Analysis of Data Source Using Autopsy

The Sleuth Kit is a library and a collection of command-line tools used to investigate disk images. Autopsy is the GUI program for TSK. The results of the forensic search carried over the images are displayed here. These results help the investigator to locate relevant sections of data in their investigation. It is used by law enforcement, military, and corporate examiners to investigate the actions taken place on the evidence computer, however, it can be used to recover deleted data from digital devices too.

Autopsy performs operations onto disk images which can be created using tools like FTK Imager. Here an already created image is used. You may download Autopsy from [here](#) and the disk image used in this article from [here](#).
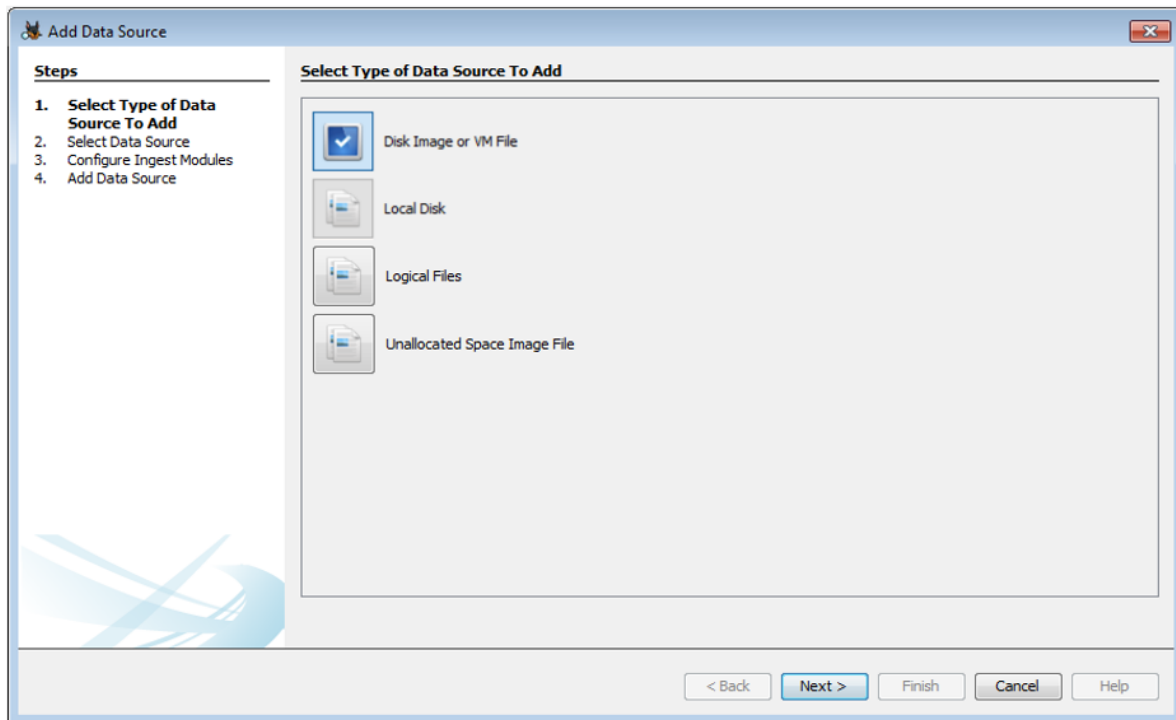
1. Getting Started
Open Autopsy and create a new case.


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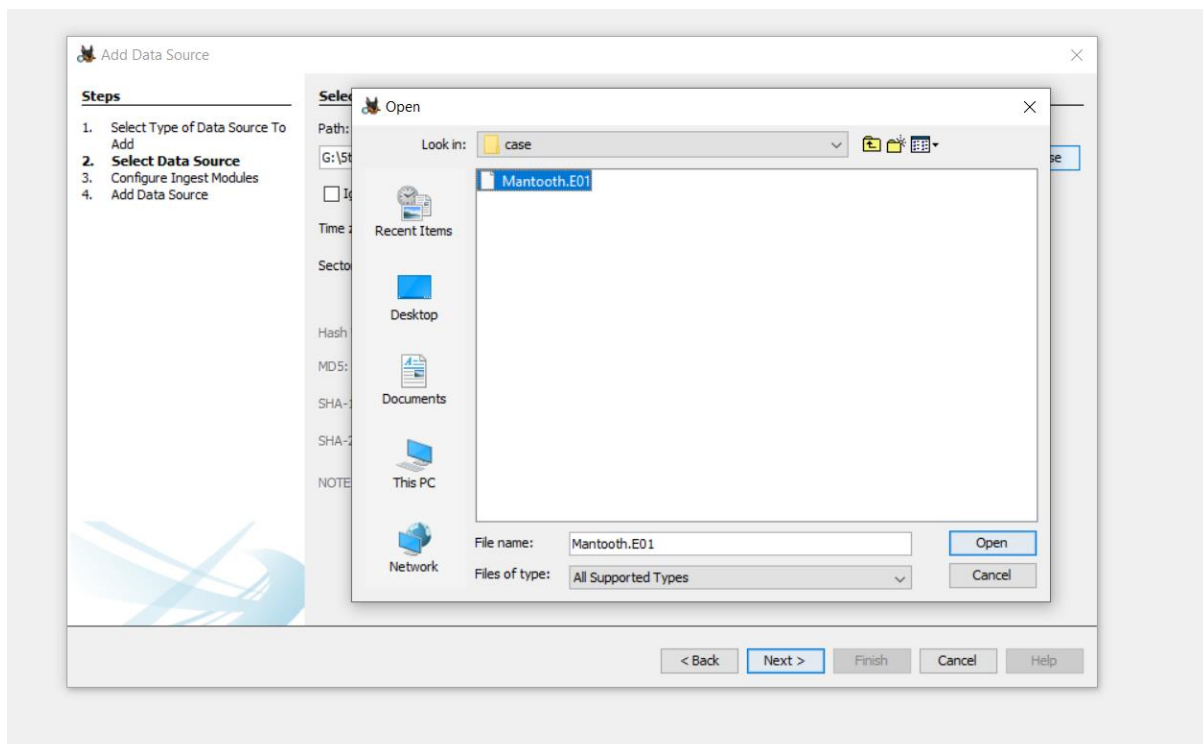
Configure ingest modules.
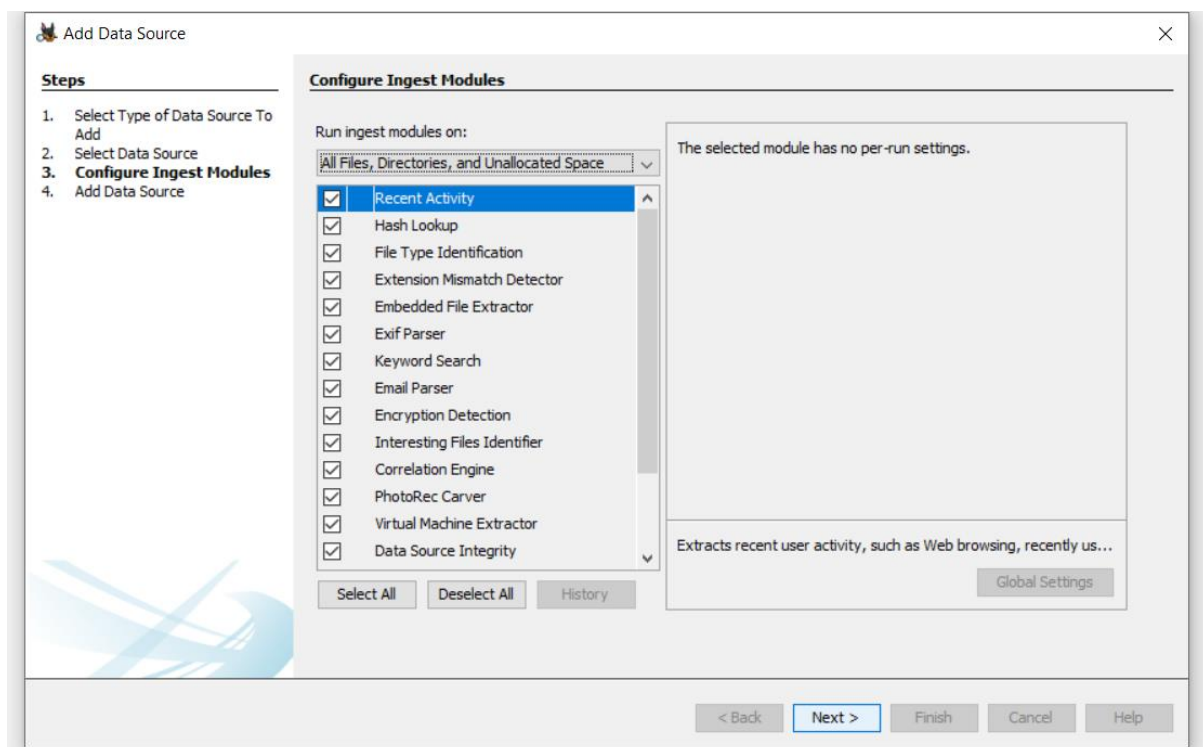
The ingest modules determine factors for which the data in the data source is to be analyzed. Here is a brief overview of each of them.

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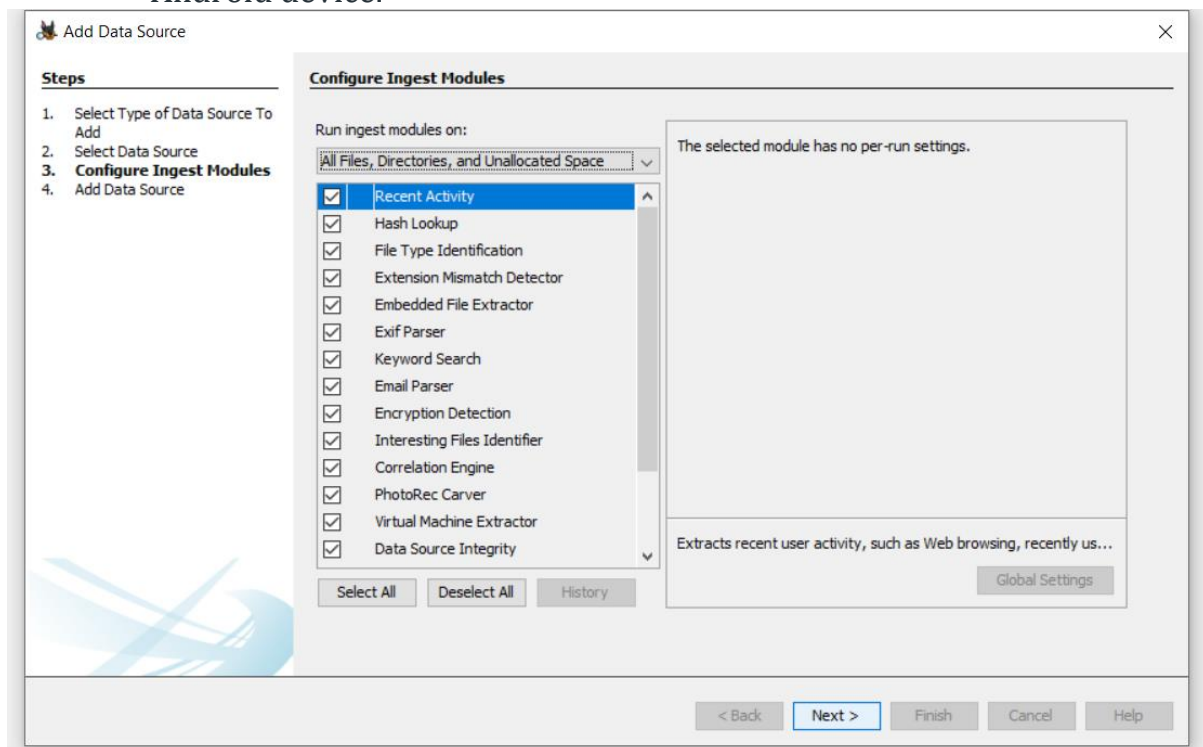
Select all that will serve the purpose of your investigation and click Next. Once the data source is added, click Finish. It will take some buffer time to extract and analyze the data depending upon the size of the Data Source.

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.
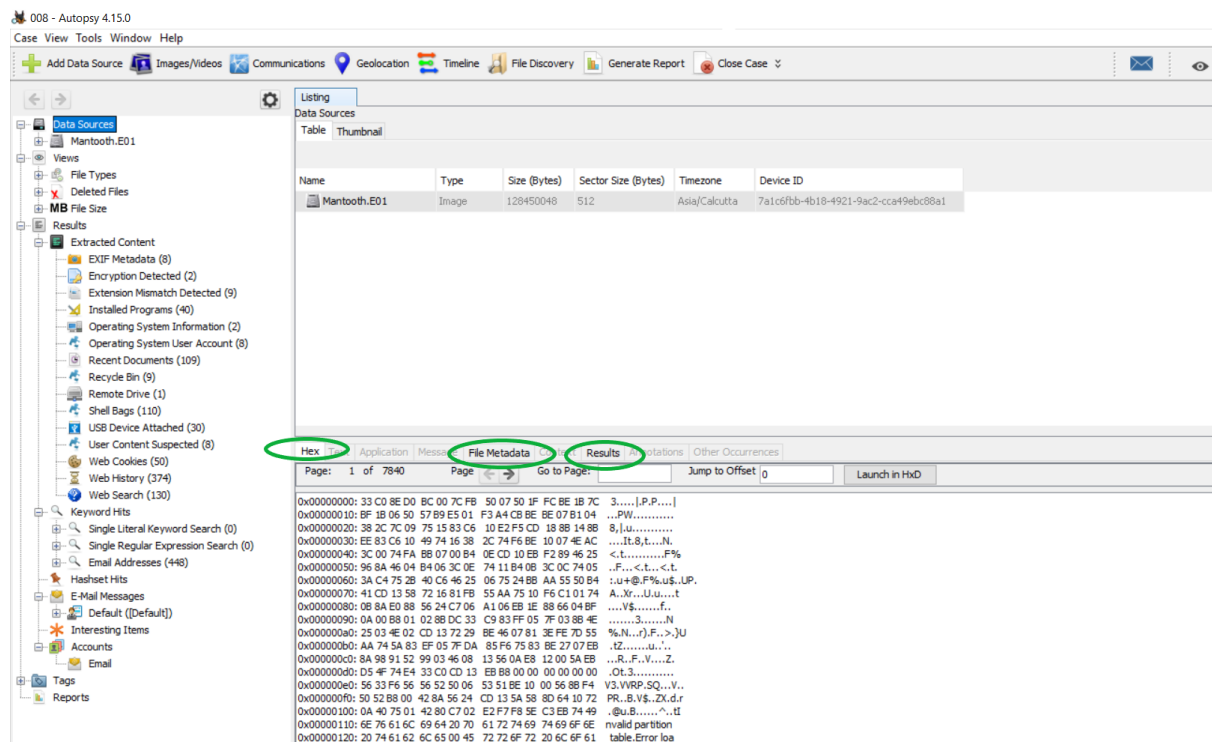
The disk image is then broken down based upon its volume partitions.
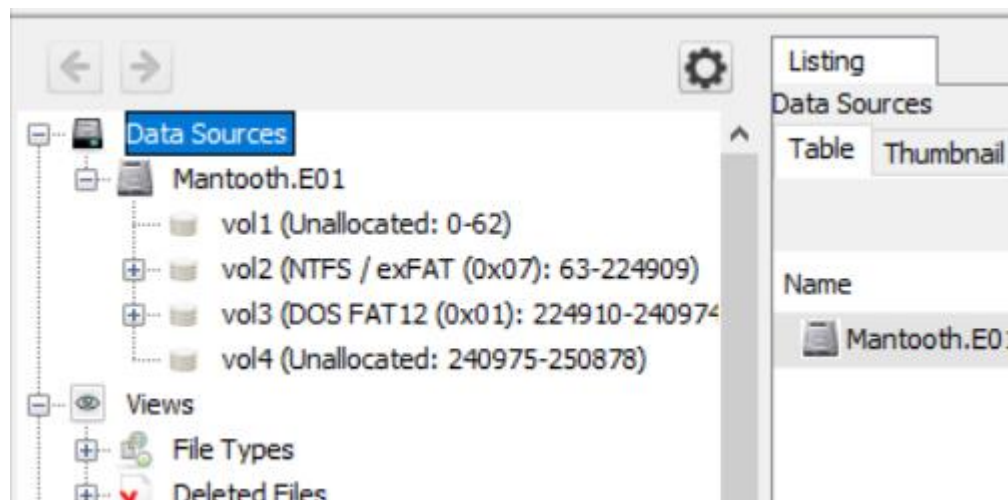
Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> Mantooth.E01 -> MSOCache-> [Parent Folder].
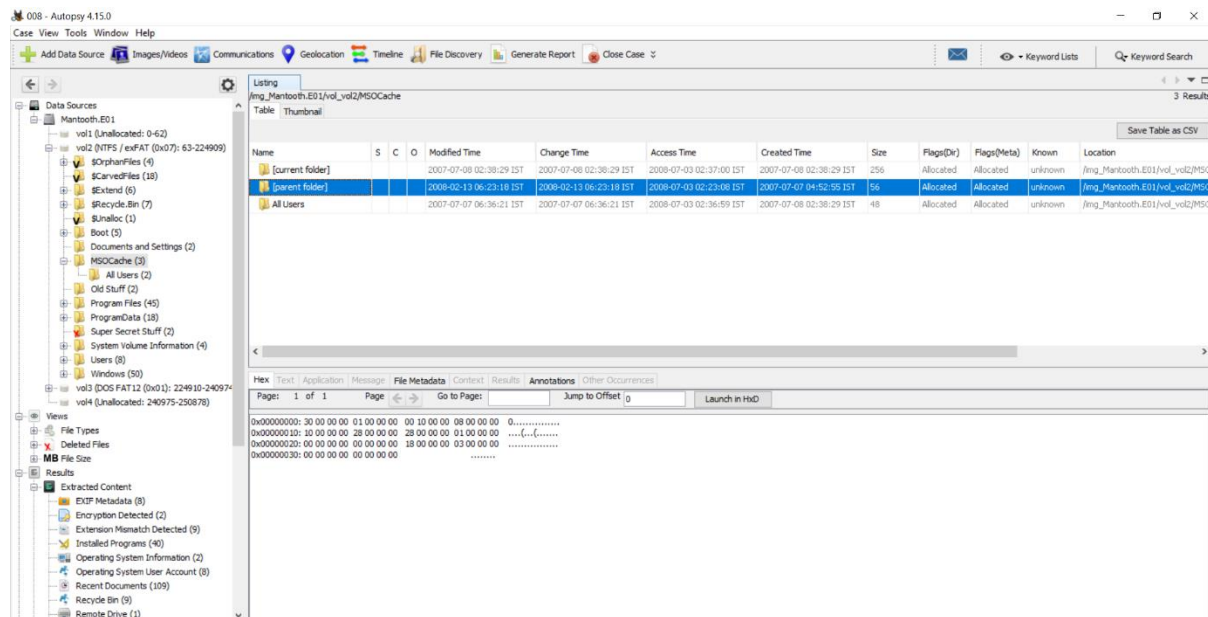
Views (Determines the factor of file classification)

- **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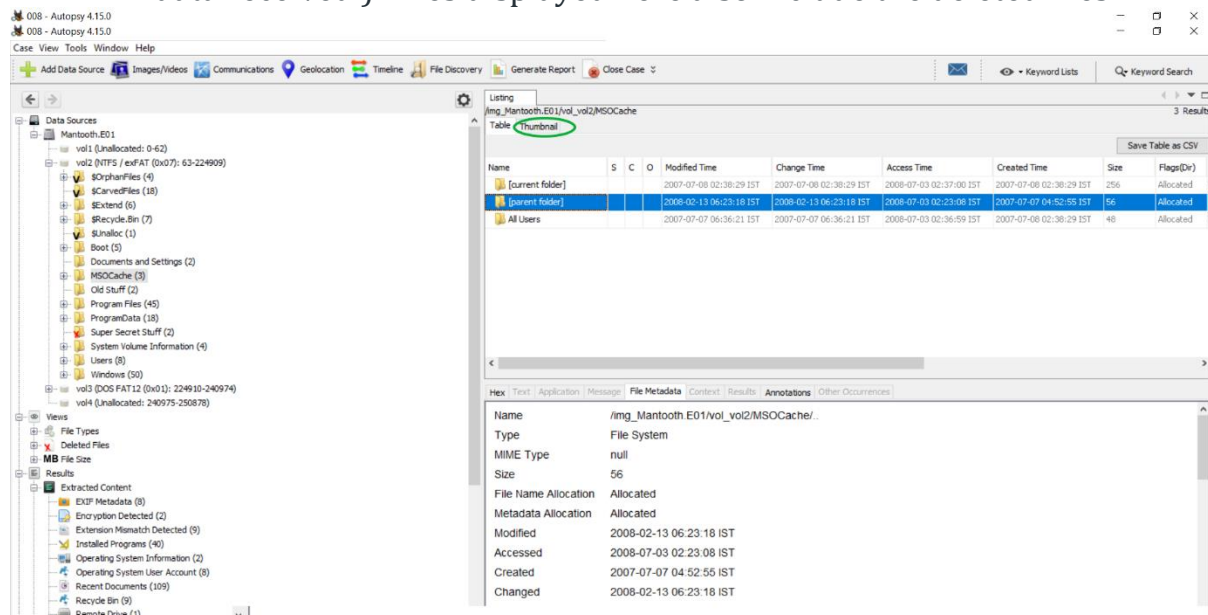 be used to open a file and MIME types are used by the browser to decide about how to present the data (or by the server on how to interpret the data received). Files displayed here also include the deleted files.

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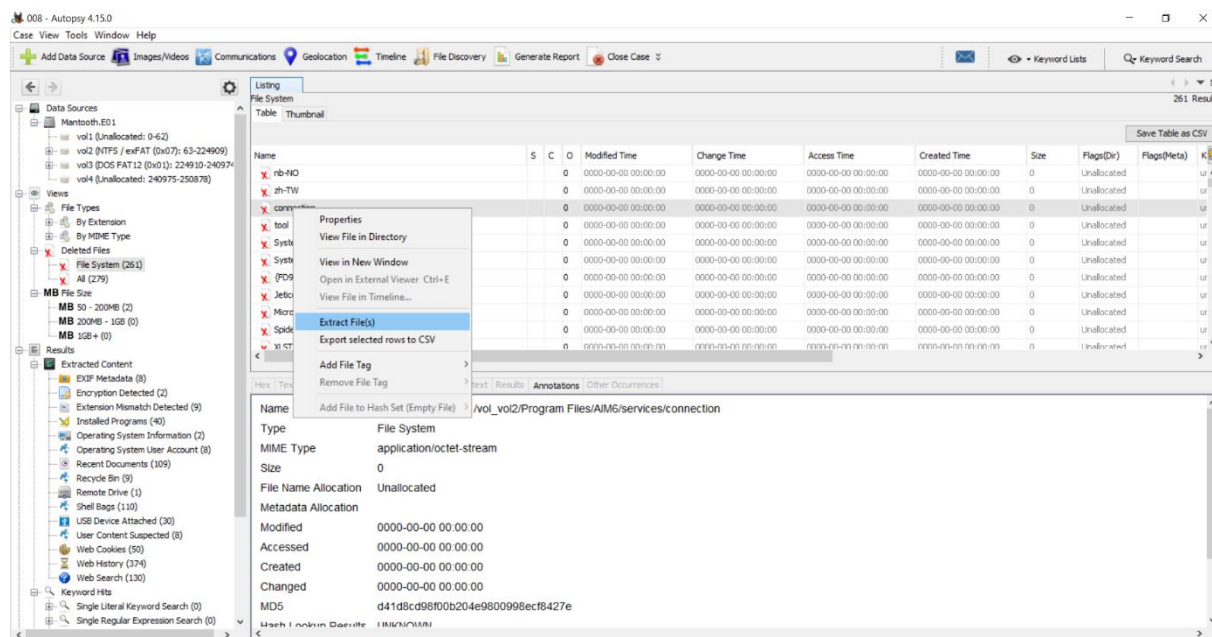
- **MB Size Files:** Here files are classified based upon their size. The range starts from 50MB. This enables the examiner to determine exclusively large files.

Note: It is usually advised to not scan or extract any suspected files/ disks such as payload files, etc. in the main system, rather scan them in safe environments such as a virtual machine, and then extract the data, as they hold the possibility of being corrupt and may infect the examiner's system with viruses.

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.
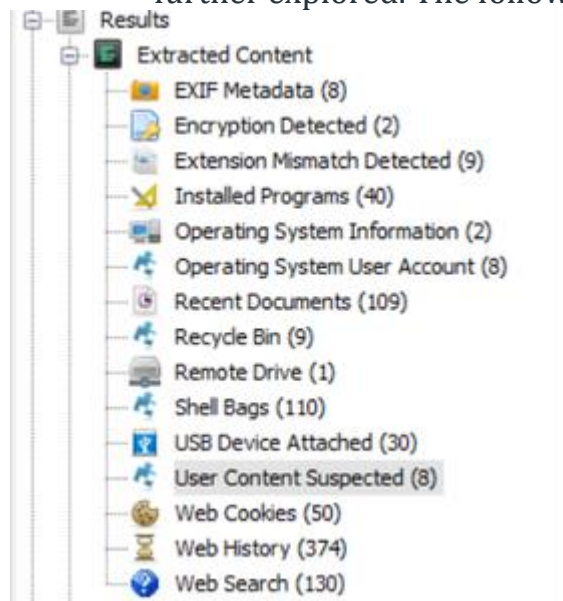
- **EXIF Metadata:** It contains all the .jpg images that have EXIF Metadata associated with them, this Metadata can be analyzed further.

- **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.
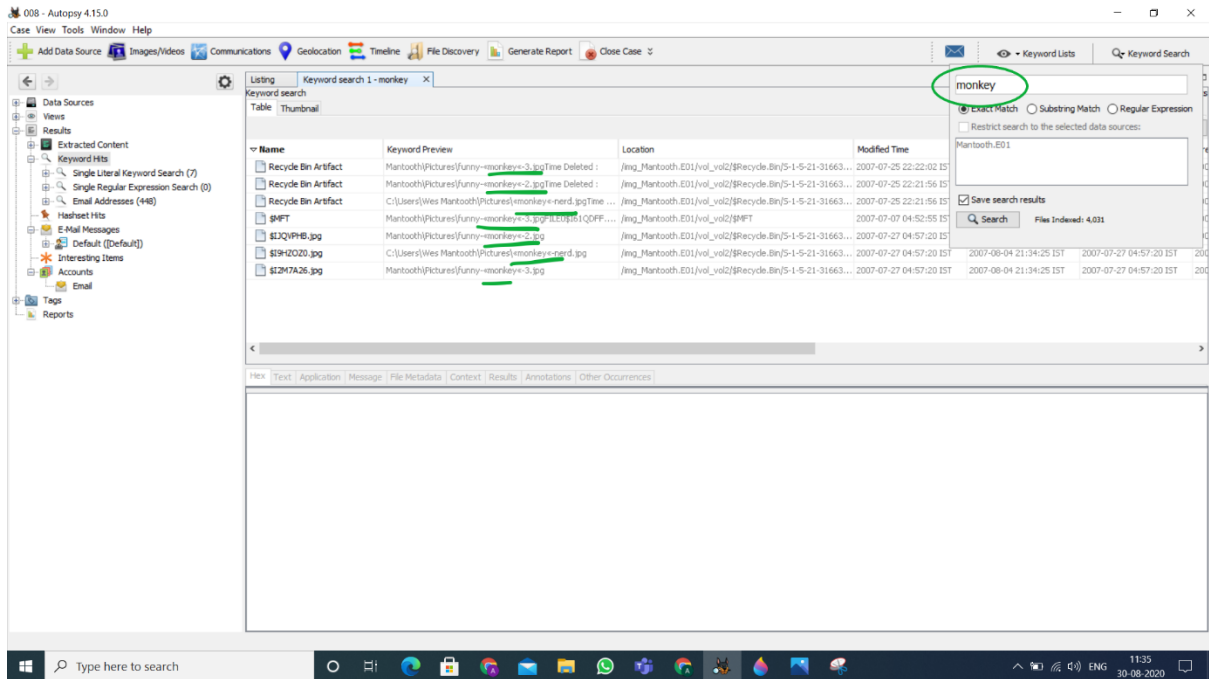
- **HashSet Hits:** Here the search can be made using hash values.
- **E-mail Messages:** Here all the *outlook.pst* files can be explored.
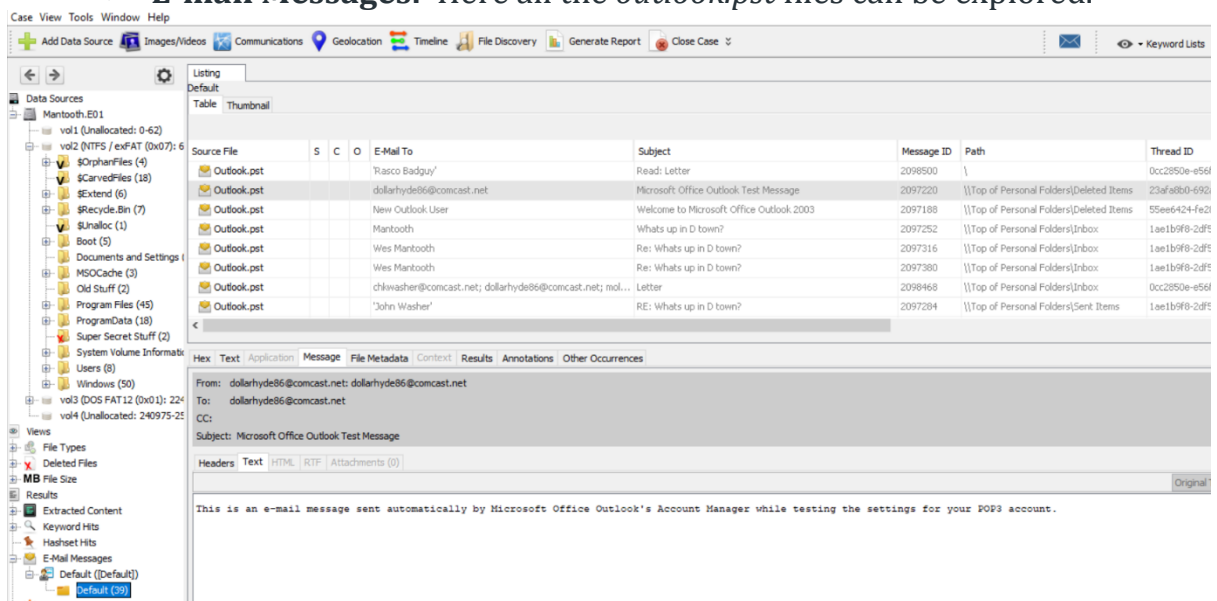
- **Interesting Items:** As discussed before, these are the file results based upon the custom rules set by the examiner.
- **Accounts:** Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts.

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

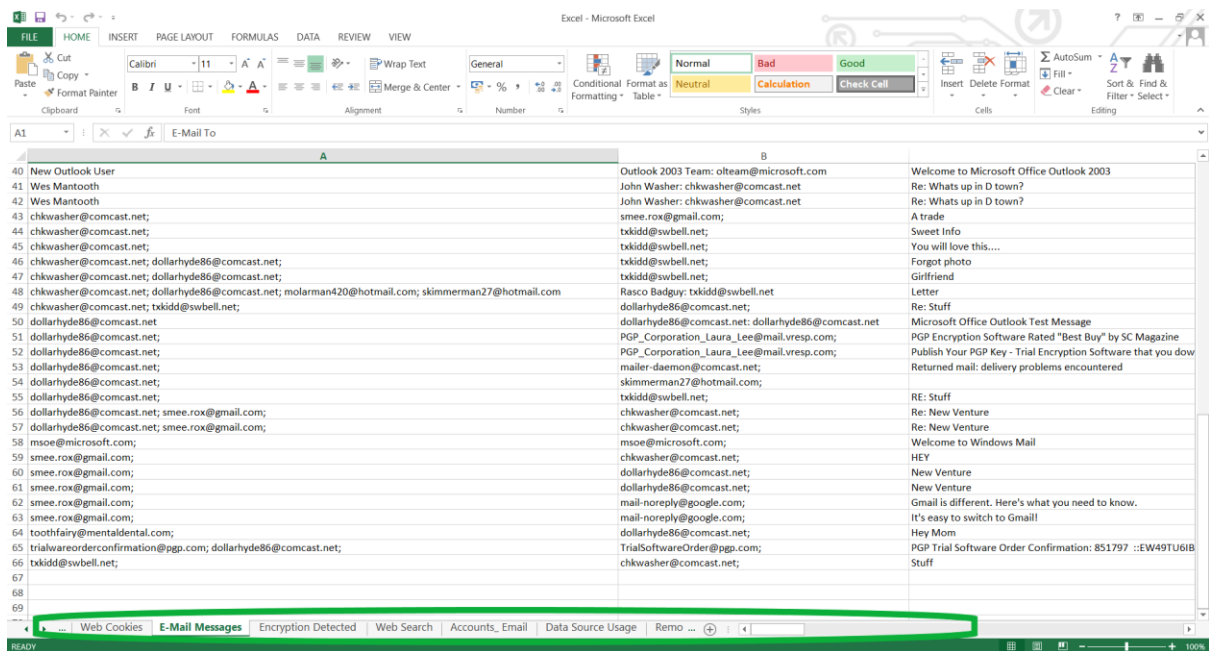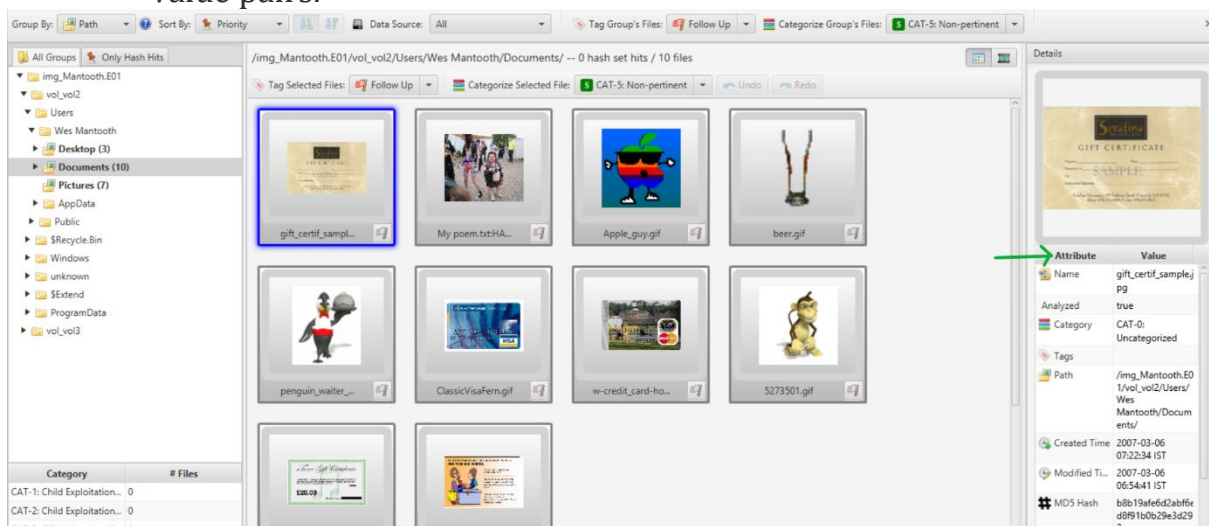|	A	B	
40	New Outlook User	Outlook 2003 Team: olteam@microsoft.com	Welcome to Microsoft Office Outlook 2003
41	Wes Mantooth	John Washer: chkwasher@comcast.net	Re: Whats up in D town?
42	Wes Mantooth	John Washer: chkwasher@comcast.net	Re: Whats up in D town?
43	chkwasher@comcast.net;	smee.rox@gmail.com;	A trade
44	chkwasher@comcast.net;	txkidd@swbell.net;	Sweet Info
45	chkwasher@comcast.net;	txkidd@swbell.net;	You will love this....
46	chkwasher@comcast.net; dollarhyde86@comcast.net;	txkidd@swbell.net;	Forgot photo
47	chkwasher@comcast.net; dollarhyde86@comcast.net;	txkidd@swbell.net;	Girlfriend
48	chkwasher@comcast.net; dollarhyde86@comcast.net; molarman420@hotmail.com; skimmerman27@hotmail.com	Rasco Badguy: txkidd@swbell.net	Letter
49	chkwasher@comcast.net; txkidd@swbell.net;	dollarhyde86@comcast.net;	Re: Stuff
50	dollarhyde86@comcast.net	dollarhyde86@comcast.net: dollarhyde86@comcast.net	Microsoft Office Outlook Test Message
51	dollarhyde86@comcast.net;	PGP_Corporation_Laura_Lee@mail.vresp.com;	PGP Encryption Software Rated "Best Buy" by SC Magazine
52	dollarhyde86@comcast.net;	PGP_Corporation_Laura_Lee@mail.vresp.com;	Publish Your PGP Key - Trial Encryption Software that you dow
53	dollarhyde86@comcast.net;	mailer-daemon@comcast.net;	Returned mail: delivery problems encountered
54	dollarhyde86@comcast.net;	skimmerman27@hotmail.com;	
55	dollarhyde86@comcast.net;	txkidd@swbell.net;	RE: Stuff
56	dollarhyde86@comcast.net; smee.rox@gmail.com;	chkwasher@comcast.net;	Re: New Venture
57	dollarhyde86@comcast.net; smee.rox@gmail.com;	chkwasher@comcast.net;	Re: New Venture
58	msoe@microsoft.com;	msoe@microsoft.com;	Welcome to Windows Mail
59	smee.rox@gmail.com;	chkwasher@comcast.net;	HEY
60	smee.rox@gmail.com;	dollarhyde86@comcast.net;	New Venture
61	smee.rox@gmail.com;	dollarhyde86@comcast.net;	New Venture
62	smee.rox@gmail.com;	mail-noreply@google.com;	Gmail is different. Here's what you need to know.
63	smee.rox@gmail.com;	mail-noreply@google.com;	It's easy to switch to Gmail!
64	toothfairy@mentaldental.com;	dollarhyde86@comcast.net;	Hey Mom
65	trialwareorderconfirmation@pgp.com; dollarhyde86@comcast.net;	TrialSoftwareOrder@pgp.com;	PGP Trial Software Order Confirmation: 851797 ::EW49TU6IB
66	txkidd@swbell.net;	chkwasher@comcast.net;	Stuff
67			
68			
69			

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.
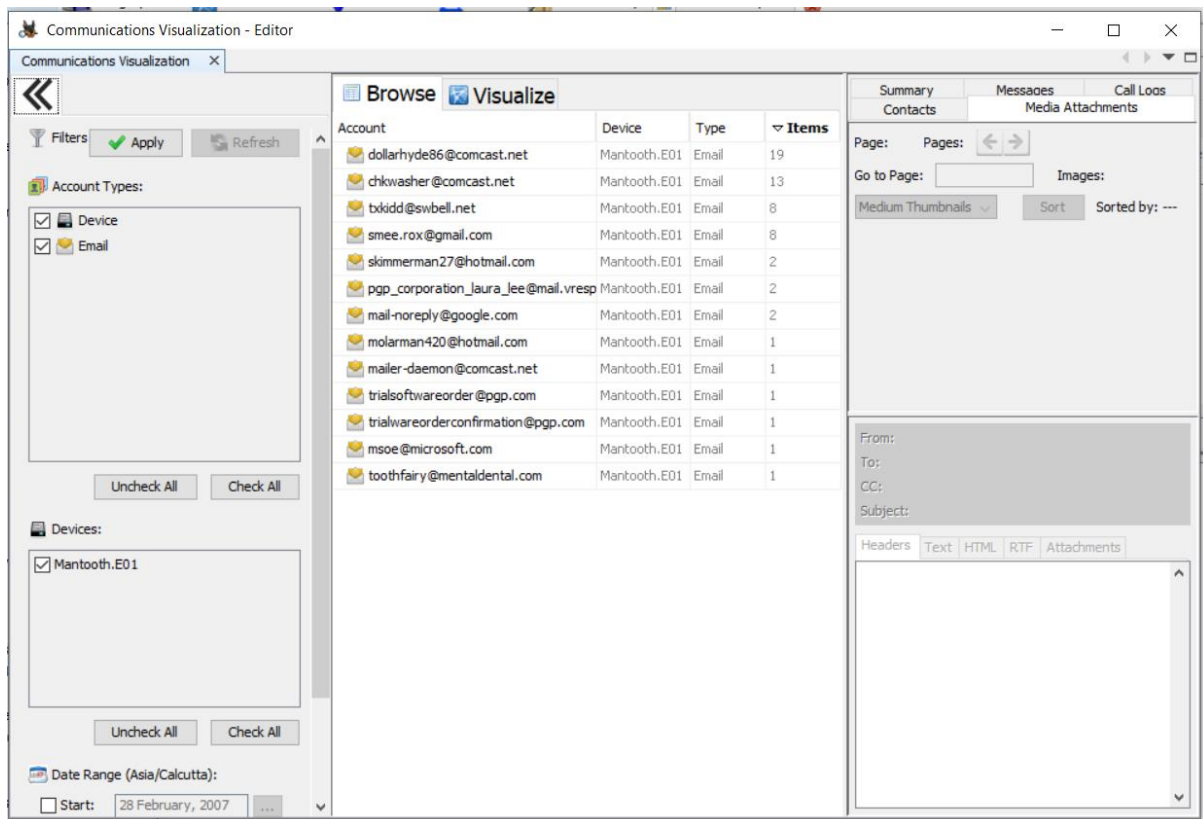
- **Geolocation:** This window displays the artifacts that have longitude and latitude attributes as waypoints on a map. Here the data source has no waypoints.
- **Timeline:** Information about when the computer was used or what events took place before or after a given event can be found, this greatly helps in investigating events near about a particular time.
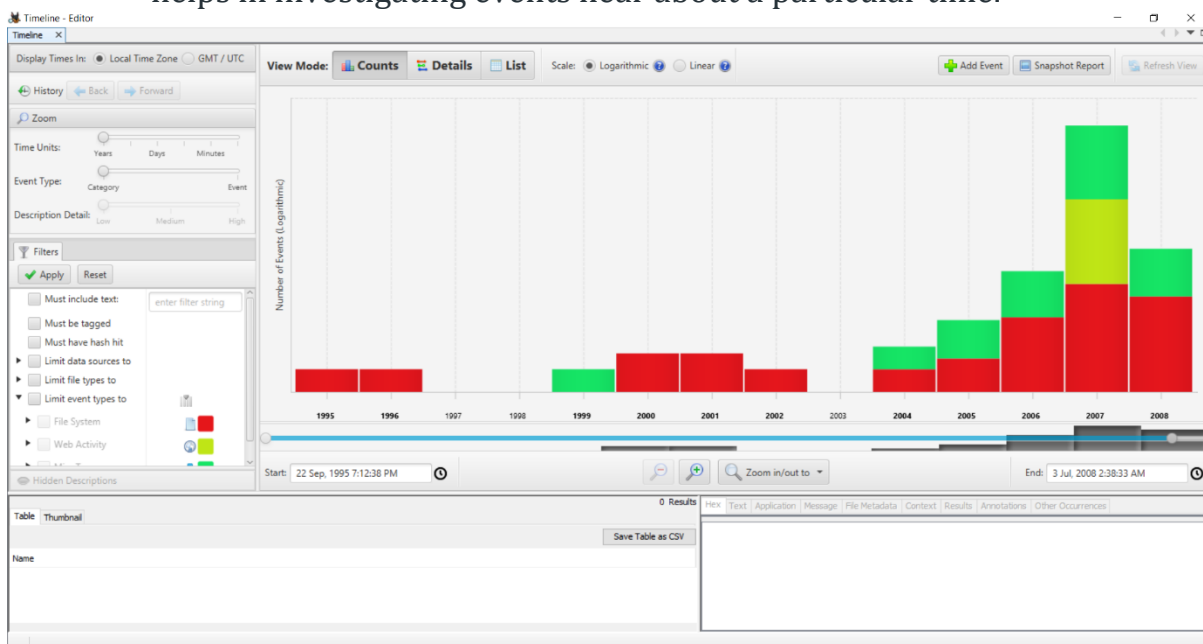
Almost all the basic features and how actually Autopsy works have been discussed in this article. However, it is always recommended to go through different sample data sources to explore even more.