11. Digital Forensics

Objective: To learn the basics of digital forensics and evidence collection

Tools: Autopsy, FTK Imager

Digital forensics is the process of investigating and analyzing electronic data to uncover and present evidence in a way that is legally admissible. It involves recovering, preserving, and examining data from computers, smartphones, servers, and other digital devices to solve crimes, resolve disputes, or investigate incidents.

Here's a breakdown of what digital forensics entails:

1. **Data Collection**: Identifying and gathering data from digital devices while ensuring that the process doesn't alter or damage the evidence. This often involves creating forensic copies (or images) of the data.
2. **Data Preservation**: Ensuring that the collected data remains unchanged throughout the investigation. This involves using specialized tools and techniques to maintain the integrity of the evidence.
3. **Data Analysis**: Examining the data to identify relevant information. This can involve looking at files, metadata, logs, communications, and other types of digital information.
4. **Data Presentation**: Preparing findings in a clear and understandable format for legal proceedings or other investigations. This may involve creating reports, visualizations, or expert testimony.
5. **Incident Response**: In some cases, digital forensics is used in real-time to respond to and manage ongoing security incidents or breaches.

Autopsy

Autopsy is a widely used open-source digital forensics platform that helps investigators analyzes and examine digital evidence. It provides a suite of tools for processing and investigating data from various types of digital devices, including computers, smartphones, and external storage media. Here's a closer look at what Autopsy offers:

Key Features of Autopsy:

1. **Case Management**: Allows investigators to organize and manage cases, including setting up case files and tracking evidence.
2. **Data Analysis**: Provides tools for analyzing file systems, recovering deleted files, and examining file contents. It supports a variety of file systems and can extract data from different types of devices.
3. **Search and Filtering**: Includes powerful search capabilities to find specific files or data within a case. Investigators can use keywords, file types, and other criteria to narrow down their search.
4. **Timeline Analysis**: Helps in creating and analyzing timelines based on file system activities, such as file creation, modification, and access times.
5. **File Carving**: Capable of recovering deleted or fragmented files from raw disk images.
6. **Metadata Extraction**: Extracts and analyzes metadata from files, which can provide insights into file origins, modifications, and other relevant details.
7. **Visualization**: Offers graphical representations of data, such as file trees, directory structures, and timeline charts, to aid in understanding and interpreting the evidence.

8. **Reporting**: Generates detailed reports summarizing the findings of the investigation, which can be used for legal proceedings or internal documentation.

How Autopsy Works:

- **Data Ingestion**: Forensic images of disks or individual files are imported into Autopsy. These images are often created using other forensic tools to ensure that the original data remains unaltered.
- **Analysis**: Autopsy processes the data, applying various analysis modules to identify and examine relevant evidence. Investigators can explore the data through a user-friendly interface.
- **Reporting**: After analysis, investigators can compile their findings into comprehensive reports that detail the evidence and support investigative conclusions.

Steps: Windows

1. Download the Autopsy from Google: https://www.autopsy.com/download **autopsy Sluthkit (64 Bit)**

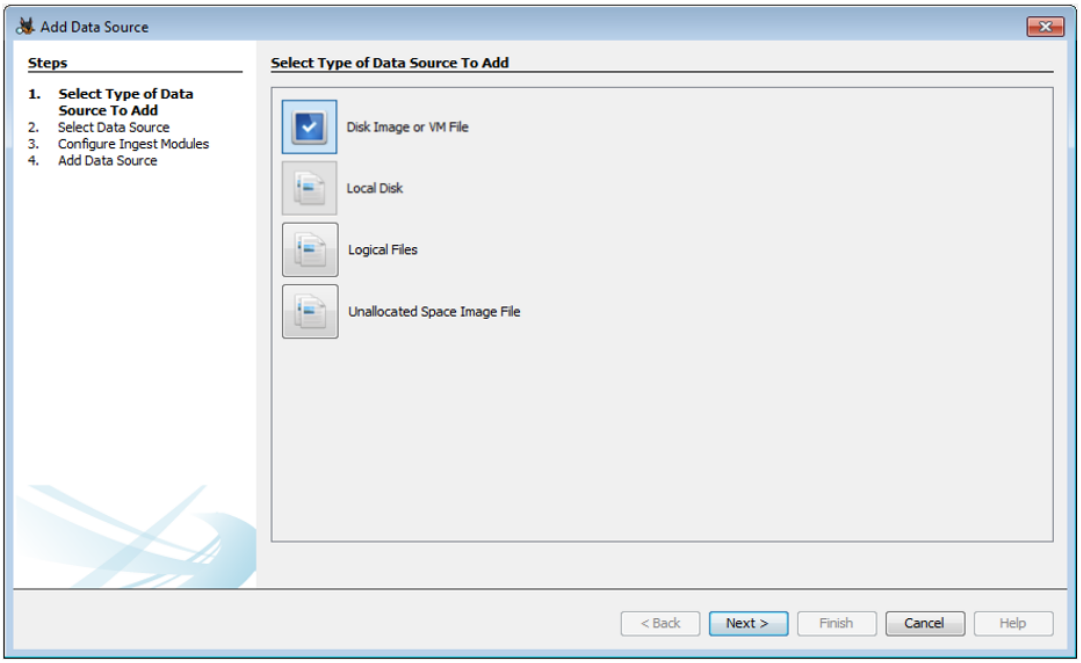
1. Getting Started

Open Autopsy and create a new case.

Click on **Finish** after completing both the steps.

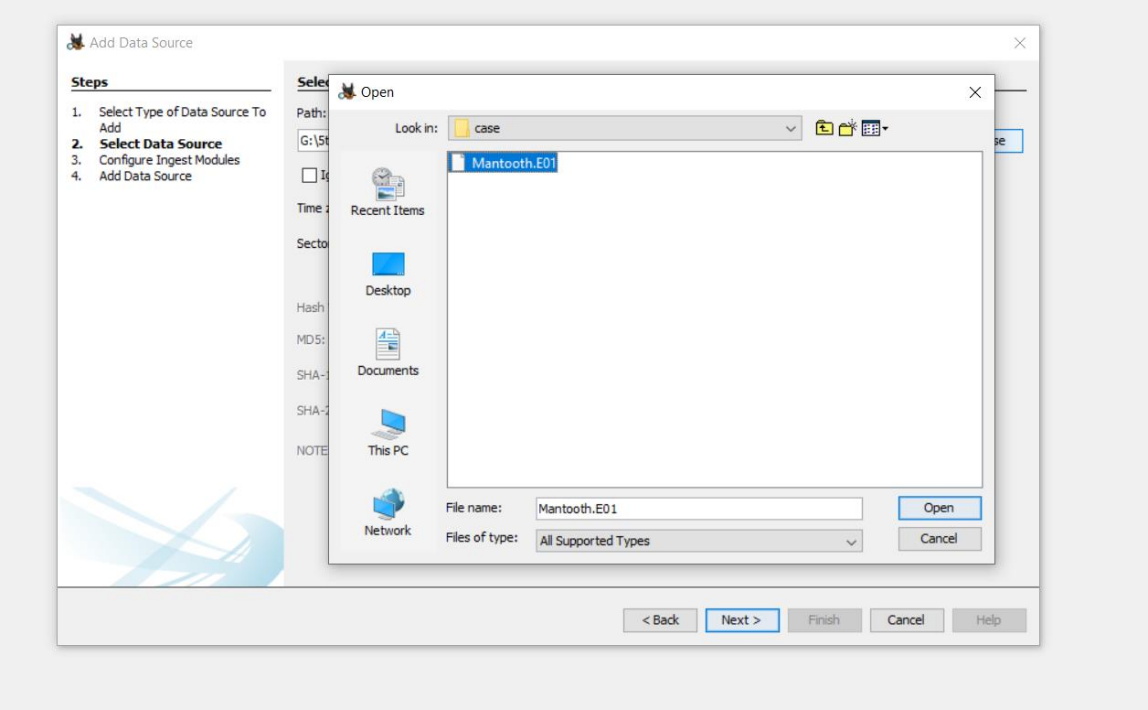
2. Add a data source.

Select the appropriate data source type.

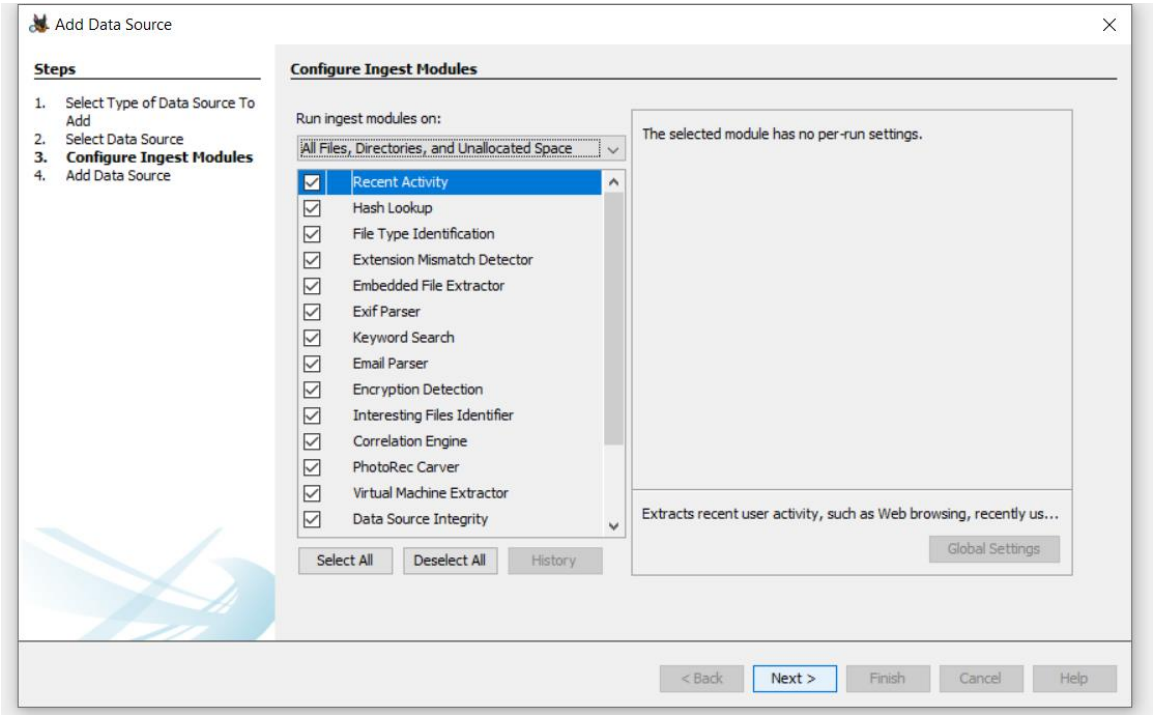


- **Disk Image or VM file:** Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.
- **Local Disk:** Includes Hard disk, Pendrive, memory card, etc.
- Logical Files. : Includes local folders or files.
- **Unallocated Space Image File**: Includes files that do not contain a file system but need to run through ingest.

The data source used here is a disk image. Add the data source destination.



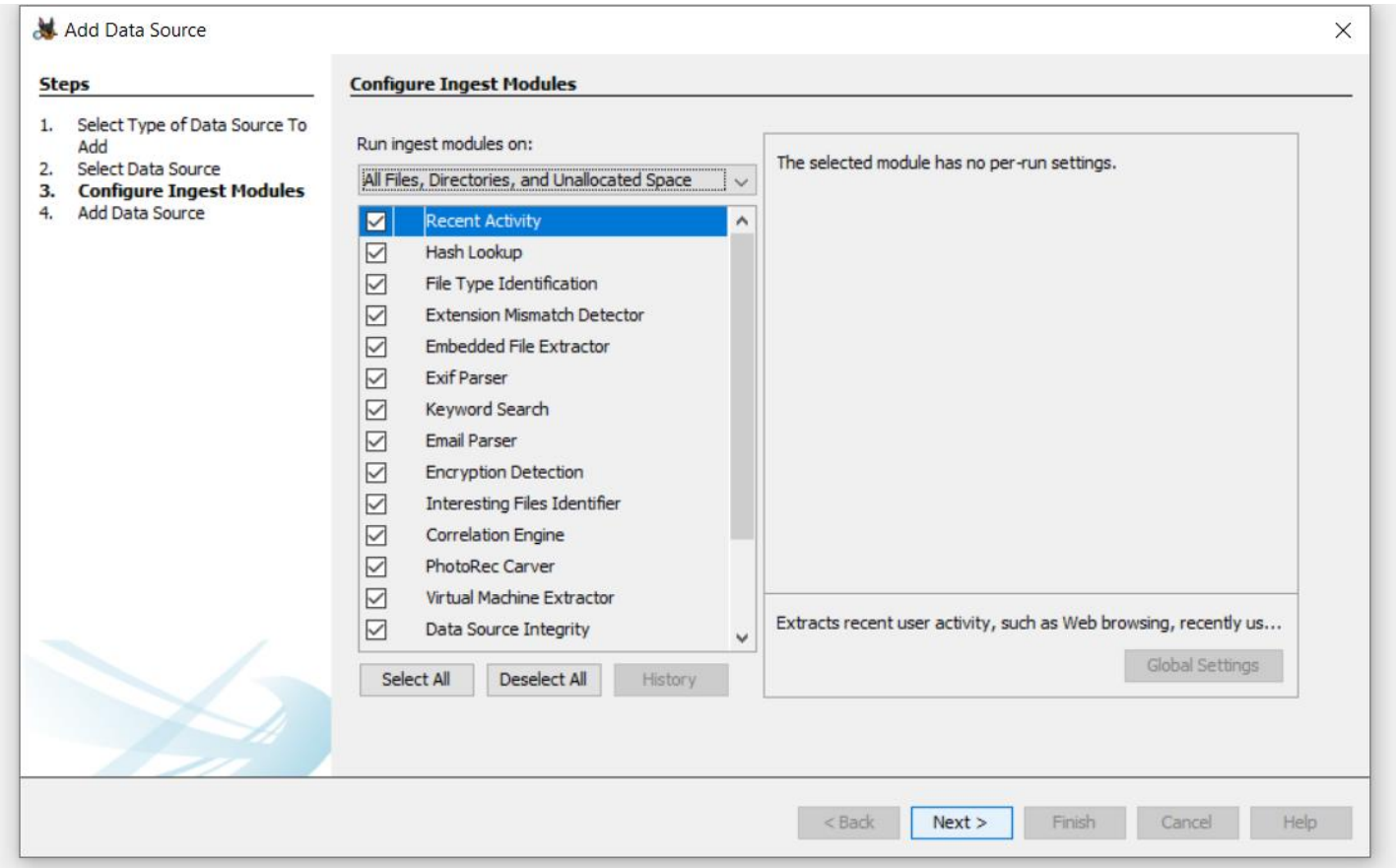
Configure ingest modules.



The ingest modules determine factors for which the data in the data source is to be analyzed. Here is a brief overview of each of them.

- **Recent Activity**: Discover the recent operations performed on the disk, for example, the files that were last viewed.
- **Hash Lookup**: Identify files using hash values.
- **File Type Identification:** Identify files based on their internal signatures rather than just file .extensions.
- **Extension Mismatch Detector:** Identify files whose extensions are tampered with/changed possibly to hide evidence.
- **Embedded File Extractor:** It extracts embedded files such as .zip, .rar, etc. and uses the derived file for analysis. Another example could be a PNG image saved inside a doc to make it appear as a document and thus hide crucial information.
- **EXIF (Exchangeable Image File Format) Parser:** It is used to retrieve metadata about the files, for example, date of creation, geolocation, etc.
- **Keyword Search:** Search for a particular keyword/pattern in the data source.
- **Email Parser:** If the disk holds any form of email database, for example, pst/ost files of outlook then information from these files can be extracted using an email parser.
- **Encryption Detection:** Detects and identifies encrypted / password-protected files.
- **Interesting File Identifier:** Let's set custom rules regarding the filtering of data. Examiner is notified when results pertaining to these rules are found.
- **Correlation Engine:** Allows saving properties in and then retrieved from the central repository. It helps in displaying correlated properties.
- **PhotoRec Carver:** Recover files, photos, etc. from the unallocated space.
- **Virtual Machine Extractor:** Extract and analyze any Virtual machine found on the data source.

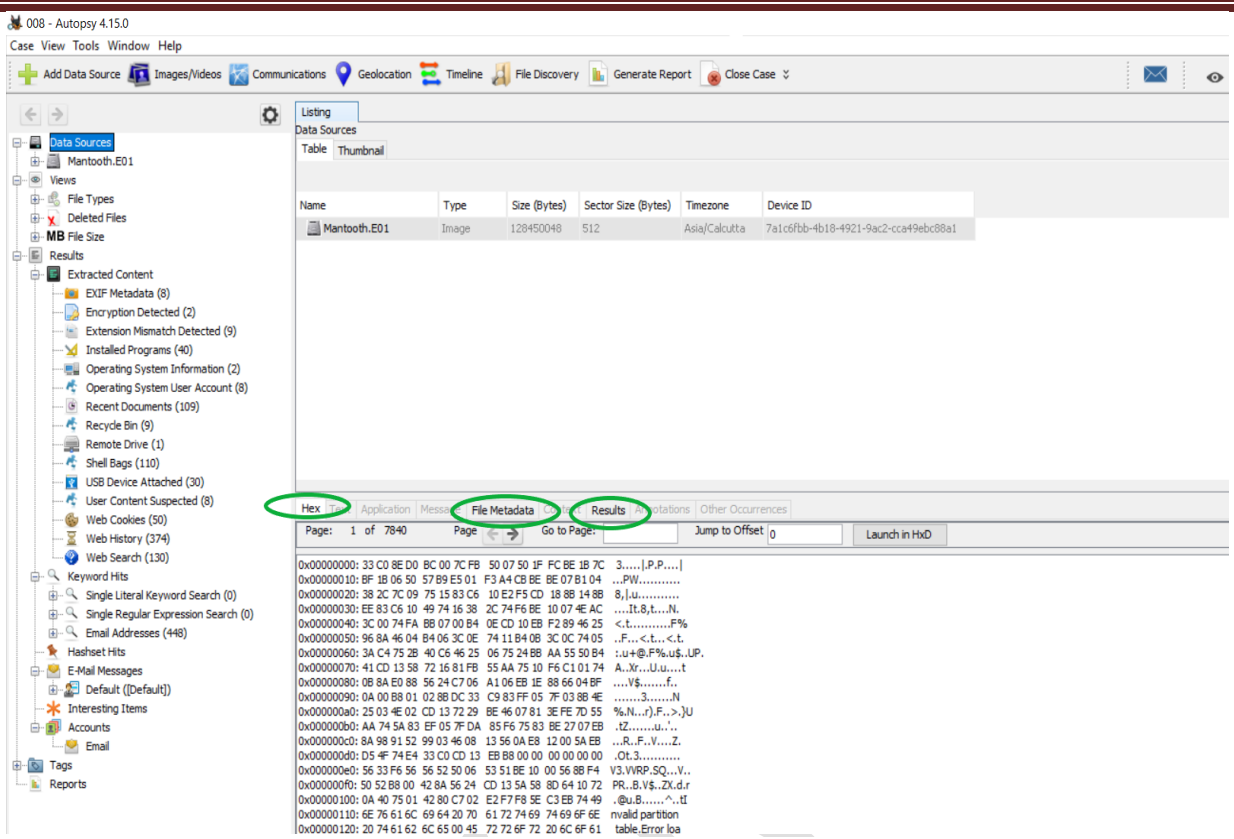
- **Data Source Integrity:** Calculates the hash values and stores them in the database in case they aren't already present. Otherwise, it will verify the hash values associated with the database.
- **Plaso:** Extract timestamp for various types of files.
- **Android Analyzer:** Analyze SQLite and other files retrieved from an Android device.



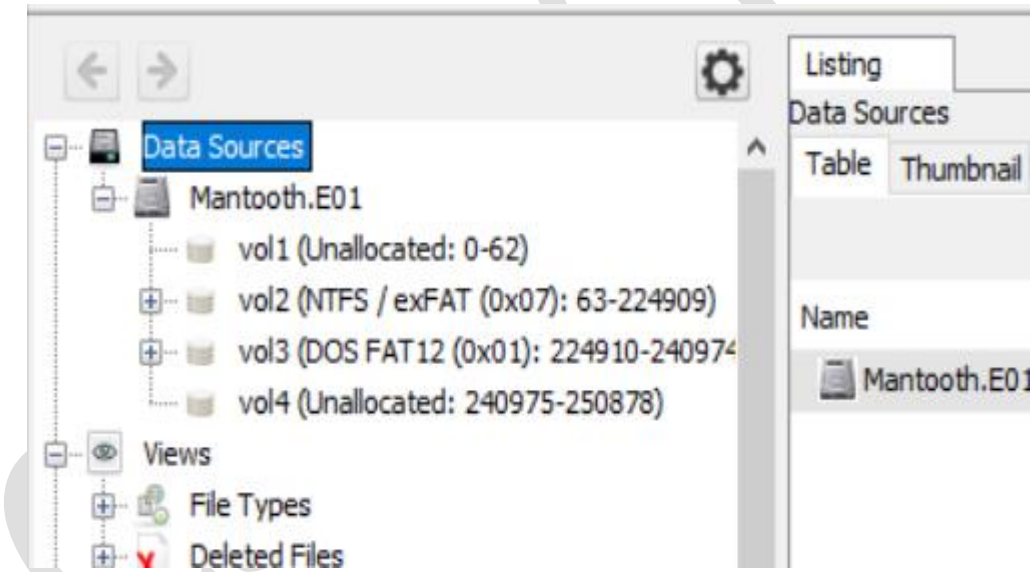
Select all that will serve the purpose of your investigation and click Next. Once the data source is added, click Finish. It will take some buffer time to extract and analyze the data depending upon the size of the Data Source.

3. Exploring the data source:

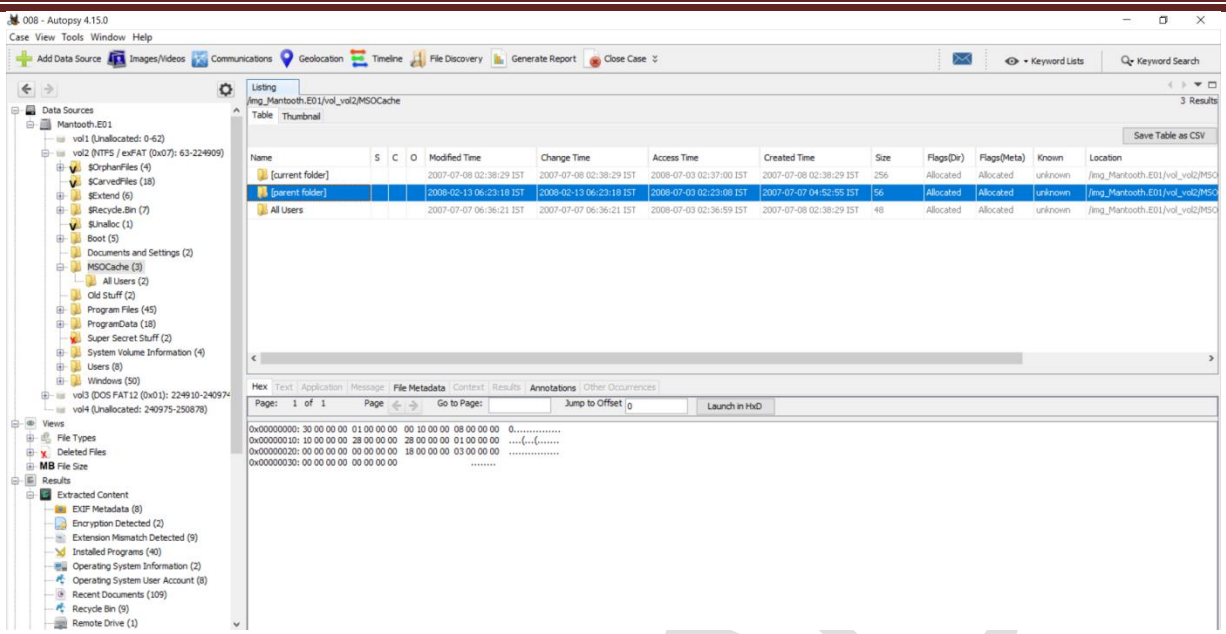
The Data Source information: Here the basic metadata is shown. A detailed analysis is displayed in the bottom section. These details can be extracted in the form of Hex values, Results, File Metadata, etc.



The disk image is then broken down based upon its volume partitions.

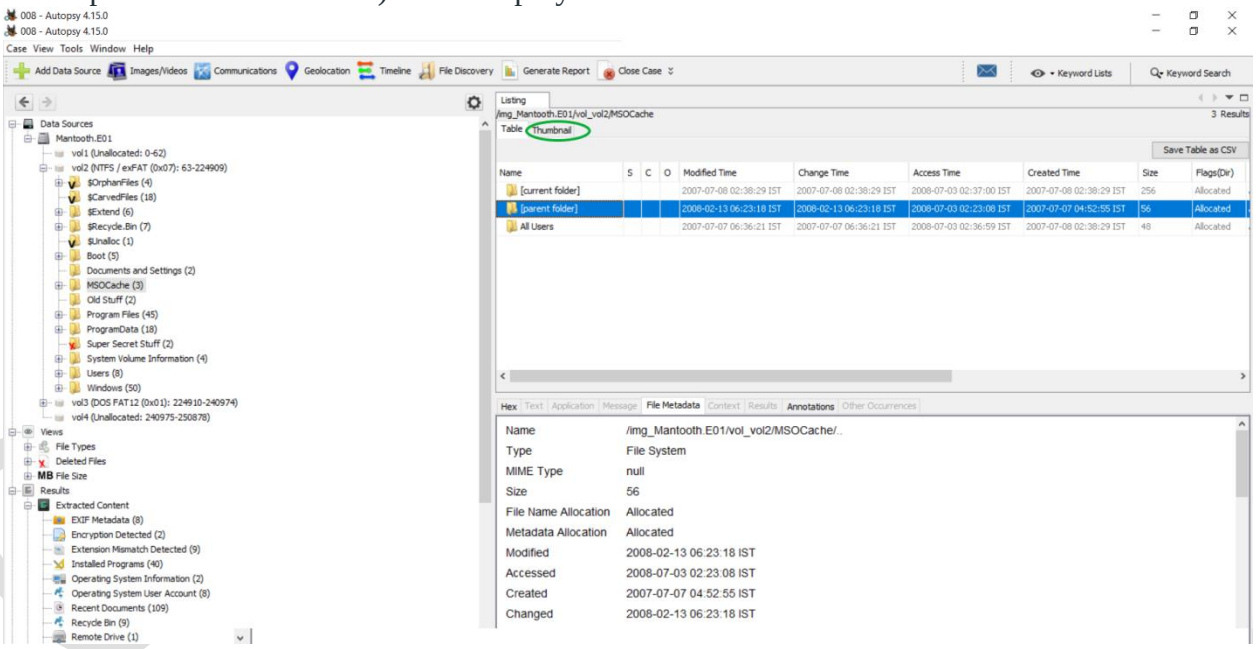


Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> Mantooth.E01 -> MSOCache-> [Parent Folder].

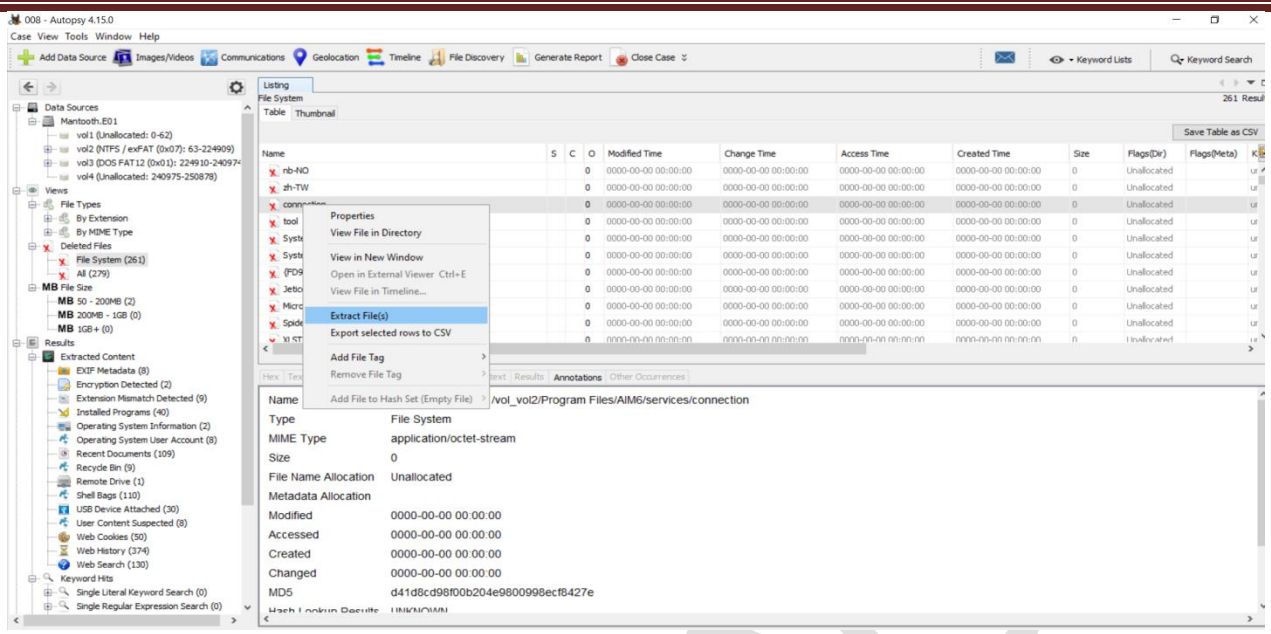


Views (Determines the factor of file classification)

- **File Type**: Here the files are categorized based upon their type. The classification can be done either on the basis of file .extension or MIME type. While both of these provide a hint about how to deal with a file, file extensions are commonly used by the OS to decide what program shall be used to open a file and MIME types are used by the browser to decide about how to present the data (or by the server on how to interpret the data received). Files displayed here also include the deleted files.



- **Deleted Files:** Here information about the files that were specifically deleted can be found. These deleted files can be recovered as well: Right-click on the file to be recovered -> click on Extract File(s). -> Save the file in an appropriate destination.

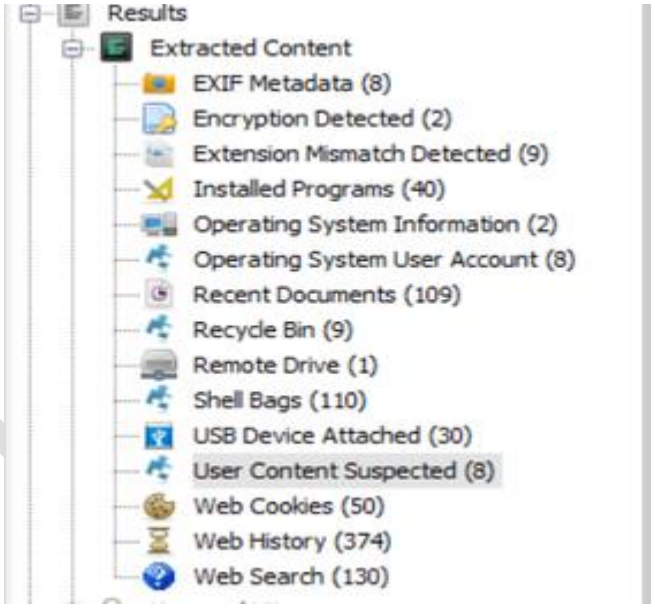


MB Size Files: Here files are classified based upon their size. The range starts from 50MB. This enables the examiner to determine exclusively large files.

Results:

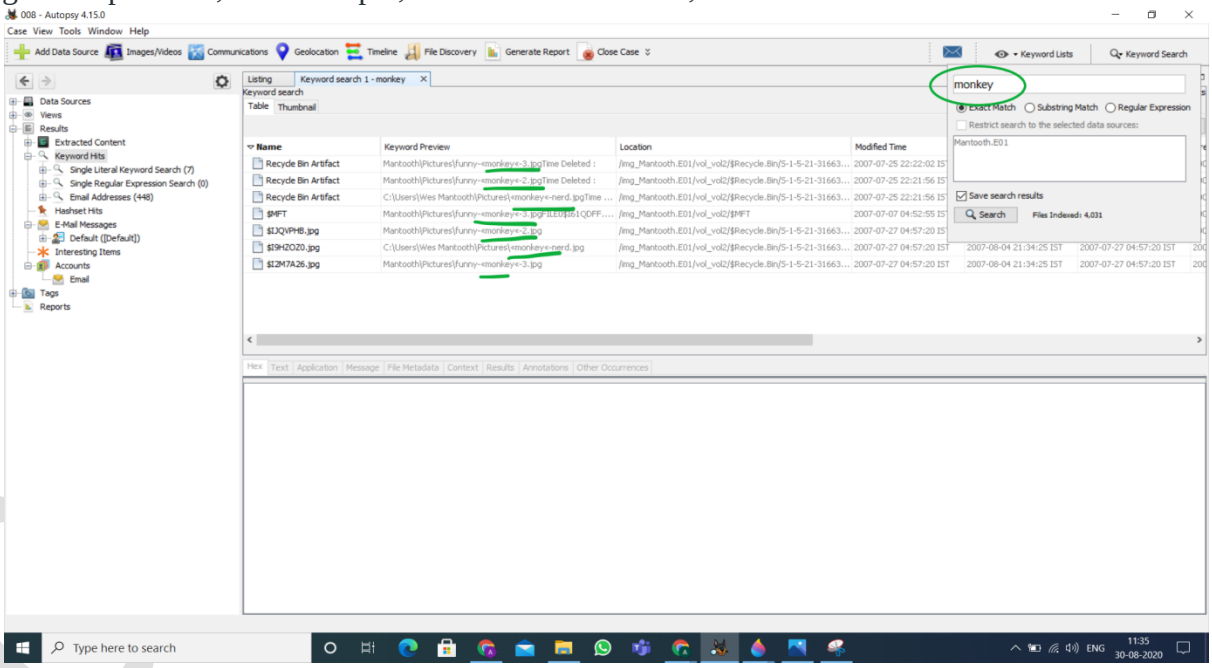
All the extracted data is viewed in ***Views/ Data Source***. In ***Results***, we get the information about this data.

- **Extracted Content:** Each Extracted Content displayed below can be further explored. The following briefly explains each of them.

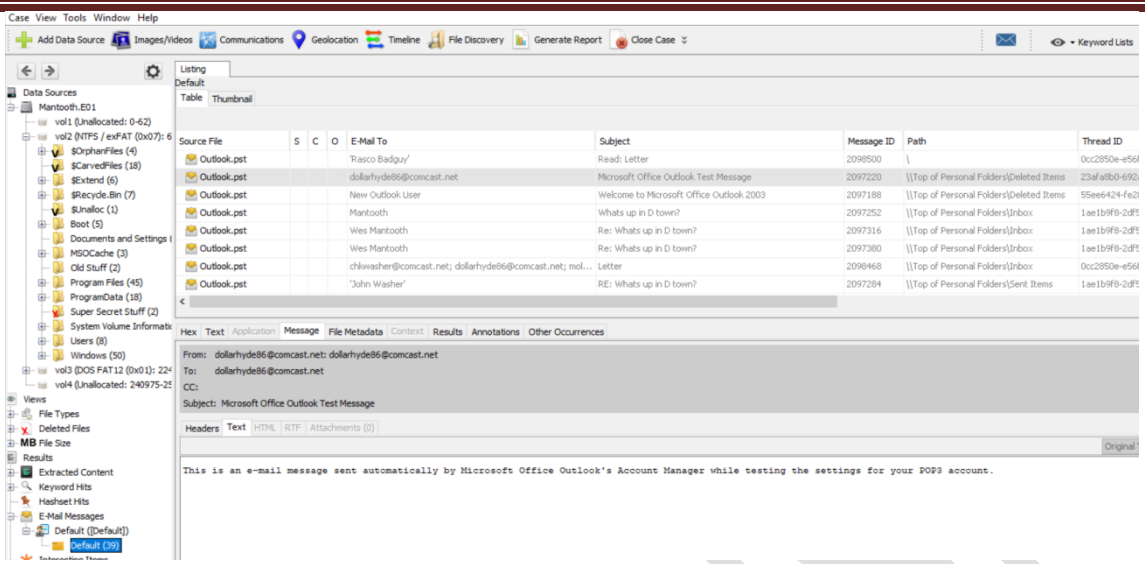


- **EXIF Metadata:** It contains all the .jpg images that have EXIF Metadata associated with them, this Metadata can be analyzed further.
- **Encryption Detection:** It detects files that are password protected/ encrypted.
- **Extension Mismatch Detection:** As explained above, it Identifies the files whose extensions do not match their MIME types and thus they may be suspicious.
- **Installed Programs:** It gives details about the software used by the user. This information is extracted with the help of the Software Registry hive.

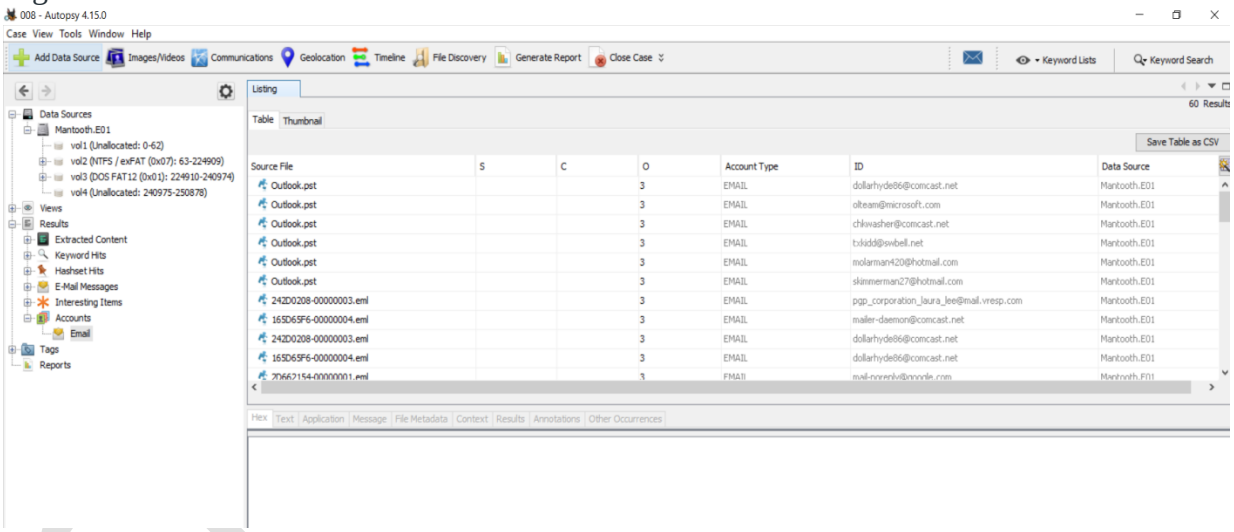
- **Operating System Information:** It gives information about the OS with the help of the Windows Registry hive and the Software Registry hive.
- **Operating System User Account:** It lists information about all the user accounts, for example, accounts belonging to the device are extracted from the Software Hive and the accounts associated with the Internet Explorer using index.data files.
- **Recent documents:** Lists all the documents that were accessed nearby the time the disk image was captured.
- **Recycle Bin:** Files that are temporarily stored on the system before being permanently deleted are visible here.
- **Remote Drive:** Shows information about all the remote drives accessed using the system.
- **Shell bags:** A shell bag is a set of registry keys that stores details about a folder being viewed, such as its position, icon, and size. All the Shell bags from the system can be viewed here.
- **USB Device attached:** All the information about the external devices attached to the system is displayed here. This data is extracted from Windows Registry which is actually a maintained database about all the activities taking place on the system.
- **Web Cookies:** Cookies saves the user information from the sites and thus provide a lot of information about the user's online activities.
- **Web History:** All the details about the browser history is shown here.
- **Web Searches:** Details about the web searches made are displayed here.
- **Keyword Hits:** Here specific keywords can be looked for in the image of the disk. Multiple data sources can be selected for the lookup. The search can be restricted to Exact match, Substring match and Regular expression, for example, emails/ IP Addresses, etc.



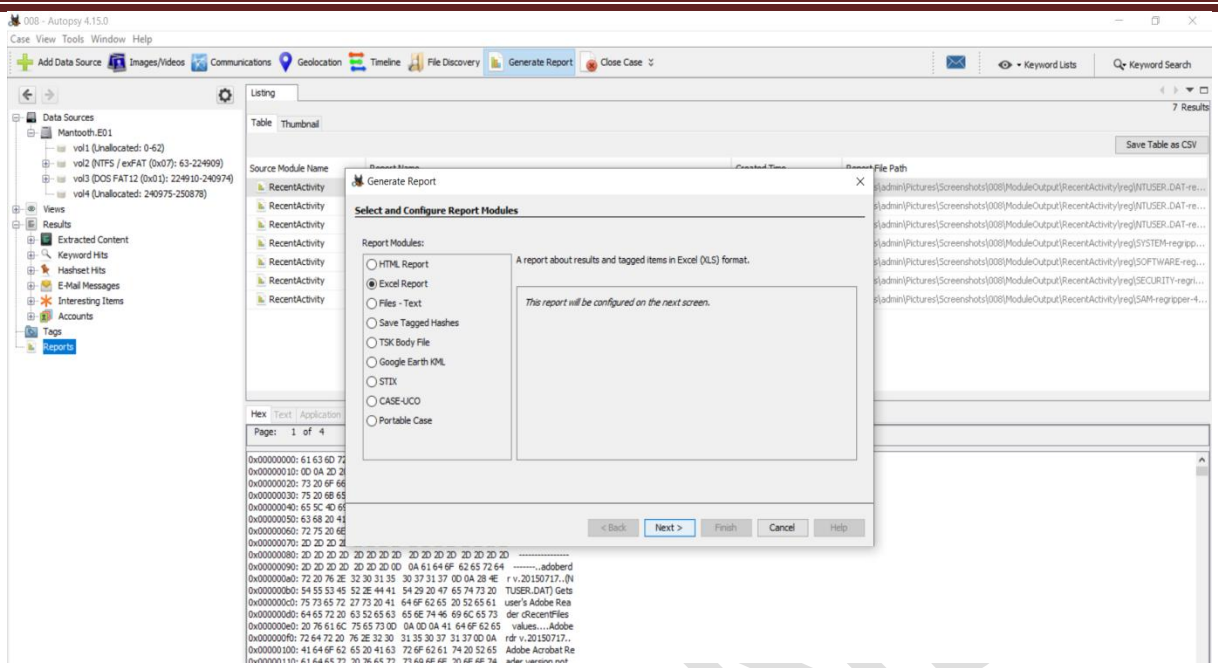
- **HashSet Hits:** Here the search can be made using hash values.
- **E-mail Messages:** Here all the *outlook.pst* files can be explored.

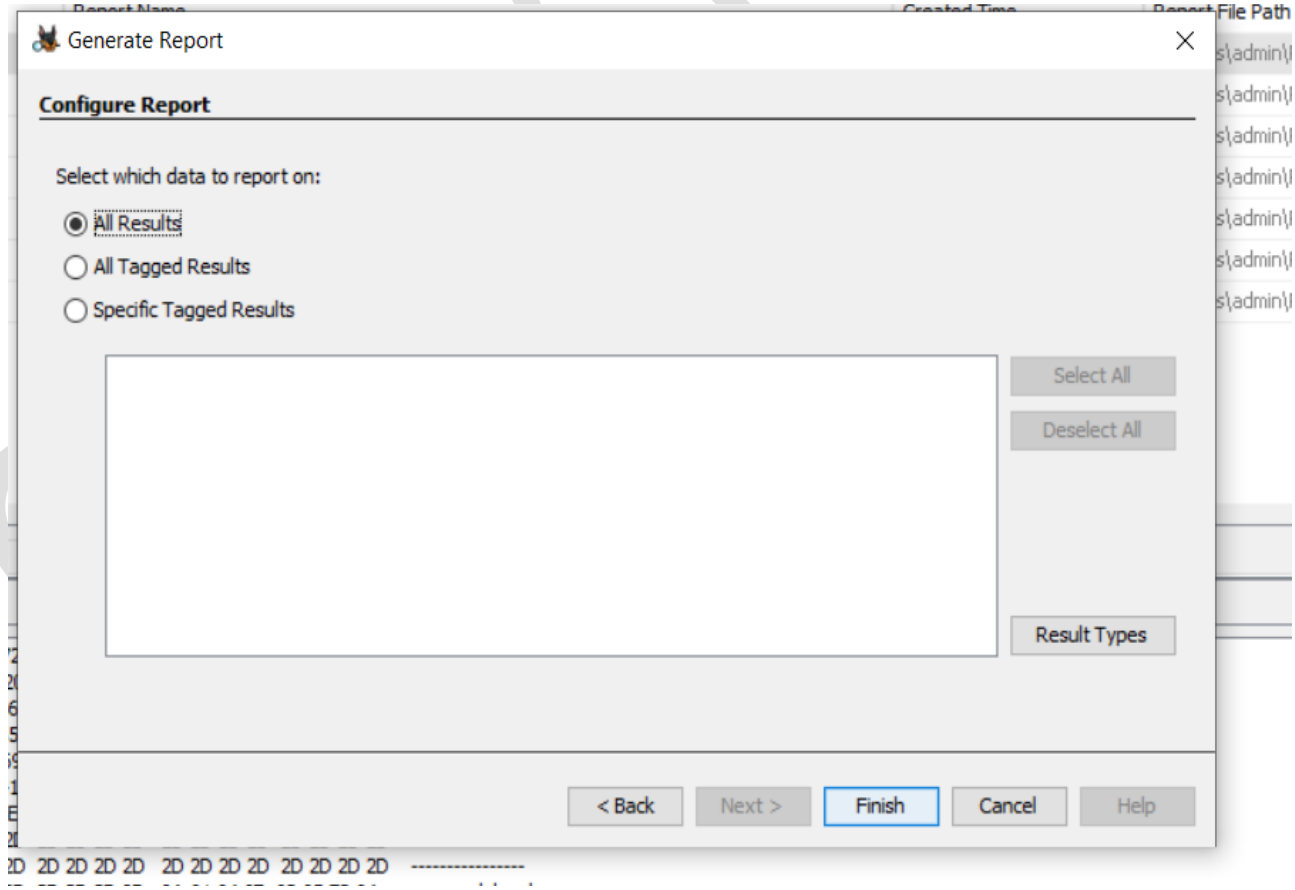


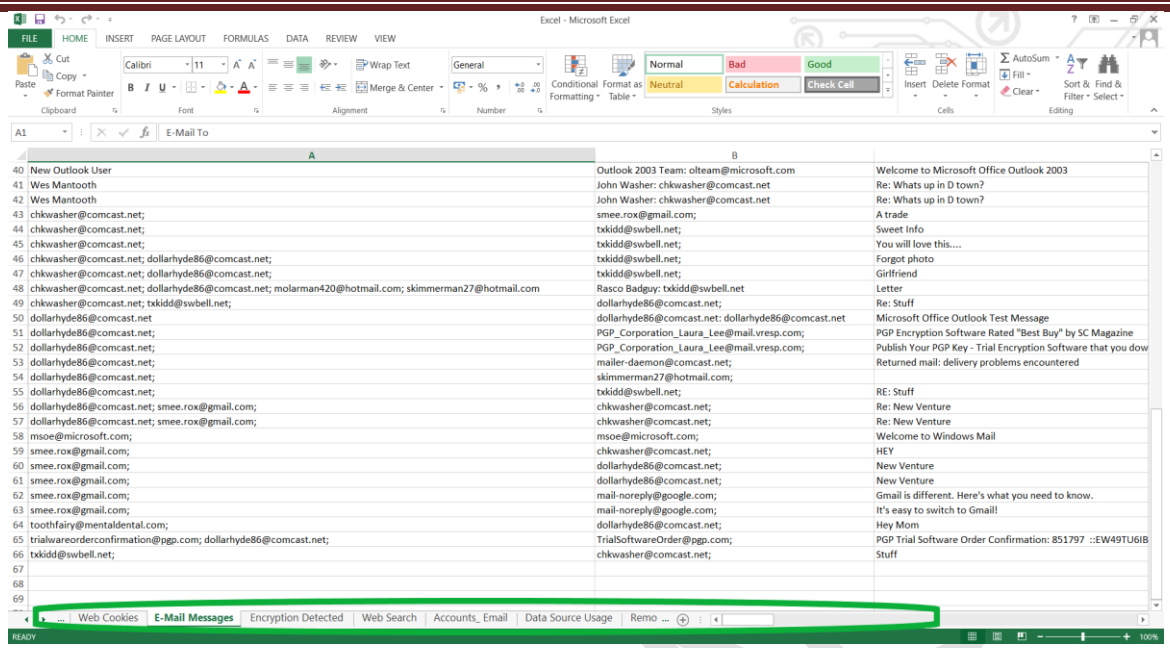
- **Interesting Items:** As discussed before, these are the file results based upon the custom rules set by the examiner.
- **Accounts:** Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts.



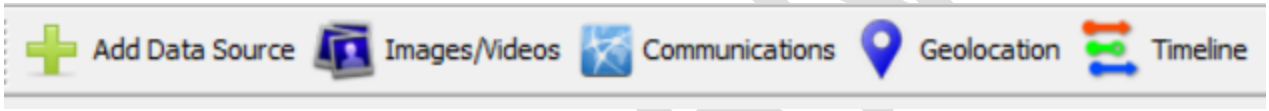
- **Reports:** Reports about the entire analysis of the data source can be generated and exported in many formats.


008 - Autopsy 4.15.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
File Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Mantooth.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-224909)
vol3 (DOS FAT12 (0x01): 224910-240974)
vol4 (Unallocated: 240975-250878)
Views
Results
Extracted Content
Keyword Hits
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Table
Thumbnail
7 Results
Save Table as CSV
Source Module Name
Report File Path
RecentActivity
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help
Hex
Text
Application
Page: 1 of 4

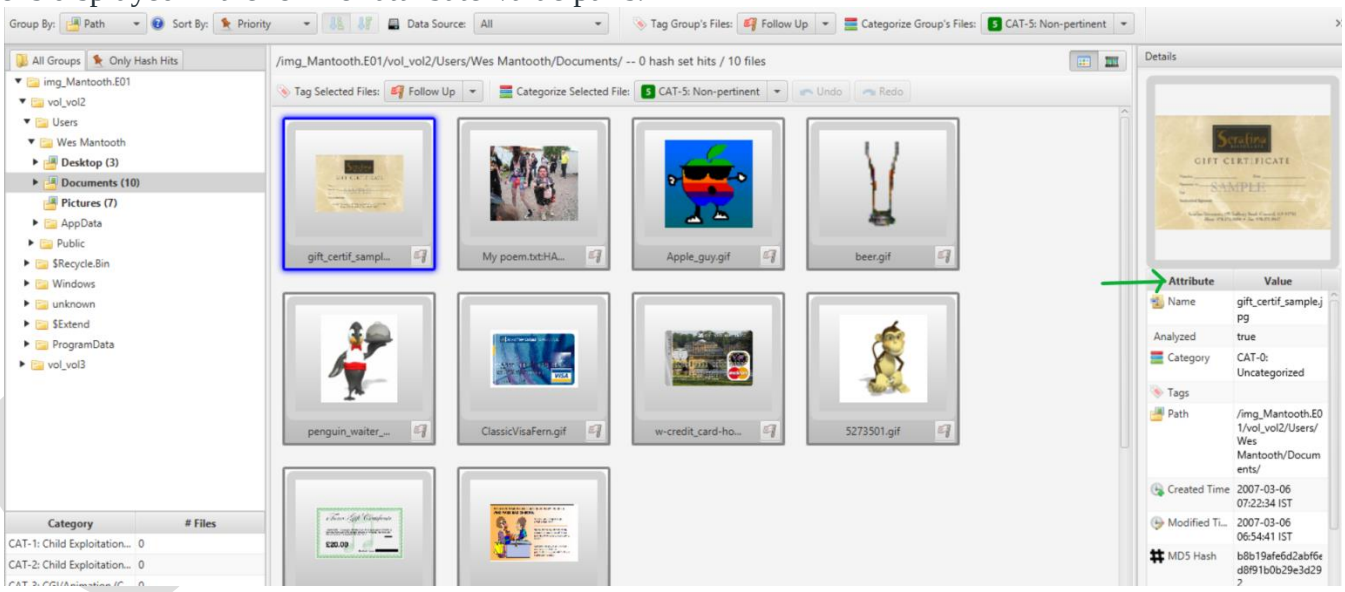

Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Result Types
< Back
Next >
Finish
Cancel
Help



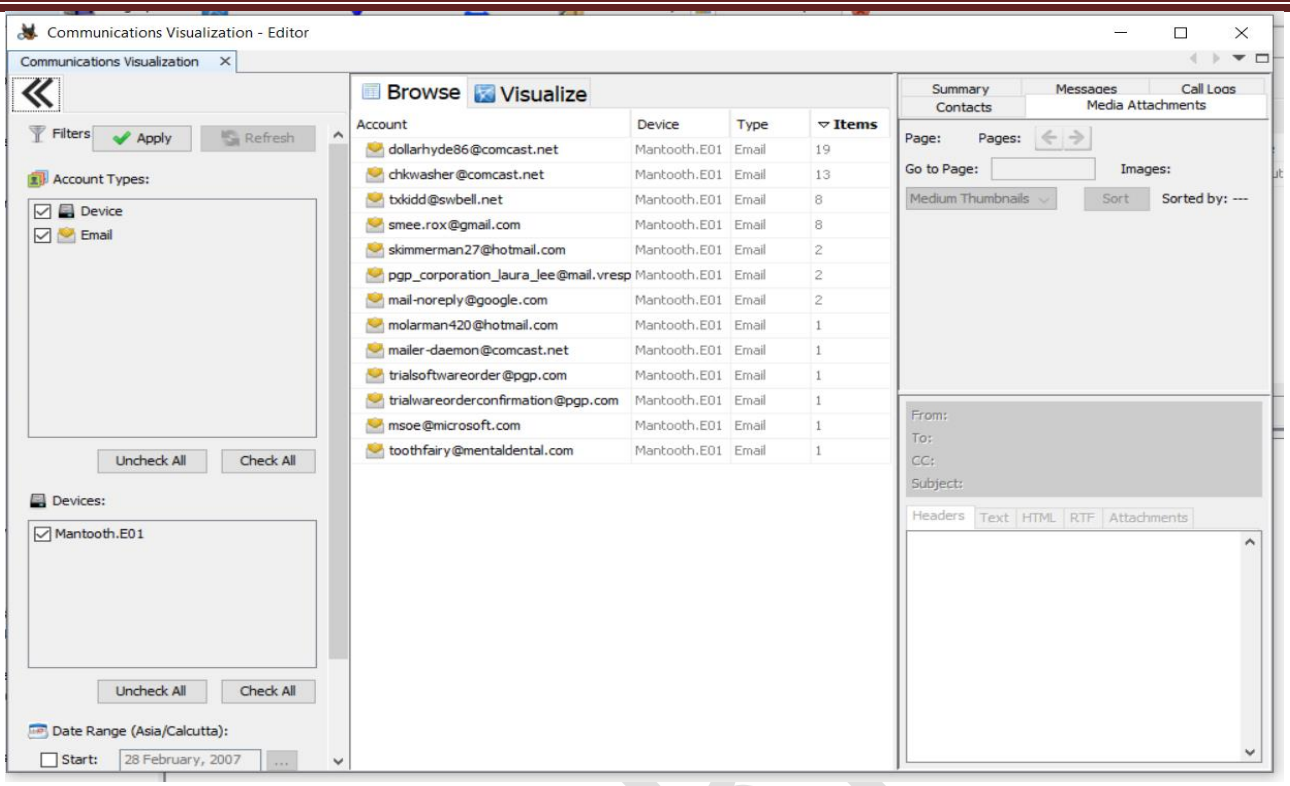
Additional Features:



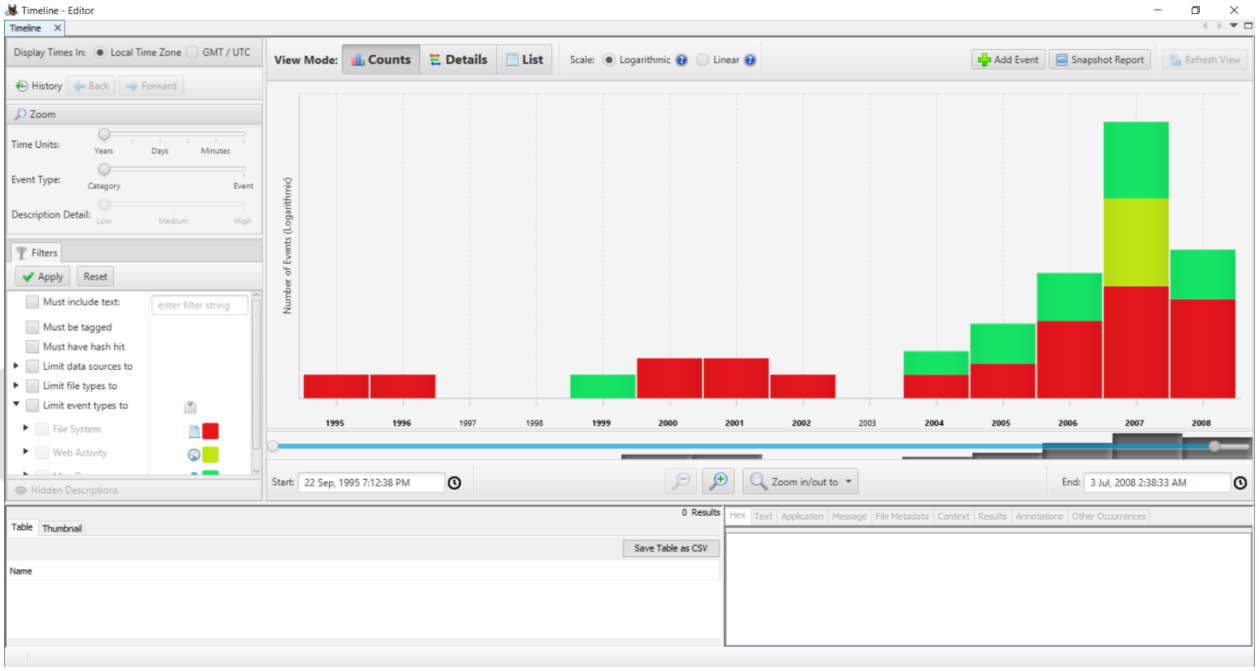
- **Add a Data Source:** Each case can hold multiple Data Sources.
- **Images/Videos:** Images/ Videos in the data source can be viewed in Gallery View. The information here is displayed in the form of attribute-value pairs.



- **Communications:** All the communications made using the source device are displayed here. This device had communications only in the form of emails.



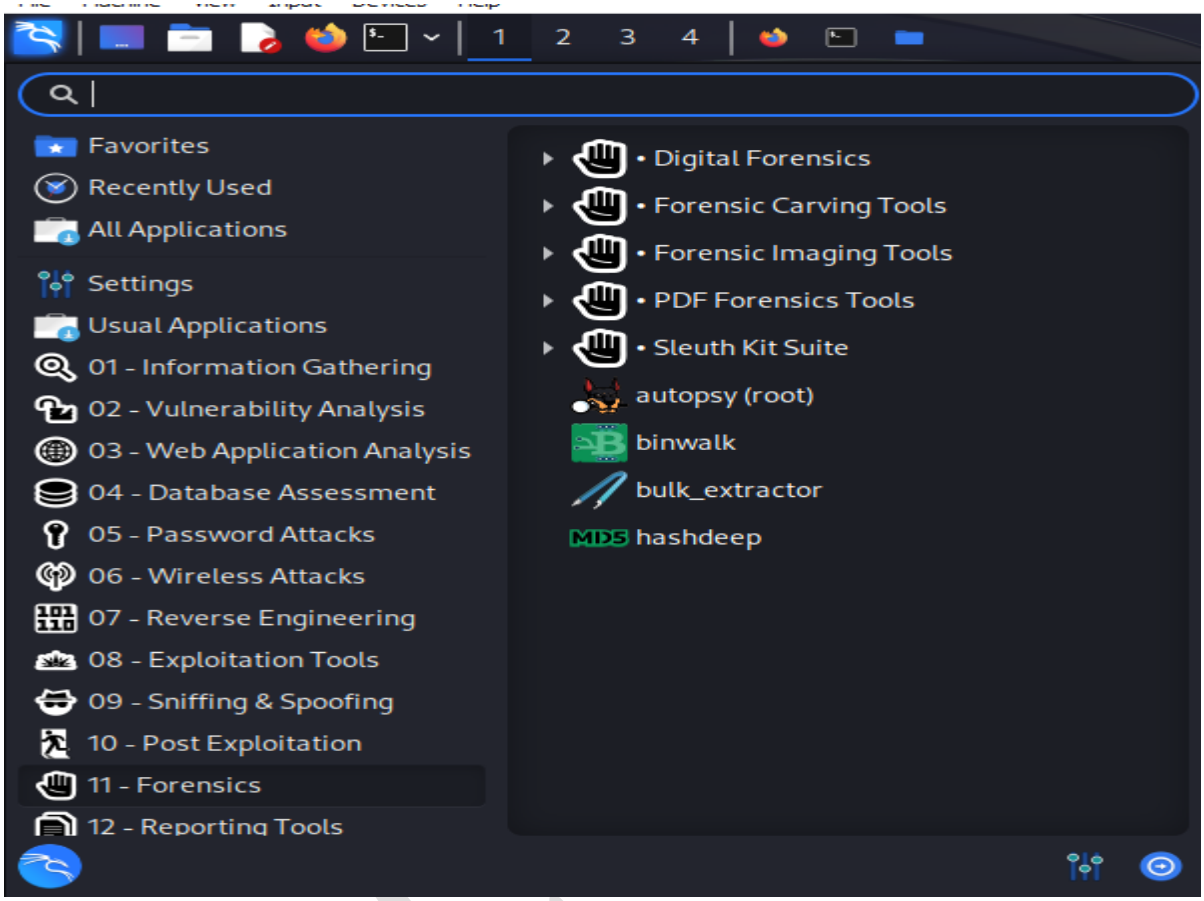
- **Geolocation:** This window displays the artifacts that have longitude and latitude attributes as waypoints on a map. Here the data source has no waypoints.
- **Timeline:** Information about when the computer was used or what events took place before or after a given event can be found, this greatly helps in investigating events near about a particular time.

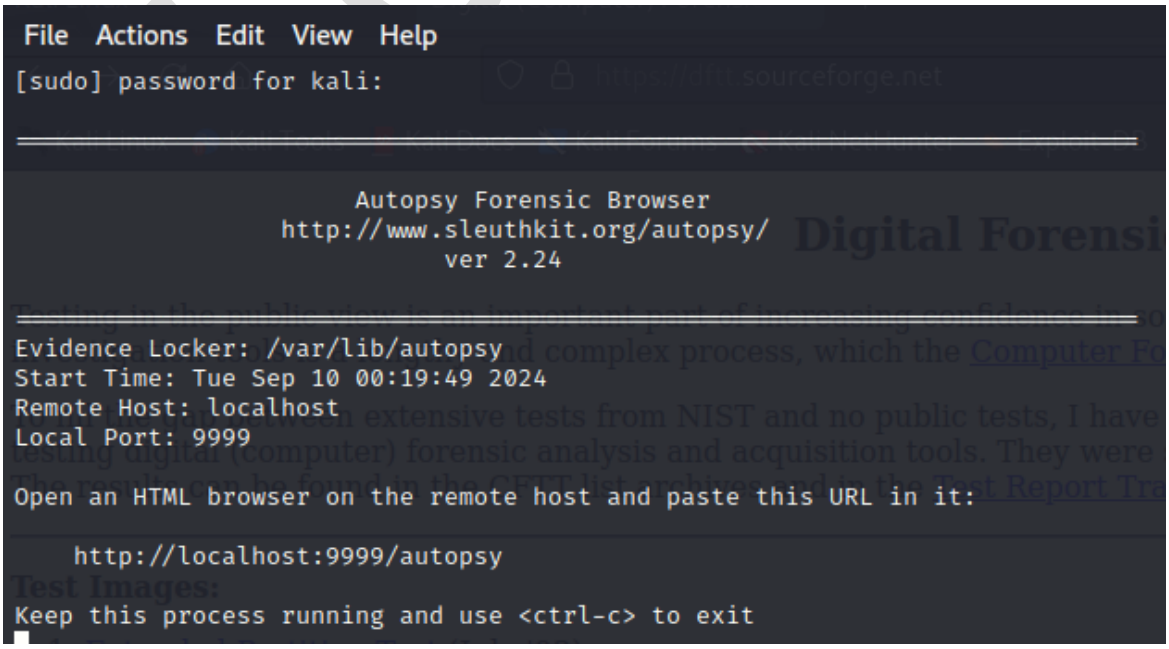


Almost all the basic features and how actually Autopsy works have been discussed in this article.

Autopsy Using Kali

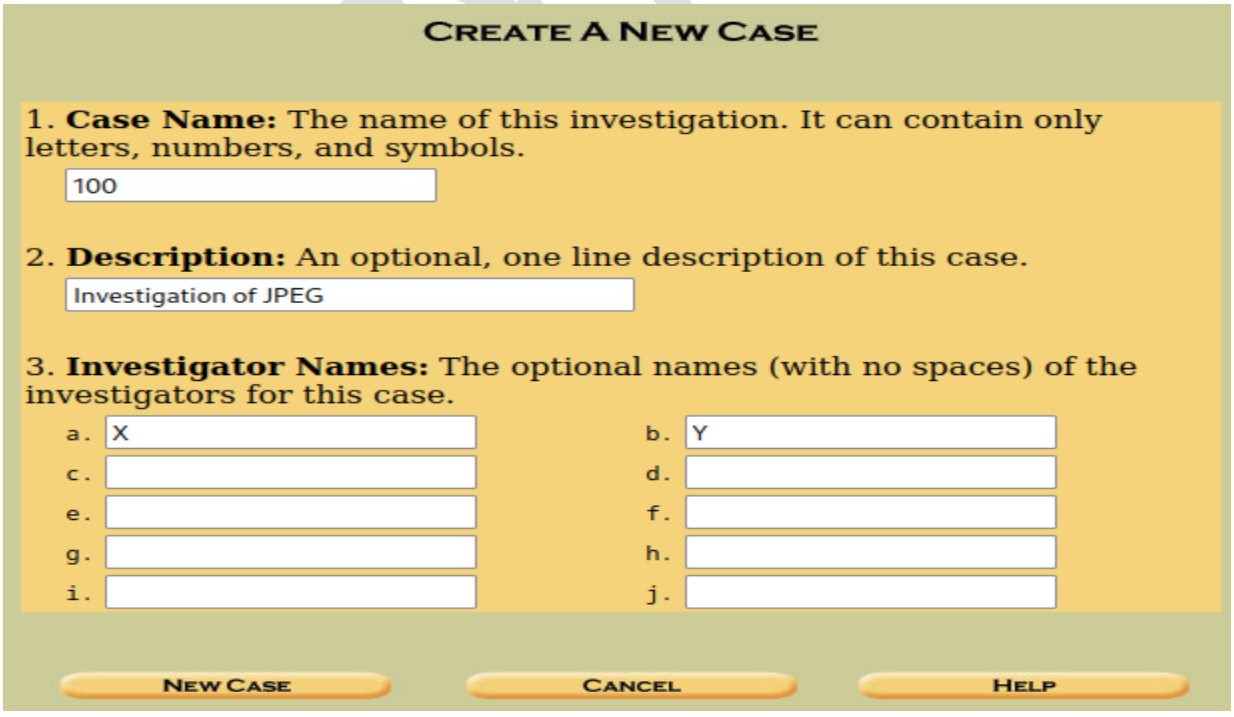
Download the images from: https://dftt.sourceforge.net/ in that select (8) JPEG Search Test #1 (Jun '04), extract in one folder and select the file with extension .dd



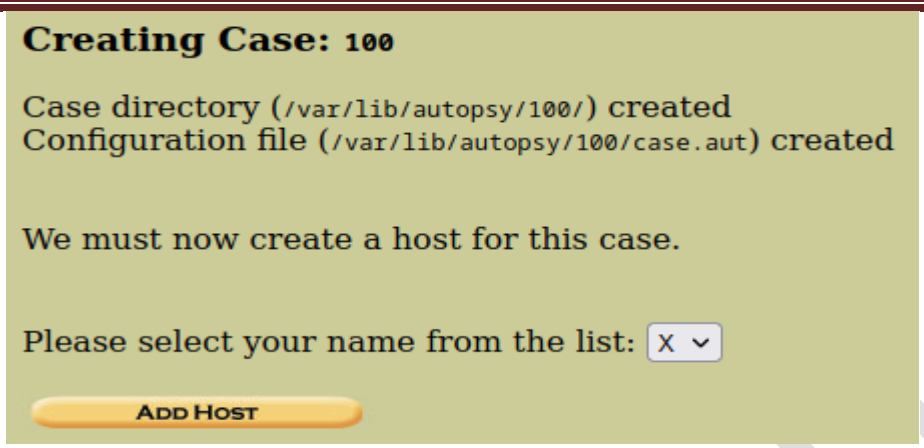


Copy the local host URL into the browser

Select New Case

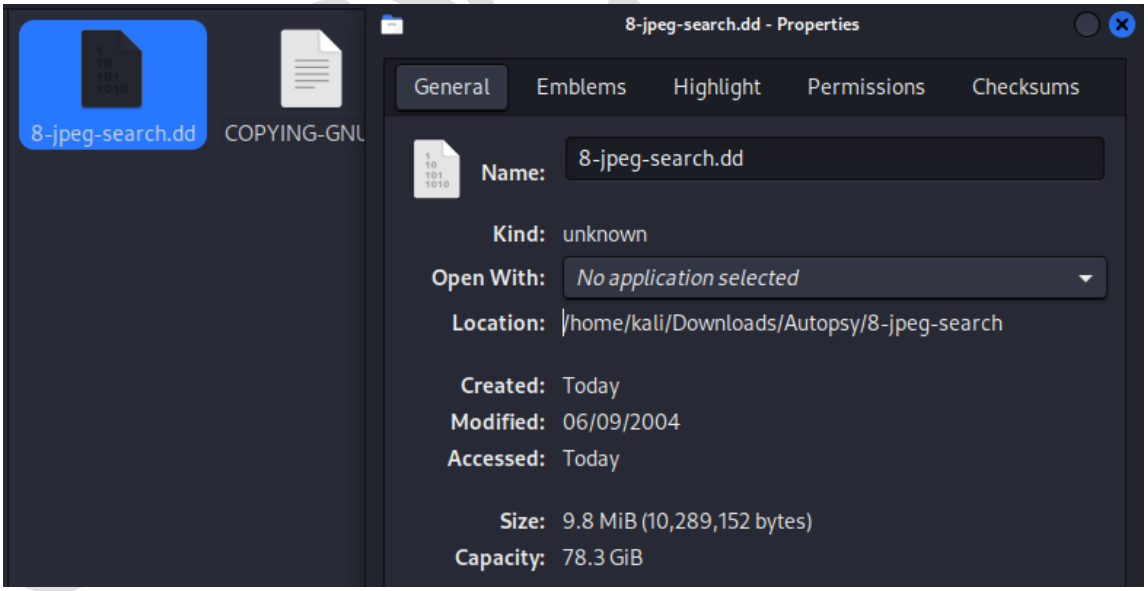


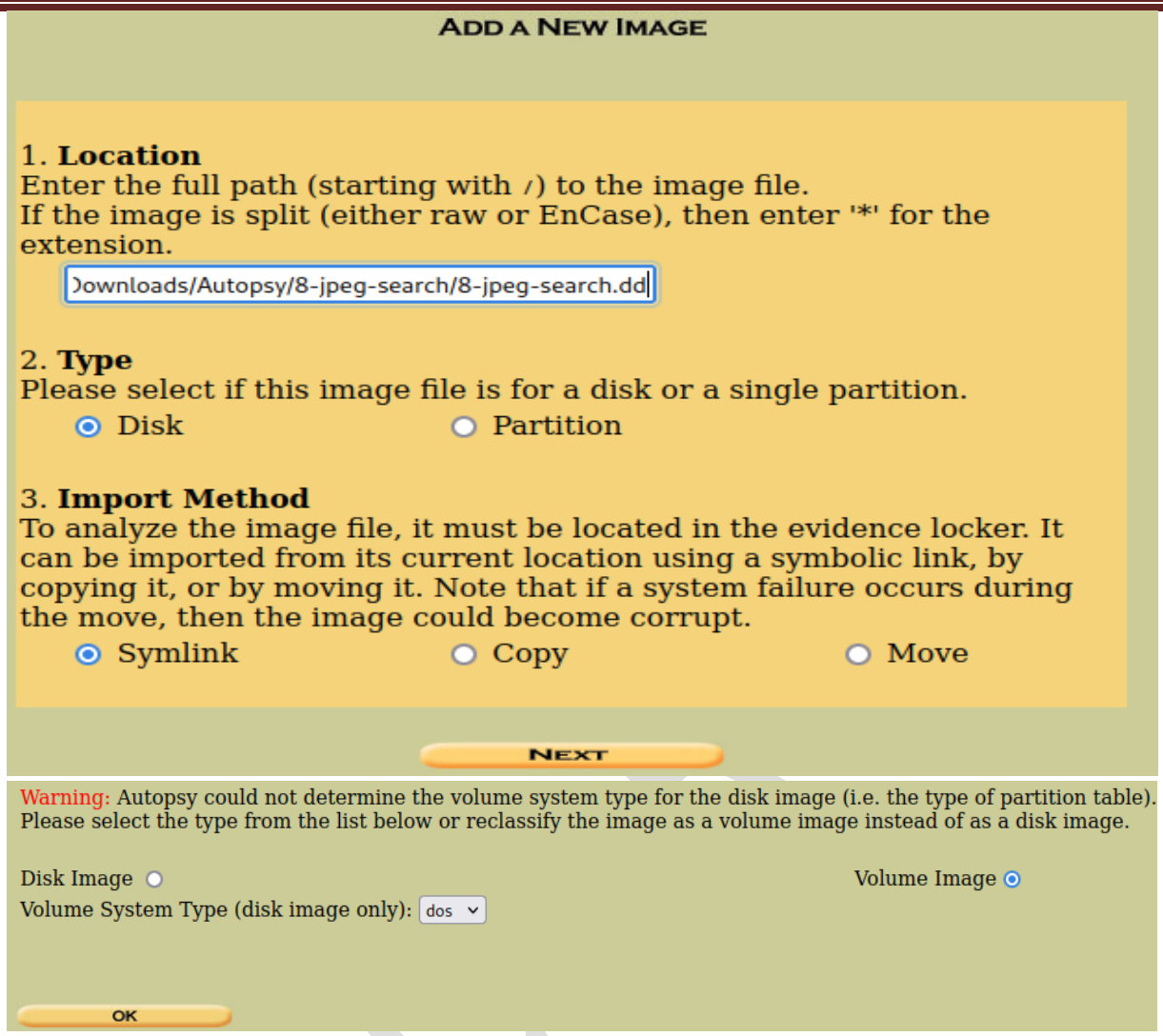
Click on new case



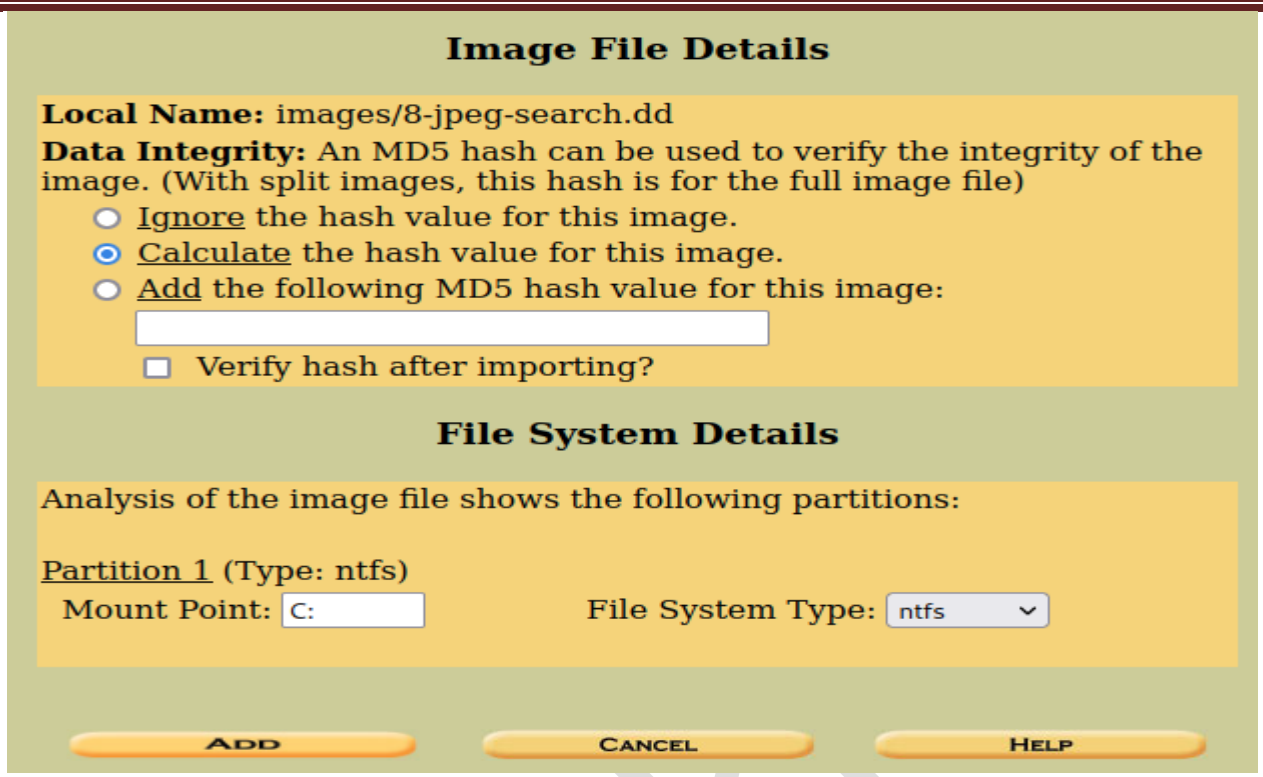
Click on add host

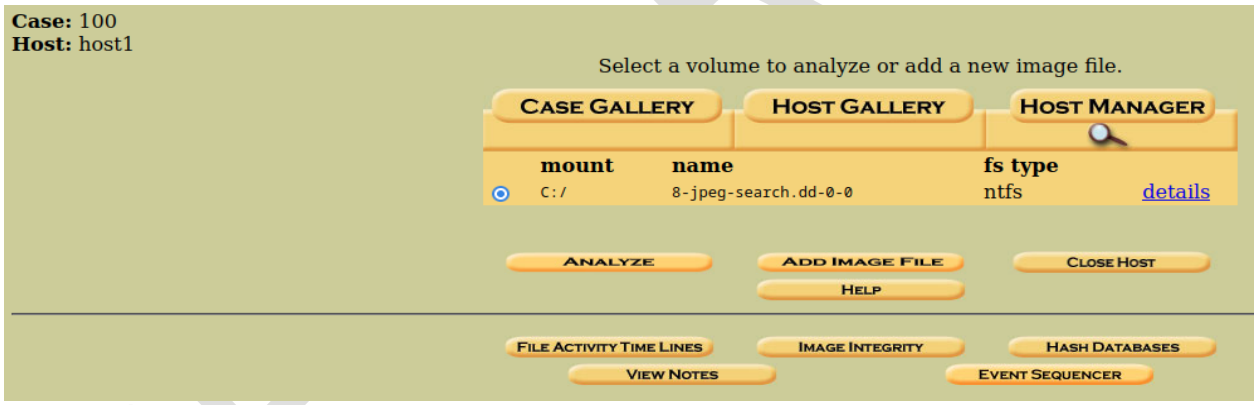
Provide host name




ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
)ownloads/Autopsy/8-jpeg-search/8-jpeg-search.dd
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.
Disk Image
Volume Image
Volume System Type (disk image only): dos
OK





Click on details, and click on analyze. It will provide the details and make analysis.

Autopsy:

https://www.youtube.com/watch?v=2PhJ4bCopGo&list=PLx2aAxxVN1NVk9JwAQwCNA159FrSXQ5Hn&ab_channel=SridharIyer

FTK Imager: https://www.youtube.com/watch?v=TkG4JqUcx_U&ab_channel=DFIRScience