# PERFORM A FORENSIC ANALYSIS THROUGH "AUTOPSY" SLEUTH KIT


**Create By :-**

- **Aditya_Bhalsod (175690693001)**
- **Sachin_Parmar (185693693016)**

# Introduction of autopsy

→ The Autopsy Forensic Browser is a graphical interface to the The Sleuth Kit and other digital investigation tools. Together, they can analyse Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3, etc.).

→ Autopsy 3 is Java-based and designed to be an end-to-end platform for digital forensics. That means that it can be extended by other developers. Full details can be found on the sleuthkit.org site.

→ Autopsy 2 is an old-school HTML-based interface. You can get the list of official features at the sleuthkit.org site.

- **Cases and Adding Data Sources**
  - Cases
  - Data Sources
  - UI Layout

- **Automated Analysis (Modules)**
  - Ingest Modules
  - Recent Activity Module
  - Hash Database Lookup Module
  - File Type Identification Module
  - Embedded File Extraction Module
  - EXIF Parser Module
  - Keyword Search Module
  - Email Parser Module
  - Extension Mismatch Detector Module
  - E01 Verifier Module
  - Android Analyser Module
  - Interesting Files Identifier Module
  - PhotoRec Carver Module

- **Manual Analysis**
  - Tree Viewer
  - Result Viewer
  - Content Viewer
  - Image Gallery Module
  - File Search
  - Ad Hoc Keyword Search
  - Timeline
  - STIX
  - Logs, Output, and Progress

- **Reporting**
  - Tagging
  - Reporting

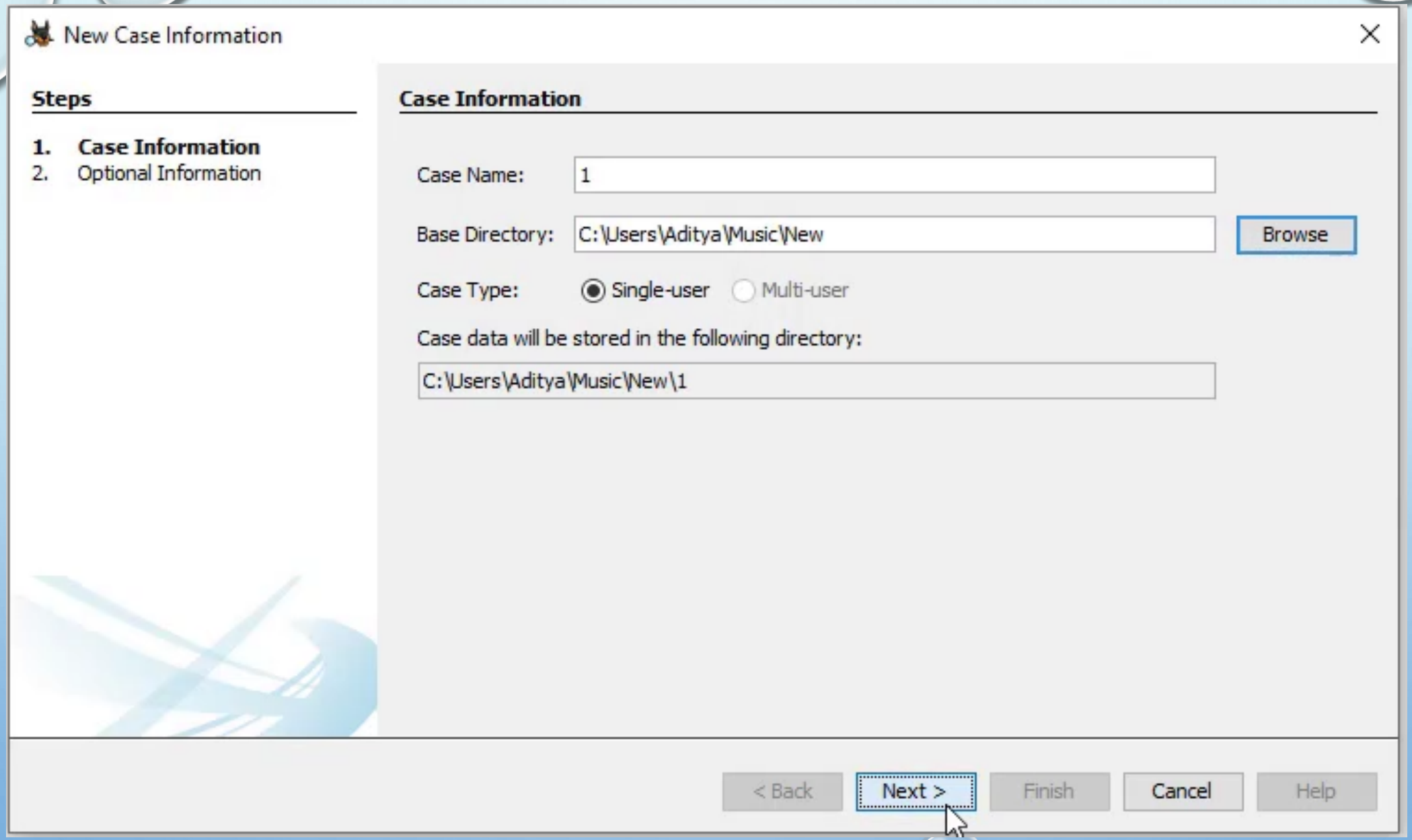
# Creating a Case


- 04:15

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.


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

- 04:24

# Opening a Case

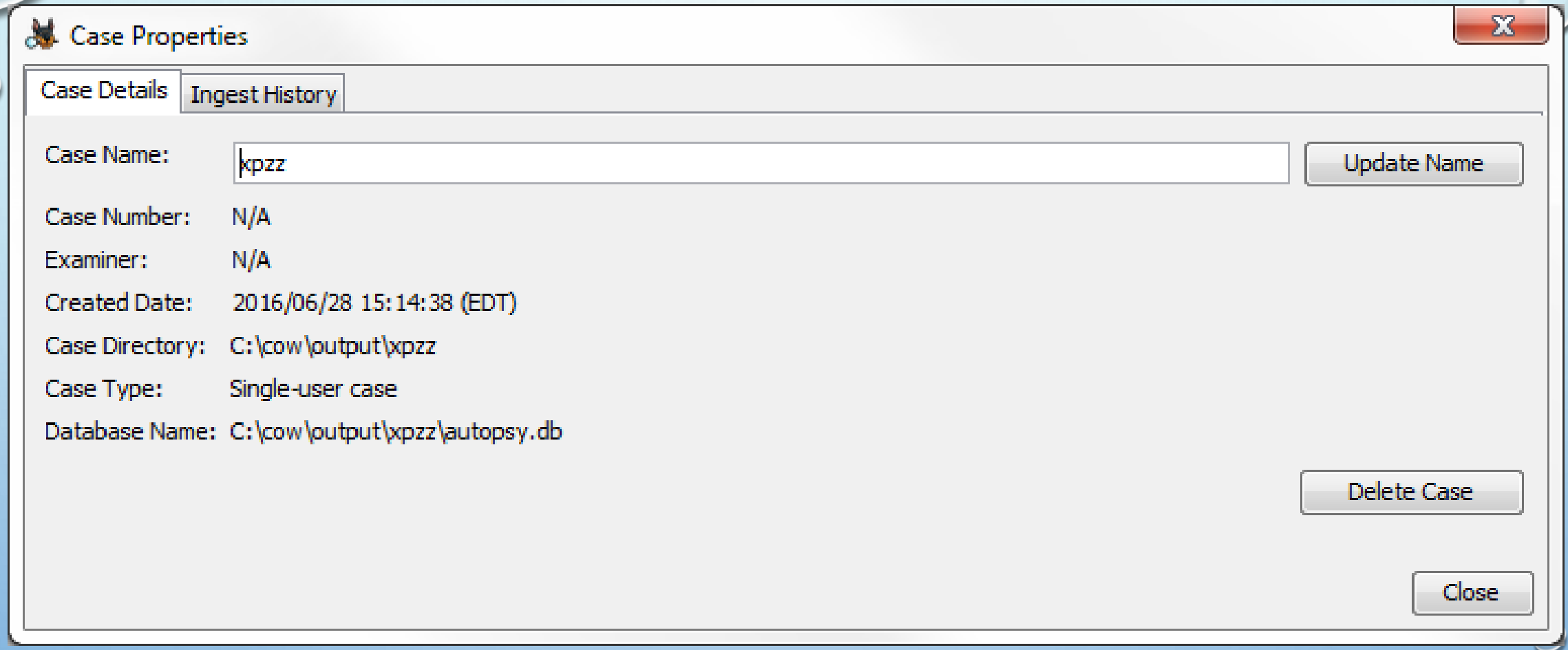
To open a case, either:

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

Navigate to the case directory and select the ".aut" file.

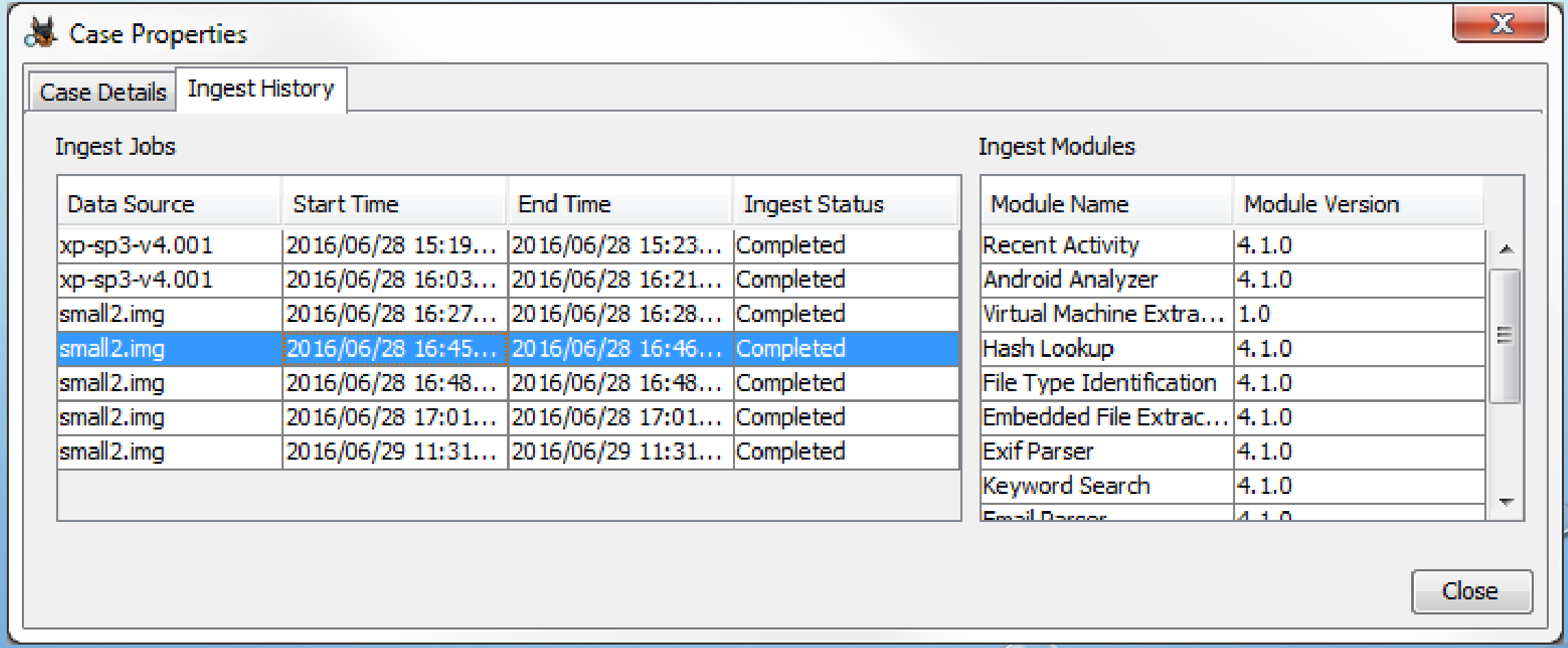
# Viewing Case Properties

You can view the case properties by going to the "Case" menu and clicking "Case Properties".
This will open a screen similar to one of the two following screenshots:




https://sleuthkit.org/autopsy/docs/user-docs/4.3/single-user-case-properties.PNG

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.




https://sleuthkit.org/autopsy/docs/user-docs/4.3/case-properties-history-tab.PNG

# Data Sources

A data source is the thing you want to analyse. 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)

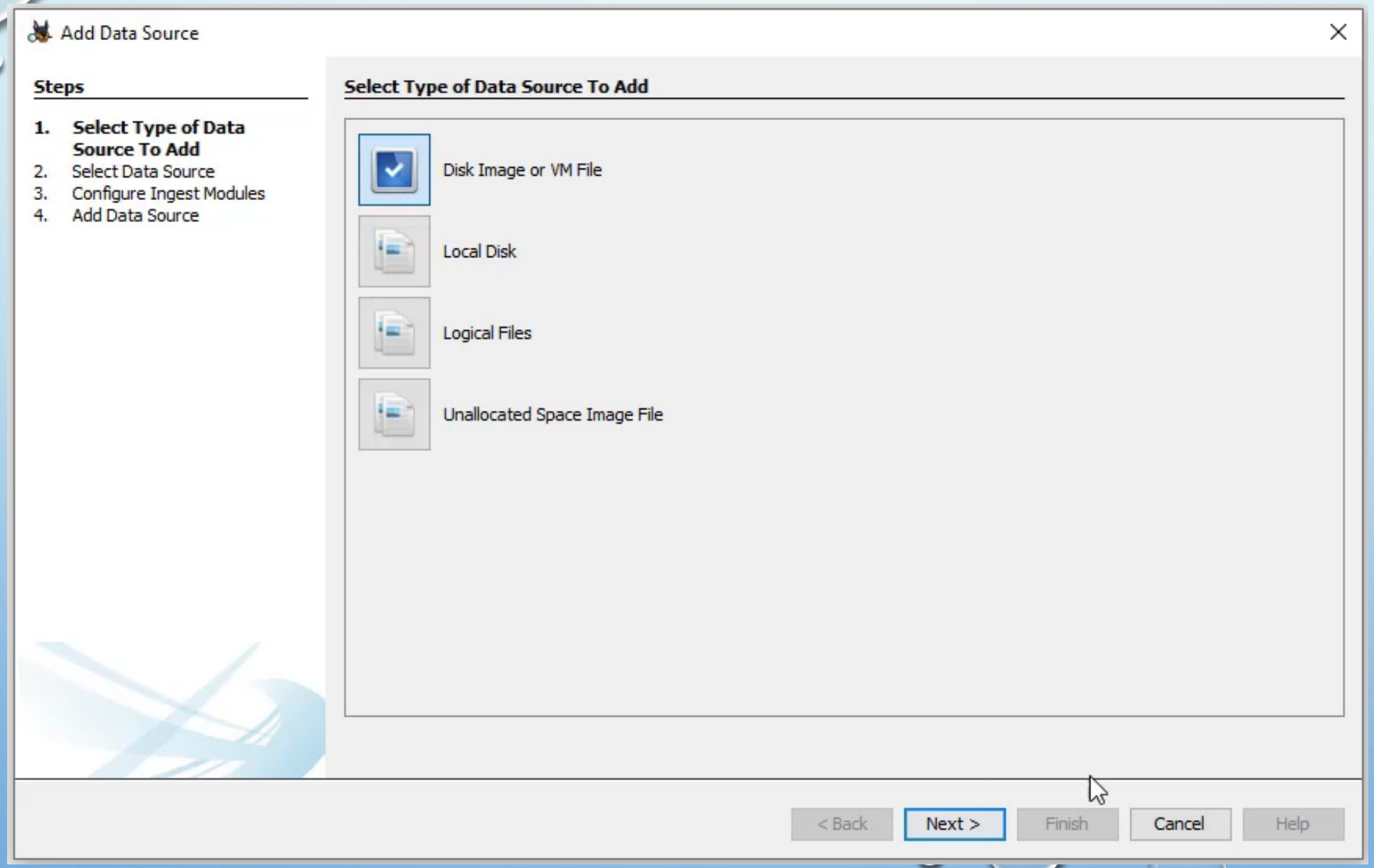
# Adding a Data Source

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.

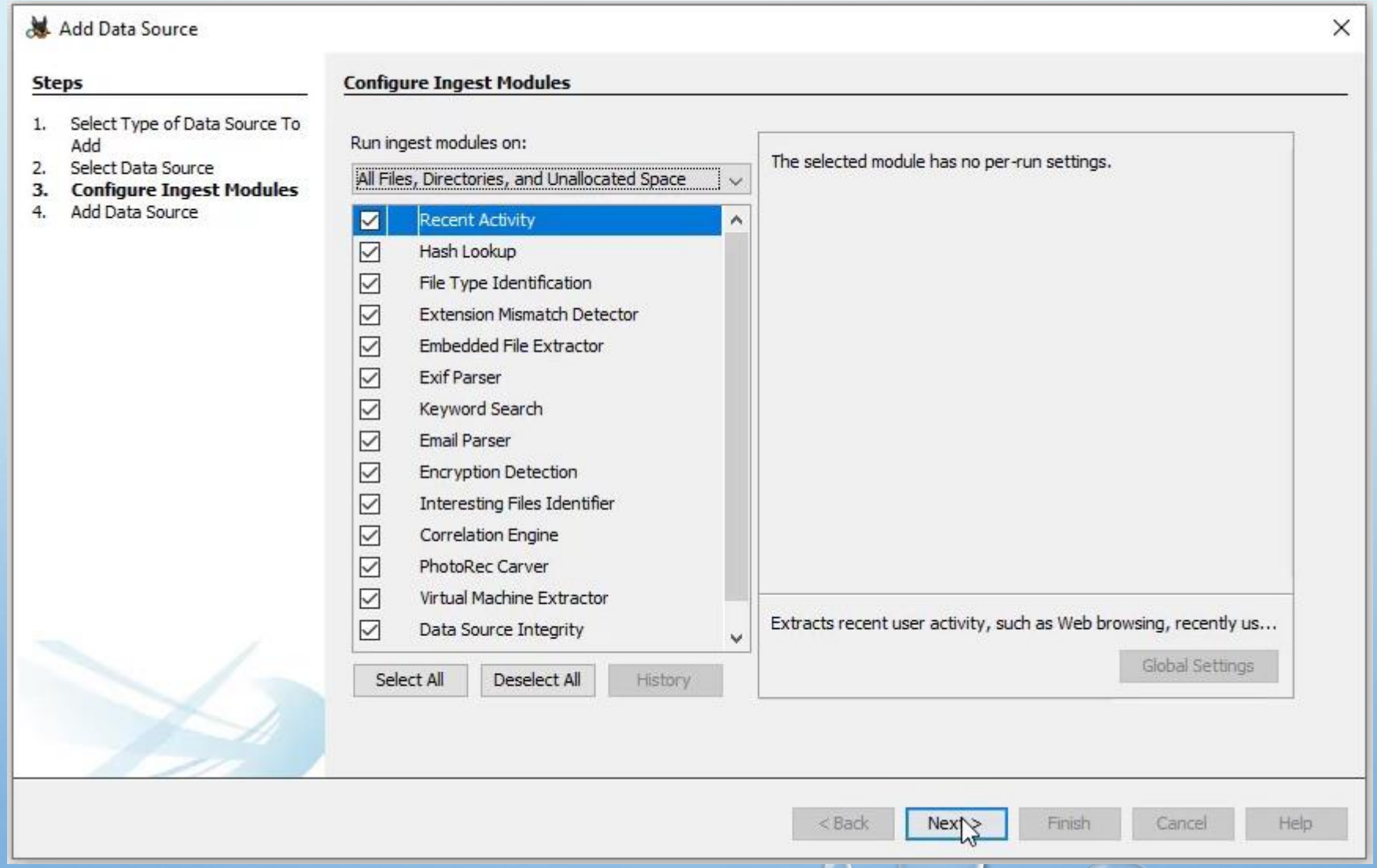


2) You will be prompted to specify the data source to add. This screen varies based on the data source type. Details on adding each type of data source are provided below.

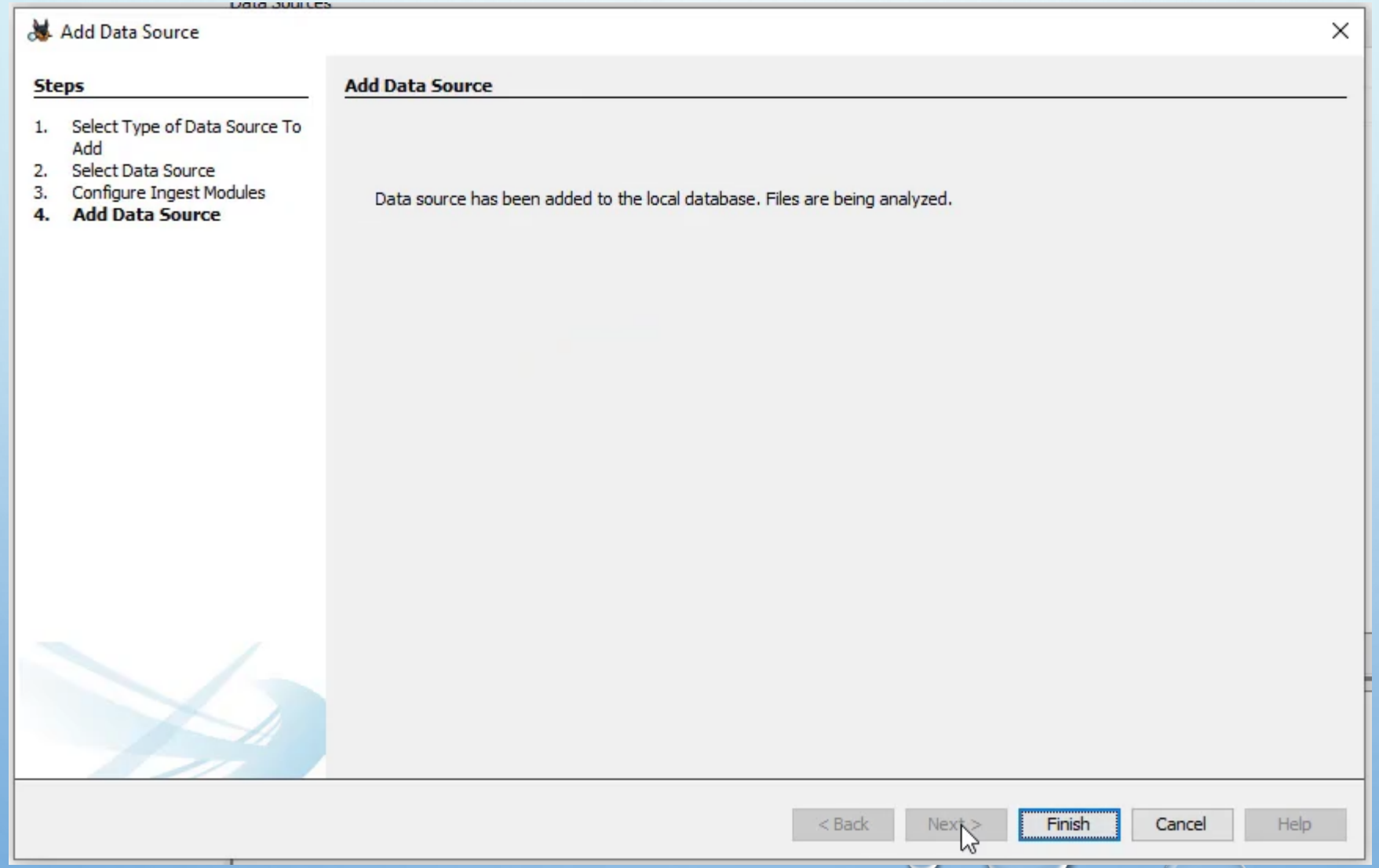
NOTE: If you are adding a data source to a multi-user case, ensure that all Autopsy clients will have access to the data source at the same path. We recommend using UNC paths to ensure this consistent mapping.

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 analysed 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.




- 05:10

6) After the ingest modules have been configured and the basic examination of the data source is complete, the ingest modules will begin to analyse 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 time zone that the disk image came from. This is most important for when adding FAT file systems because it does not store time zone 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.

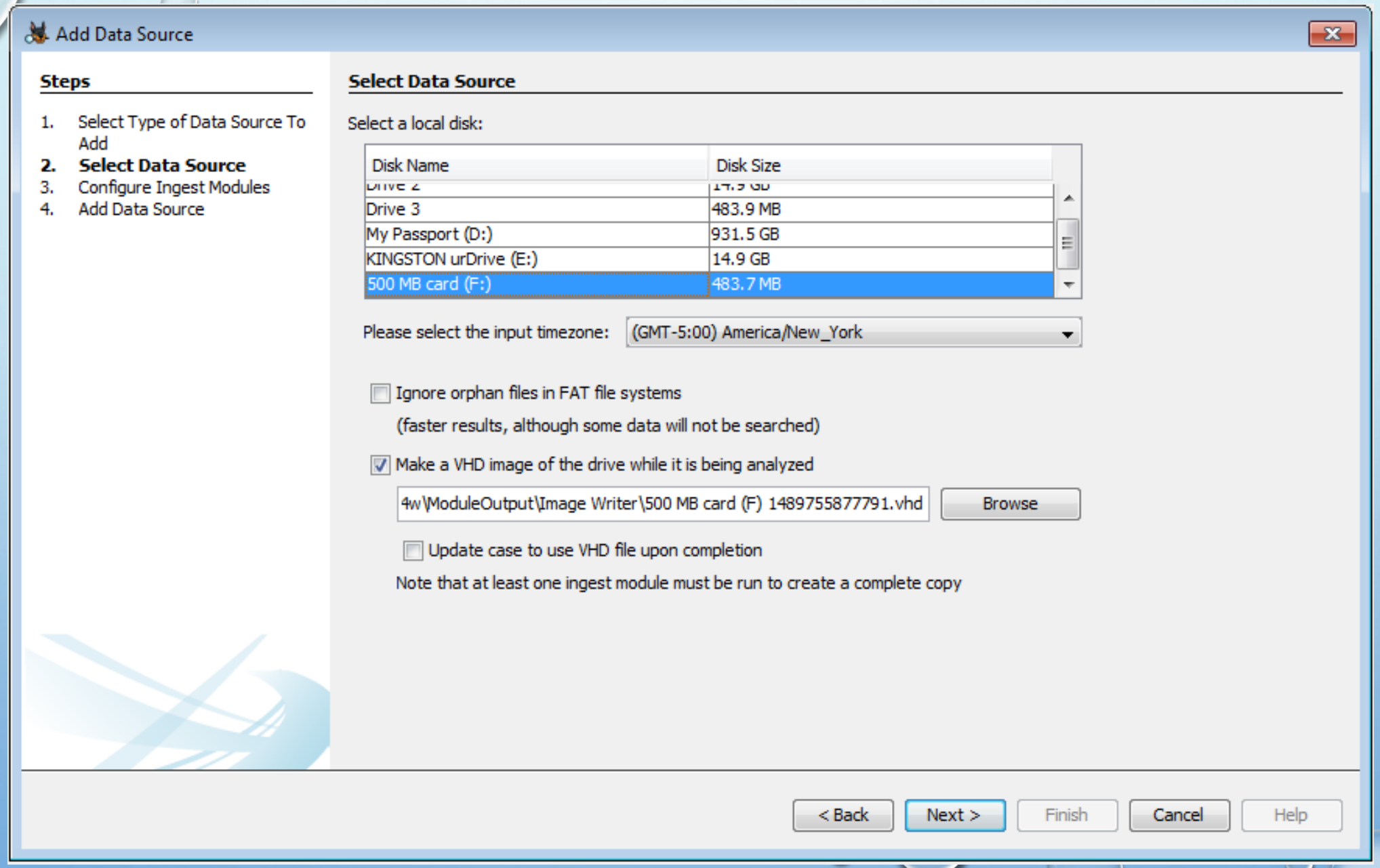
# Adding a Local Disk

- Autopsy can analyse a local disk without needing to first make an image copy of it.

  This is most useful when analysing a USB-attached device through a write blocker.

  Note that if you are analysing 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 analysed 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.




https://sleuthkit.org/autopsy/docs/user-docs/4.3/local-disk-data-source.PNG

- To add a local drive:

1. Choose "Local Disk" from the data source types.

2. Choose the device from the pull down list.

3. Choose to perform orphan file finding. See comment in **Adding a Disk Image** about this setting.

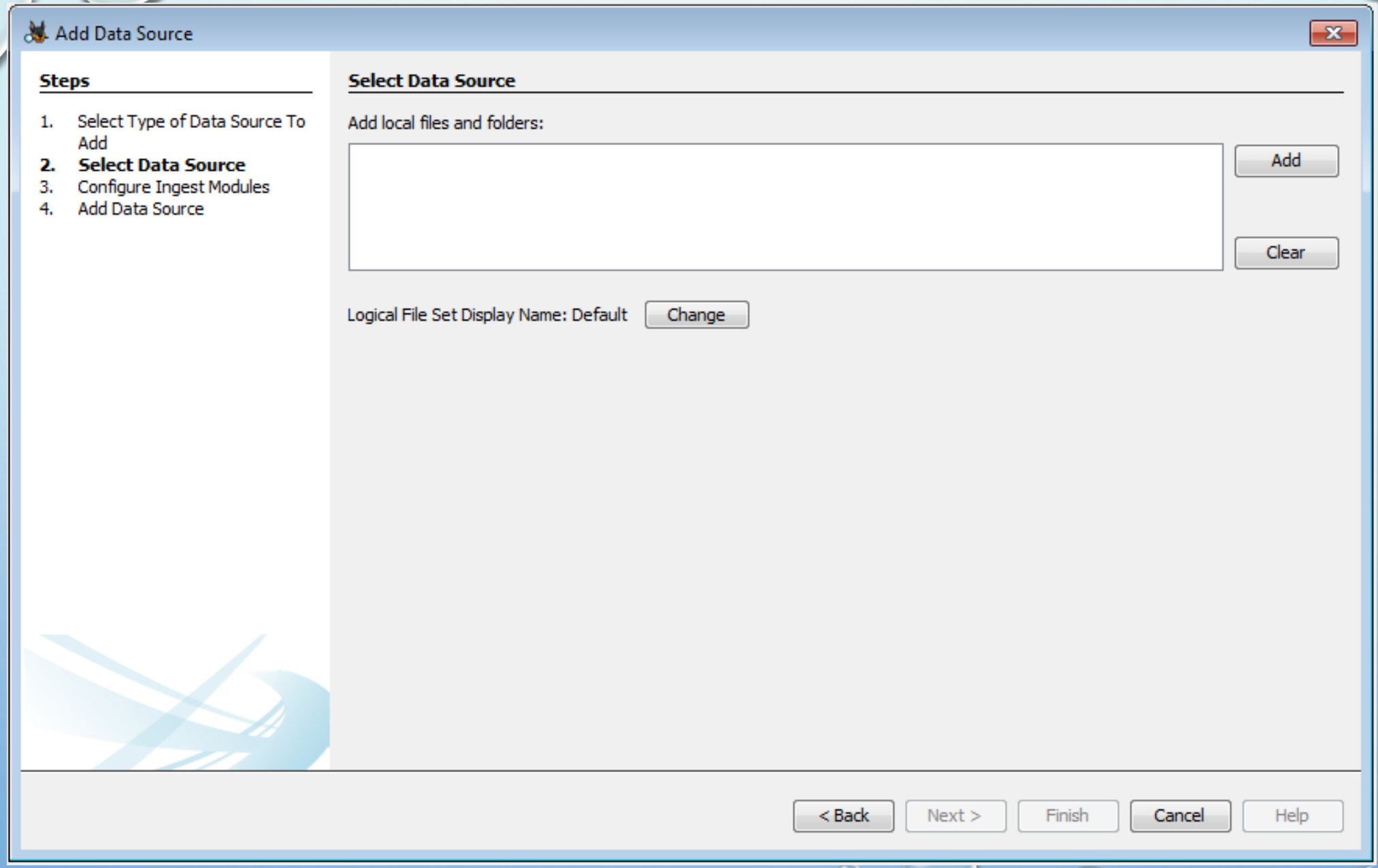
4. Choose whether to create a VHD copy of the local disk and whether to update the image path.

# 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 analyse.

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 analysing 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 analyse 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:




https://sleuthkit.org/autopsy/docs/user-docs/4.3/change_logical_file_set_display_name.PNG

To add logical files:

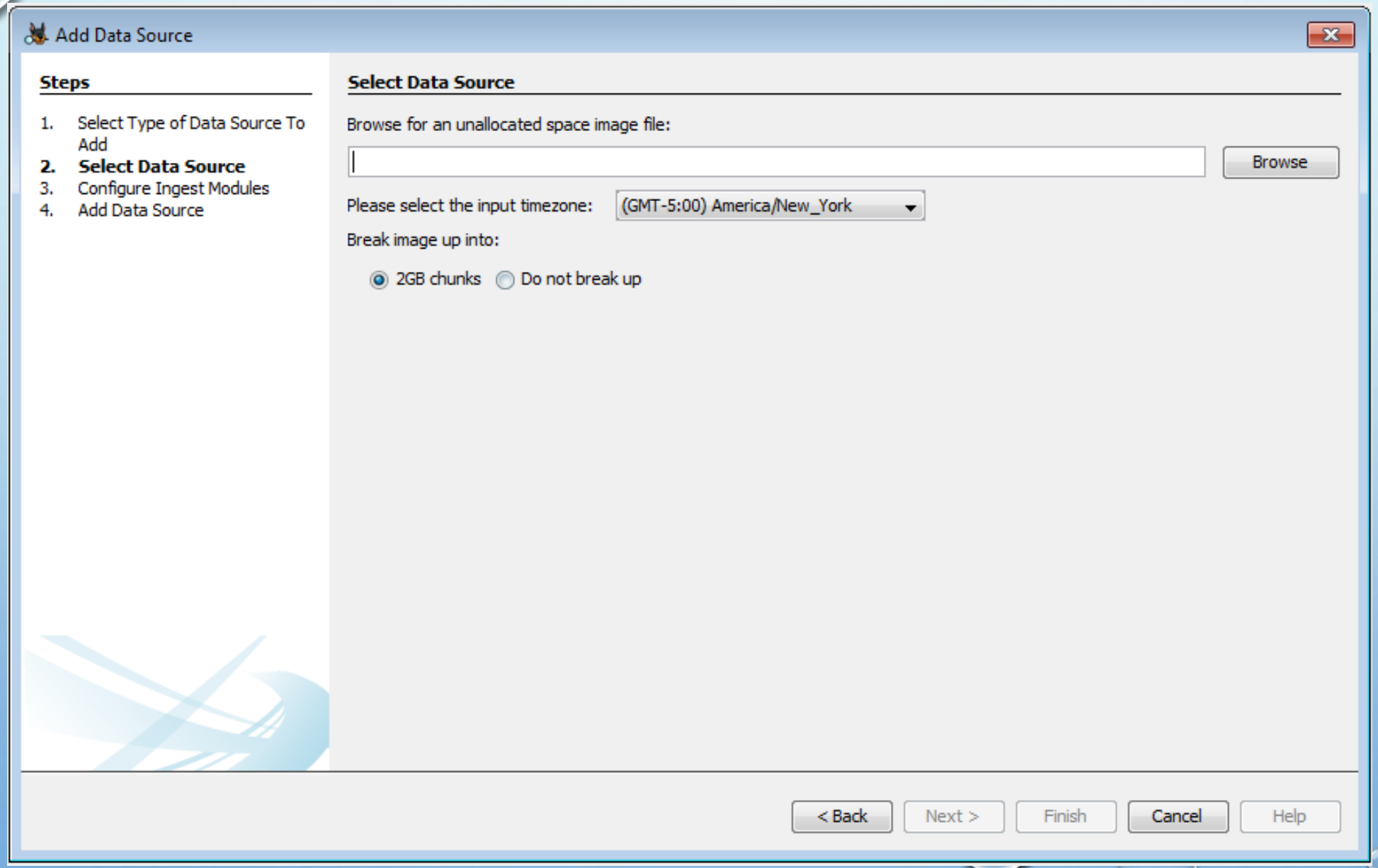
1. Choose "Logical Files" from the data source types.

2. 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.

3. 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.

# Adding an Unallocated Space Image File




https://sleuthkit.org/autopsy/docs/user-docs/4.3/unallocated_space_options.PNG

To add unallocated space image files:

1. Choose "Unallocated Space Image File" from the data source types.

2. Browse to the file.

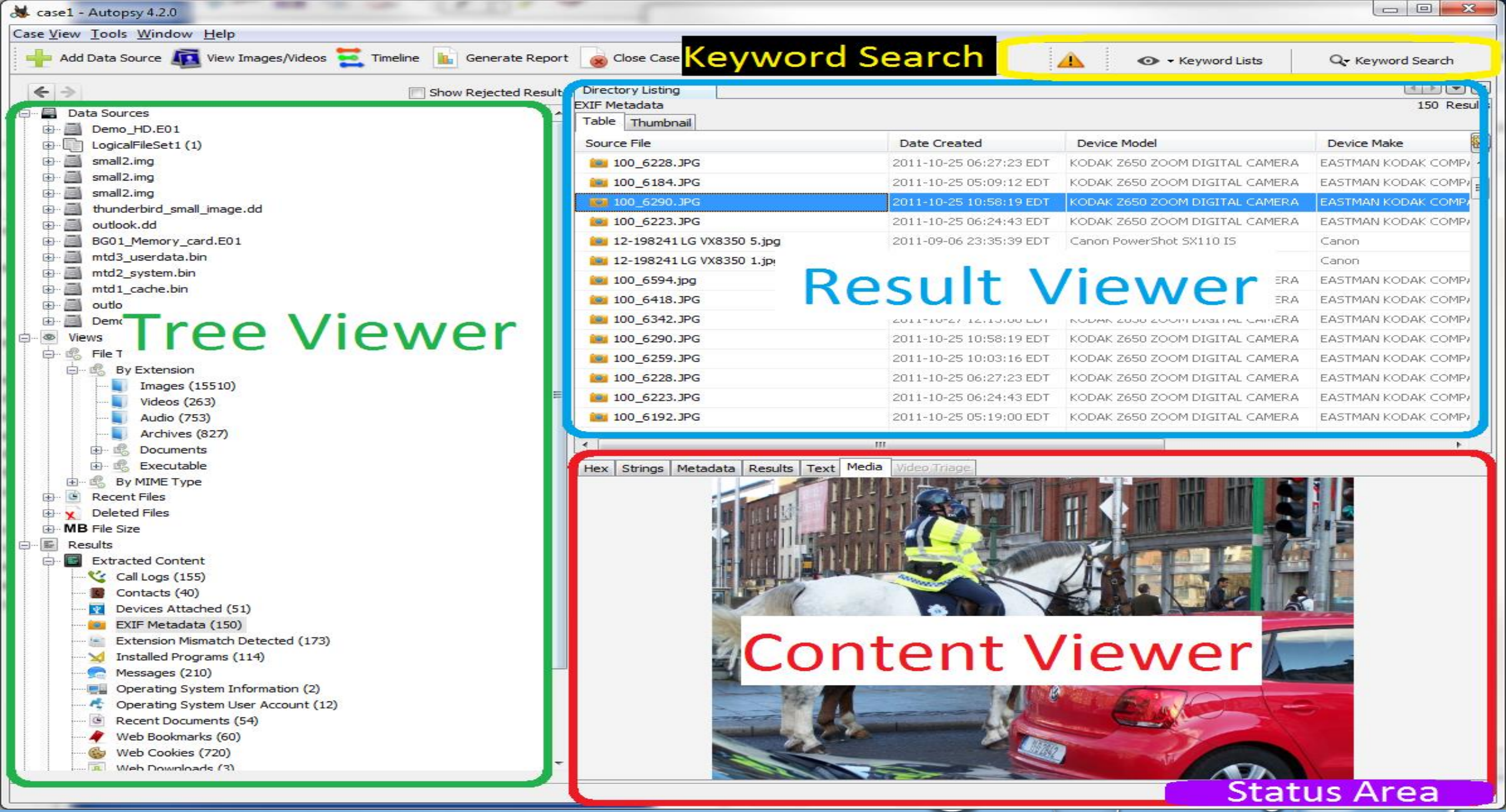
3. Choose whether to break the image up into chunks. Breaking the image up will give better performance since the chunks can be processed in parallel, but there is a chance that keywords or carved files that span chunk boundaries will be missed.

# 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




https://sleuthkit.org/autopsy/docs/user-docs/4.3/ui-layout-1.PNG

# 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

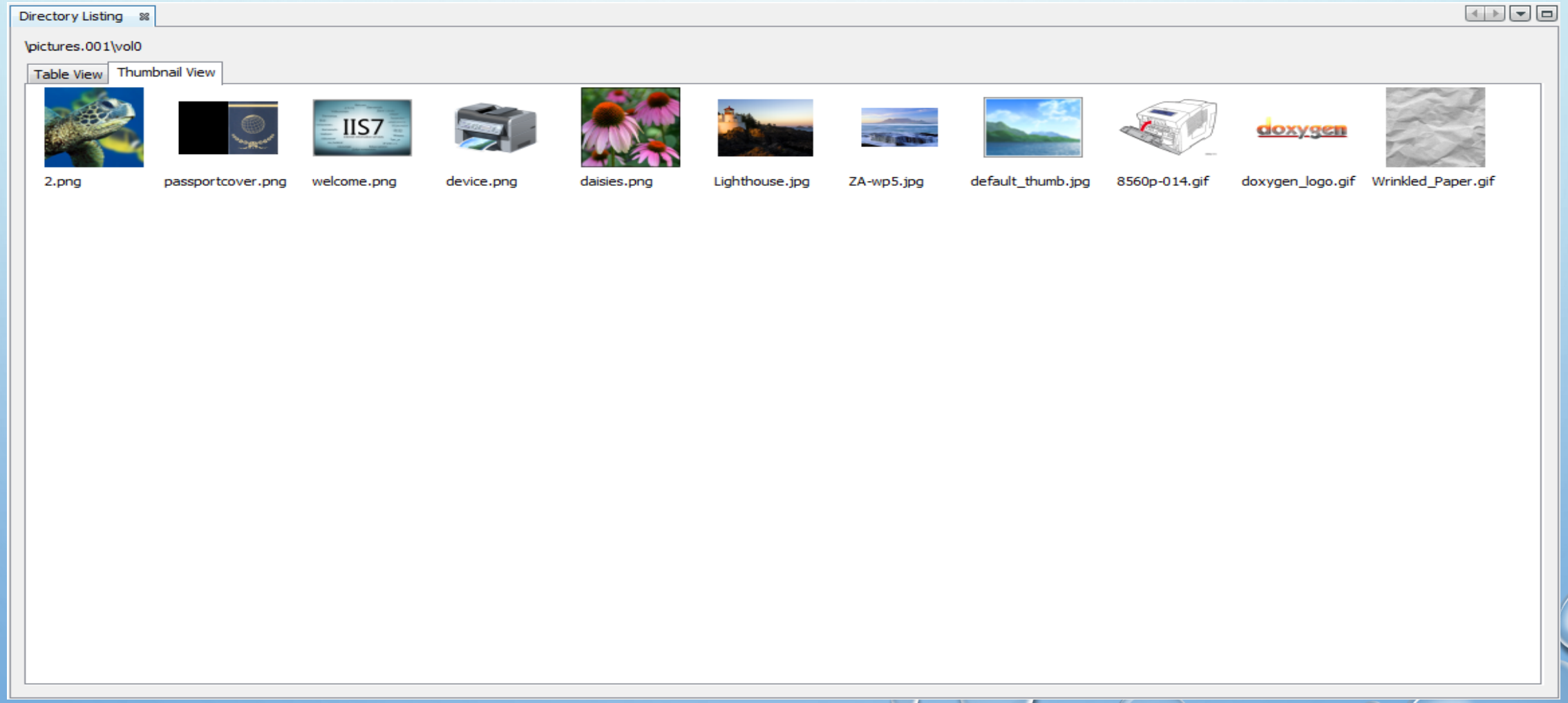
- **Extracted Content:** Many ingest modules will place results here; EXIF data, GPS locations, or Web History for example
- **Keyword Hits:** Keyword search hits show up here
- **Hashset Hits:** Hashset hits show up here
- **E-Mail Messages:** Email messages show up here
- **Interesting Items:** Things 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

# Result Viewers

- **Thumbnail Result Viewers**

**Example**

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

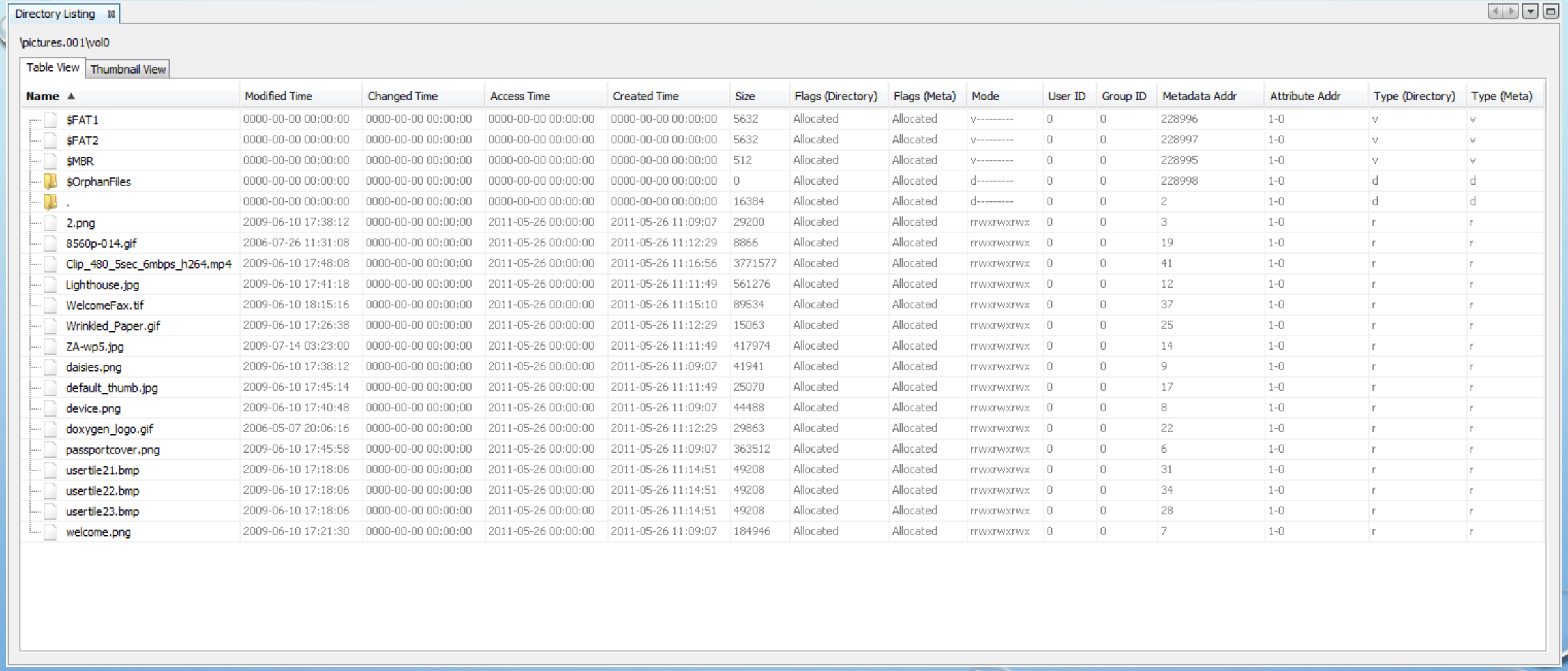



https://sleuthkit.org/autopsy/docs/user-docs/4.3/thumbnail-result-viewer-tab.PNG

# Table Result Viewers

## Example

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



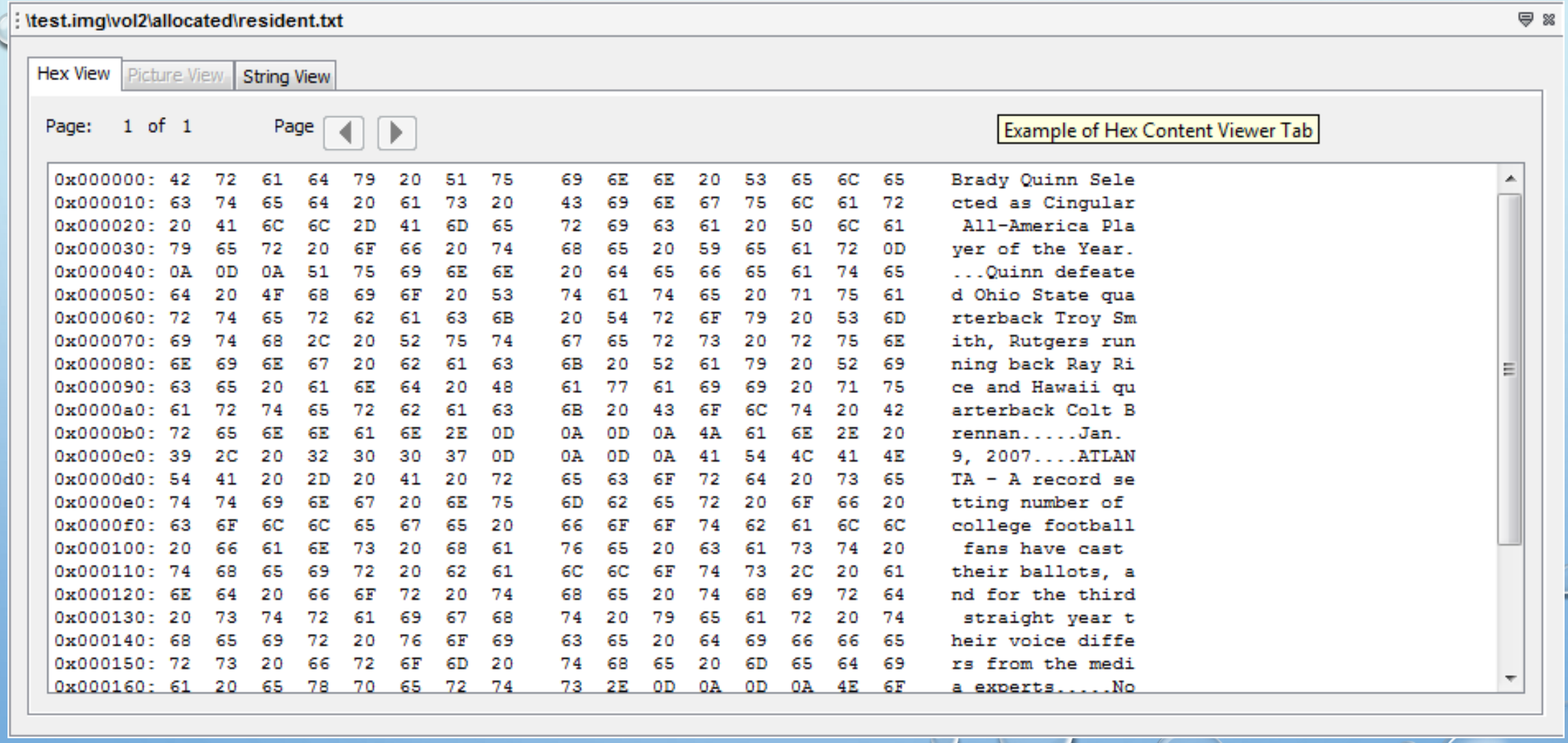

| Name | Modified Time | Changed Time | Access Time | Created Time | Size | Flags (Directory) | Flags (Meta) | Mode | User ID | Group ID | Metadata Addr | Attribute Addr | Type (Directory) | Type (Meta) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $FAT1 | 0000-00-00 00:00:00 | 0000-00-00 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 |

https://sleuthkit.org/autopsy/docs/user-docs/4.3/table-result-viewer-tab.PNG

# Hex Content Viewer

## Example

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

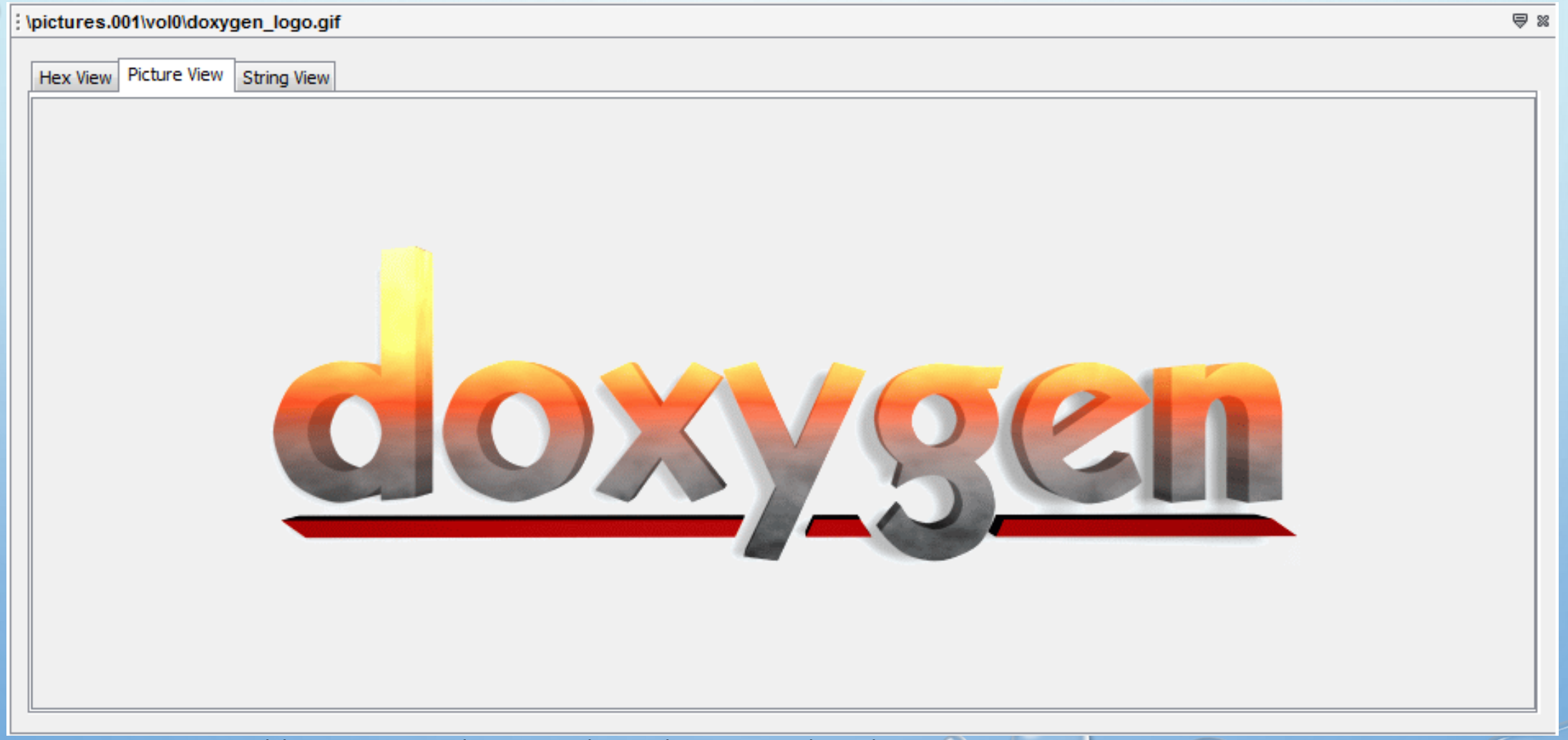



https://sleuthkit.org/autopsy/docs/user-docs/4.3/hex-content-viewer-tab.PNG

# Media Content Viewer

## Example

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

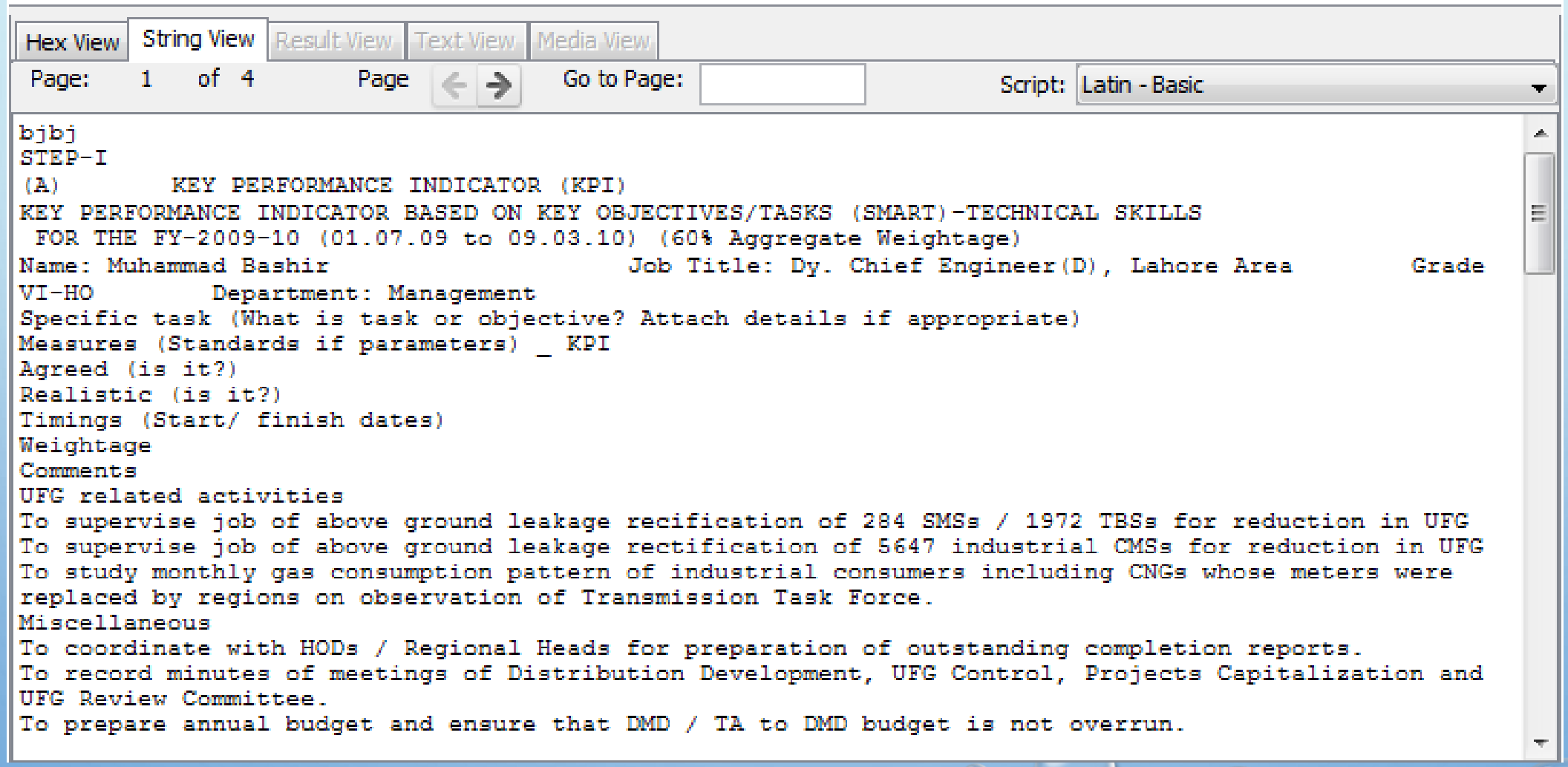



https://sleuthkit.org/autopsy/docs/user-docs/4.3/picture-content-viewer-tab.PNG

# String Content Viewer

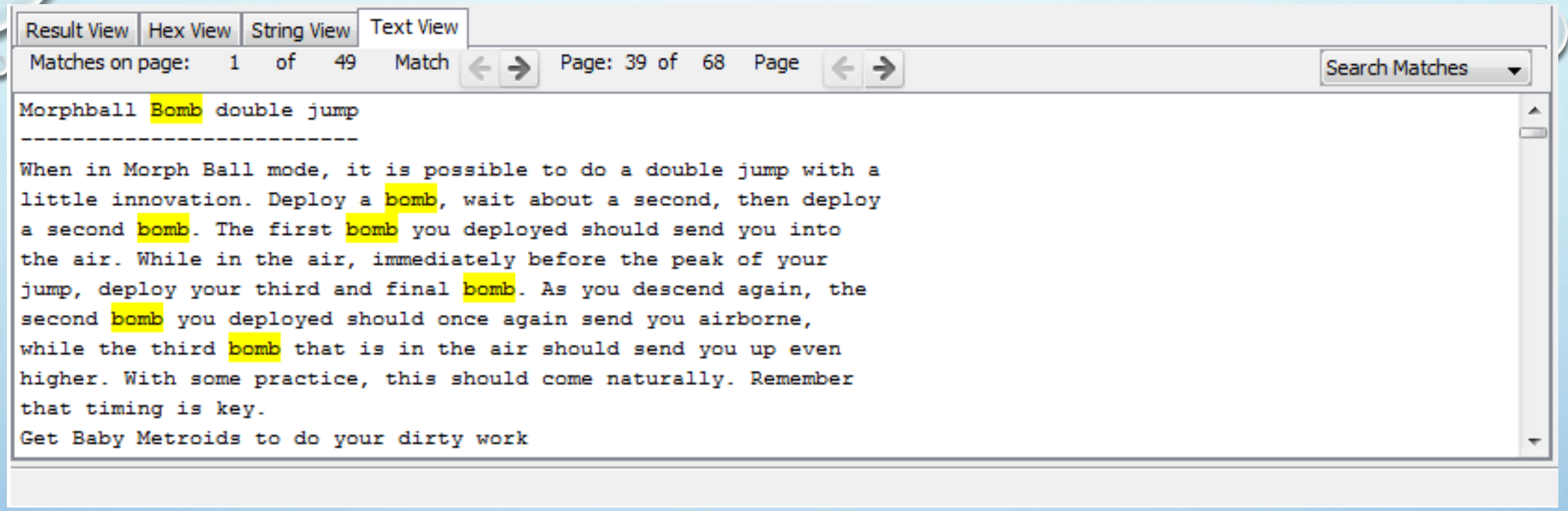
## Example

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




https://sleuthkit.org/autopsy/docs/user-docs/4.3/string-content-viewer-tab.PNG

# Text Content Viewer




https://sleuthkit.org/autopsy/docs/user-docs/4.3/text-view.PNG

## Keyword Search

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

## 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.

thank you!