1Introduction:

1.1objective:

The objective of the project is to extract website artifacts from various web browsers such as Firefox, Edge, and Chrome. The project also aims to find specific search terms on disk and phone using the Autopsy forensic tool. The extracted website artifacts and search terms can be used to conduct forensic investigations on a device.

1.2Description:

The project aims to extract website artifacts from various providers such as Firefox, Edge, and Chrome, and to find out specific search terms on disk and phone using Autopsy forensic tool.

The first step in the project is to extract website artifacts from different web browsers. This involves identifying the different browsers used on the disk or phone, and then accessing their cache files to retrieve website data. This may include saved cookies, browsing history, bookmarks, and other metadata related to web activity.

The second step is to use Autopsy forensic tool to analyze the extracted data and identify specific search terms. Autopsy is an open-source digital forensic tool that allows investigators to conduct a thorough examination of a disk image, analyze file systems, and recover deleted files.

By using Autopsy, the project team can conduct a comprehensive search of the extracted data and locate specific keywords or search terms. This may include search terms related to specific topics, products, or services, or terms that could potentially indicate suspicious or criminal activity.

Overall, the project's main objective is to gather valuable insights into a person's web activity, search history, and potentially identify any nefarious activity that may be hidden within their digital footprint. The findings of the project could be used in various domains such as law enforcement, cybersecurity, or even marketing research.

1.3scope:

The scope of the project is to extract website artifacts from various web browsers such as Firefox, Edge, and Chrome. The project will involve using forensic tools to extract data from the disk and phone of a system. The primary objective of the project is to find specific search terms used on the system by the user.

The project will require expertise in forensic analysis and knowledge of various web browsers. The data extraction process will involve using Autopsy forensic tool, which is an open-source platform used for digital forensics investigation.

The project will also require a detailed analysis of the extracted data to identify relevant information such as the user's browsing history, downloaded files, and cached data. The project will involve studying the user's internet activity and the specific search terms used by them.

The project's outcome will be a report detailing the extracted data, including the specific search terms used on the system. The report will also include a detailed analysis of the user's internet activity, including their browsing history and downloaded files.

The project's scope does not include any illegal activity, and all data extraction and analysis will be carried out within the bounds of the law. The project will adhere to ethical standards, and all user data will be kept confidential and handled with care.

2.System description:

Device name	prince
Processor	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
Installed RAM	8.00 GB (7.88 GB usable)
Device ID	32298B3C-462C-4933-B0EA-6F20EDB08E99
Product ID	00327-35845-39470-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

2.2Assumpption and dependencies:

2.2.1Assumptions:

The project assumes that the websites artifacts are stored on the disk and phone.

The project assumes that the Autopsy forensic tool can extract website artifacts from Firefox, Edge, and Chrome.

The project assumes that the search terms used to find the website artifacts are known.

2.2.2Dependencies:

The project depends on the availability of the Firefox, Edge, and Chrome browsers on the system.

The project depends on the availability of Autopsy forensic tool.

The project depends on the availability of the search terms used to find the website artifacts.

The project depends on the ability of Autopsy forensic tool to extract website artifacts from the browsers.

The project depends on the ability of the forensic analyst to interpret the extracted website artifacts.

2.3Functional Non functional dependencies:

2.3.1The functional dependencies of the project "Extract the website artifacts from various providers such as Firefox, Edge, and Chrome" could include:

1.Ability to extract website artifacts such as cookies, browsing history, bookmarks, etc. from multiple browsers such as Firefox, Edge, and Chrome.

2.Compatibility with various versions of the browsers.

3.Ability to extract artifacts from both desktop and mobile versions of the browsers.

4.Efficient storage of the extracted artifacts.

5.Providing easy access to the extracted artifacts.

2.3.2The non-functional dependencies of the project could include:

1.Performance - the time taken to extract the artifacts.

2.Reliability - ensuring that all the artifacts are extracted accurately and completely.

3.Security - ensuring that the extracted artifacts are stored and accessed securely.

4.Compatibility - ensuring that the tool is compatible with different operating systems and file formats.

5.User-friendliness - ensuring that the tool is easy to use and navigate for both technical and non-technical users.

2.3.3As for finding specific search terms on disk and phone using Autopsy forensic tool, the functional dependencies could include:

1.Ability to search for specific terms across various types of artifacts such as emails, documents, images, and videos.

2.Compatibility with various file formats and operating systems.

3.Ability to search for specific terms on both disk and mobile devices.

4.Providing the ability to refine search results and filter out irrelevant information.

5.Providing the ability to export search results for further analysis.

6.The non-functional dependencies of this project could include:

7.Performance - the time taken to perform a search and return results.

8.Reliability - ensuring that all search results are accurate and complete.

9.Security - ensuring that the search results are stored and accessed securely.

10.Compatibility - ensuring that the tool is compatible with different operating systems and file formats.

11.User-friendliness - ensuring that the tool is easy to use and navigate for both technical and non-technical users.

3.Analysis Report:

When conducting a digital forensic investigation, it is important to follow proper procedures to ensure the integrity and accuracy of the data. The first step is to acquire a forensic image of the disk or phone being analyzed. This involves creating a bit-for-bit copy of the entire storage device, including any hidden or deleted files.

Once the forensic image has been created, it can be loaded into Autopsy, which is a widely-used open-source forensic tool that provides a graphical user interface for analyzing digital evidence. Autopsy has built-in modules for analyzing various types of data, including web browsing history.

To extract website artifacts, i use Autopsy's web history module to view a list of all websites visited by the user. This list may include the URL, title, and timestamp for each site visited, as well as any search terms used on the site. i also use Autopsy's keyword search functionality to search for specific terms within the web history.

To find specific search terms on the disk or phone, i also use Autopsy's keyword search functionality to search for those terms within all files on the device. This may include text files, email messages, chat logs, and other types of documents. Autopsy can also search for deleted files and file fragments, which may contain relevant information.

After extracting and analyzing the website artifacts and search terms, icompile a report summarizing their findings. The report include detailed information about the methods used to extract and analyze the data, as well relevant findings and conclusions. i can ensure that the report is accurate, objective, and free from bias, and that any personal or confidential information is properly protected.

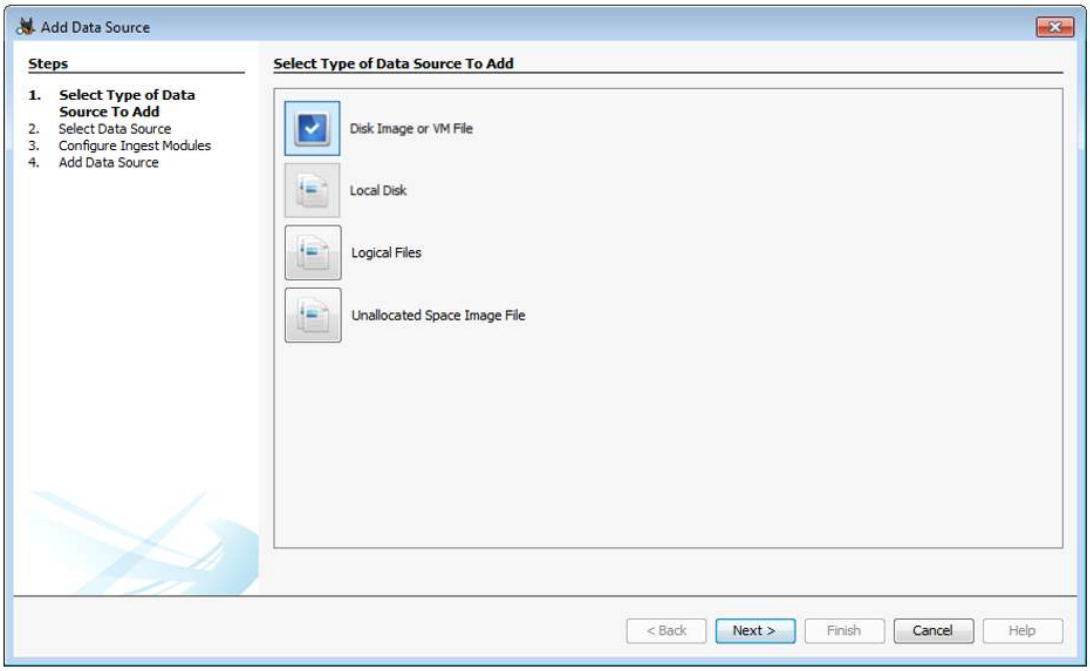
3.1.System snapshots and full analysis report:

Open Autopsy and create a new case.

Click on Finish after completing both the steps.

Add a data source.

Select the appropriate data source type.



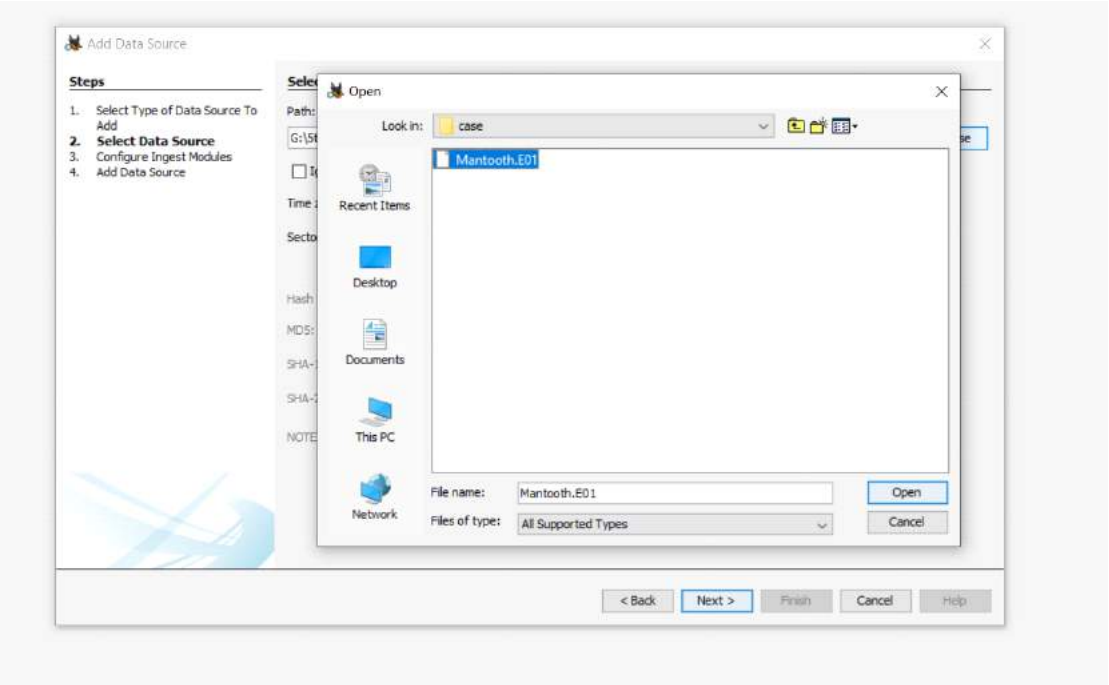
Disk Image or VM file: Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.

Local Disk: Includes Hard disk, Pendrive, memory card, etc.

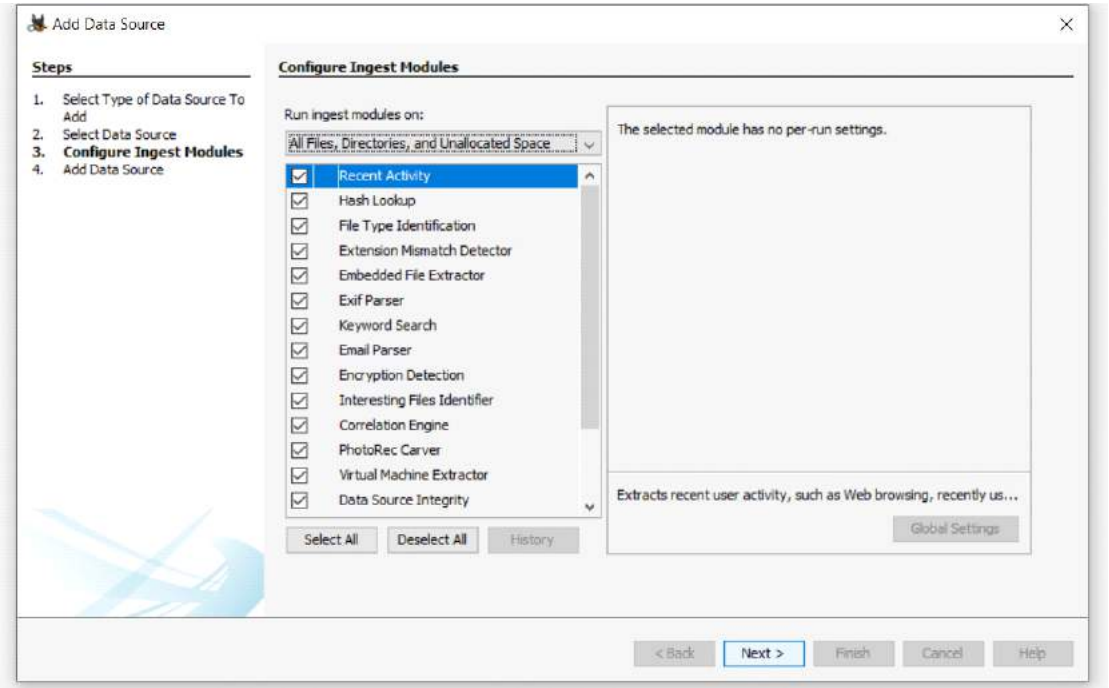
Logical Files. : Includes local folders or files.

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.

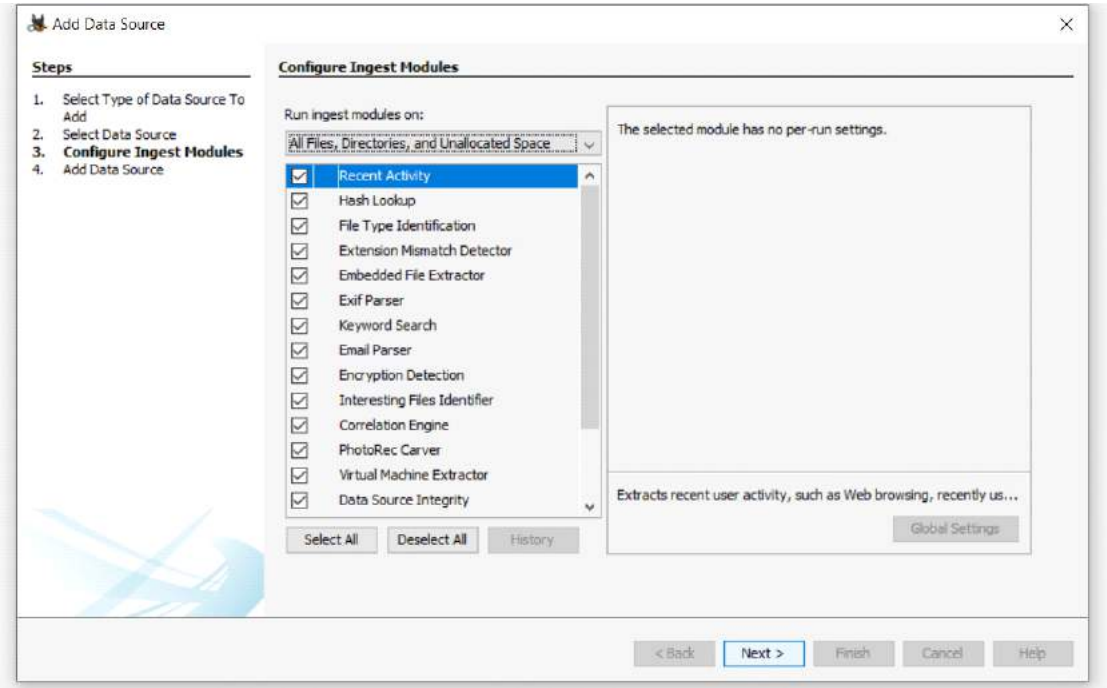
PhotoRec Carver: Recover files, photos, etc. from the unallocated space.

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.

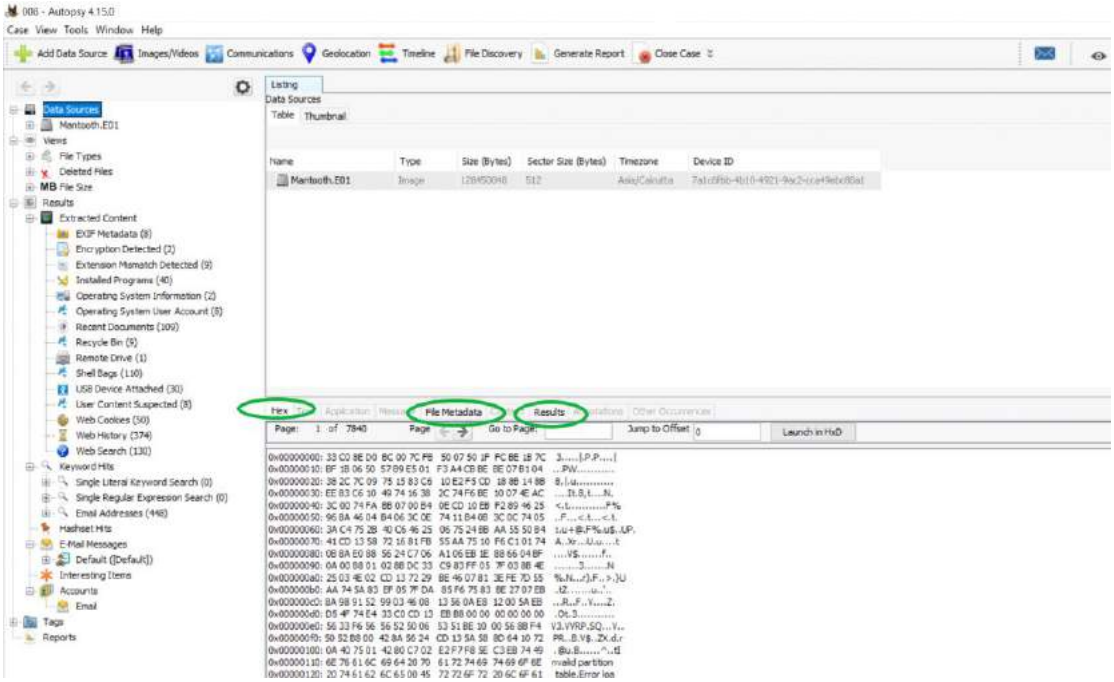
Android Analyzer: Analyze SQLite and other files retrieved from an Android device



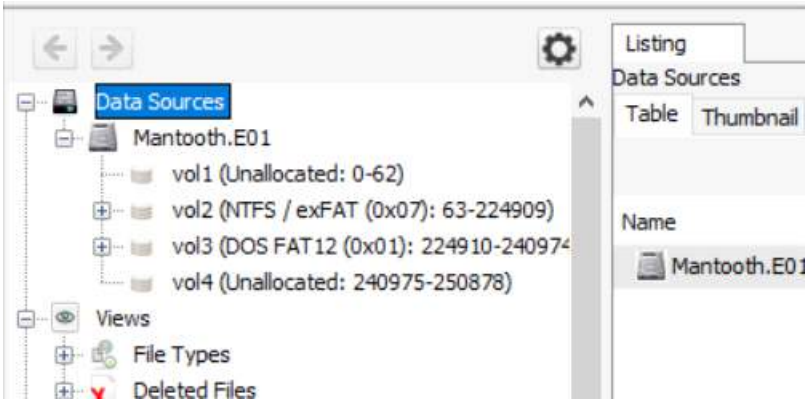
Select all that will serve the purpose of your investigation and click Next. Once the data source is added, click Finish. It will take some buffer time to extract and analyze the data depending upon the size of the Data Source.

3. Exploring the data source:

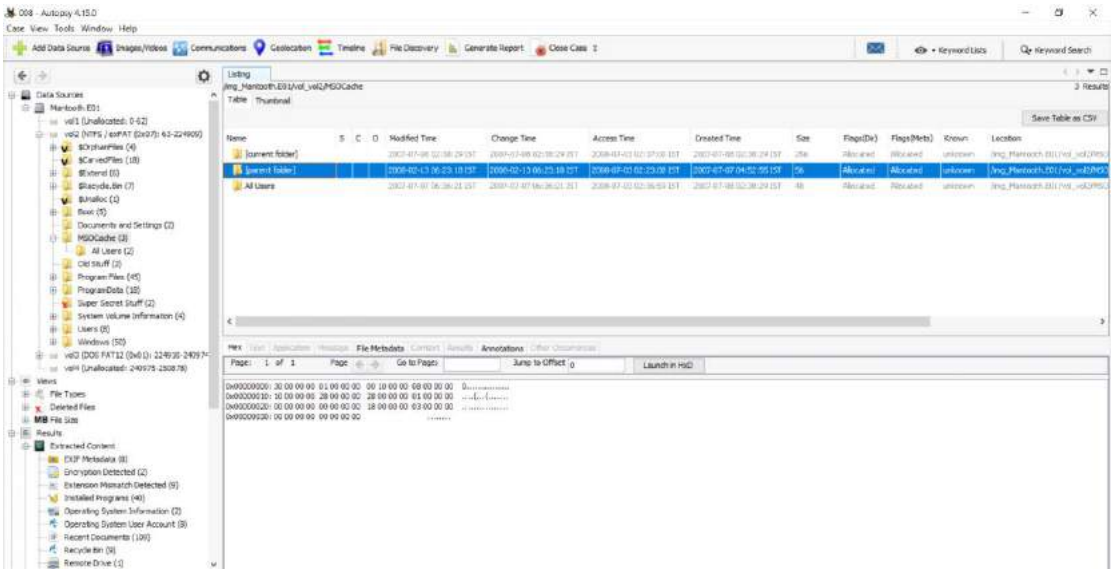
The Data Source information: Here the basic metadata is shown. A detailed analysis is displayed in the bottom section. These details can be extracted in the form of Hex values, Results, File Metadata, etc.



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

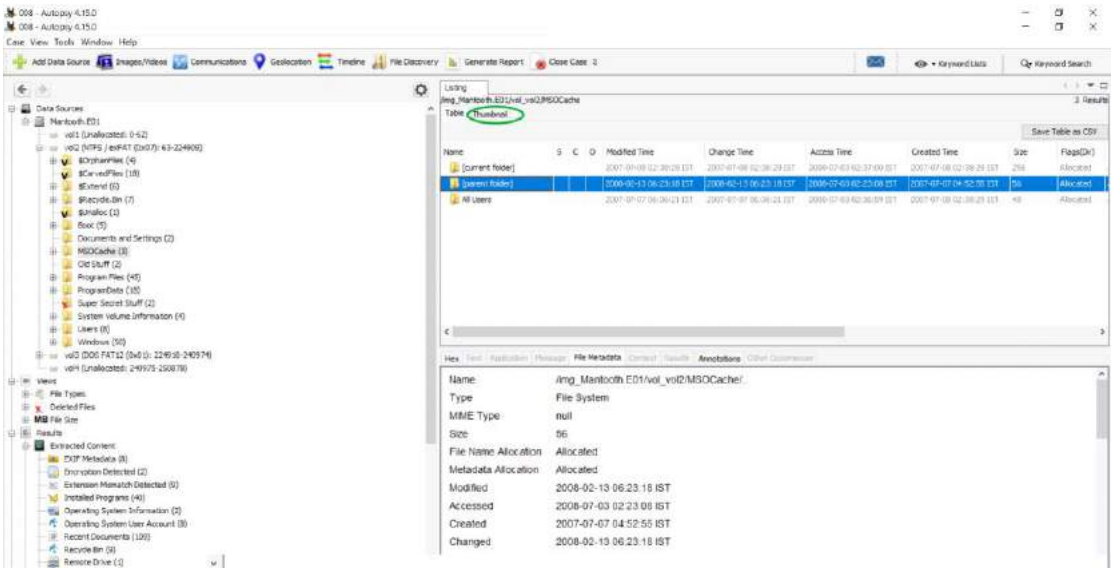


Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> Mantooth.E01 -> MSOCache-> [Parent Folder].

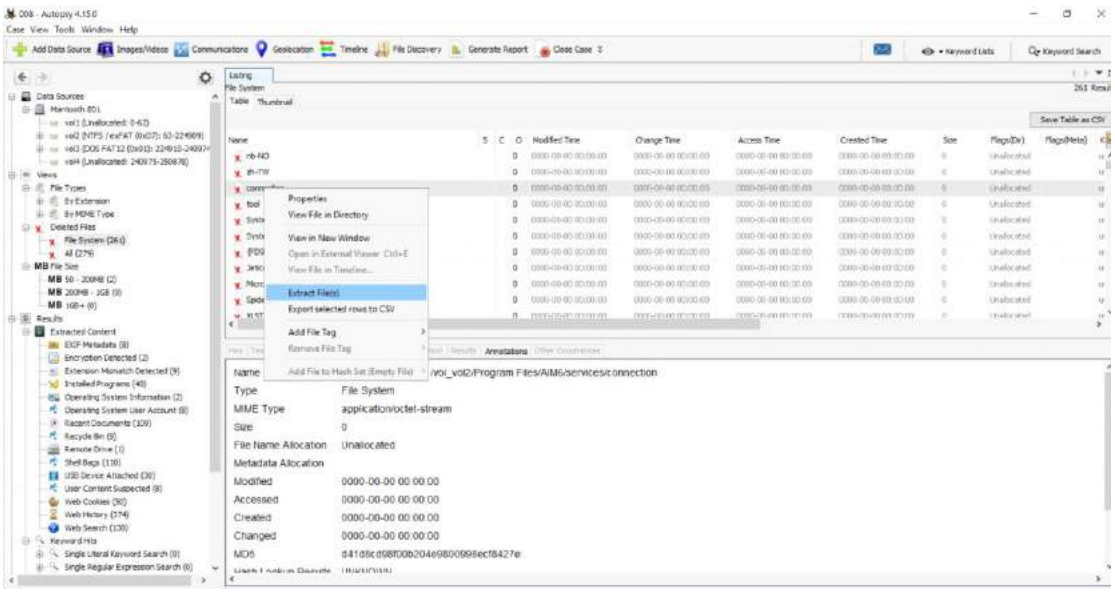


Views (Determines the factor of file classification)

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



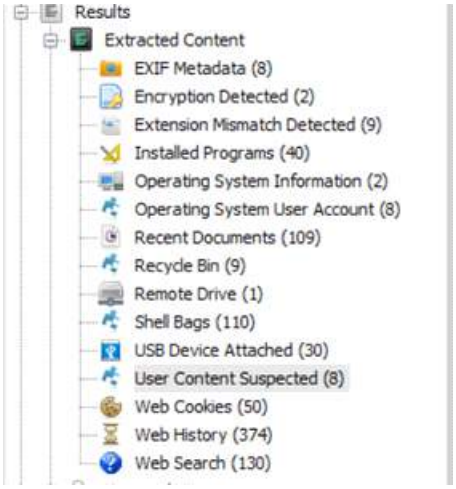
MB Size Files: Here files are classified based upon their size. The range starts from 50MB. This enables the examiner to determine exclusively large files.

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.

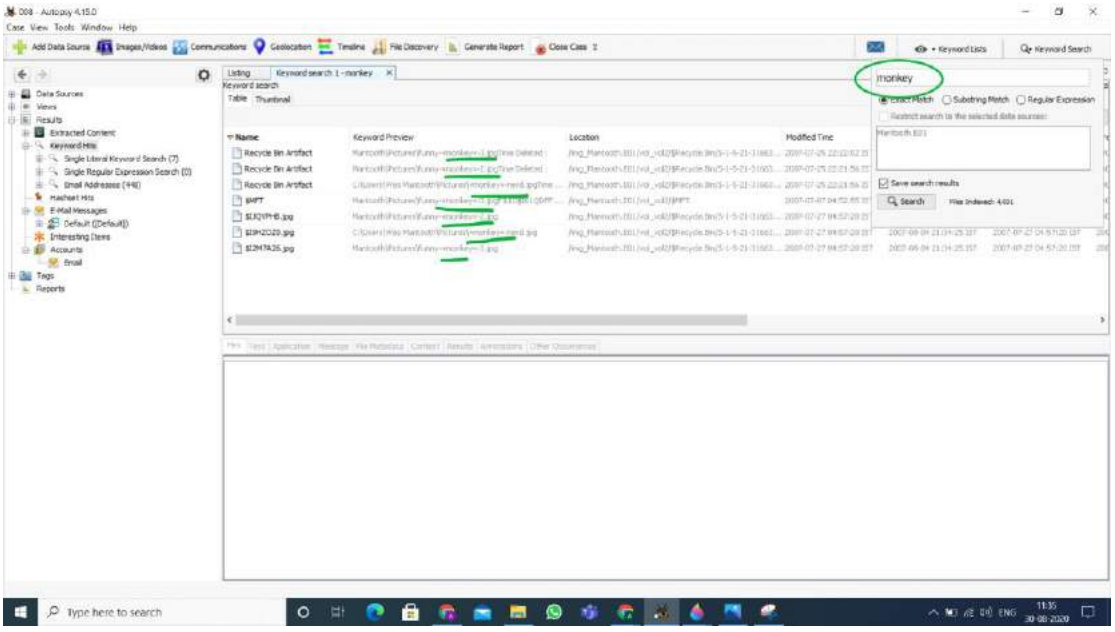
USB Device attached: All the information about the external devices attached to the system is displayed here. This data is extracted from Windows Registry which is actually a maintained database about all the activities taking place on the system.

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.

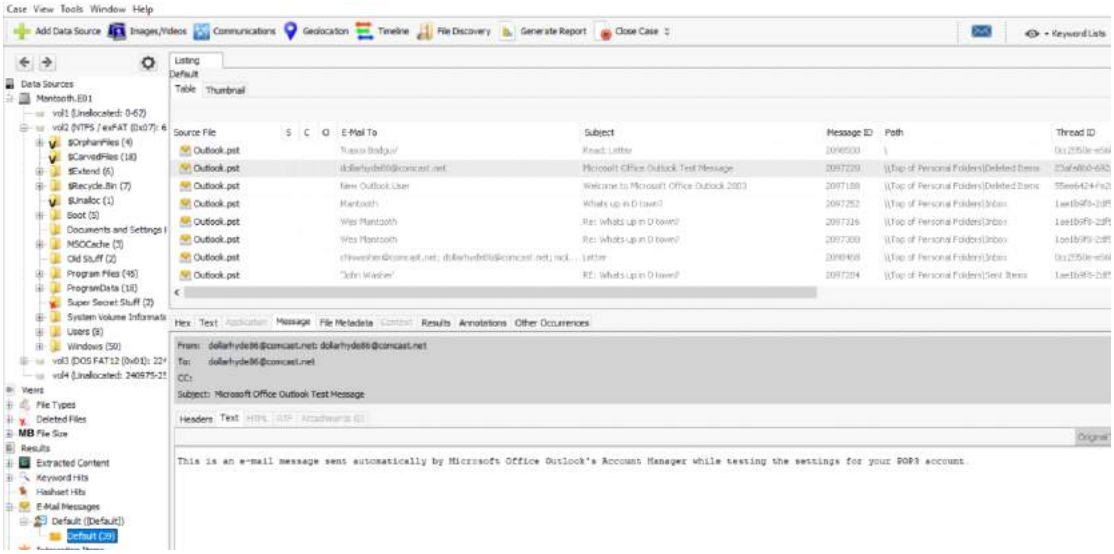
Web Searches: Details about the web searches made are displayed here.

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.



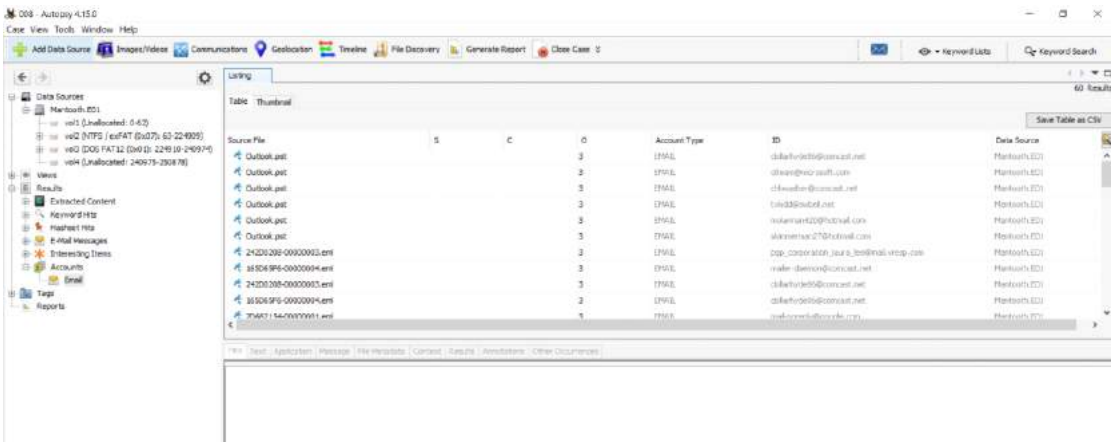
HashSet Hits: Here the search can be made using hash values.

E-mail Messages: Here all the outlook.pst files can be explored**.**

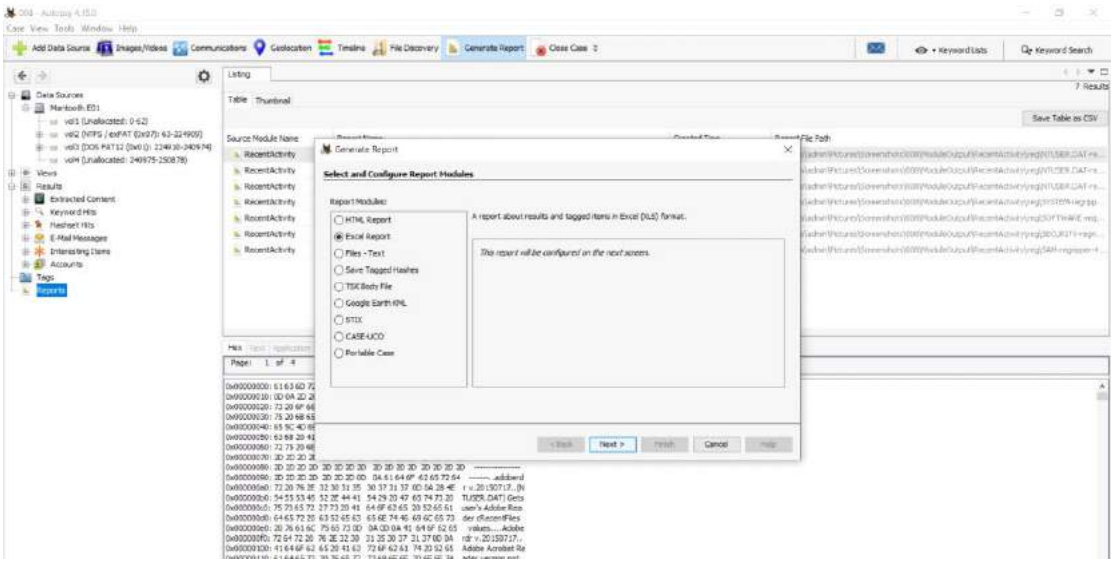


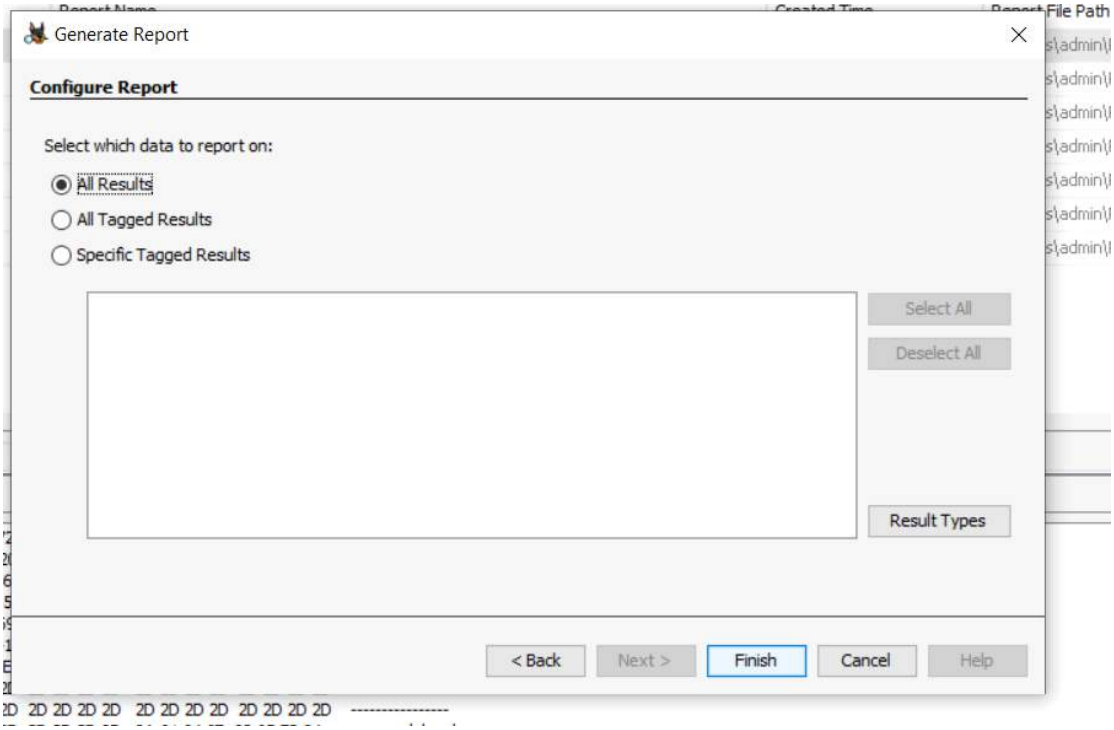
Interesting Items: As discussed before, these are the file results based upon the custom rules set by the examiner.

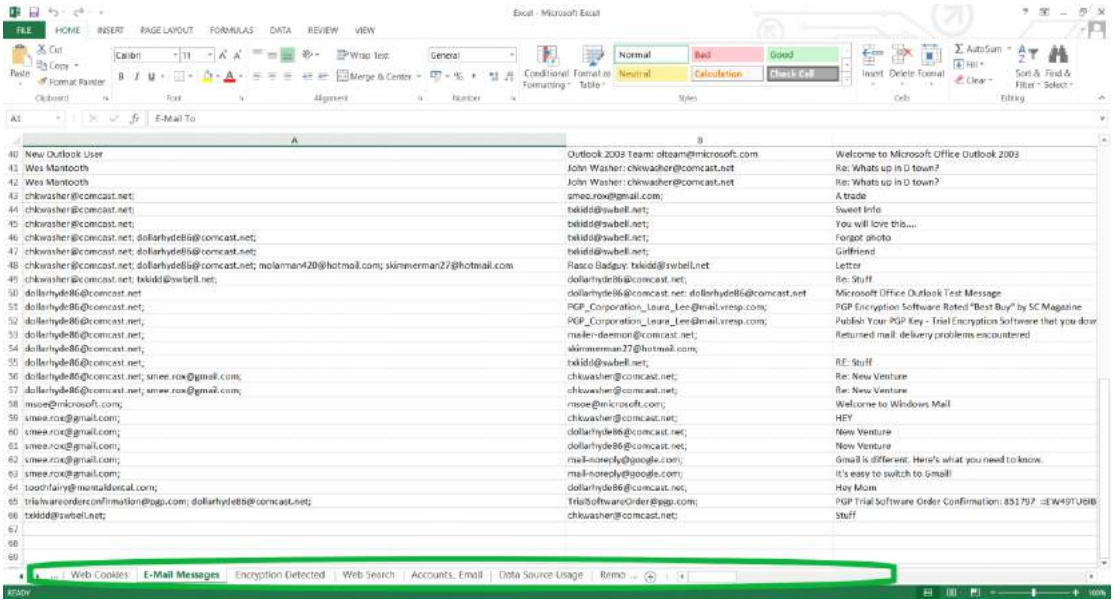
Accounts: Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts**.**



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

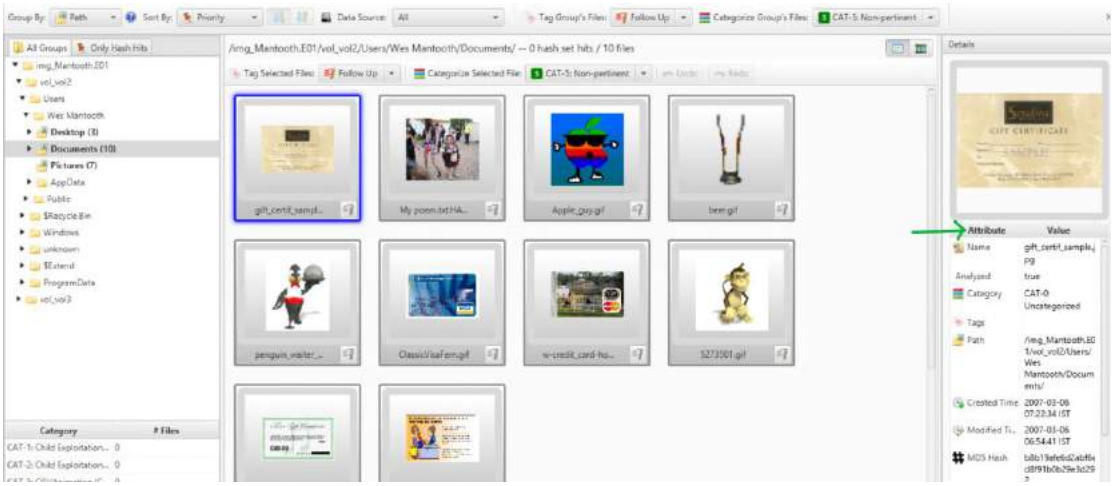



Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Result Types
< Back
Next >
Finish
Cancel
Help

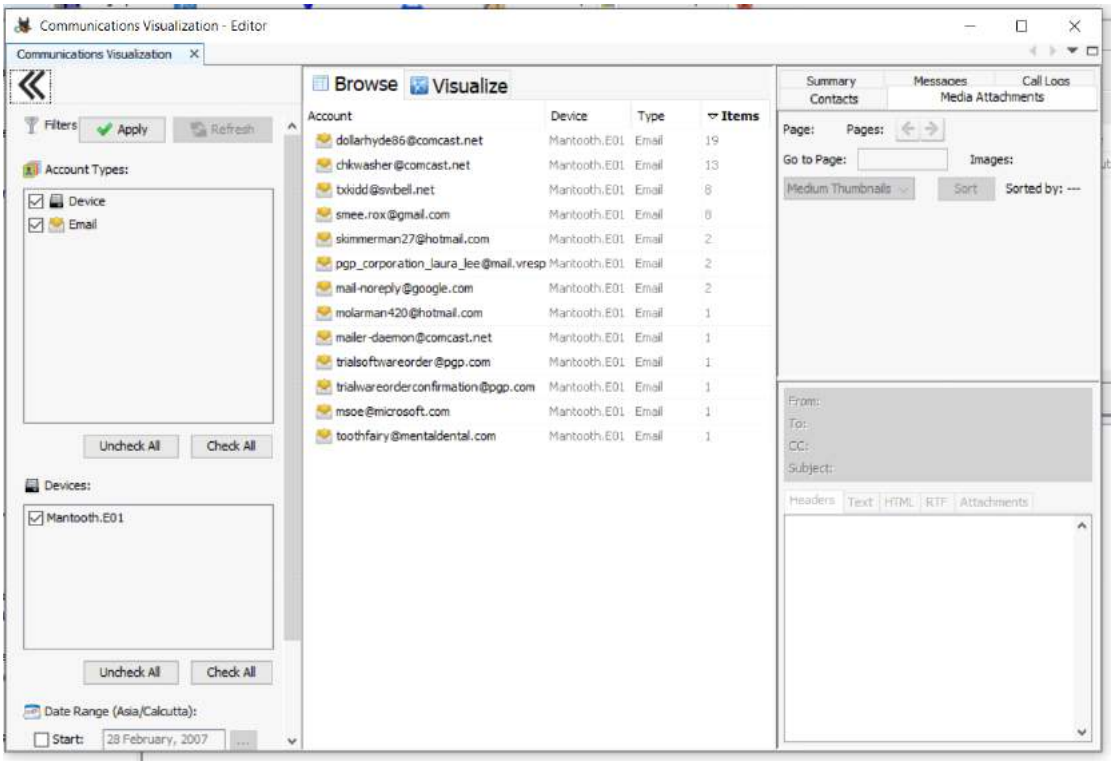


Add a Data Source: Each case can hold multiple Data Sources.

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.

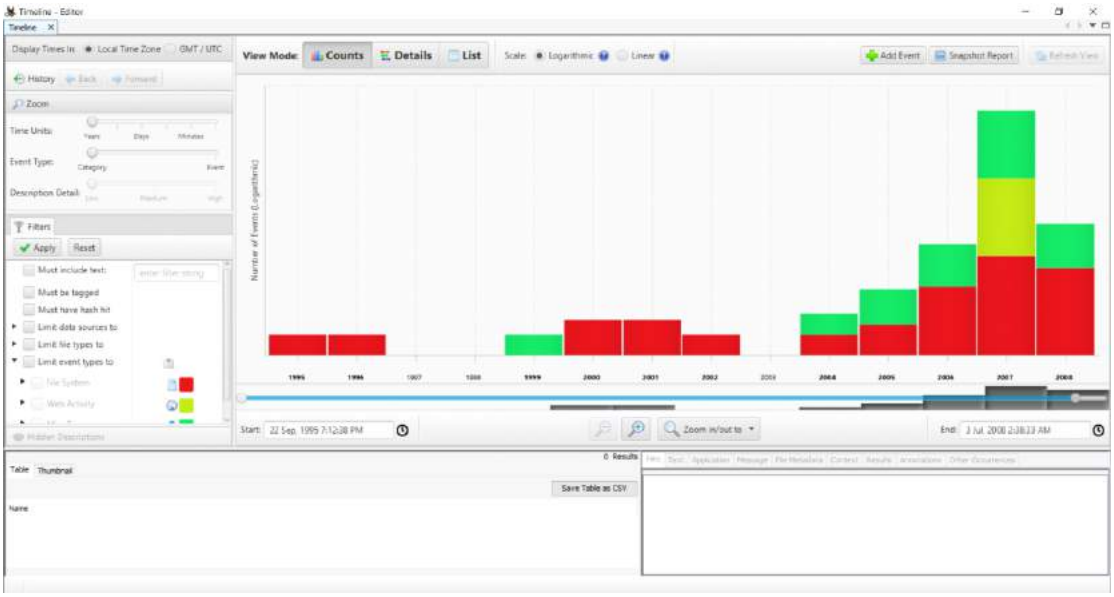


Communications: All the communications made using the source device are displayed here. This device had communications only in the form of emails**.**



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.



4.Refrence/Bibliography:

1.Autopsy User Documentation: https://www.sleuthkit.org/autopsy/docs/user-docs/

2.Autopsy YouTube Channel: https://www.youtube.com/channel/UC9XoJdndAomharxCp5aYHQA

3.Digital Forensics with Open Source Tools Book by Cory Altheide and Harlan Carvey: https://www.elsevier.com/books/digital-forensics-with-open-source-tools/altheide/978-1-59749-586-8

4."Forensic Analysis of Google Chrome Cache" article by Jonathan Rajewski: https://www.forensicfocus.com/articles/forensic-analysis-of-google-chrome-cache/

5."The Forensics of Firefox" article by Michael Bazzell: https://www.forensicfocus.com/articles/the-forensics-of-firefox/

6."Forensic Analysis of Microsoft Edge Browser Cache" article by Jitendra Kumar Singh: https://www.forensicfocus.com/articles/forensic-analysis-of-microsoft-edge-browser-cache/

7.FreeEduHub https://www.youtube.com/watch?v=S6V66G2tVr8&t=52s

8.Digital Forensic With Autopsy https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d