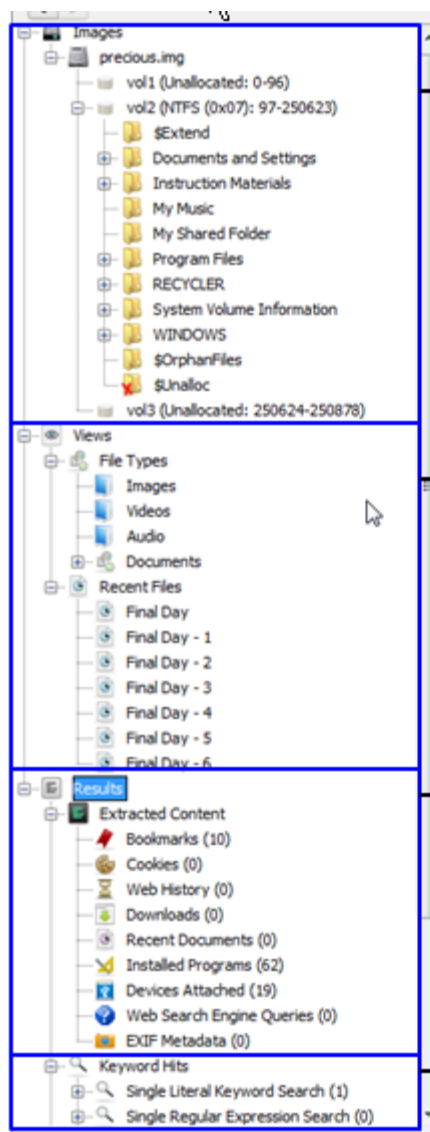


Figure 2: Autopsy Interface Window

Using the Data Explorer

As ingest runs, it categorizes information. The **Data Explorer** shows the results in a tree view.



The **Images** section shows the image contents in Windows Explorer format.

The **Views** section shows the files that Autopsy could categorize based on the file metadata.

The **Results** section shows the results of the data extracted during the ingest process.

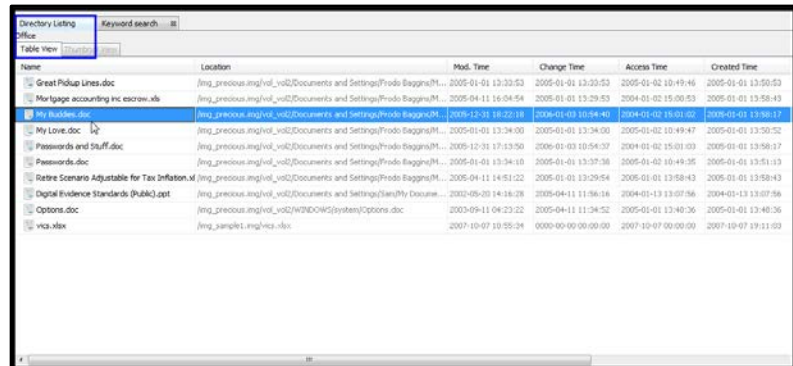
The **Keyword Hits** section shows search results from custom or pre-defined search criteria.

Figure 3: The Data Explorer Panel

If you click any item in the tree, the **Result Viewer** shows the contents.

Using the Result Viewer

When you select an item in the **Data Explorer**, the **Result Viewer** shows the results. You can display the results in different formats, depending on the type of file. Figure 4 shows a list of files categorized as Microsoft Office file types.



Name	Location	Mod. Time	Change Time	Access Time	Created Time
Great Pickup Lines.doc	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-01-01 13:33:53	2005-01-01 13:33:53	2005-01-02 10:49:46	2005-01-01 13:50:53
Mortgage accounting inc excel.xls	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-04-11 16:04:54	2005-01-01 13:29:53	2004-03-02 15:00:53	2005-01-01 13:58:43
My Notes.doc	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-11-30 18:20:18	2006-01-03 10:04:40	2004-02-02 15:01:02	2005-01-01 13:58:11
My Love.doc	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-01-01 13:34:09	2005-01-01 13:34:09	2005-01-02 10:49:47	2005-01-01 13:50:52
Passwords and Stuff.doc	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-12-30 17:13:50	2006-01-03 10:04:37	2004-03-02 15:01:03	2005-01-01 13:58:17
Passwords.doc	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-01-01 13:34:10	2005-01-01 13:37:38	2005-01-02 10:49:35	2005-01-01 13:51:13
Retire Scenario Adjustable for Tax Inflation.xls	img_previous.img\vol_02\Documents and Settings\FredRaggs\M...	2005-04-11 14:51:22	2005-01-01 13:39:54	2005-01-01 13:50:43	2005-01-01 13:50:43
Digital Evidence Standards (Public).opt	img_previous.img\vol_02\Documents and Settings\SaraMy Docume...	2002-09-20 14:16:28	2005-04-11 11:56:16	2004-03-13 13:07:56	2004-01-13 13:07:56
Options.doc	img_previous.img\vol_02\WINDOWS\system\Options.doc	2003-09-11 04:23:22	2005-04-11 11:54:52	2005-01-01 13:40:36	2005-01-01 13:40:36
vca.xlsx	img_samplet.img\vca.xlsx	2007-10-07 10:55:24	0000-00-00 00:00:00	2007-10-07 00:00:00	2007-10-07 17:11:03

Figure 4: Result Viewer Directory View

You can use the **Table View** tab under the **Directory Listing** view to display the data as a table showing the properties of each file. The properties shown are:

- name
- time (modified, changed, accessed, and created)
- size
- flags (directory and metadata)
- mode
- user ID
- group ID
- metadata address
- attribute address
- type (directory and meta)

If you view a list of images, in addition to the **Table View**, you can use the **Thumbnail View** tab to see the images, instead of a list of files. Autopsy supports viewing JPG, PNG, and GIF image formats. See Figure 5: Result Viewer Thumbnail View.

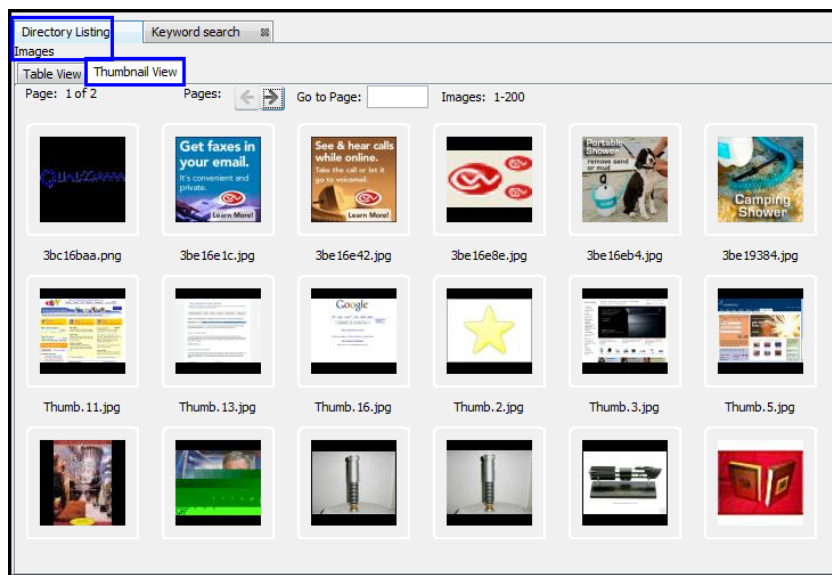
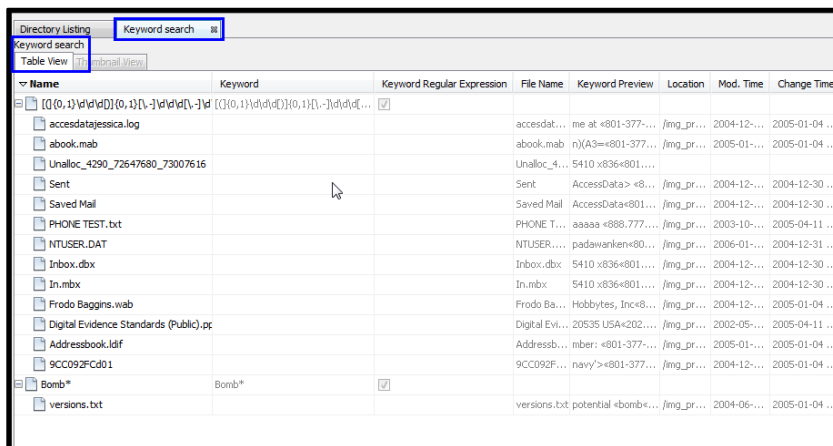


Figure 5: Result Viewer Thumbnail View

If you perform a keyword search (see “Chapter 4 – Searching File Contents” on page 24), to see the results, click the **Keyword search** tab. See Figure 6: Result Viewer Keyword Search.



Name	Keyword	Keyword Regular Expression	File Name	Keyword Preview	Location	Mod. Time	Change Time
accessdatajessica.log			accessdat...	me at <801-377...	/img_pr...	2004-12...	2005-01-04 ...
abook.mab			abook.mab	n)(A3=<801-377...	/img_pr...	2005-01...	2005-01-04 ...
Unalloc_4290_72647680_73007616			Unalloc_4...	5410 x836<801...	/img_pr...	2004-12...	2004-12-30 ...
Sent			Sent	AccessData> <8...	/img_pr...	2004-12...	2004-12-30 ...
Saved Mail			Saved Mail	AccessData<801...	/img_pr...	2004-12...	2004-12-30 ...
PHONE TEST.txt			PHONE T...	aaaa <888.777...	/img_pr...	2003-10...	2005-04-11 ...
NTUSER.DAT			NTUSER...	padawanken<80...	/img_pr...	2006-01...	2004-12-31 ...
Inbox.dbx			Inbox.dbx	5410 x836<801...	/img_pr...	2004-12...	2004-12-30 ...
In.mbx			In.mbx	5410 x836<801...	/img_pr...	2004-12...	2004-12-30 ...
Frodo Baggins.wab			Frodo Ba...	Hobbytes, Inc<8...	/img_pr...	2004-12...	2005-01-04 ...
Digital Evidence Standards (Public).pp			Digital Evi...	20535 USA<202...	/img_pr...	2002-05...	2005-04-11 ...
Addressbook.lidf			Addressb...	mber: <801-377...	/img_pr...	2005-01...	2005-01-04 ...
9CC092FCd01			9CC092F...	navy>><801-377...	/img_pr...	2004-12...	2005-01-04 ...
Bomb*	Bomb*		versions.txt	potential <bomb...	/img_pr...	2004-06...	2005-01-04 ...

Figure 6: Result Viewer Keyword Search

The **Keyword search** tab separates the list into keyword matches for each keyword list. Once you close the **Keyword search** tab, to view the list again, click the list name under the **Keyword Hits** section of the **Data Explorer**.

When you click a file in any view of the **Result Viewer**, the contents appear in the **Content Viewer**.

Viewing File Contents

You can view the file contents in different formats, depending on the file type. You can view the file contents in either the **Content Viewer** at the bottom of the screen or in a new window.

Text View

The **Keyword Search** ingest module creates an index of words it can identify in the files on the disk image. This index is the basis for running keyword searches. If ingest used the module, to view the search results for a file, click the **Text** tab.

The text view and the string view are different because the string view relies on searching the file for data that appears to be text. Some file types, such as PDF files, do not have text data at the byte level, but the keyword indexing process can interpret a PDF file and produce text. For files the module can identify, the file metadata (such as creation date and author) may appear at the end of the displayed text. Unlike the string view, the text view cannot view the data in another language.

If this tab is not available, either the file has no text or you did not enable **Keyword Search** ingest module.

Result View

The **Result View** shows file properties that were extracted during ingest. This tab is normally available for items shown under **Results** or **Keyword Hits** in the **Data Explorer**. For email messages, this is usually the most useful view.

String View

The **String View** tab shows possible text strings in files, which could be in binary format. The view shows the strings after they have been decoded and interpreted as UTF8/16 for the selected language. The default language is English. To change the language, on the **Tools** menu, click **Options**.

Hex View

The **Hex View** tab shows the raw contents of a file. The file data is represented as hexadecimal values grouped in two groups of eight bytes, followed by one group of 16 ASCII characters which are derived from each pair of hexadecimal values (each byte). Non-printable ASCII characters and characters that require more than one character space are typically represented by a dot (".") in the following ASCII field.

Media View

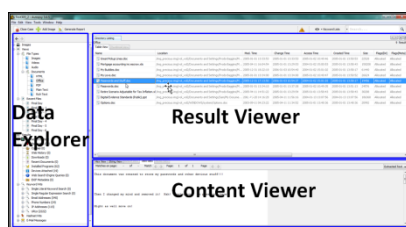
The **Media View** is only available for graphic images (JPG, GIF, and PNG format) and video files. You can use the controls at the bottom of the screen to play a selected video.

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 extract the file.

To view the file in the Content Viewer



See the picture below if you need to locate the **Result Viewer**.



1. Click the file in the list in the **Result Viewer**. The contents appear in the **Content Viewer** in the window at the bottom of the screen.

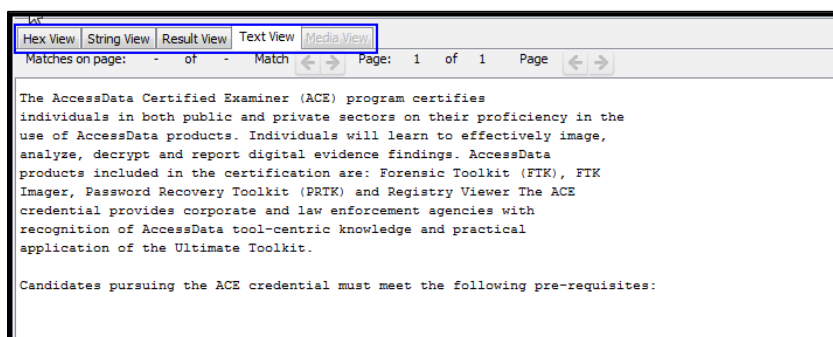


Figure 7: The Content Viewer

2. Click the tabs to view the file in various formats.

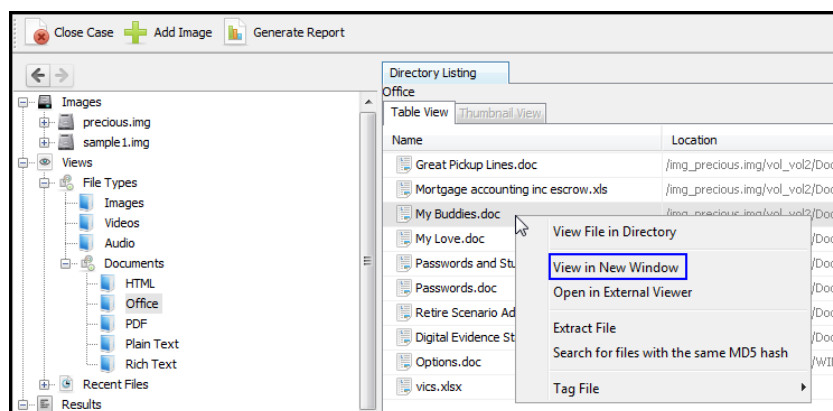
You can view the file contents in the **Content Viewer** in a new window or with an external program. Autopsy chooses the external viewer based on file type.



If you want to open the file in an external viewer from within Autopsy, you need to have the program installed on your computer.

To view the file contents in a new window

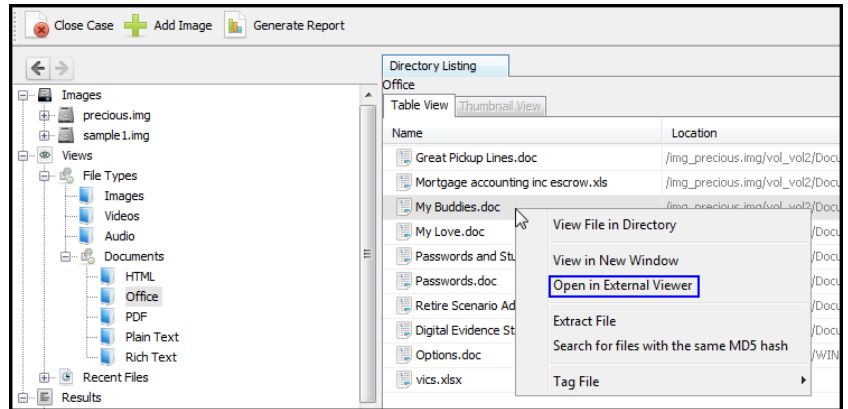
- Right-click the file in the **Result Viewer** and click **View in New Window**.



The **Content Viewer** appears in a new window. You can view the file contents in the supported formats.

To view the file contents using an external viewer

- Right-click the file in the **Result Viewer** and click **Open in External Viewer**.



The file contents appear in a new window using the program associated with the file type. For example, if the file is a Microsoft Word file, Microsoft Word runs and the file appears in a Microsoft Word window.

Chapter 4 – Searching File Contents

You can search the files in the disk image for specific keywords. Keywords can be simple strings or regular expressions. If the search produces useful results, you can save the location of the files. In this section you will find information about

- How to search using built-in keywords
- How to create a keyword list
- How to save file locations

After these tasks, you may want to

- Generate a report (see page 33)
- Extract the file contents from Autopsy for analysis with other tools (see page 45)

Searching Using Built-in Keywords

Autopsy includes built-in keyword search expressions that enable you to search for:

- URLs
- IP Addresses
- Email addresses
- Phone numbers

To search using these expressions, ensure that the **Keyword Search** ingest module was enabled when you ran ingest.



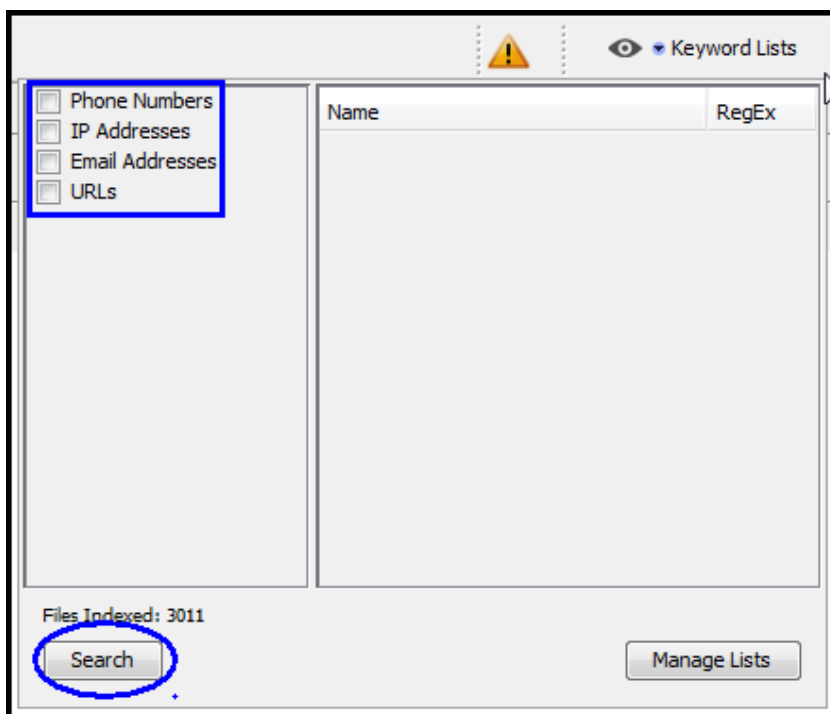
These search expressions can produce a large list of results with many false positives.

To search using built-in keywords



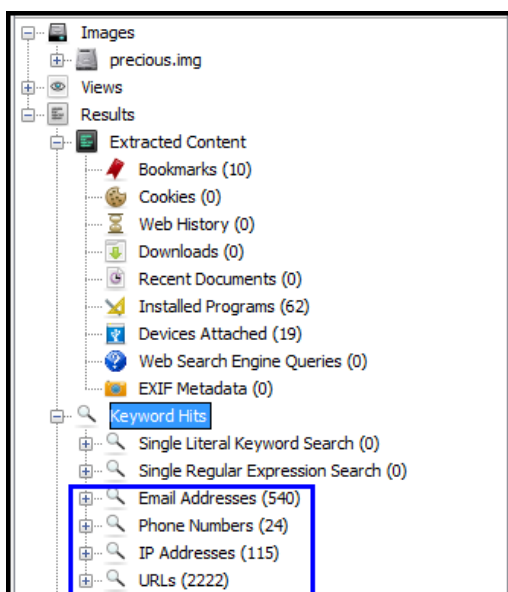
You can select more than one search option and search for all keywords simultaneously.

1. On the toolbar, click **Keyword Search**. The menu appears.



2. Select the check box for the search options you want to use and click **Search**.

The information appears in the **Keyword Hits** section of the **Data Explorer**. The following view shows search results for all the built-in expressions.



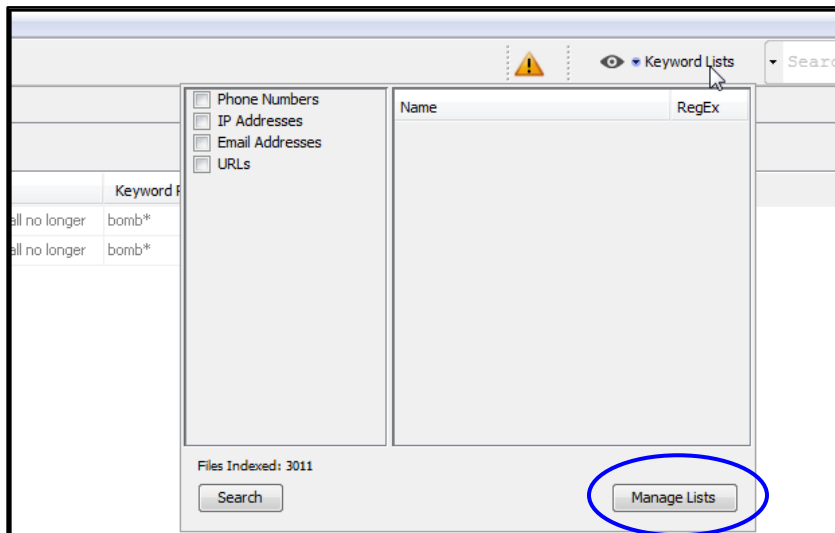
Creating and Managing Keyword Lists

The **Keyword Search** ingest module uses the keyword list when Autopsy analyzes the disk image contents. If you add new keywords to the list, you need to restart ingest to perform the search. Keyword lists are global to Autopsy; Autopsy uses them for all cases.

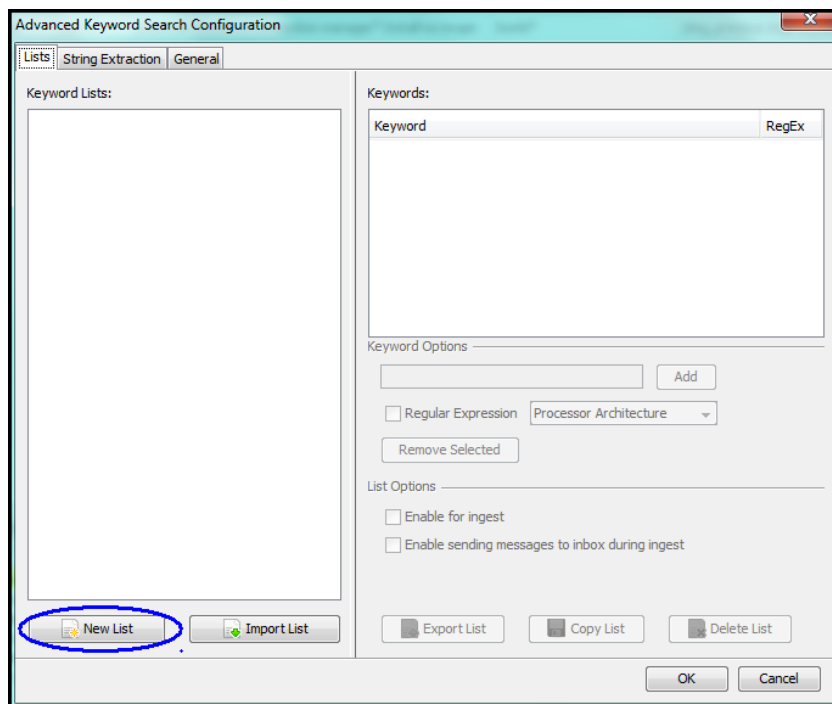
The list can contain simple strings or regular expressions. Regular expressions are a sequence of special characters that enable you to match a set of strings. The built-in searches for IP addresses and URLs are examples of regular expressions. Autopsy uses the [Java regular expressions syntax](http://www.java.com/7/docs/5/regex/).

To create a keyword list

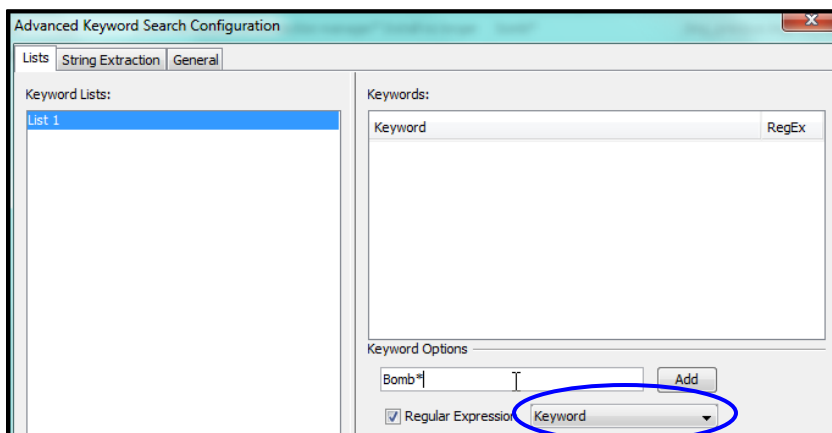
1. On the toolbar, click **Keyword Search**. The menu appears.



2. In the bottom right corner of the menu, click **Manage Lists**. The **Advanced Keyword Search Configuration** window opens.

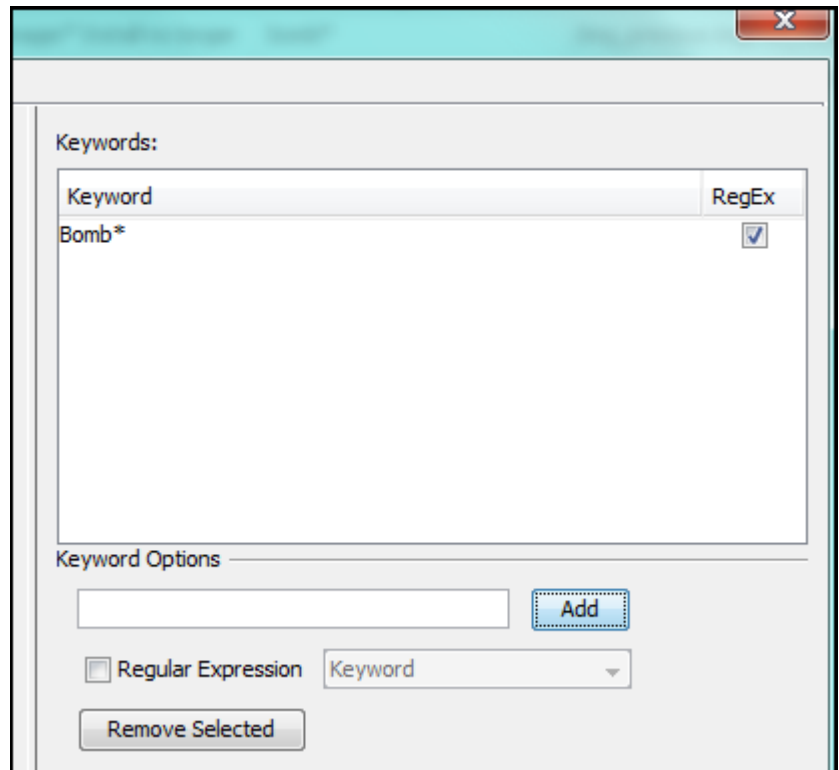


3. In the bottom left corner of the window, click **New List**.
4. In the **New keyword list name** box that appears, type a descriptive name for the list and click **OK**. The list name appears in the **Keyword Lists** column.



5. In **Keyword Lists**, click the list name you entered. In the **Keyword Options** box, type the keyword or regular expression you want to search for. If your keyword is a regular expression
 1. Select the **Regular Expression** check box.
 2. On the **Keyword** menu, you can choose a type of regular expression.

6. Click **Add**. The keyword appears in the **Keywords:** list on the right side of the window.



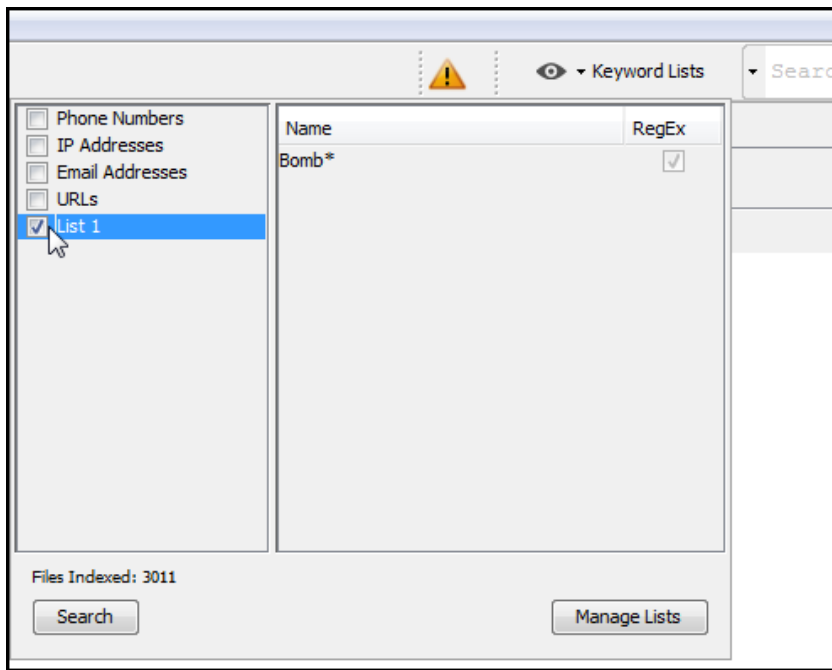
If you make a mistake, click the keyword in the **Keywords:** list and click **Remove Selected**.

7. You can add more keywords to the same list. When you finish, click **OK**.

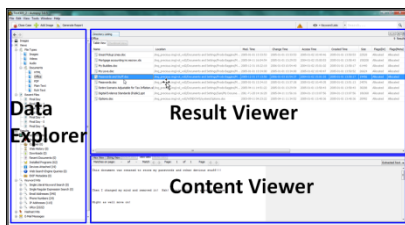
You now have a list of keywords for ingest to use.

To run the search

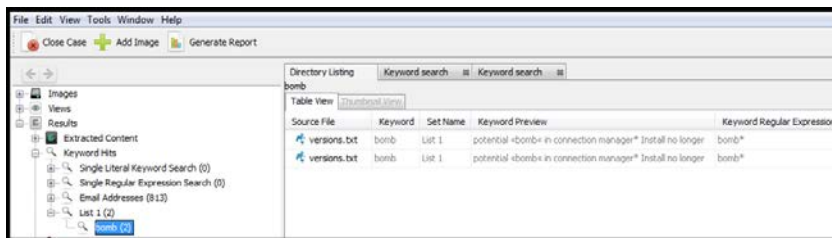
1. To run the search on the , on the toolbar, click **Keyword Lists**.
2. On the menu that appears, select the list name check box and click **Search**.



See the picture below if you need to locate the **Result Viewer**, **Data Explorer**, or **Content Viewer**.



Results appear in the **Keyword Hits** section of the **Data Explorer**. To view the list of files with matching keywords in the **Results Viewer**, click the keyword in the **Data Explorer**. To view the file list in the directory, click the **Directory Listing** tab. To see the details of each file with matching keywords, click the **Keyword search** tab. See “Using the Result Viewer” on page 19.



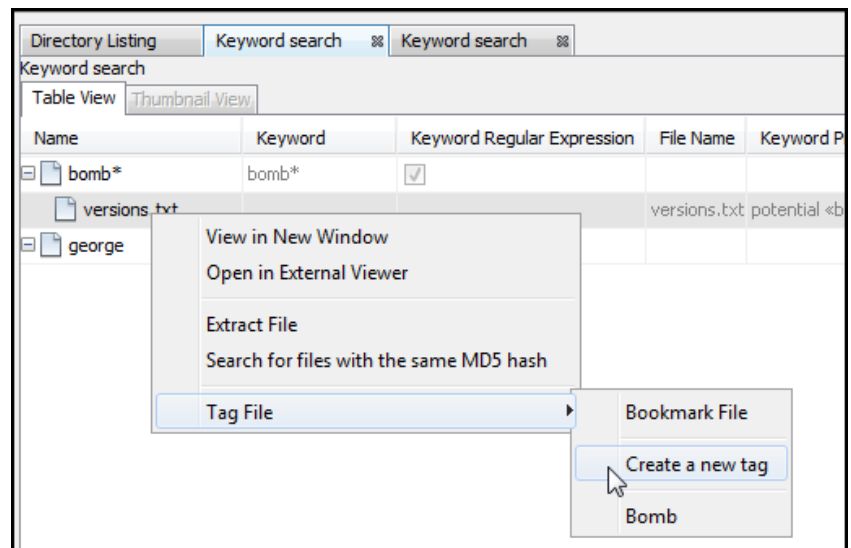
Saving File Locations

You can save the file locations of any file you see in the **Result Viewer**. After you run a keyword search, you may want to save the location of a file with a keyword match. Autopsy uses tags, which are similar to bookmark folders in a

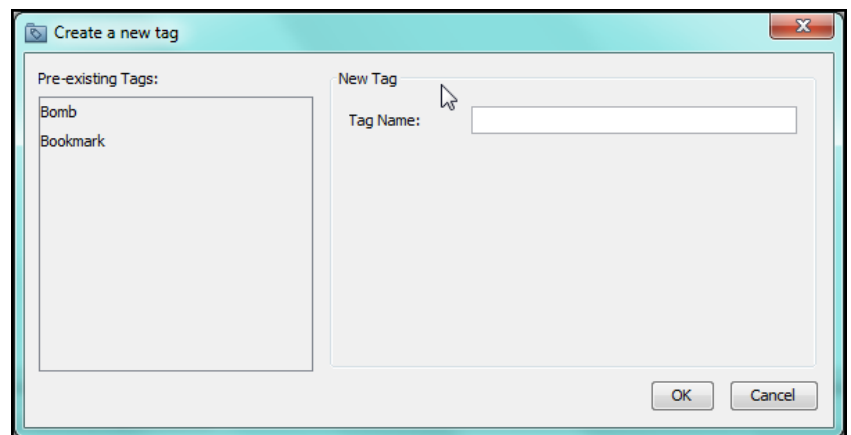
bookmark list in a web browser. After you create a tag, you assign the file to the tag. Tagging the file is similar adding a bookmark to a web page bookmark folder. Before you tag a file, you need to create a tag list.

To create a tag list

1. In the **Result Viewer**, click the **Keyword search** tab.
2. Right-click the file you want to tag, point to **Tag File** and then click **Create a new tag**.

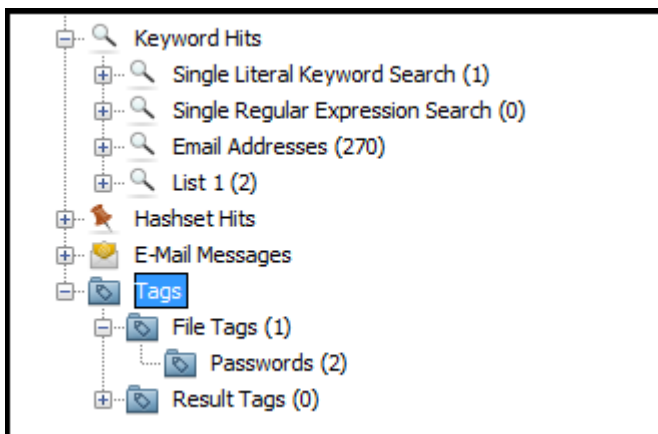


The **Create a new tag** window opens.



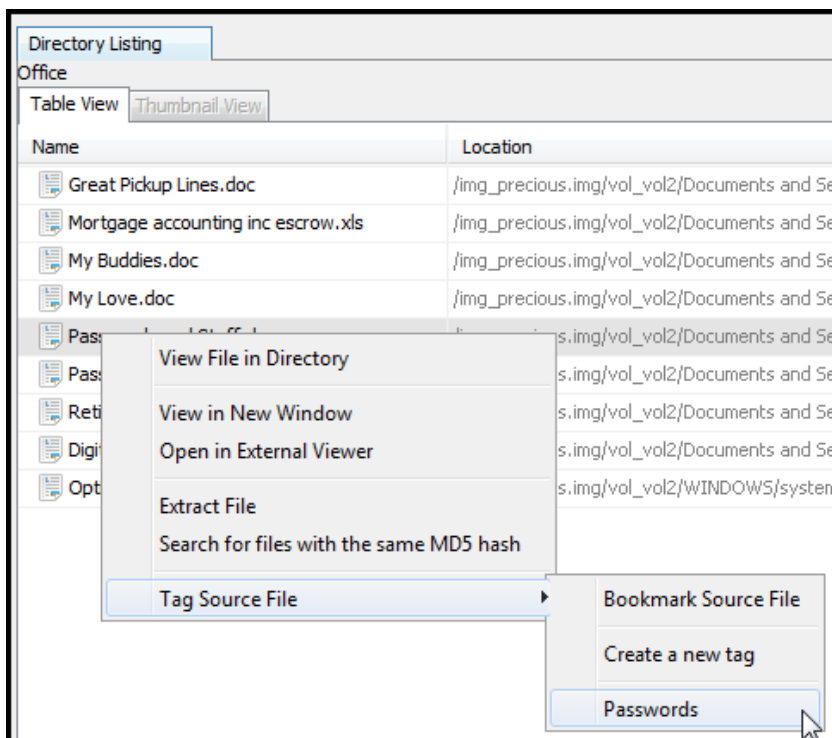
3. In the **Tag Name** box, type a descriptive name for the tag. Click **OK**.

The tag name appears under the **Tags** area in the **Data Explorer**.



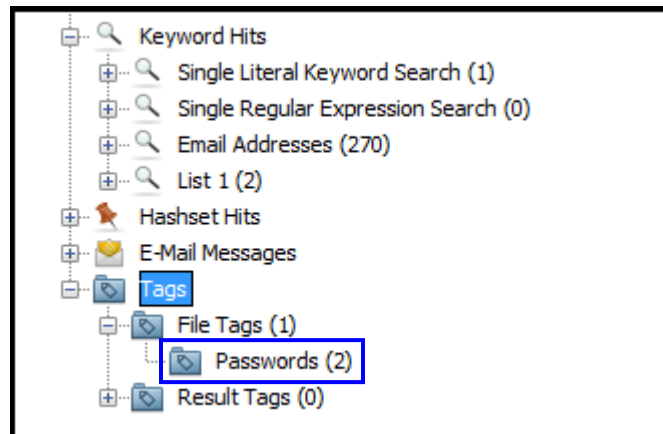
To tag a file

- In the **Result Viewer**, right-click the file you want to tag, point to **Tag Source File** and then click the name of the tag you want to apply to the file. In the example below, the tag **Passwords** is applied to the file.

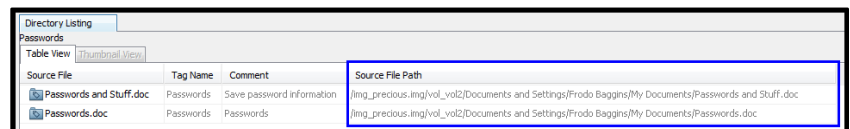


Chapter 4 – Searching File Contents

To see the list of files you marked, under the **Tags** area in the **Data Explorer**, click the tag name.



The list of tagged files and their locations appears in the **Result Viewer**.



You have now saved the location of the file for later use.

Chapter 5 – Generating Reports

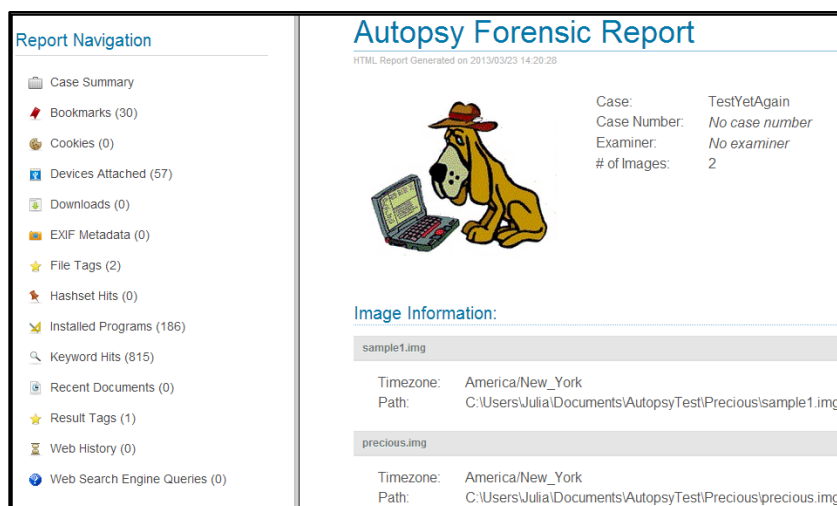
Autopsy enables you to create reports about the analyzed data and any files you tagged. You may want to create a report to include as part of your overall investigation report.

You can create reports in HTML and CSV format.



To open reports in CSV format, you need a spreadsheet program that supports viewing the CSV file format, such as Microsoft Excel.

An HTML report shows links in the left pane for each category of analyzed data. If you click a link, the data appears in the main browser window.



If you open a CSV report in Excel, the report uses a separate worksheet for each category of data. Each column contains one field of the report, which makes it suitable to convert into database format. Autopsy refers to CSV report format as Excel format.

In this section, you will learn about

- How to create HTML and Excel reports that show all available analyzed data
- How to create HTML and Excel reports that show only data you tagged (see “Saving File Locations” on page 29 for information about tags)
- How to create HTML and Excel reports that show data you select

At the end of this section, you will know how to create reports that contain information that is important to you.

Creating a Basic Report

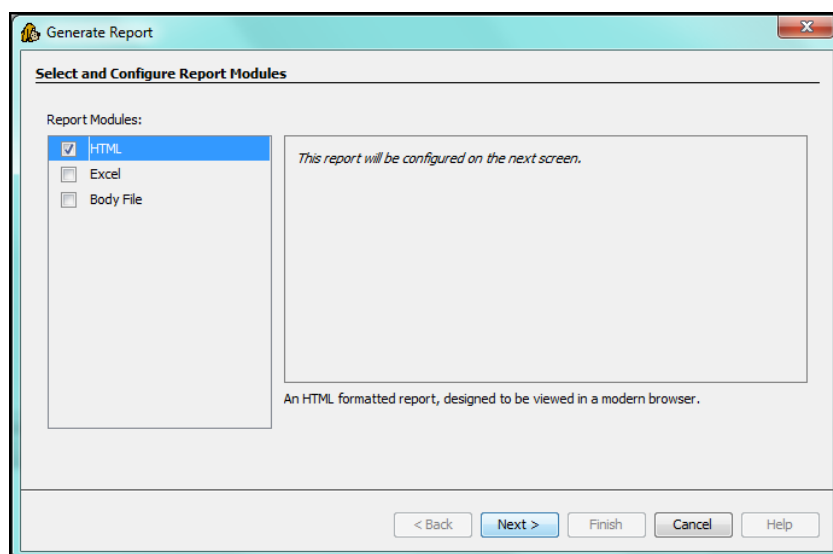
A basic report uses the default data selections. You need to choose the format you want to use for the report.

To create a basic report

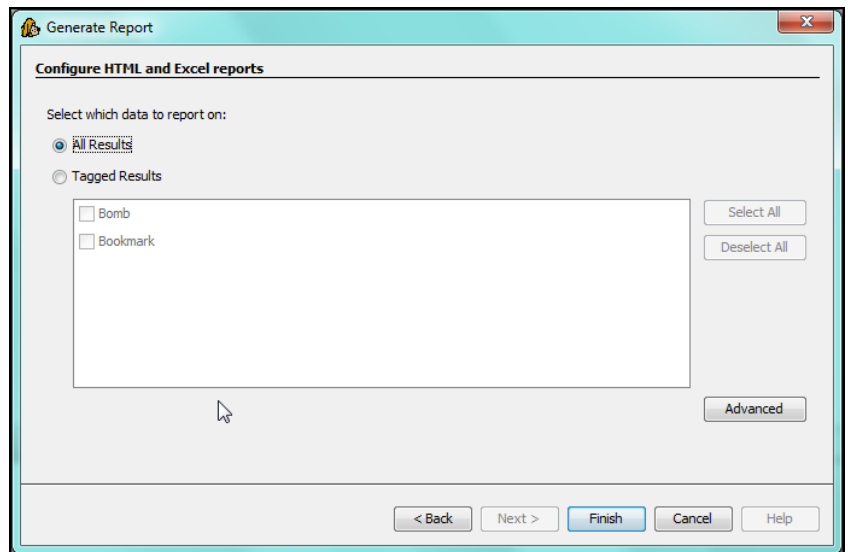


You can create more than one report format at the same time.

1. Click **Generate Report** on the toolbar. The **Generate Report** window appears.

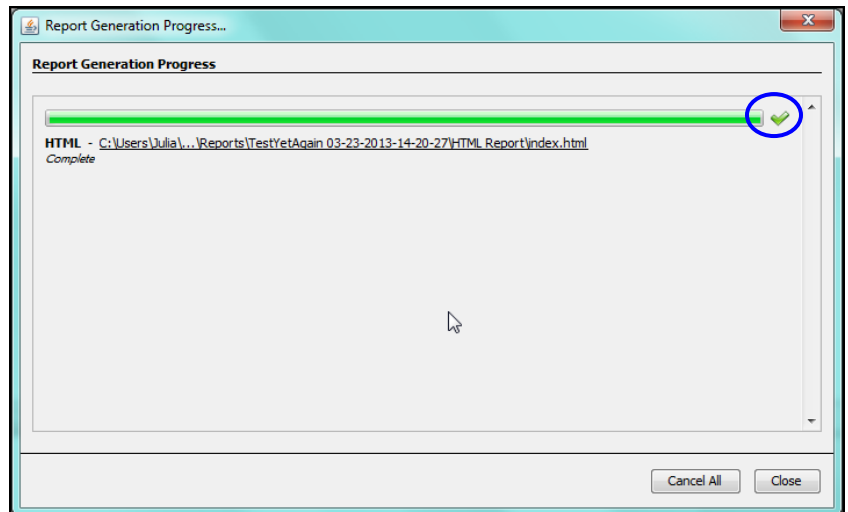


2. Select the report types you want to create and click **Next**. The **Generate Report** window updates to show **Configure HTML and Excel reports**.



By default, Autopsy reports all results.

3. To create a basic report, click **Finish**. The **Report Generation Progress** window appears.



Depending on the size of the report, it may take a few seconds to complete the report. The report is ready to view when you see the checkmark beside the progress bar. Autopsy shows links for the reports you generated.



If you want to look at a report later, you can find it in the **Reports** subdirectory of the case directory.

4. To view the HTML report, click the link for an HTML report. Your default browser opens and shows the report. To view an Excel report, click the link for an Excel report. Microsoft Excel opens and shows the report.
5. To close the window, click **Finish**.

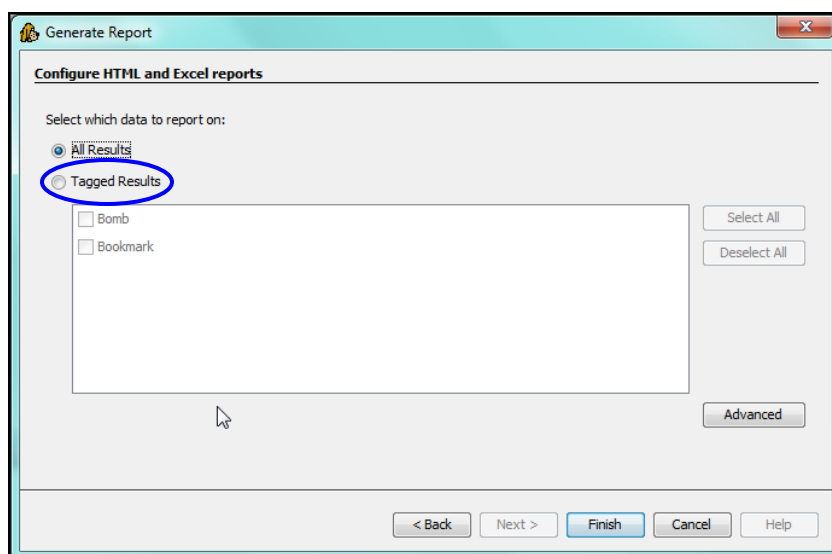
Creating a Custom Report

You can create two kinds of custom reports

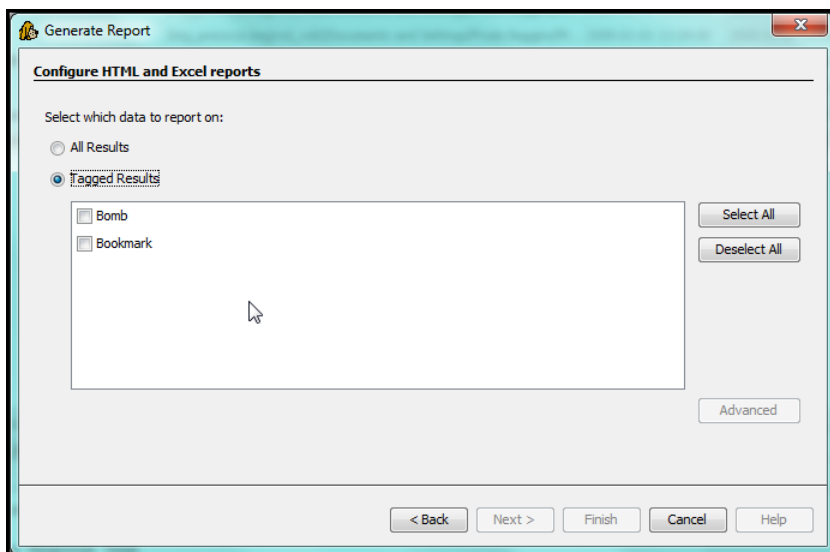
- A report that shows a list of files you tagged
- A report that shows only the data you select, for example, a report showing all Internet artifacts.

To create a report showing tagged files

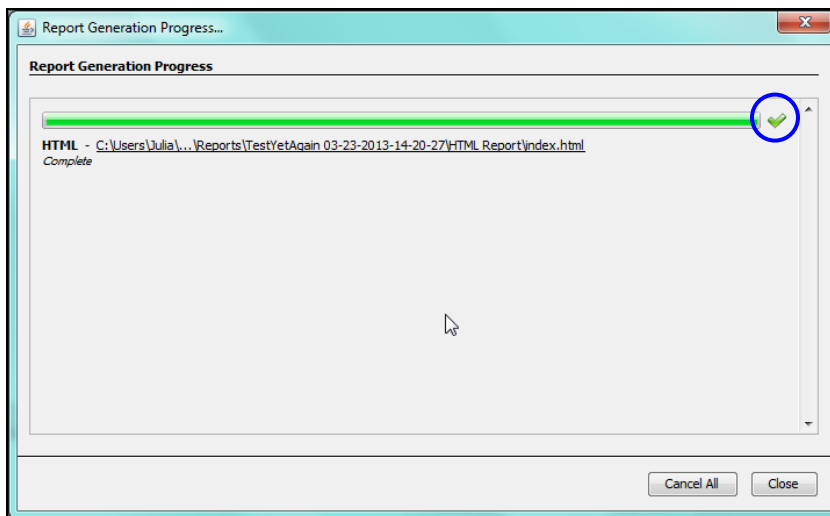
1. On the toolbar, click **Generate Report**. The **Generate Report** window appears.
2. Select the check box for the report types you want to create and click **Next**. The Generate Report window updates to show **Configure HTML and Excel reports**.



3. To create a report that shows a list of files you tagged, click **Tagged Results**. The tag names become available.



4. Select the tag name check box for the tags you want to report. Click **Finish**. The **Report Generation Progress** window appears.



Depending on the size of the report, it may take a few seconds to complete the report. The report is ready to view when you see the checkmark beside the progress bar.

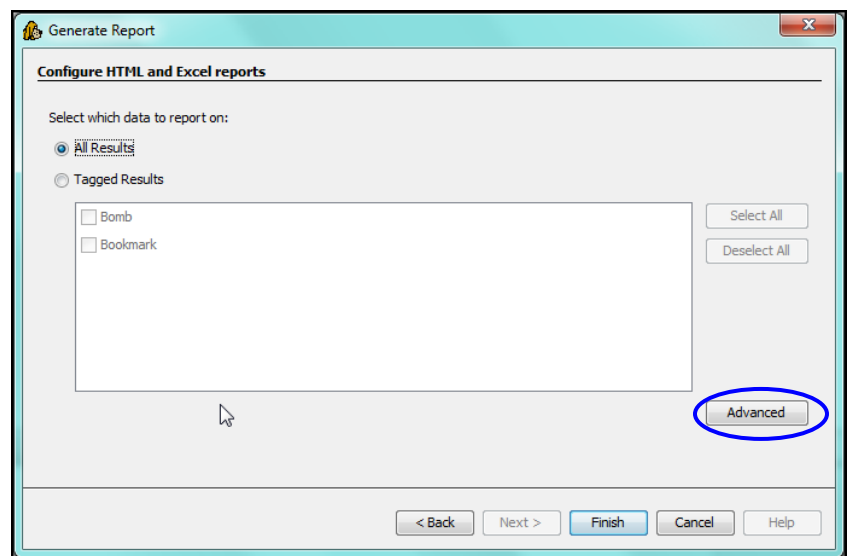
- When the report finishes, click the link for the report type you want to view. The following shows an example of a tagged results report in HTML format.

Bomb		
Comment	File Name	File Path
Bomb matches	versions.txt	/img_precious.img/vol_02/Program Files/Trillian/versions.txt
	versions.txt	/img_precious.img/vol_02/Program Files/Trillian/versions.txt

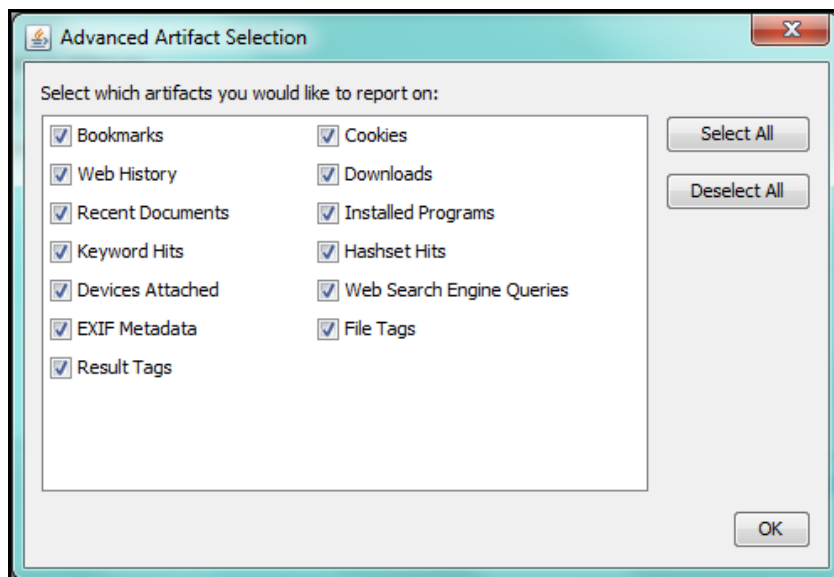
- To close the **Report Generation Progress** window, click **Finish**.

To create a report with selected categories of data

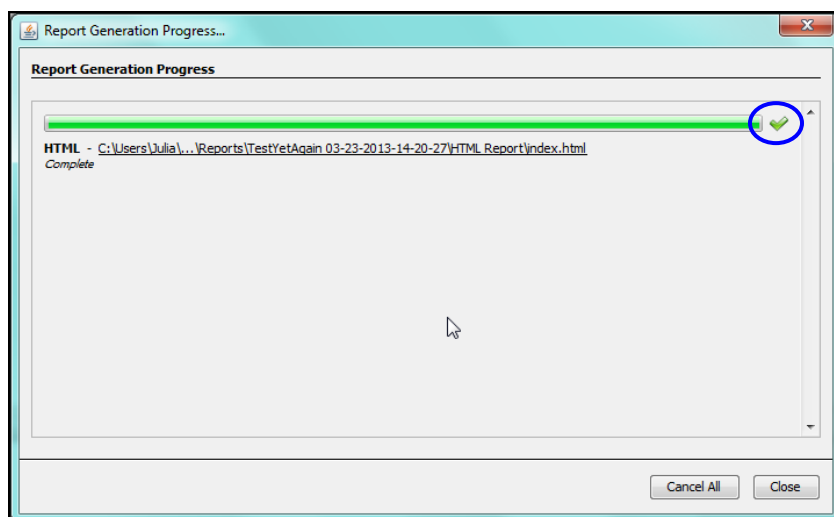
- On the toolbar, click **Generate Report**. The **Generate Report** window appears.
- Select the check box for the report types you want to create and click **Next**. The Generate Report window updates to show **Configure HTML and Excel reports**.



- Click **Advanced**. The **Advanced Artifact Selection** window appears.



4. Select the check box for the items you want to view in your report. To return to the **Configure HTML and Excel reports** window, click **OK**.
5. Click **Finish**. The **Report Generation Progress** window appears.



Depending on the size of the report, it may take a few seconds to complete the report. The report is ready to view when you see the checkmark beside the progress bar.

6. When the report finishes, click the link for the report type you want to view.
7. To close the window, click **Finish**.

Chapter 6 – Creating a Timeline

Each file in the disk image has information about time the file was create or changed, when it was modified, and when it was accessed.



If the files were copied to another storage device, such as a USB flash drive, before the image was created, the original time data may be lost. Some programs do not preserve the original file attributes when files are copied.

Autopsy bases timeline information on MAC time, which is a numeric representation of a file's time attributes, which are

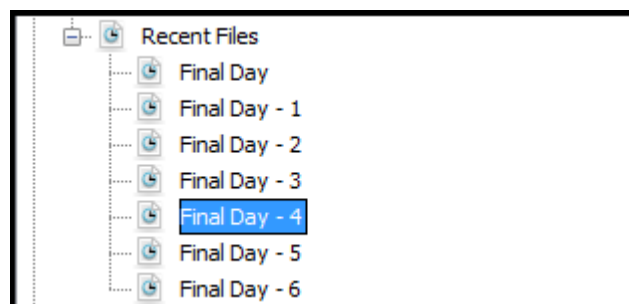
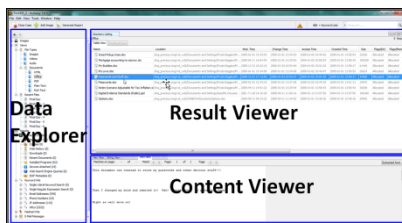
- Modification time - the last time the file contents changed
- Access time – the last the file was most recently opened to read the contents
- Change time – file permissions changed (Unix)
- Creation time – when the file was created (Windows)

Different operating systems treat change time and creation time differently. Unix file systems do not store creation time, and consider that a file changed when the file's metadata changed, not necessarily the file contents. Windows file systems store creation time and change time indicates when the internal file data table entry changed.

As part of the initial analysis, the **Recent Activity** ingest module reports the last seven days of activity on the disk in the **Recent Activity** section of the **Data Explorer**.



See the picture below if you need to locate the **Result Viewer**, or the **Data Explorer**.



Click the day you want to view and the results appear in the **Result Viewer**. If there was no activity on a given day, the **Result Viewer** will not show any results.

In this section, you will learn about

- How to create a graphical timeline using Autopsy's timeline feature
- How to create a timeline report

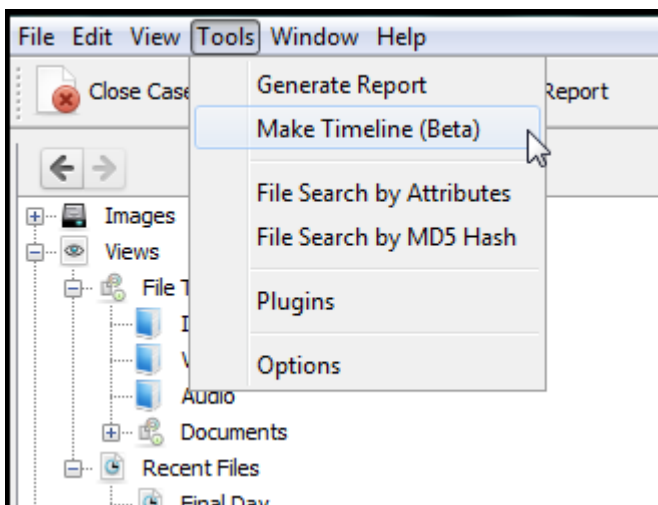
At the end of this section, you will know how to view information about the files in the disk image based on time.

Creating a Graphical Timeline

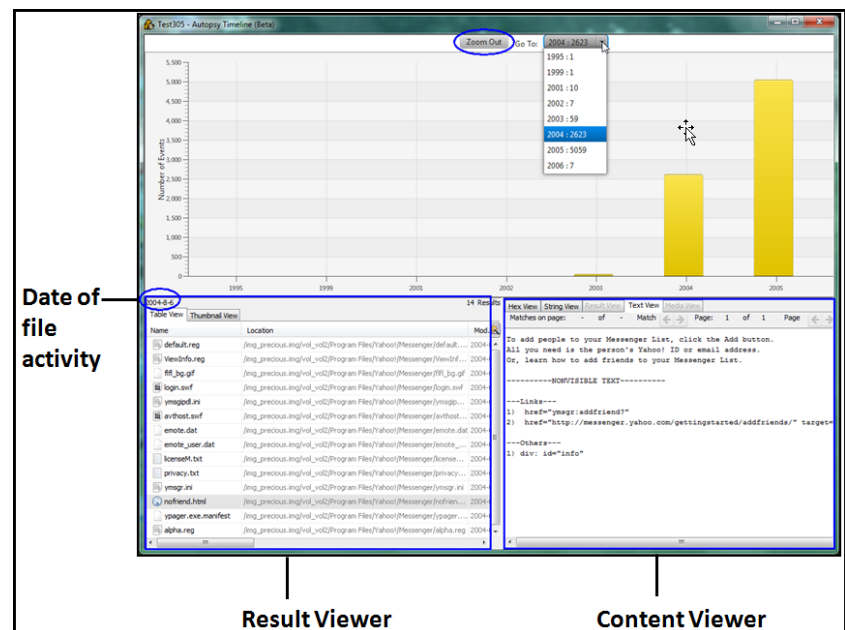
You can use the timeline feature in Autopsy to create a graphical view of the file timelines. This feature is currently in beta status; however, you may find the data useful to quickly view file activity based on a particular date.

To create a graphical timeline

1. On the **Tools** menu, click **Make Timeline (Beta)**.



The **Autopsy Timeline** window appears. You may have to minimize the main Autopsy window to view the timeline window.



2. To show the months when file activity took place, click the bar for the year you want to view.
3. To show the days when file activity took place, click the bar for the month you want to view.
4. To see the file activity for a particular day, click the day you want to view. The list of files appears in the **Result Viewer**.
5. To view the file contents, click a file in the **Result Viewer**. The file contents appear in the **Content Viewer**.
6. To return to a month or year view, click **Zoom Out**.

Creating a Timeline Report

Autopsy enables you to create a report containing the time information about each file in the disk image. You can view the report with a spreadsheet program, such as Microsoft Excel, and work with the data outside of Autopsy. Using a spreadsheet view you can view the time information for every file in the disk image, whereas with the timeline view in Autopsy, you can only see the files on a per day basis.

Autopsy generates a text delimited file that you can import into Excel. The delimiter is "|" (vertical bar). For each item in the file system, the spreadsheet contains a subset of the information shown in the directory listing in the **Result Viewer**.

The spreadsheet does not show column headings. It shows the information in separate columns in the following order

- MD5 sum
- File or directory name, including the full path
- Meta Id
- File permissions
- User Id
- Group Id
- File size
- Modified time
- Access time
- Change time
- Created time

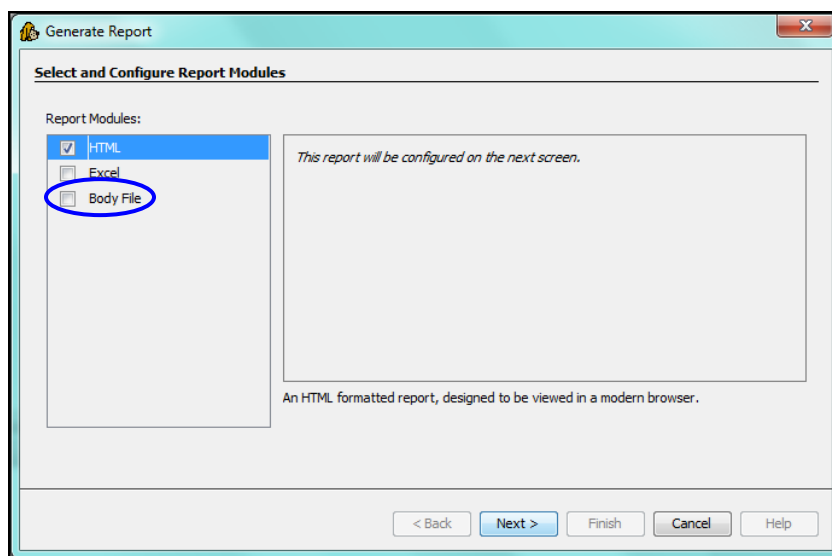
You can use the spreadsheet features to sort by modification time, access time, creation time, and change time.



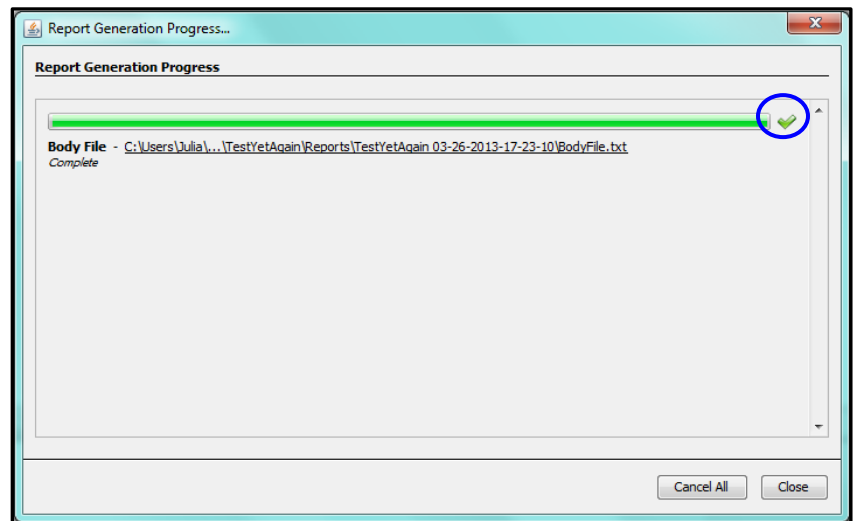
To view the file, you need a spreadsheet program that can open delimited files, such as Microsoft Excel.

To create a timeline report

1. On the toolbar, click **Generate Report**. The **Generate Report** window appears.



2. Under **Report Modules**, select the check box **Body File**. Clear the check boxes for any other modules and click **Finish**. The **Report Generation Progress** window appears.



Depending on the size of the report, it may take a few seconds to complete the report. The report is ready to view when you see the checkmark beside the progress bar.

To open the file with your default program (typically Notepad), click the **Body File** link.

3. To open the file in Excel or another spreadsheet program, run the program and open the file BodyFile.txt in the directory shown in the **Report Generation Progress** window.
4. Follow the procedure in your spreadsheet program to import a text file and be sure to specify the character "|" (vertical bar) as the delimiter.

Chapter 7 – Collecting Files for Later Analysis

You can extract data from the disk image to examine outside Autopsy. For example, you may want to

- Examine data with other tools
- Capture information to attach to a report
- Examine unallocated space as a single, large file because it may be easier to use with other data carving tools

The following sections describe how to:

- How to extract file and directory contents
- How to extract unallocated disk space

At the end of this section you will know how to extract information from the disk image to use with other programs outside Autopsy.

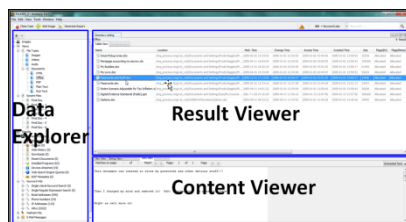
Extracting File and Directory Contents

You can extract individual files and entire directories of files. You may want to extract files you tagged, files that Autopsy identified during ingest, such as Microsoft Offices files, or other files in the disk image. You may also want to extract the entire contents of the **Documents and Settings** directory from one of the user directories.

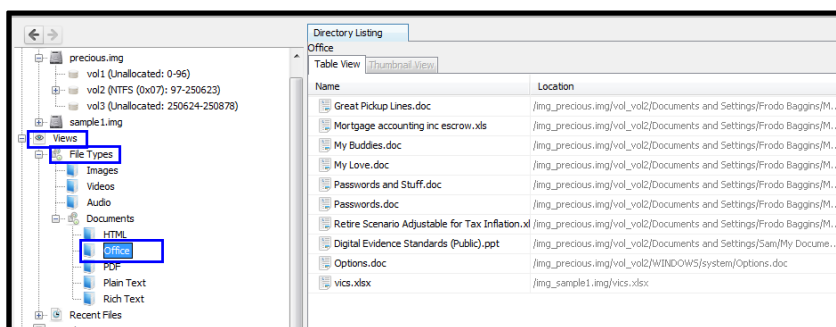
To extract file and directory contents



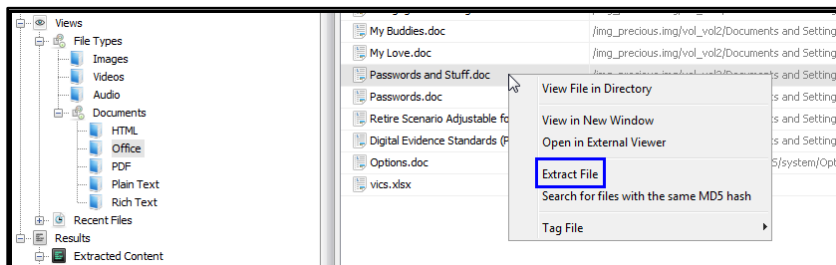
See the picture below if you need to locate the **Result Viewer**, **Data Explorer**, or **Content Viewer**.



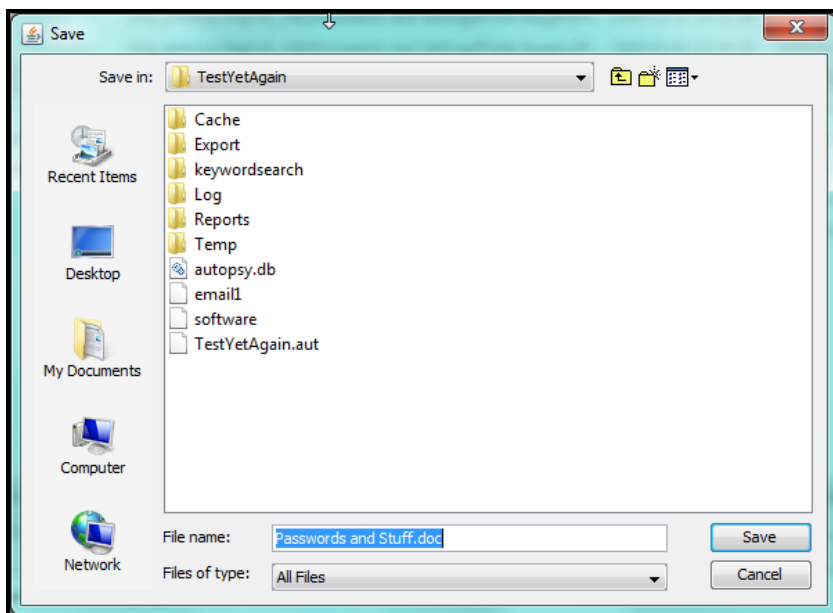
1. In the **Data Explorer**, click the folder that contains the file or directory you want to extract. For example, click **Views** to see the analyzed files.
2. Click the subfolders until you see the folder contents in the **Result Viewer**. In the example, to see the list of Microsoft Office files in the **Result Viewer**, click the folders **View**, **File Types**, **Documents**, and **Office**.



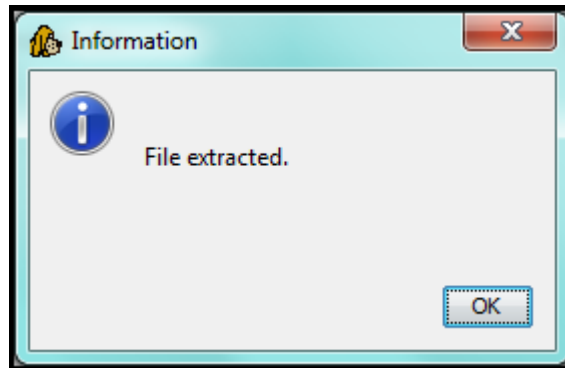
3. In the **Result Viewer**, right-click the file or directory that you want to extract and then click **Extract File**.



A new window opens to enable you to save the file.



4. If you want to save the file in a different directory, navigate to it.
5. If you want to change the file name, in the **File name** box, type the file name you want to use.
6. Click **Save**. The **Information** dialog box appears.



7. To close the box, click **OK**.

You have finished extracting the file.

Extracting Unallocated Disk Space

Unallocated disk space is composed of chunks of the file system that are not currently in use. Unallocated space can store deleted files and other interesting artifacts.

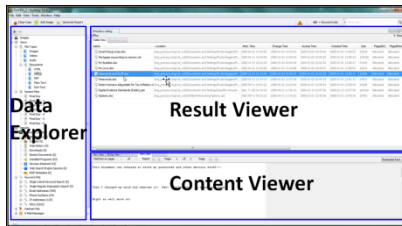
You can extract the individual contents of the unallocated space using the same steps as extracting individual files, or you can extract the space to a single file.

In the image, unallocated space is stored in blocks with distinct locations on the system. However, because of the way various carving tools work, it may be more useful to collect the data into a single, large file.

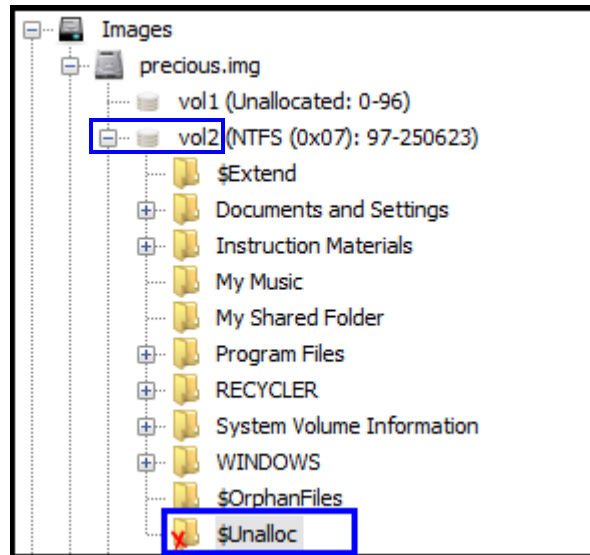
To extract unallocated space as individual blocks



See the picture below if you need to locate the **Result Viewer**, or the **Data Explorer**.



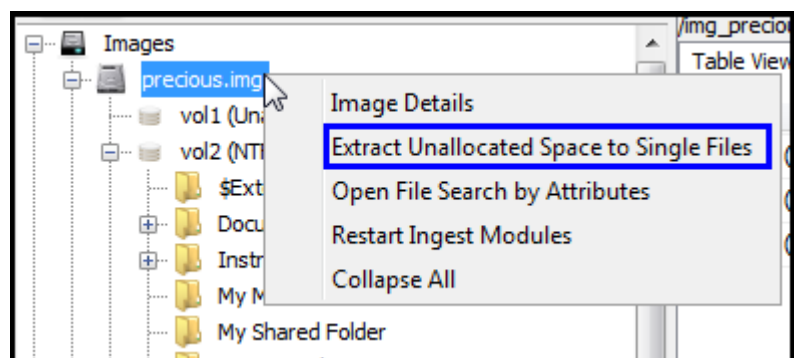
1. In the **Data Explorer**, under the folder for the image name, click the volume (in the example below, the volume is **vol2**) and click the folder **Unalloc**.



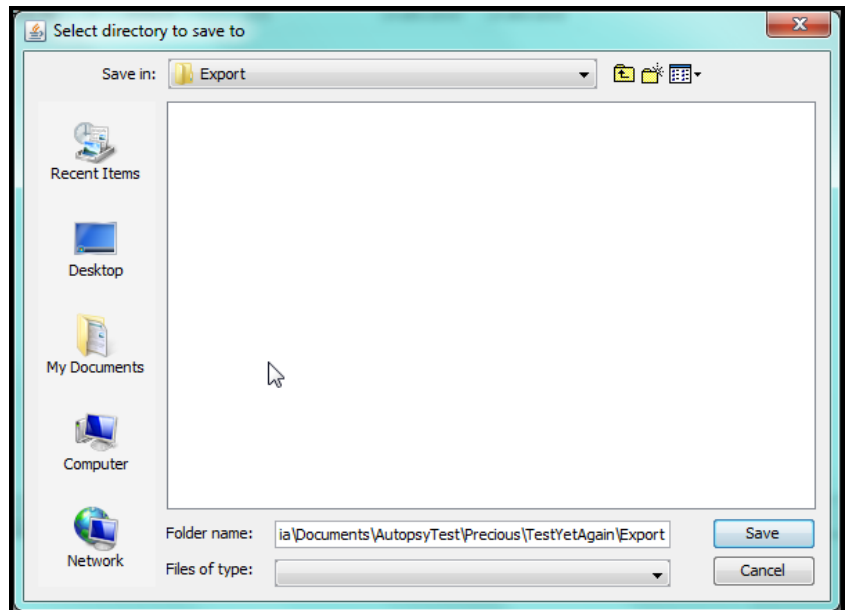
2. The list of files appears in the **Result Viewer**. You can extract the file the same way you can extract any other type of file under the **Directory Tree** tab of the **Data Explorer** (see "To extract file and directory contents" on page 45).

To extract unallocated space into a single file

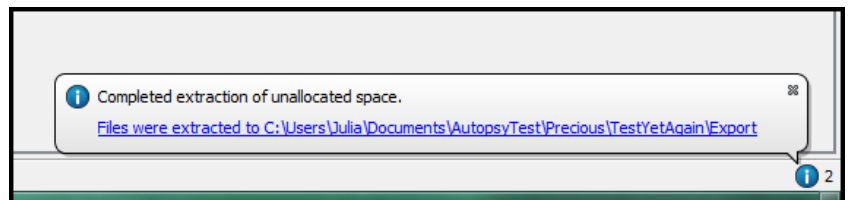
1. In the **Data Explorer**, under the **Images** folder, right-click the image name and then click **Extract Unallocated Space to Single Files**.



The **Select directory to save to** window appears.



2. If you want to save the files in a different directory, navigate to it. Click **Save**. The progress indicator in the bottom right corner of the screen shows the status of the extraction. A message appears when the process completes.

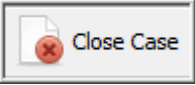
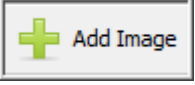
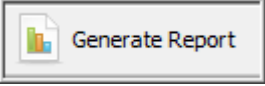

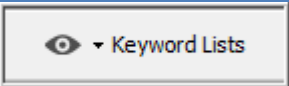



3. To view the extracted file, navigate to the directory shown in the message. Files are named according to *ImageName-Unalloc-ImageObjectID-VolumeID.dat*. This naming scheme ensures that no duplicate file names occur, even if there are two images with the same name in a case.

You have finished extracting the unallocated space.

Appendix A: Toolbar Reference

This toolbar reference provides you with reminders about each button on the toolbar and where to find related information in the manual.

Icon	Purpose
	Closes the currently open case.
	Opens the Add Image wizard and takes you through the steps to add a disk image and configure ingest. See “Adding a Disk Image” on page 6 for information.
	Opens the Generate Report window that enables you to create basic or custom reports. See “Chapter 5 – Generating Reports” on page 33 for information. You can also create a timeline report. See “Creating a Timeline Report” on page 42
	Shows ingest progress messages.
	Opens the Keywords Lists menu. You can search based on existing lists, and manage new and existing lists. See “Creating and Managing Keyword Lists” on page 26.
	Searches all files for the simple keyword you type in the box.

Appendix B: Troubleshooting

This section provides information to help you understand error messages you may see in Autopsy, possible causes, and suggested solutions.

Message	Possible Cause	Solution
The ingest message list shows "No known bad database set"	You did not supply a hash database that lists known bad files.	If you want Autopsy to analyze known bad files, you need to provide separate databases for both known good and bad files. If a database contains both sets of definitions, such as the NIST NSRL database, you must designate it as a list of good or bad files. You may find information on the Internet about methods to separate the database into two parts.
Error extracting file from image: (ntfs_uncompress_compunit: Phrase token offset is too large: 1 (max:0))	This message occurs when trying to process a compressed NTFS file that is corrupt. This can occur when a file has been deleted and the clusters have been reallocated to another file.	Compare the MD5 sum of the file you received with that of the original file. If it matches, the file is corrupt and you need to capture a new image from the original disk. If the MD5 sum does not match, the image was corrupted in transit. Ask the originator of the image to send it to you again.
Options window shows "Error: Index does not exist"	After you add a hash database, Autopsy needs to create an index to use it.	In the Options window, click Index .
In the Data Explorer, the file status of all the files is "unknown".	<ul style="list-style-type: none"> You did not add a hash database to categorize files as known or unknown. You did not identify the hash database you added as NSRL, which indicates that the files in the database are known good files. 	<ul style="list-style-type: none"> If you did not add a hash database, follow the steps in "Adding a Hash Database" on page 13 to add one. You must identify a hash database as either NSRL or Known Bad; it cannot function as both types. Either you need to add a hash database for known good files (NSRL), or change the type of database you already added.

Appendix C: FAQ

This section provides answers to common user questions.

How do I speed up ingest?	<p>You can disable some ingest modules, such as the Exif Parser module, which can take a long time to run on a large disk image. You can also exclude the unallocated disk space, although you may miss some important information. See “</p> <p>Configuring Disk Analysis” on page 8 for more information.</p>
I started ingest through the wizard, but I want to add or remove modules. How do I stop it and restart it?	<p>To cancel ingest, right-click the blue progress bar in the bottom right corner of the window and then click Cancel Process. See “To cancel ingest” on page 11. After you reconfigure ingest, to restart it, right-click the image name in the Data Explorer and then click Restart Ingest Modules. See “To restart ingest” on page 12.</p>
Can I add more than one disk image to a case?	<p>Yes. On the toolbar, click Add Image and the Add Image wizard will guide you through the process.</p>
What disk image formats can I use?	<p>You can use raw disk images, which can be single or multiple files, and E01 (EnCase) format.</p>
What file systems can Autopsy analyze?	<ul style="list-style-type: none"> • NTFS • HFS+ • ISO9660 • Ext2, Ext3 • FAT12, FAT16, FAT32 • UFS
How do I remove a disk image from a case?	<p>You cannot remove a disk image from a case. You need to create a new case and ensure that you only add the images you want to analyze.</p>
Why is the timeline information empty?	<p>Timeline features are only supported for Windows file system formats (FAT, NTFS).</p>
Why does the search for IP addresses show items that are not IP addresses?	<p>The search tries to match four numbers separated by periods, which is a standard IP address format. However, this format is often used for other types of information, such as version numbers. If the list contains too many unrelated results, you may need to create a custom search.</p>

Glossary

Apache SOLR	An open-source search server based on the Lucene Java search library
CSV	Comma separated file, a text file with a series of fields separated by a delimiter
E01	EnCase disk image format
EnCase	EnCase computer forensics software by Guidance Software Inc.
Ext2	Extended file system format version 2, used by Linux operating systems
Ext3	Extended file system format version 3, used by Linux operating systems
FAT	File Allocation Table, file system formats used by Windows operating systems FAT12, FAT16, FAT32
GIF	Graphic Interchange Format, a graphics file type/extension
HFS+	Hierarchical File System Plus, used by Apple operating systems
HTML	Hyper-Text Markup Language
Ingest	Autopsy's term for analyzing the contents of a disk image
IP address	Internet Protocol address
ISO9660	File system for optical disk media, also known as Compact Disk File System (CDFS)
JPG	Graphics file type/extension (lossy compressed 24-bit color image storage format developed by the Joint Photographic Experts Group)
MAC	Modify, Access, Create and Change time, a numeric representation of file date and time
MD5	Message Data 5 – a one way hash function
Metadata	Properties of a file attached to the file by some programs
NIST	National Institute of Standards and Technology
NSRL	National Software Reference Library
PNG	Portable Network Graphic, a graphics file type/extension
Tag	A file bookmark in Autopsy
UFS	Unix file system, also known as Berkeley Fast File System
URL	Universal Resource Locator
UTF	Universal Transformation Format

Index

B

bookmark. *See* tag

C

cancelling ingest, 11

case, 4

 creating a case, 4

content viewer, 18, 21, 22

 hex view, 21

 media view, 21

 new window, 22

 result view, 21

 string view, 21

 text view, 21

 using an external viewer, 23

D

data explorer, 12, 18, 21

 extract files, 45

 keyword hits, 29

 unallocated disk space, 48

deleted files. *See* unallocated disk space

delimiter, 42

disk analysis. *See* ingest, *See* ingest

disk image

 adding a disk image, 6

 adding an image, 7

 format, 2

 formats, 52

E

Excel, 35, 42

export. *See* extract

extract files

 collecting files for later analysis, 45

 extracting unallocated disk space as individual blocks, 48

F

file system

 Ext2, Ext3, 2, 52

 FAT, 2, 52

 HFS, 2, 52

ISO9660, 2, 52

NTFS, 2, 52

UFS, 2

H

hash database, 8, 13, 51

 adding a hash database, 13

 EnCase, 2, 13

 HashKeeper, 1

 known bad files, 14

 NIST NSRL, 2, 13

I

image. *See* disk image

ingest, 4, 8

 cancelling ingest, 11

 configuring disk analysis, 8

 restarting ingest, 12

 stopping ingest, 11

ingest module

 exif parser, 8

 hash database, 8

 keyword search, 8, 18, 21, 26

 recent activity, 40

 Thunderbird parser, 8

internet artifacts, 8, 36

K

keyword search

 creating and managing keyword lists, 26

 searching file contents, 24

 searching using built-in keywords, 25

M

metadata, 2, 8, 18, 21, 40, 53

R

report

 creating a basic report, 34

 creating a report showing tagged files, 36

 creating a report with selected categories of data, 38

 creating a timeline report, 43

- CSV format, 33
- generating reports, 33
- HTML report, 33
- Microsoft Excel, 33, 35
- restarting ingest, 12
- result viewer, 18, 29, 42
 - directory listing, 18
 - extract files, 45
 - thumbnail view, 18
 - unalloc, 48
 - using the result viewer, 18

S

- search. *See* keyword search
- Sleuth Kit, 1, 2

T

- tag
 - creating a report showing tagged files, 36
 - creating a tag list, 30
 - tagging a file, 31
- timeline, 40
 - content viewer, 41
 - creating a timeline, 41
 - creating a timeline report, 43
 - Microsoft Excel, 42
 - result viewer, 41

U

- unallocated disk space, 8, 45
 - extracting unallocated space as individual blocks, 48
 - extracting unallocated space into a single file, 48
- unalloc, 48