iGNITE Technologies

AUTOPSY

LINUX AND WINDOWS

WWW.HACKINGARTICLES.IN

Table of Contents

Abstract

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is an open-source tool for digital forensics which was developed by Basis Technology. This tool is free to use and is very efficient in the nature investigation of hard drives. It also consists of features like multi-user cases, timeline analysis, keyword search, email analysis, registry analysis, EXIF analysis, detection of malicious files, etc

The forensic investigation that is carried out on the disk image is displayed here. The results obtained here are of help to investigate and locate relevant information. This tool is used by law enforcement agencies, local police and can also be used in the corporates to investigate the evidence found in a computer crime. It can likewise be utilized to recuperate information that has been erased.

AUTOPSY KALI LINUX

Autopsy for Kali Linux

The tool can manage cases, check the integrity of the image, keyword search and other automated operations.

- Investigator can analyse Windows and UNIX storage disks and file systems like NTFS, FAT, UFS1/2, Ext2/3 using Autopsy.
- Autopsy is used by law enforcement, military, and corporate examiners to conduct investigations on a victim's or a criminal's PC.
- One can also use it to recover photos from one's camera's memory card.

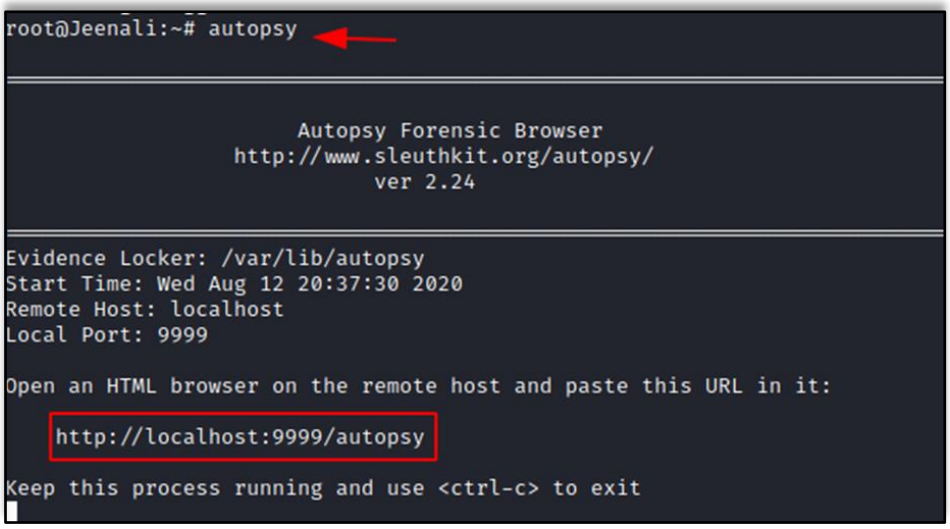
Autopsy Forensic Browser is a built-in application in Kali Linux operating system, so let's power on the Kali in a Virtual Machine.

Purpose of Autopsy

- For analysis of metadata information.
- To recover the deleted data.
- To search data based on regular expression.
- To analyse the contents of a folder and its deleted files.
- To report the activities of the recovered image.

Creating a New Case

Open a new terminal and type 'Autopsy' and open ***http://localhost:9999/autopsy*** in your browser where you will be redirected to the home page of Autopsy Forensic Browser. It will run on our local web server using the port 9999.

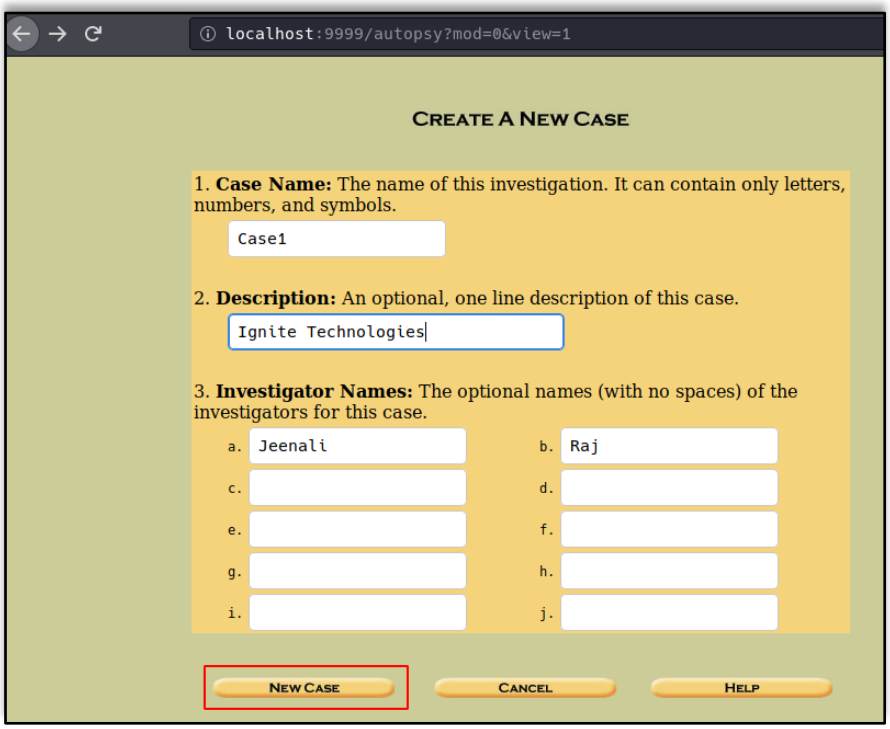


Now you will see three options on the home page.

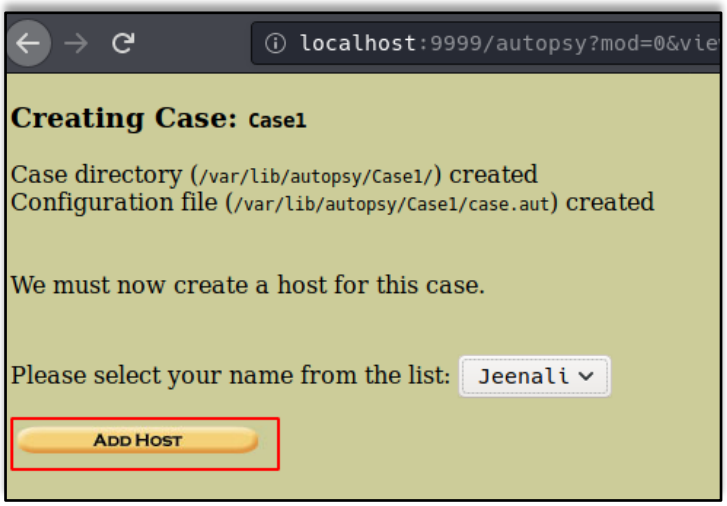
- Open Case
- New Case
- Help

For investigation, you need to create a new case and click on **'New case'**. In doing this it will add a new case folder to the system and allow you to begin adding evidence to the case.

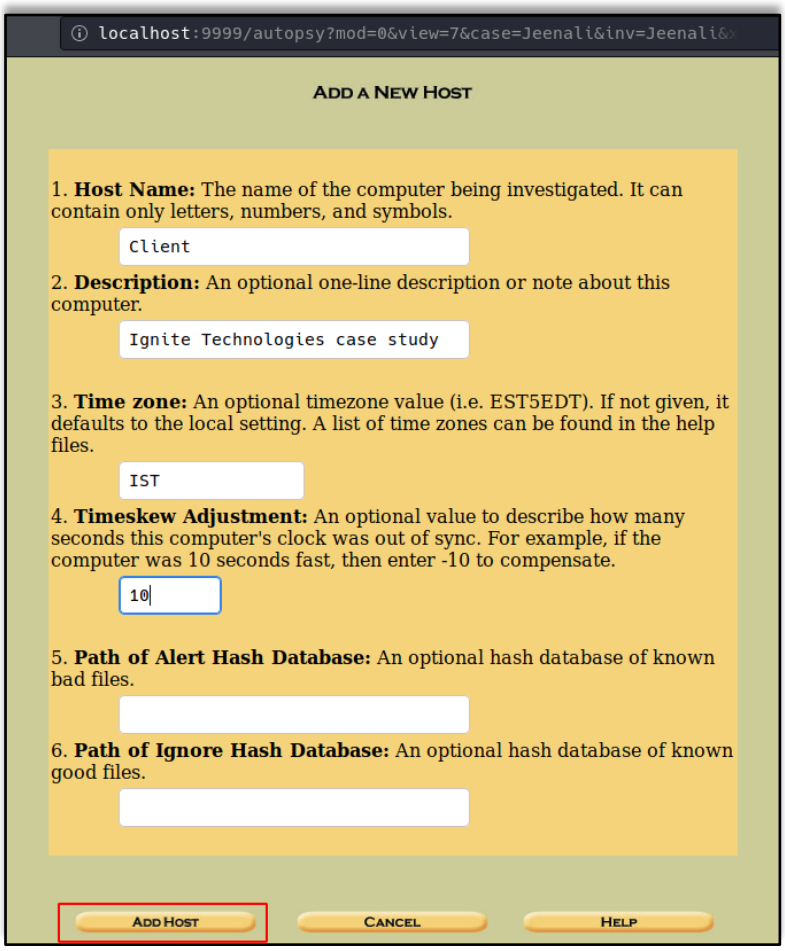
Now you will be directed to a new page, where it will require case details. You can Name the case and mention the description. You can also mention the names of multiple investigators working the case. After filling in these details, now you can select **'New case'.**



The new case will be stored in i.e., **/var/lib/autopsy/case1/**, and the configuration file will be stored in **/var/lib/autopsy/case01/case.aut**. Now, create the host for investigation and click on 'Add Host'.

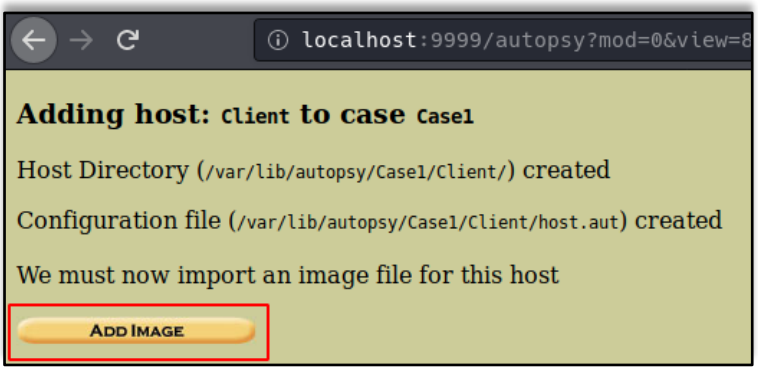


Once you add the host, put the name of the computer you are investigating and describe the investigation. You can also mention the time zone or you can also leave it blank which will select the default setting, time skew adjustments may be set if there is a difference in time and you can add the new host. Click on **'Add Host'**.

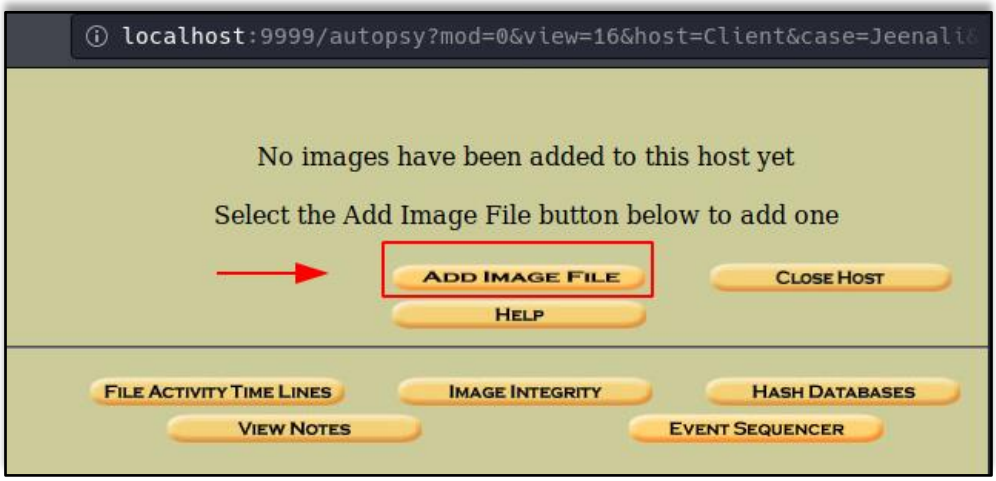


Add Image File

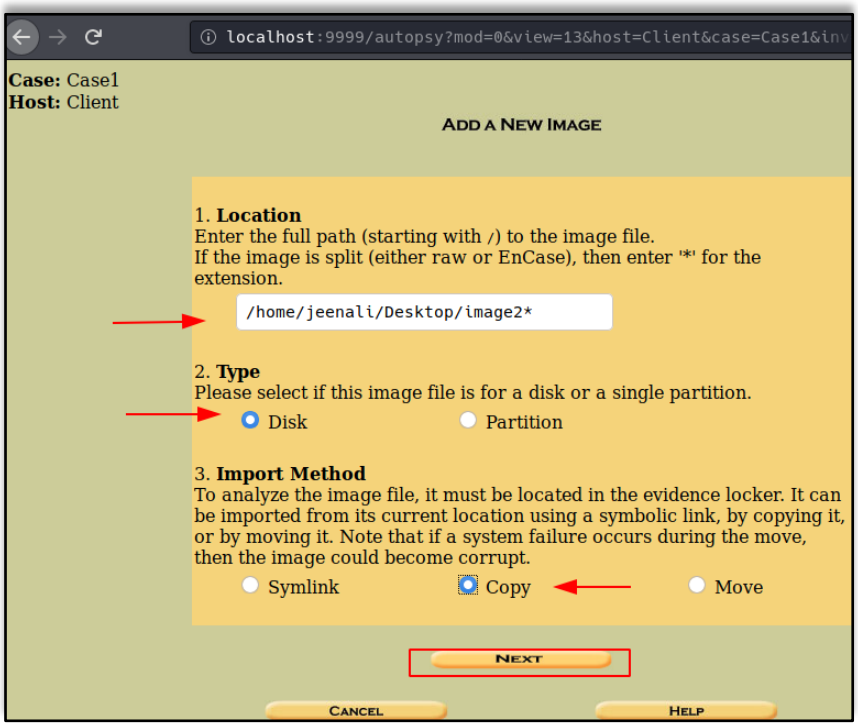
The path to the evidence directory will be displayed and now you can proceed to add an image for investigation.



It is a golden rule of Digital forensics, that one should never work on the original evidence and hence an image of the original evidence should be created. An image can be created in various methods and tools as well as in various formats.
Once the image is acquired, the **'Add Image File'** option will allow you to import the image file to analyse.



Mention the path to the image file and select the file type. Also, choose the import method of your choice and click on **'Next'**.



You can now confirm the Image file being added to the evidence locker and click on 'Next'.

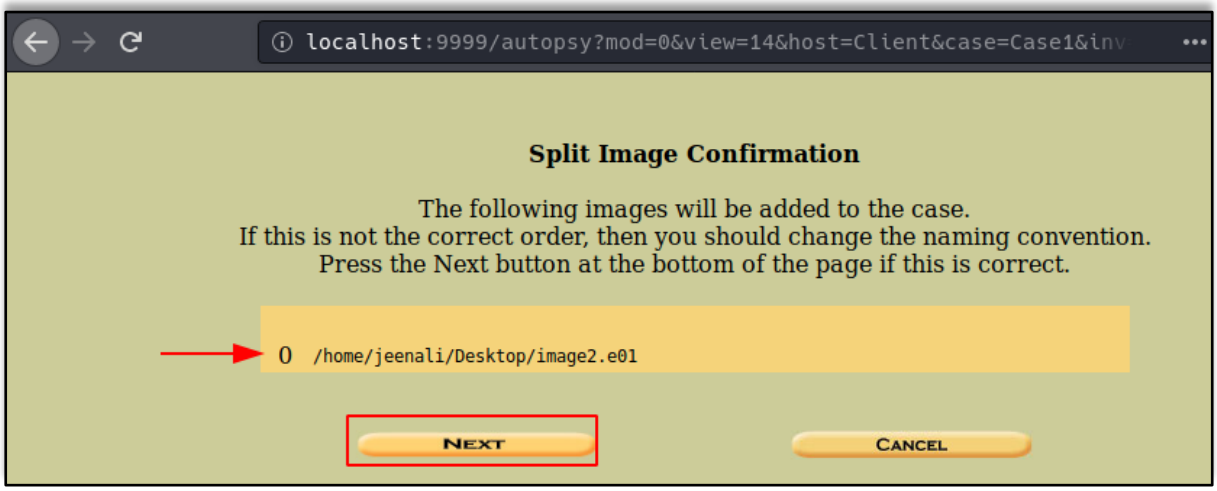
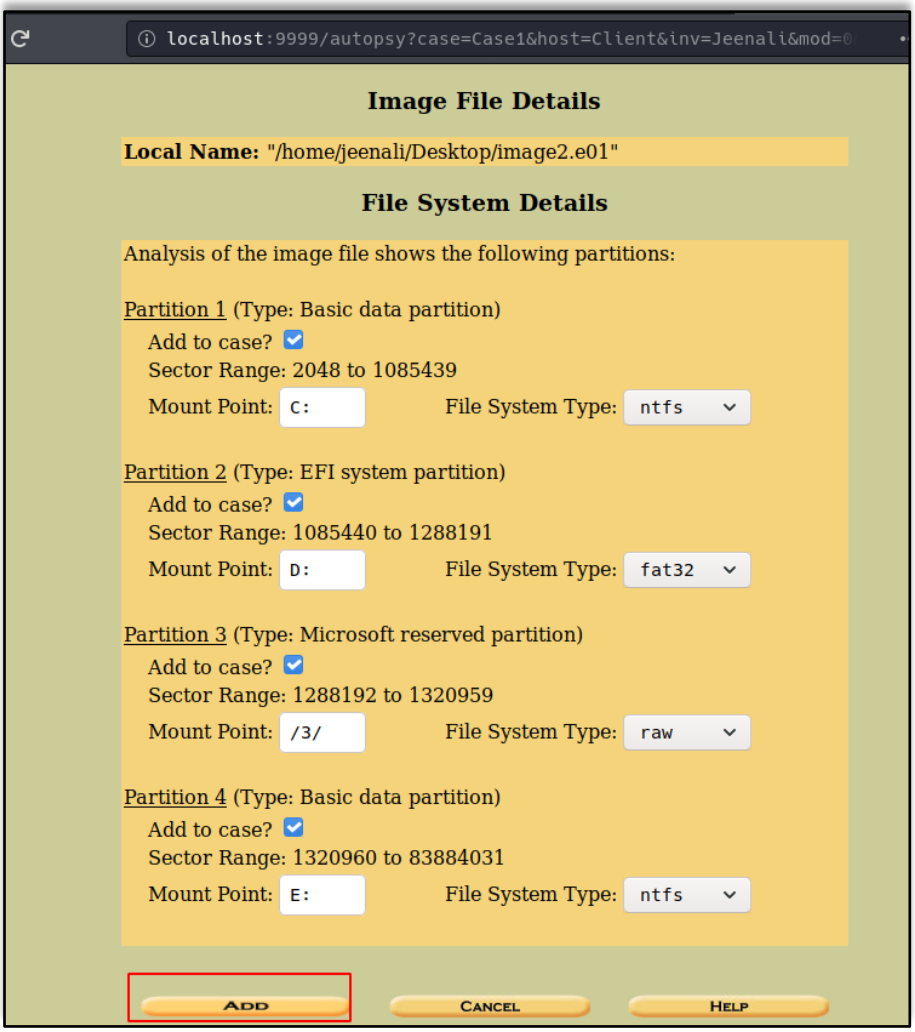
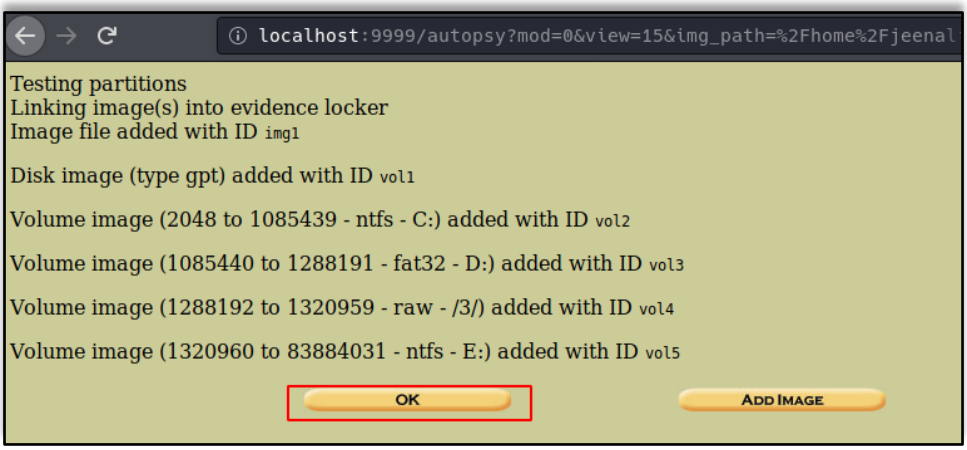


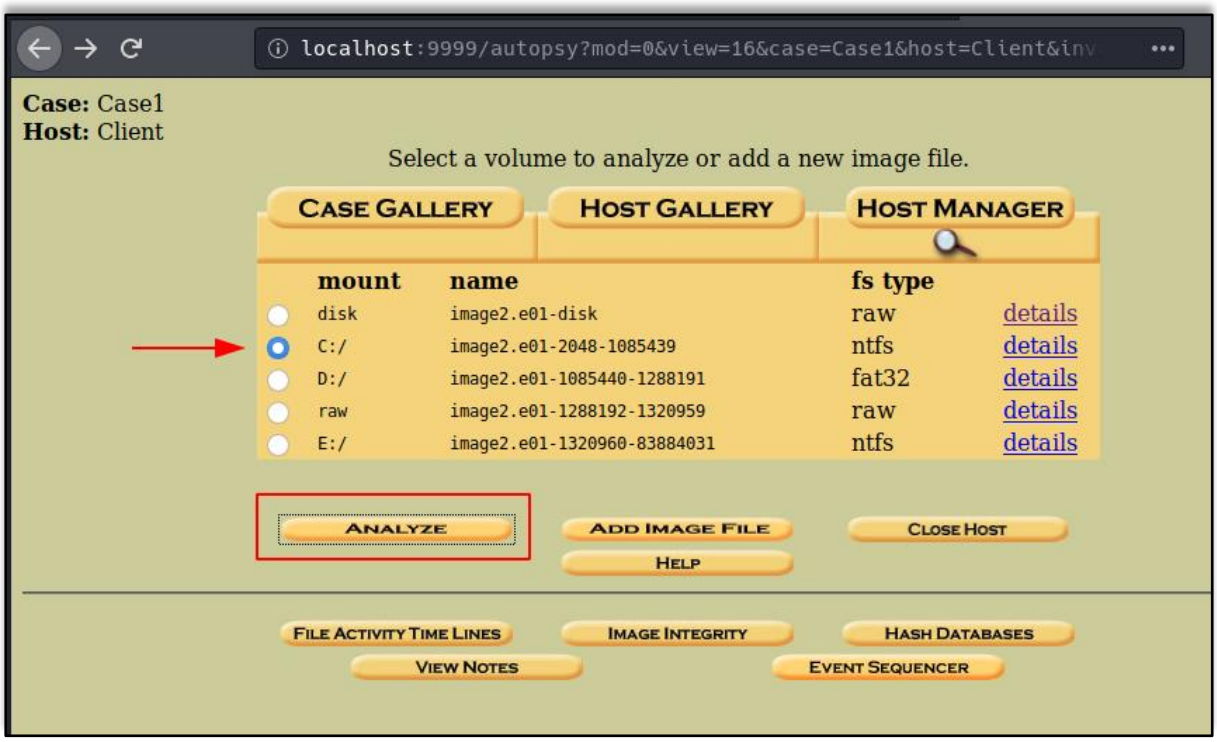
Image file details will appear and the details of the file systems, the number of partitions and the mount points will be displayed and then you can click on 'Add' to proceed.



Now the Autopsy will test the partitions and links them to the evidence locker, then click on 'Ok' to proceed.

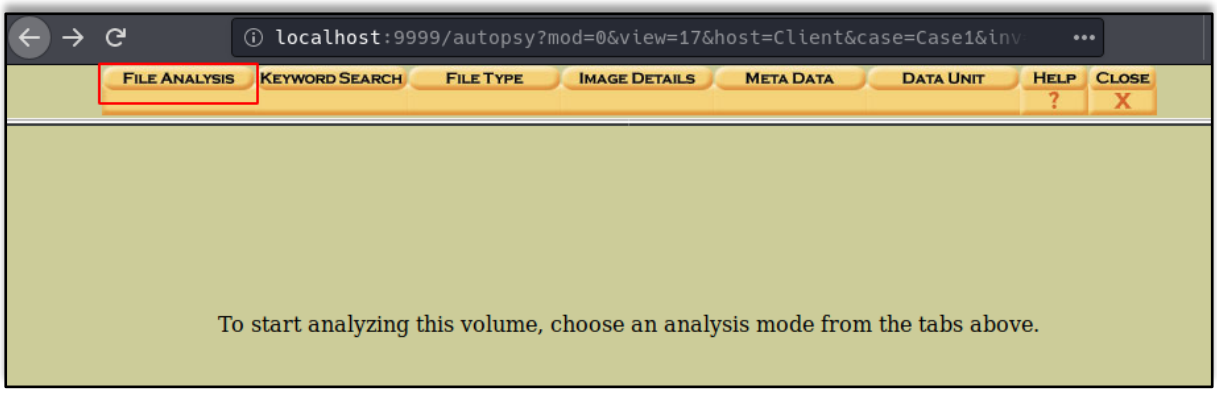


Now select the volume to be analyzed and click on 'Analyze'.

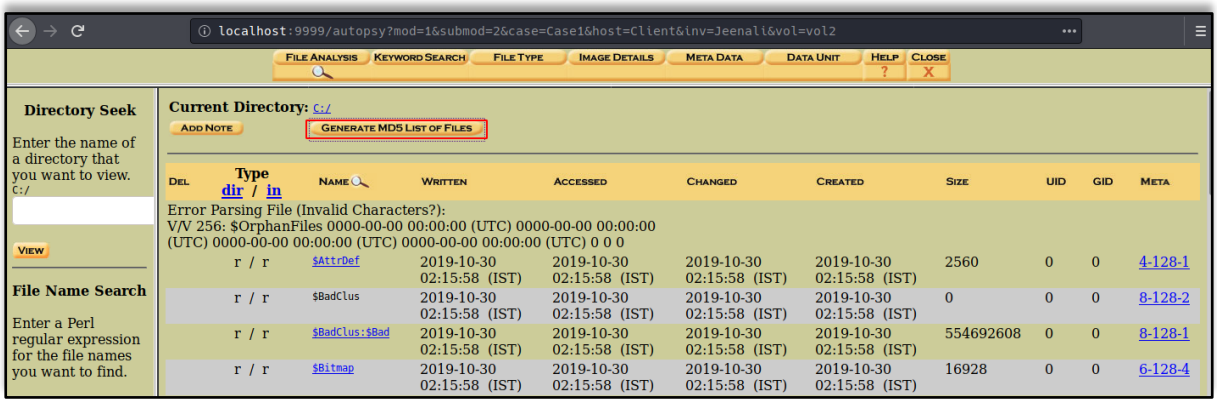


File Analysis

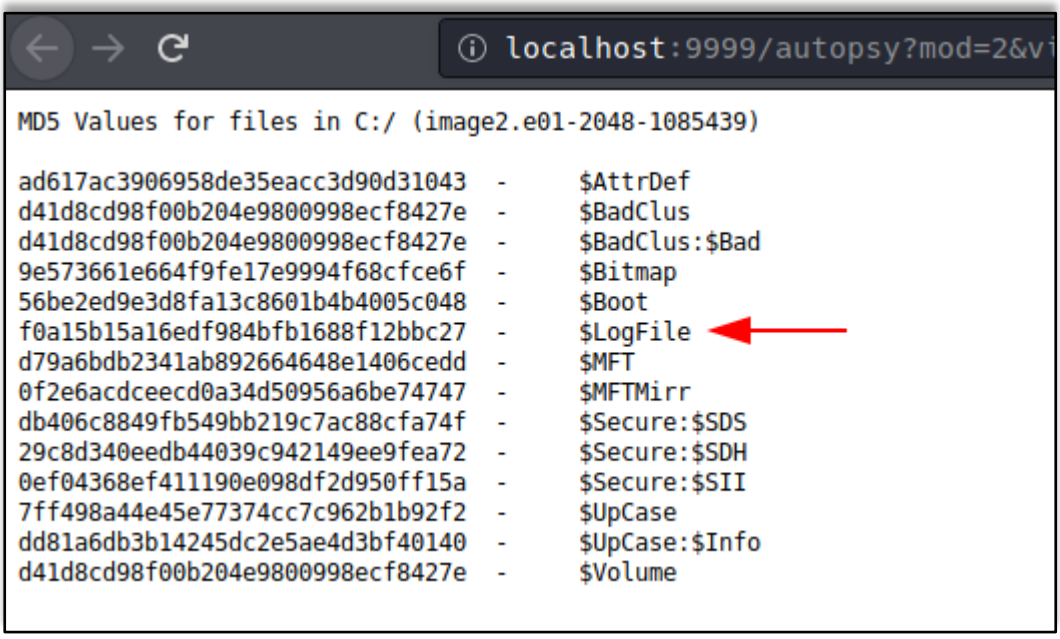
Now, it will ask you to choose the mode of analysis that you want to conduct and here we are conducting analysis of file, therefore click on 'File Analysis'.



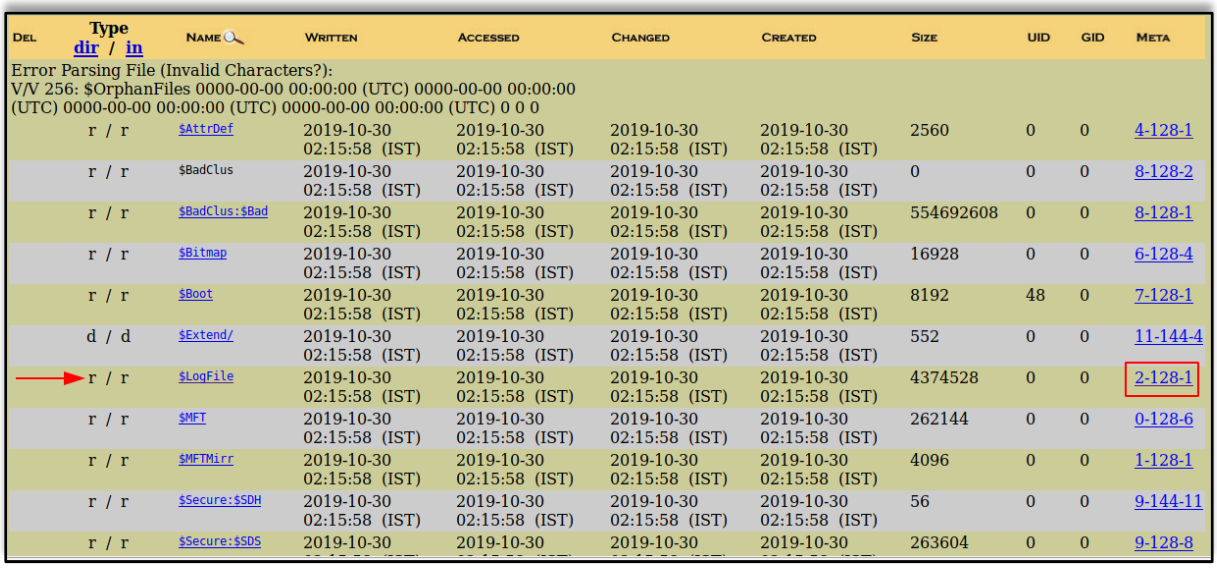
Now files will appear, which will give you the list of files and directories that are inside in this volume. From here you can analyze the content of the required image file and conduct the type of investigation you prefer. You can first generate a MD5 hash list of all the files present in this volume to maintain the integrity of the files, hence click on 'Generate MD5 List of Files'.



Now you can see the MD5 values of the files in volume C of the image file.

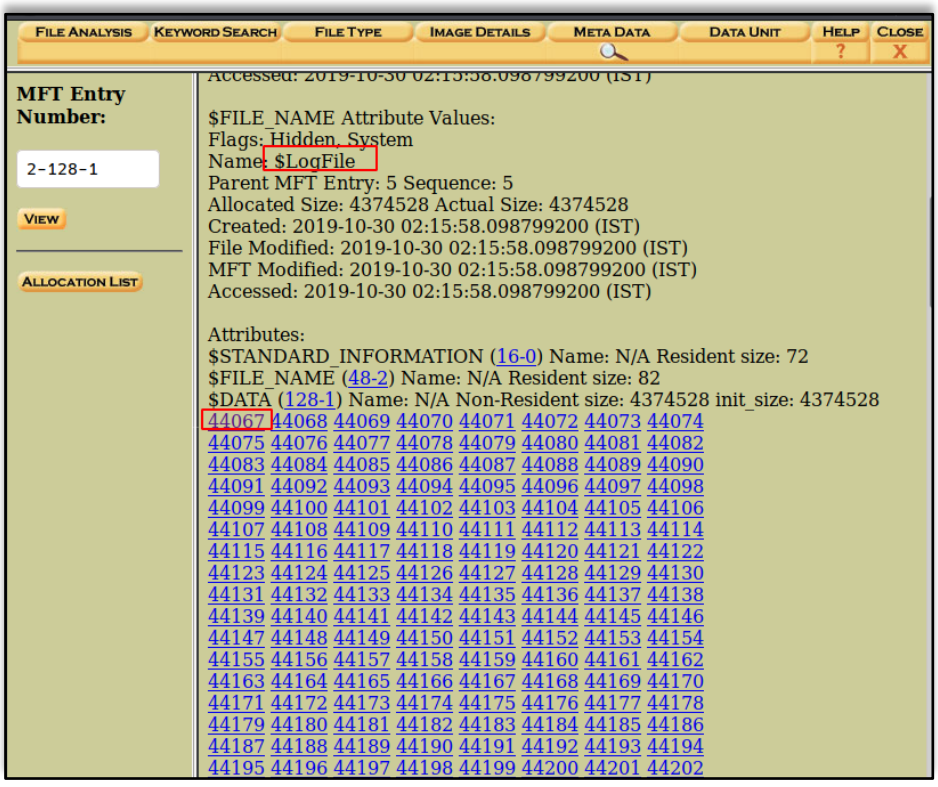


The file browsing mode consists of details of the directories that are shown below. The details include the time and date of the last time the directories were Written, Accessed, Changed and the time it was created with its size and also about its metadata. All the details are displayed in this, so in order to view the metadata, click on the 'Meta' option of Log file that you want to view.

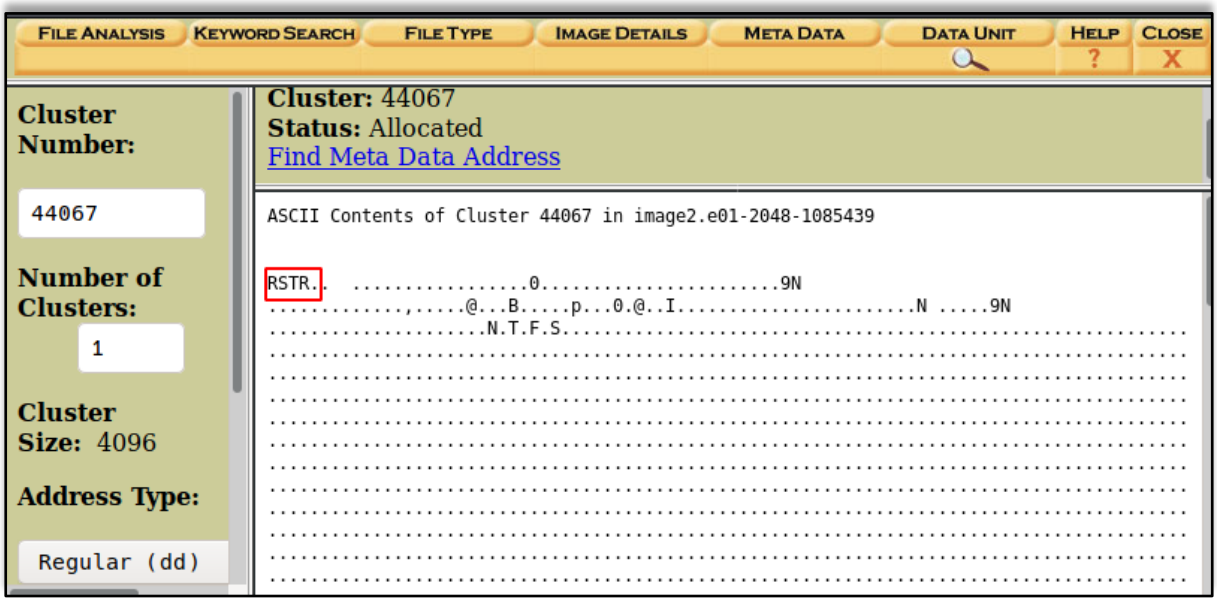


Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
Error Parsing File (Invalid Characters?): V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	r / r	$AttrDef	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2560	0	0	4-128-1
	r / r	$BadClus	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	0	0	0	8-128-2
	r / r	$BadClus:$Bad	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	554692608	0	0	8-128-1
	r / r	$Bitmap	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	16928	0	0	6-128-4
	r / r	$Boot	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	8192	48	0	7-128-1
	d / d	$Extend/	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	552	0	0	11-144-4
	r / r	$LogFile	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	4374528	0	0	2-128-1
	r / r	$MFT	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	262144	0	0	0-128-6
	r / r	$MFTMirr	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	4096	0	0	1-128-1
	r / r	$Secure:$SDH	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	56	0	0	9-144-11
	r / r	$Secure:$SDS	2019-10-30	2019-10-30	2019-10-30	2019-10-30	263604	0	0	9-128-8

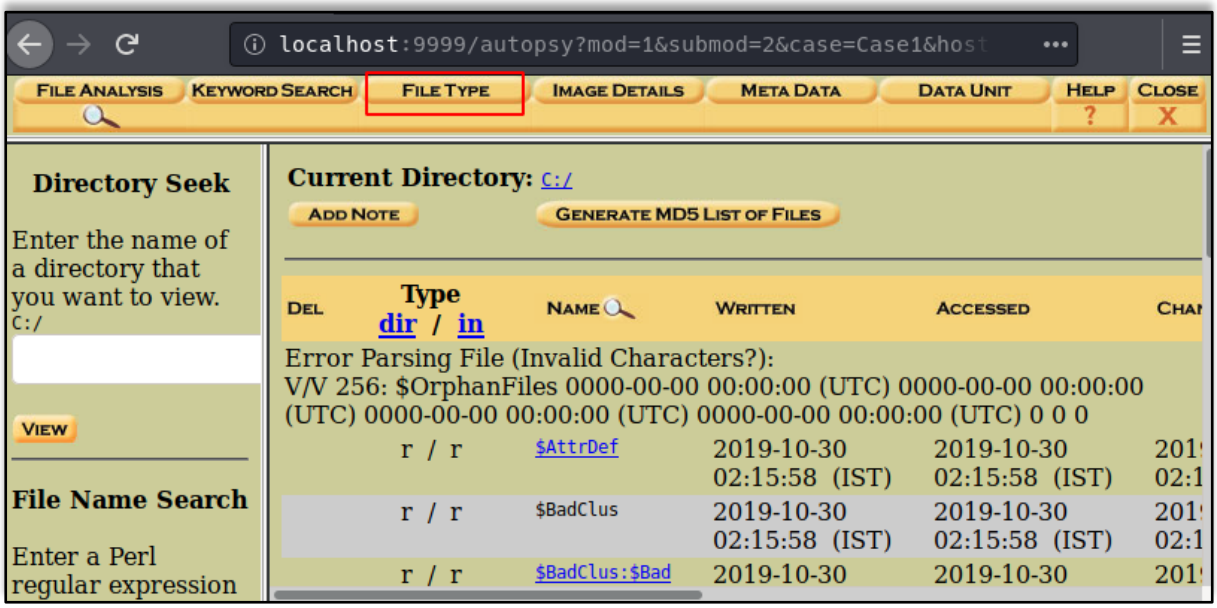
Here you can see the metadata information about the directory. In order to see more details, click on the first cluster '44067' in order to view its header information to find any relevant information to the case.



Here you can see the information about the header of the cluster.

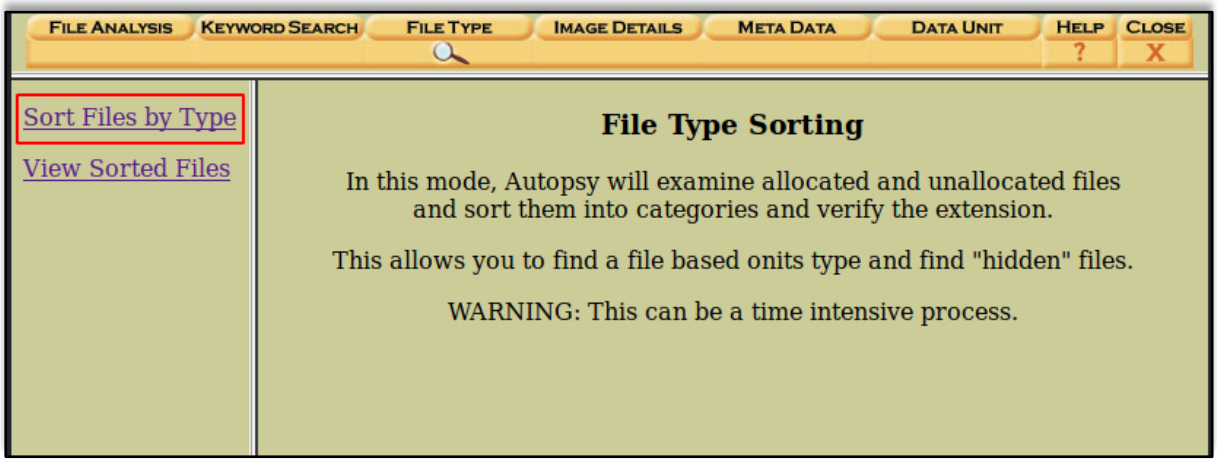


Then in order to view the file types of the directories, then click on 'File Type'

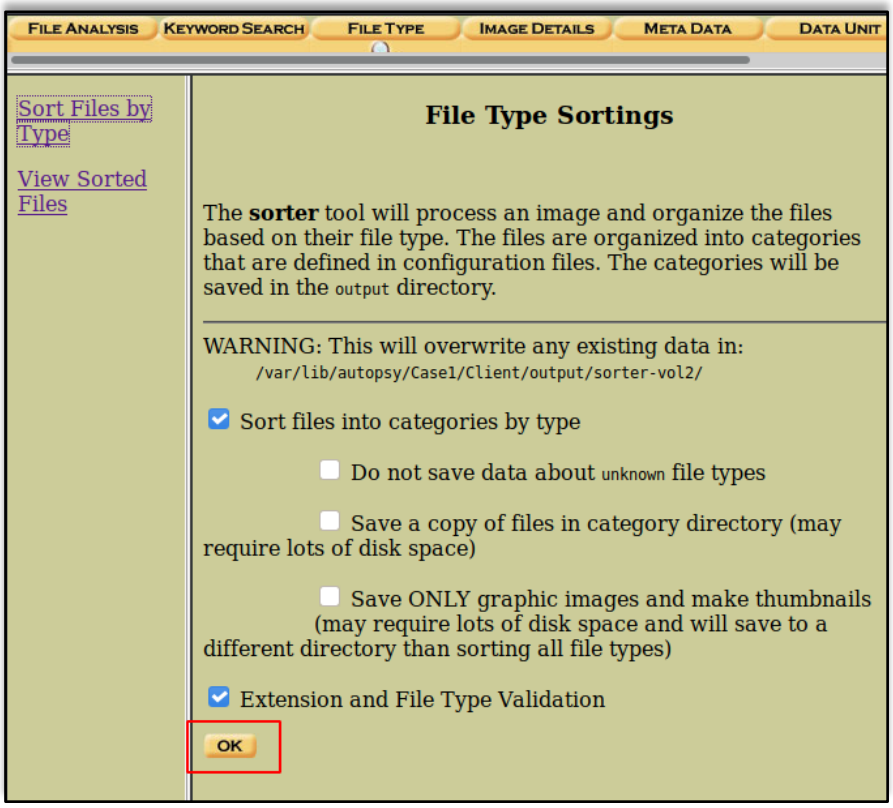


File Type

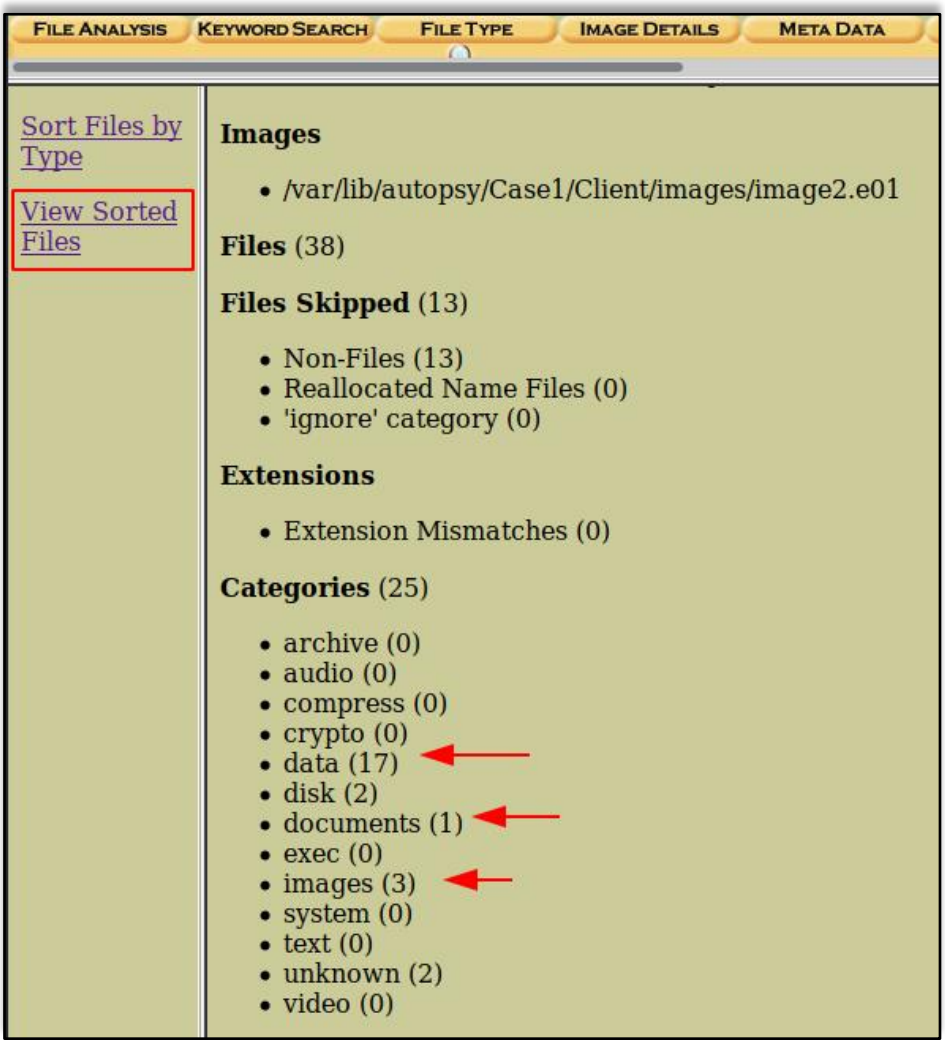
Here you will be able to sort the files based on the different types of files in the volume. By using this feature, you can examine allocated, unallocated as well as hidden files. To sort the file, click on **'Sort Files by Type'**.



Click on 'Sort files into categories by type' which is selected by default and then click 'OK' to start sorting the files.



The categories of the file types will be displayed. Now to view the sorted files, click on 'View sorted files' and you will be displayed the list of sorted files.



The output folder locations will vary depending on the information specified by the user when first creating the case, but can usually be found at /var/lib/autopsy/Case1/Client/output/sorter-vol2/index.html. Once the index.html file has been opened, click on the images to view its contents.

Now you can see Images categories and further investigate the files depending on the case requirement.

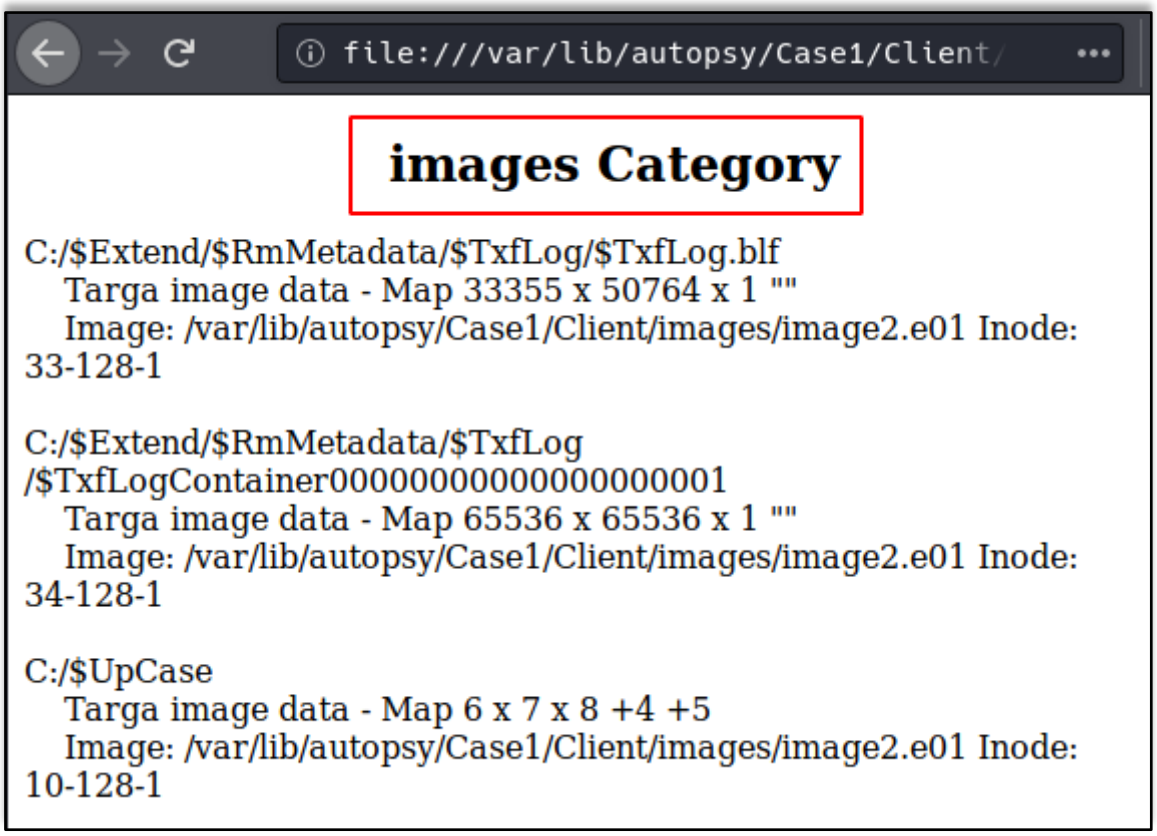
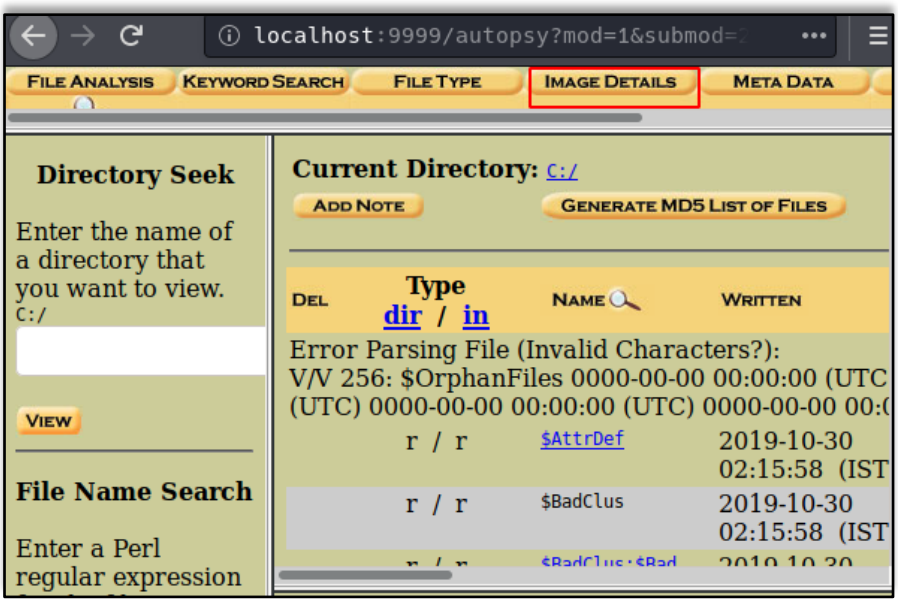
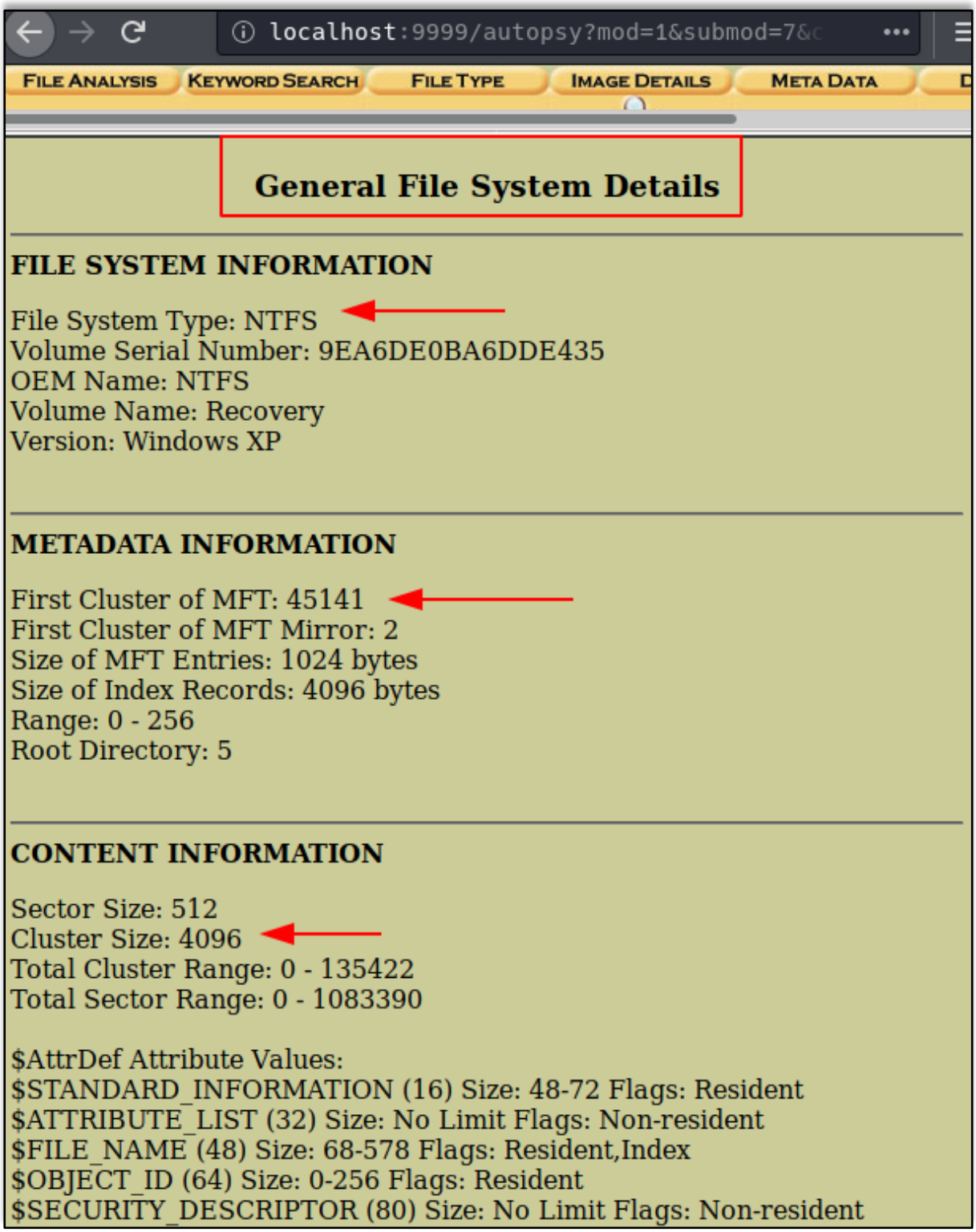


Image Details

Now click on the Image details options to view the important details about this image file.

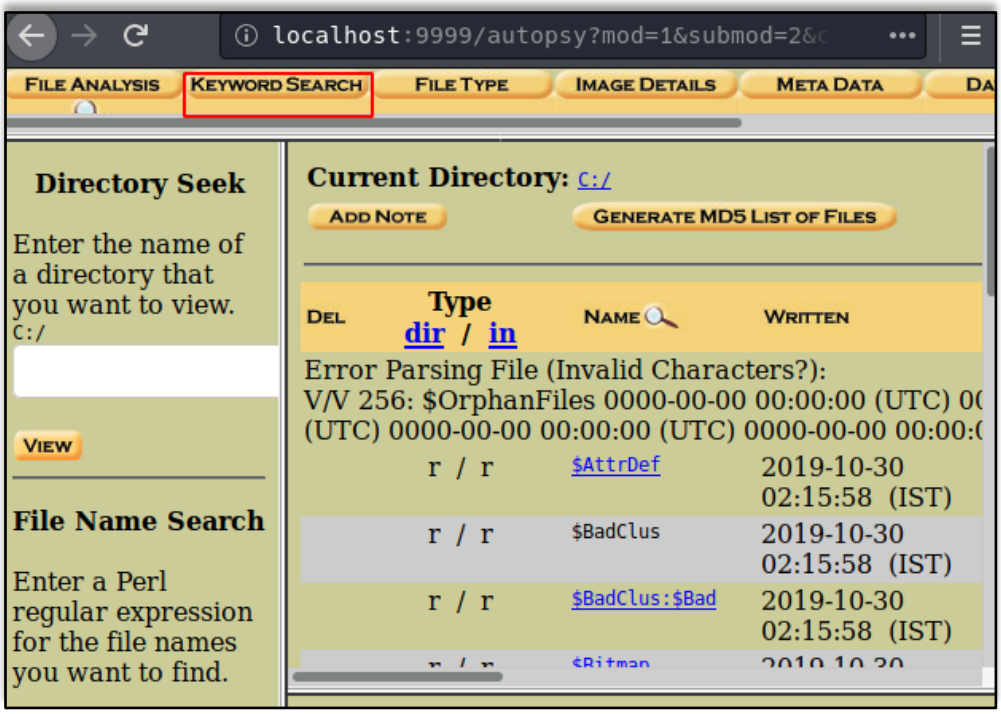


Here in this option of file analysis you can see file system information, first cluster of MFT, cluster size etc.

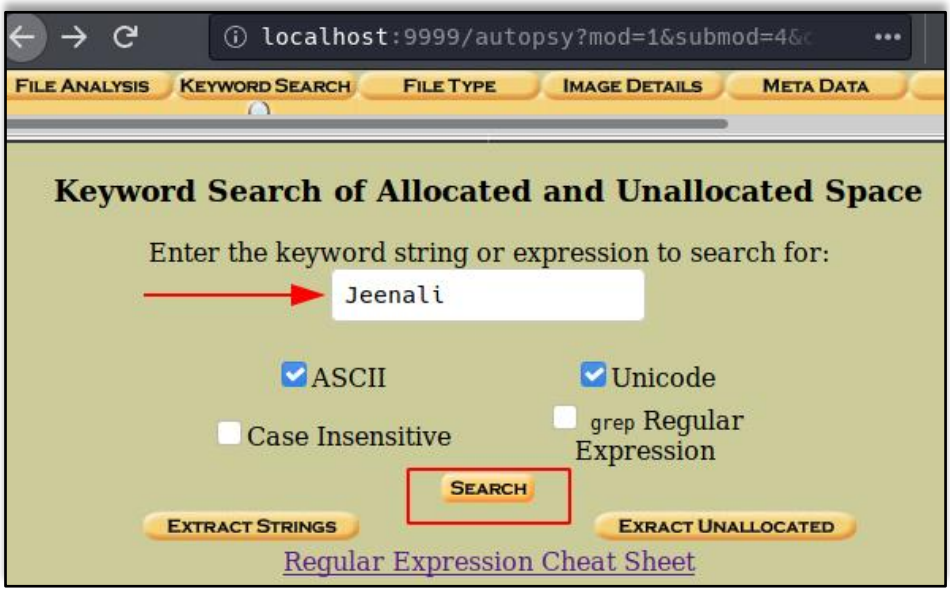


Keyword Search

To ease the search of a file or document you can make use of keyword search option to make your investigation time-efficient. Click on 'Keyword Search 'to proceed.



You can input the keyword or any relevant string to proceed with the investigation and click on search.



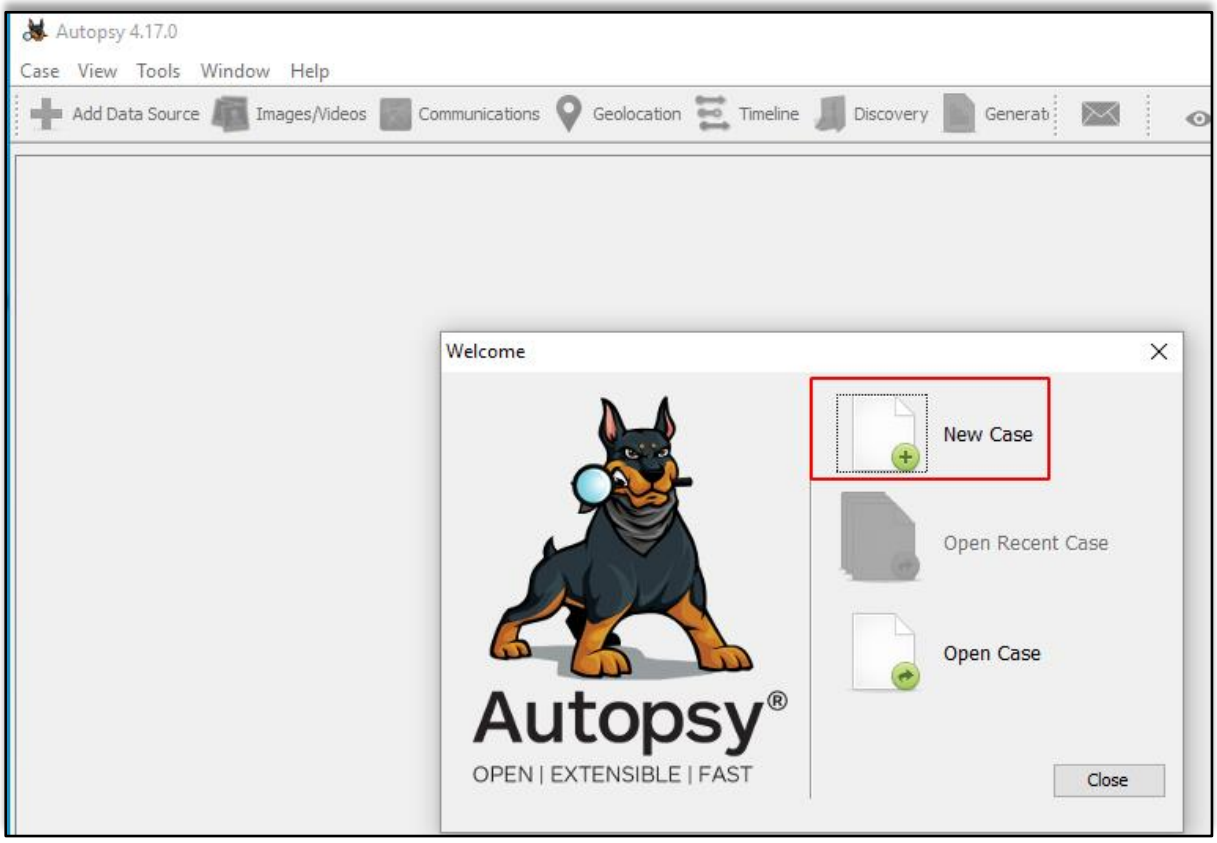
AUTOPSY WINDOWS

Autopsy for Windows

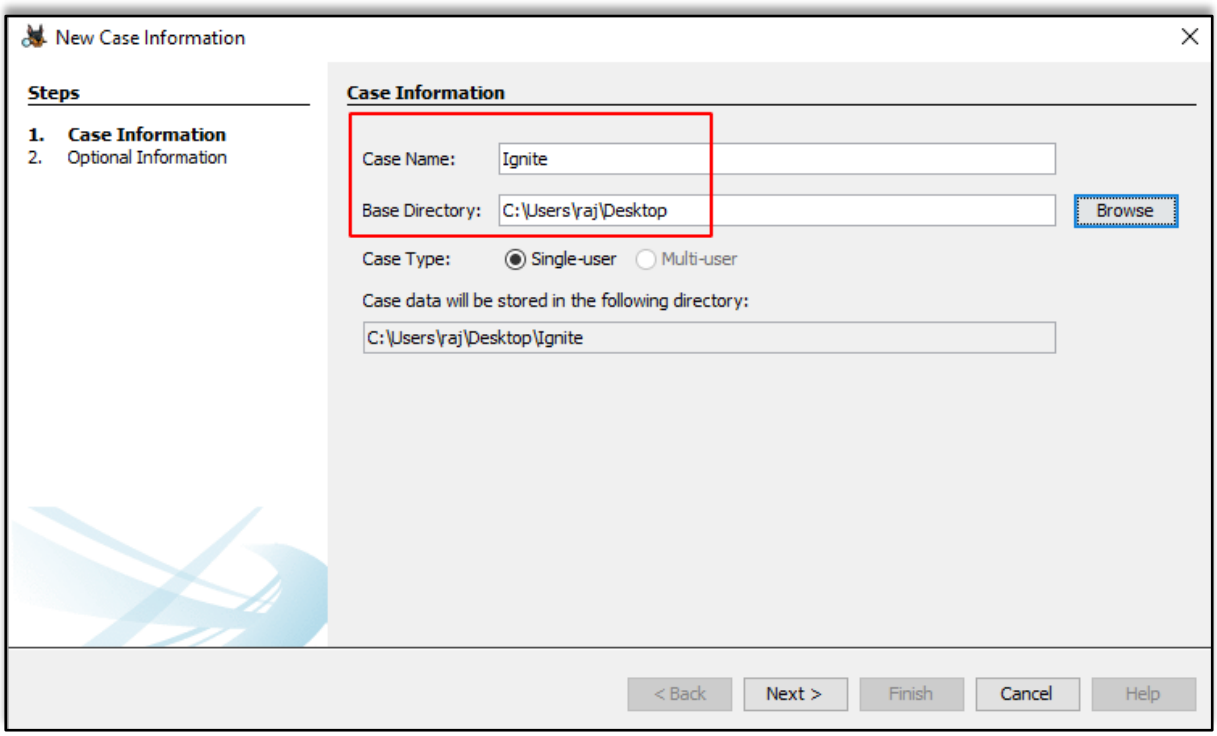
You can download the Autopsy Tool for Windows from here.

Creating a New Case

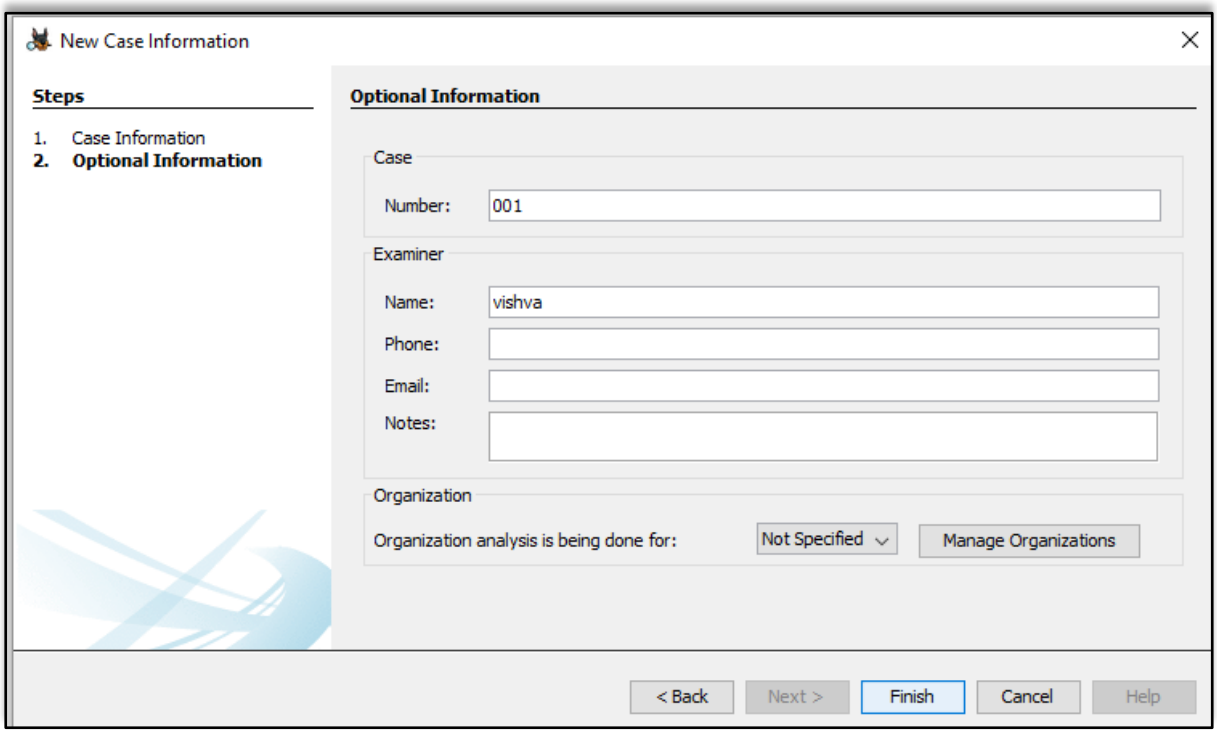
Run the Autopsy tool on your Windows Operating System and click on “New Case” to create a new case.



Then fill in all the necessary case information like the case name and choose a base directory to save all the case data in one place.

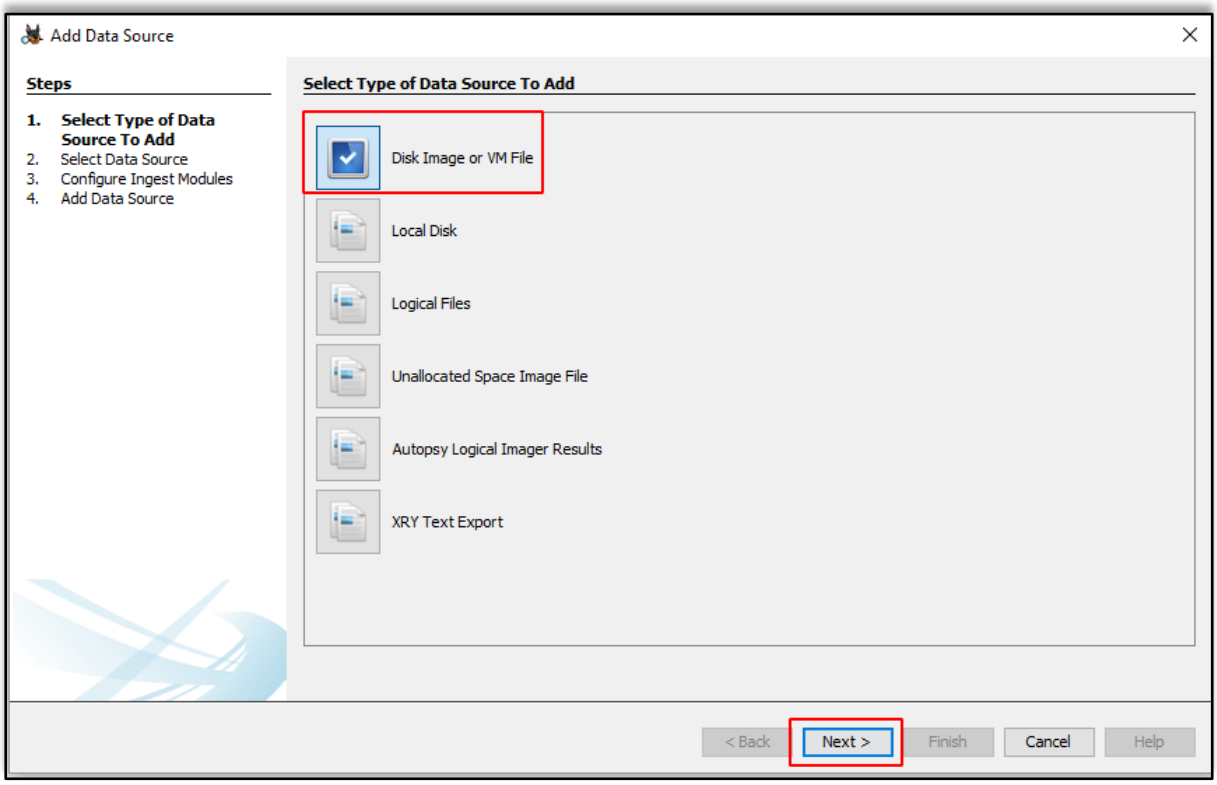


You can also add additional optional information about the case if required.

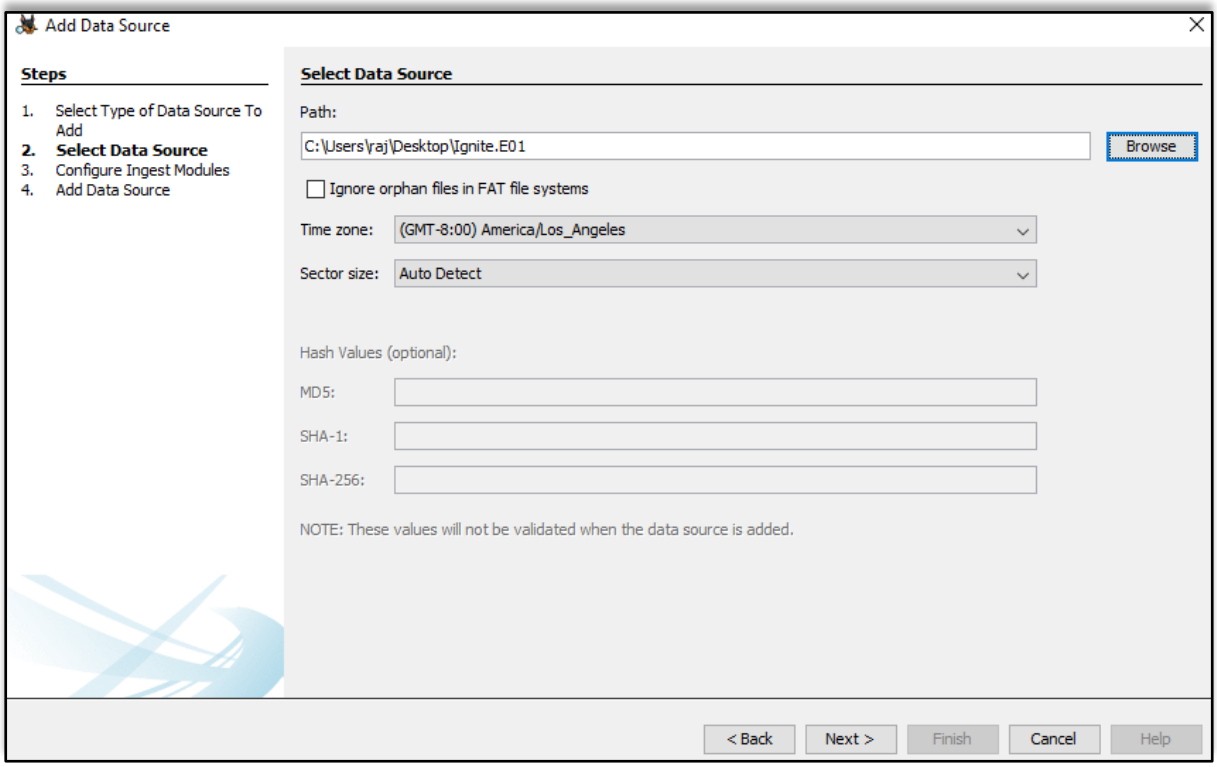


Now let us add the type of data source. There are various types to choose from.

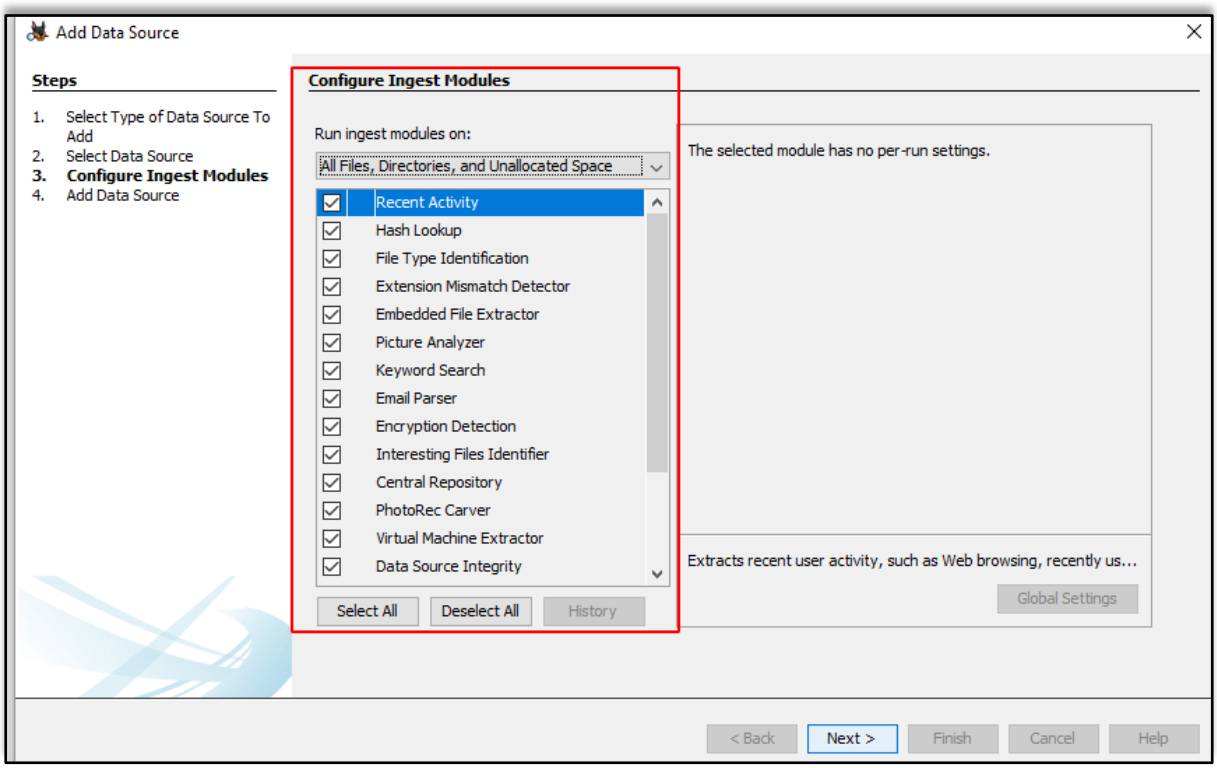
- **Disk Image or VM file:** This includes the image file which can be an exact copy of a hard drive, media card, or even a virtual machine.
- **Local Disk:** This option includes devices like Hard disk, Pen drives, memory cards, etc.
- **Logical Files**: It includes the image of any local folders or files.
- **Unallocated Space Image File**: They include files that do not contain any file system and run with the help of the ingest module.
- **Autopsy Logical Imager Results:** They include the data source from running the logical imager.
- **XRY Text Export:** This includes the data source from exporting text files from XRY.



Now let us add the data source. Here we have a previously created image file, so we will add the location of that file.



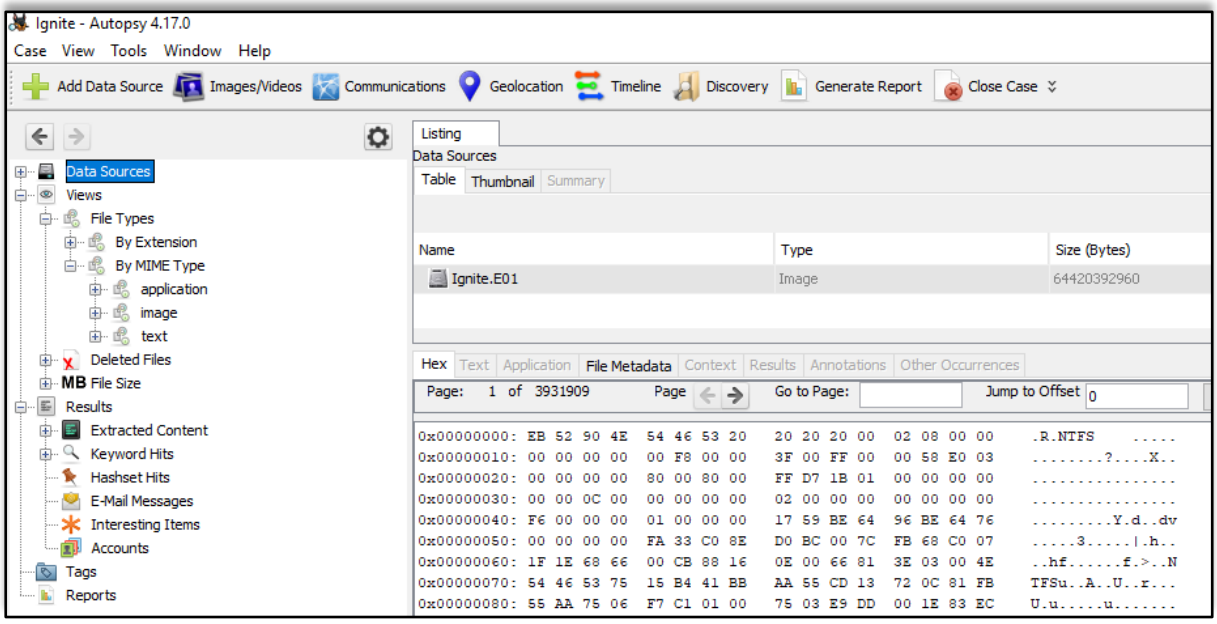
Next, you will be prompted to **Configure the Ingest Module.**



The contents of the Ingest module are listed below:

INGEST MODULE	
Recent Activity	It is used to discover the recent operations that were performed on the disk, like the files that were viewed recently.
Extension Mismatch Detector	It is used to identify files whose extensions were tampered with or had been changed to hide the evidence.
Hash Lookup	It is used to identify a particular file using its hash value.
File Type Identification	This is used to identify files based on their internal file signatures than just the file extensions.
Embedded File Extractor	It is used to extract embedded files like .zip, .rar, etc. and use those files for analysis.
Keyword Search	This is used to search for any particular keyword or a pattern in the image file.
Email Parser	This is used to extract information from email files if the disk holds any email database information.
Encryption Detection	This helps to detect and identifies encrypted password-protected files.
Interesting File Identifier	Using this feature the examiner is notified when results pertaining to the set of rules that are defined to identify a particular type of file.
PhotoRec Carver	This helps the examiner to recover files, photos, etc. from the unallocated space on the image disk.
Virtual Machine Extractor	It helps to extract and analyze if any Virtual machine is found on the disk image.
Data Source Integrity	It helps to calculate the hash value and store them in the database.

Data Source information displays basic metadata. Its detailed analysis is displayed at the bottom. It can be extracted one after the other.

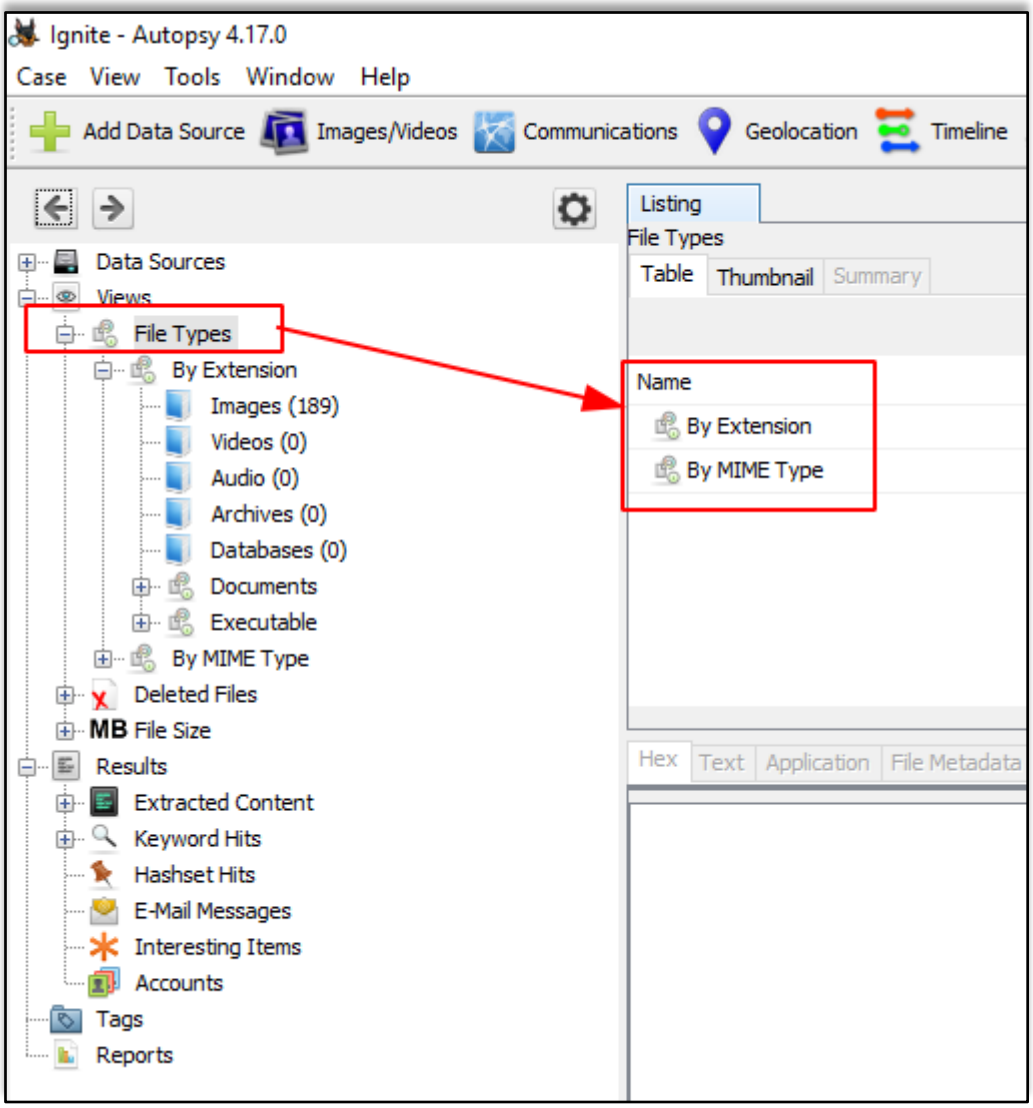


Views

File Type

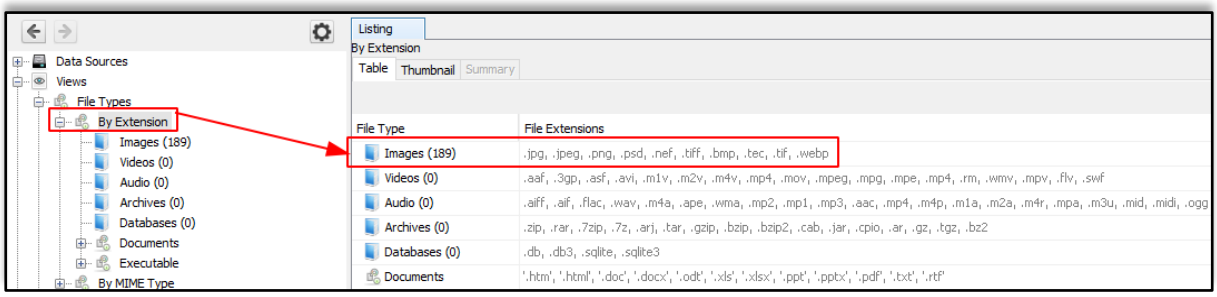
It can be classified in the form of File extension or MIME type.
It provides information on file extensions that are commonly used by the OS whereas MIME types are used by the browser to decide what data to represent. It also displays deleted files.

Note: These file types can be categorized depending on Extension, Documents, Executables.

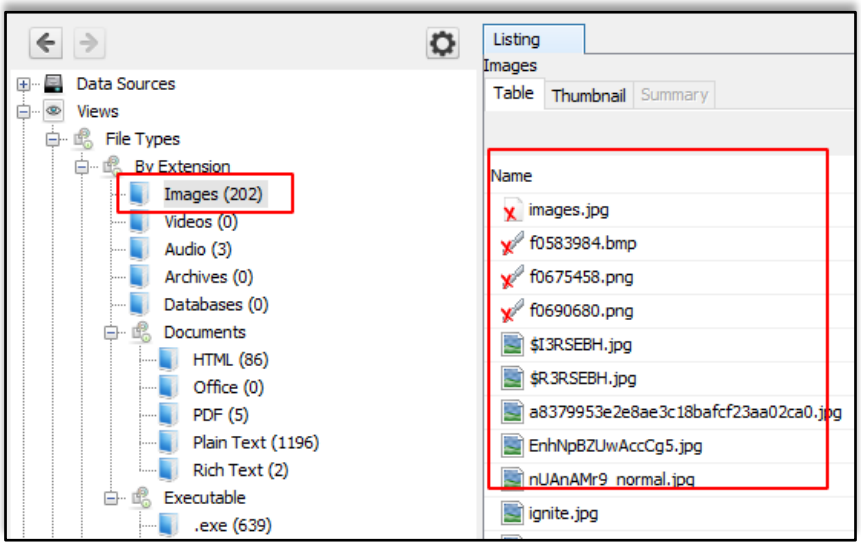


By Extension

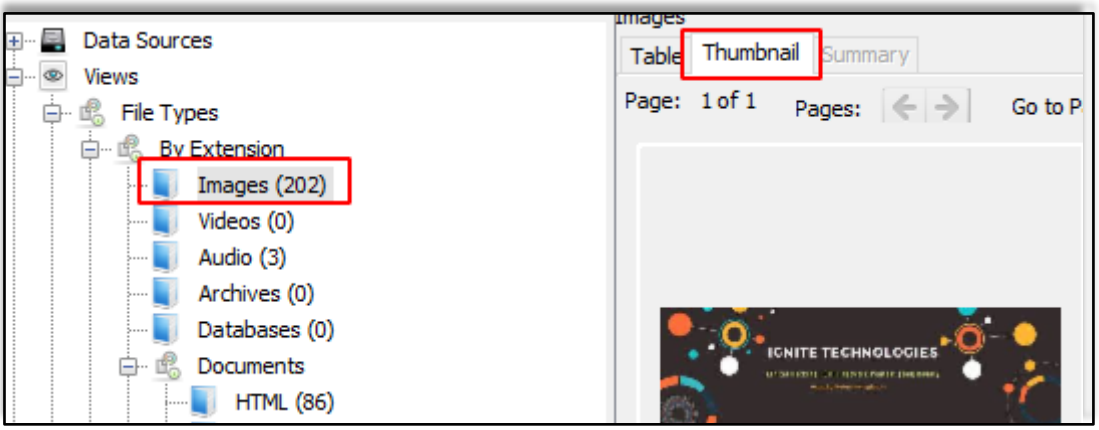
In the category Filetypes by extension and you can see that this has been sub-divided into file types like images, video, audio, archives, databases, etc.



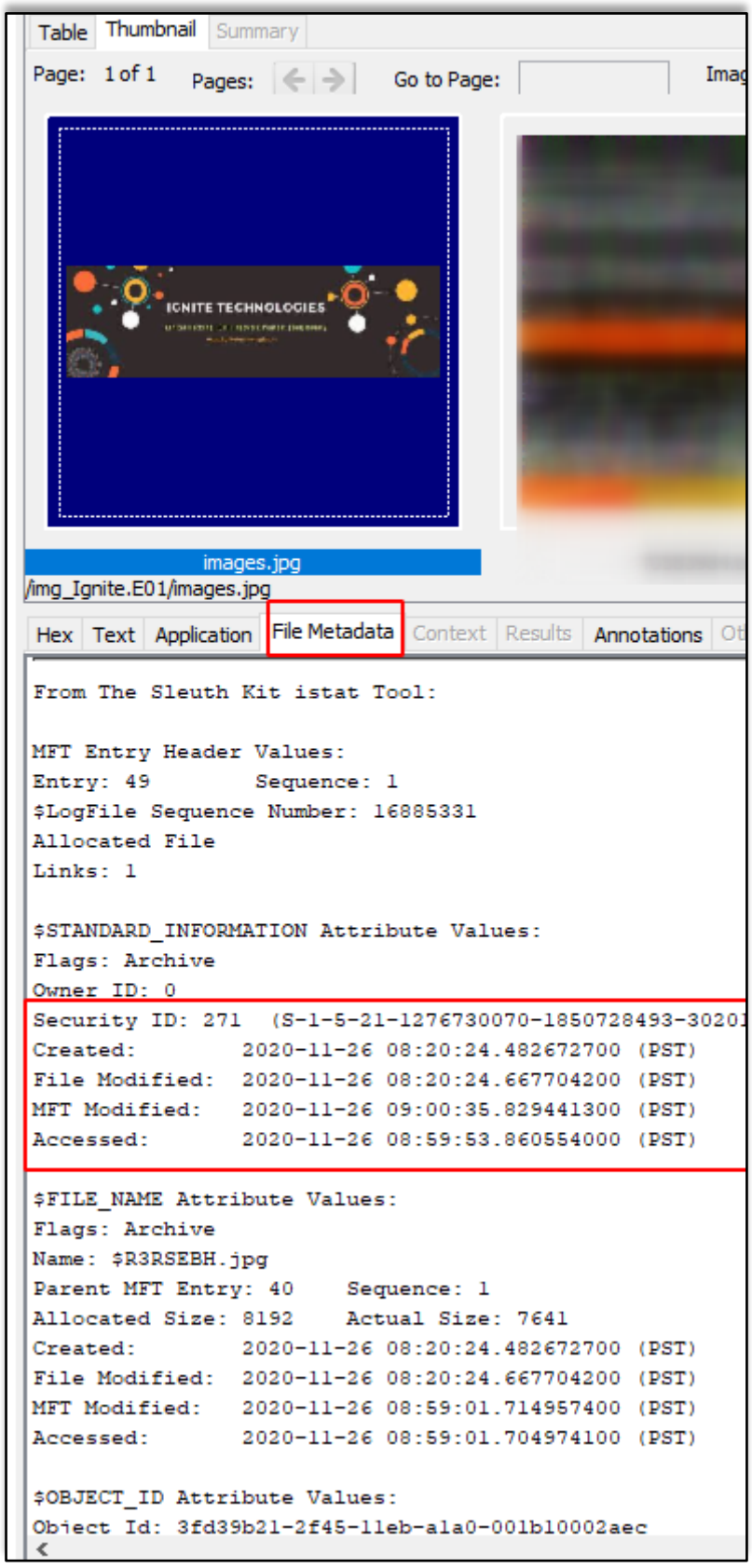
Let us click on images and explore the images that have been recovered.



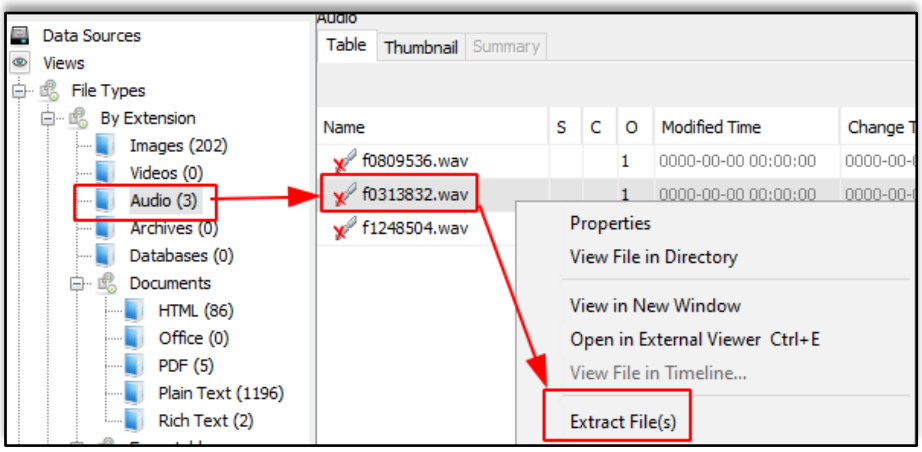
We can also view the thumbnail of the images.



On viewing the thumbnail, you can view the file metadata and details about the image.

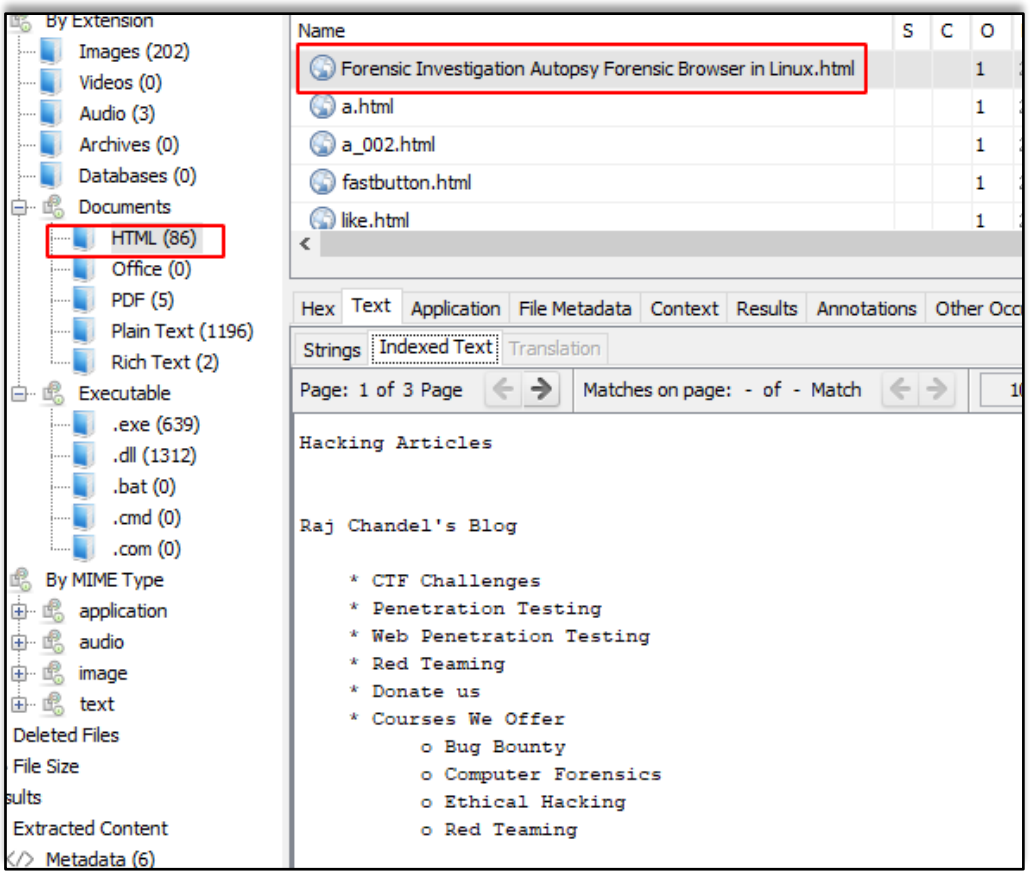


Here we can also view a few audio files that have been recovered. We can extract these files from the system and hear to them using various software.

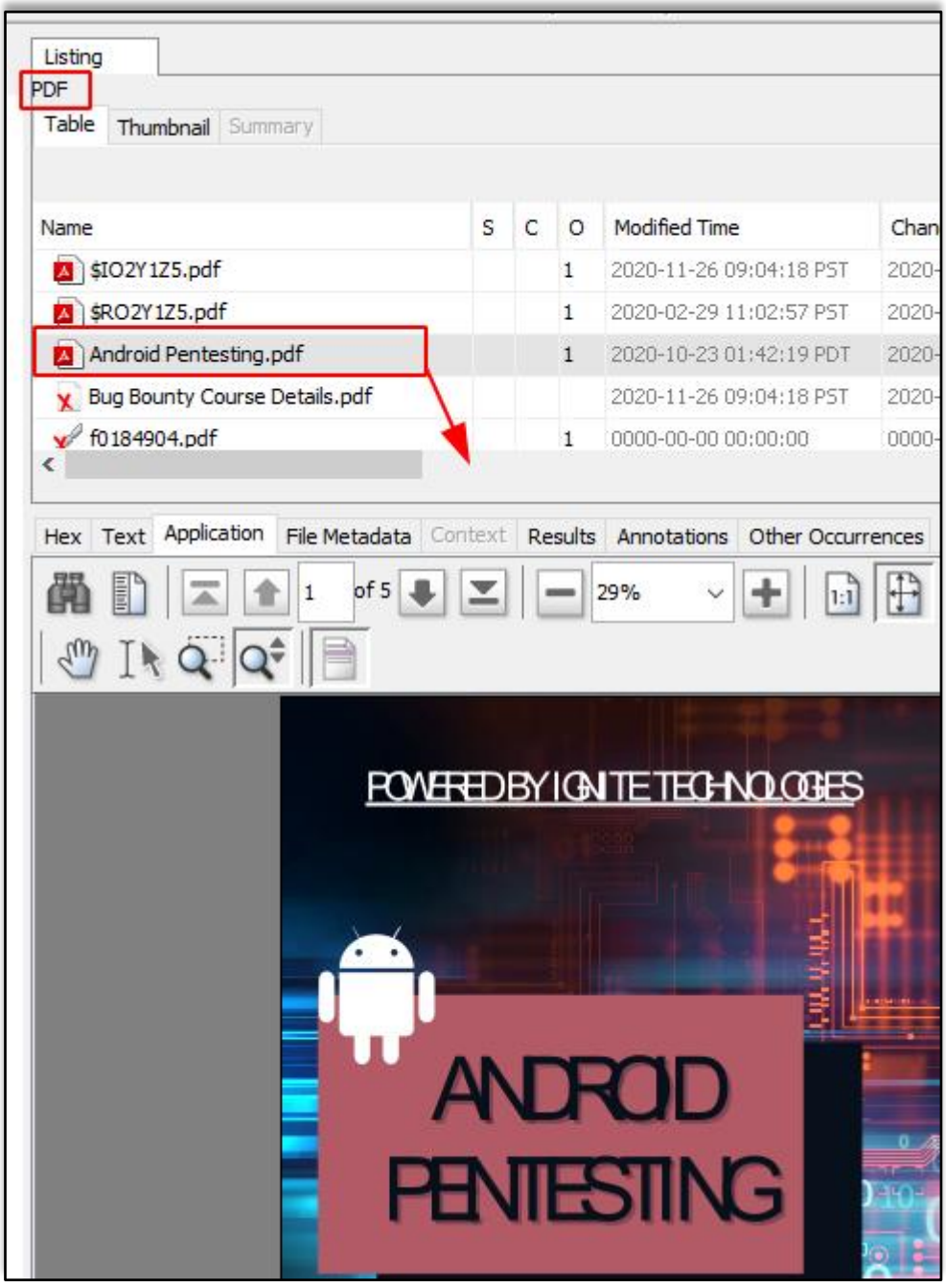


Documents

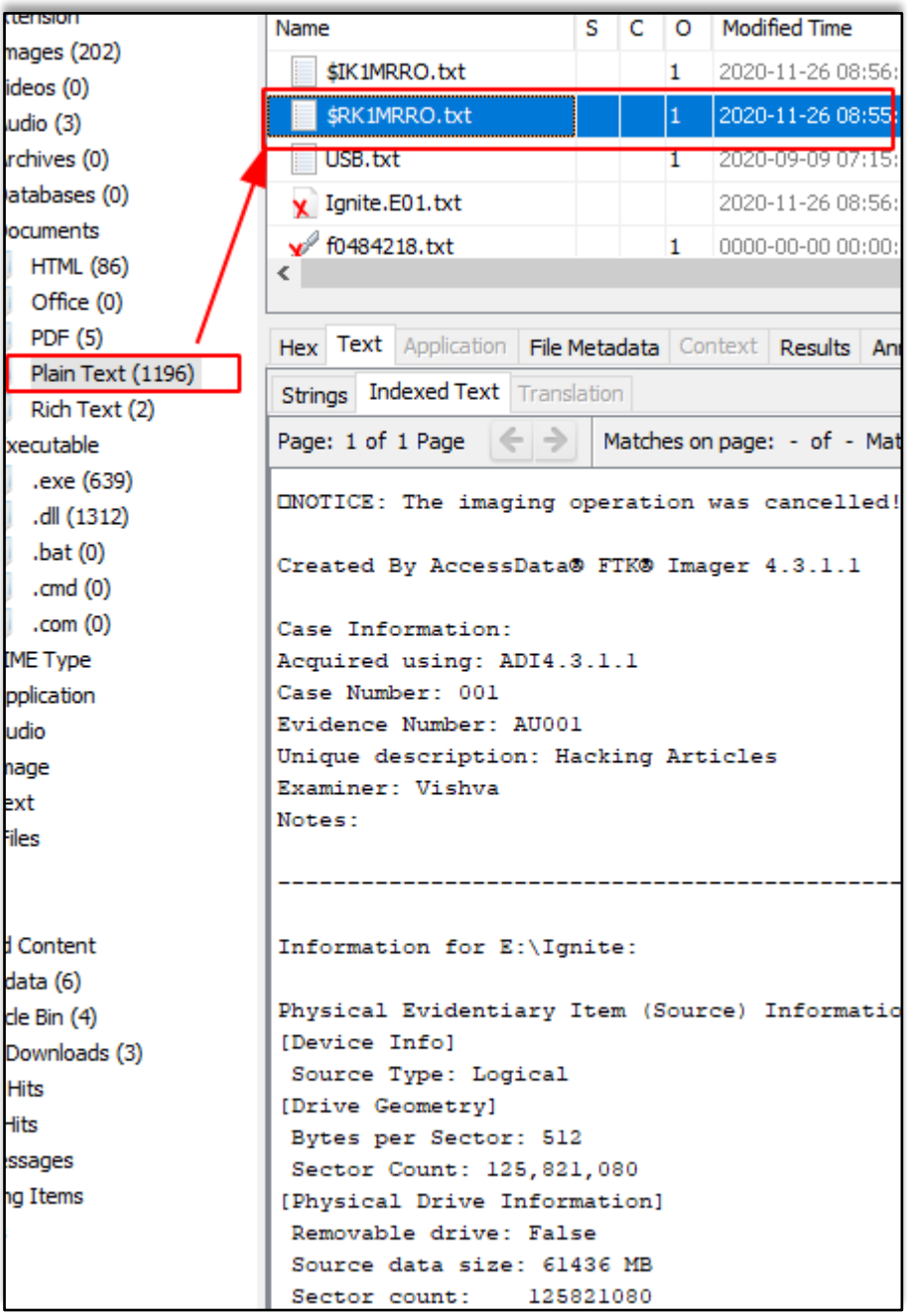
The documents are categorized into 5 types: HTML, office, PDF, Plain Text, Rich Text.
On exploring the documents option, you can see all the HTML documents present, you can click on the important ones to view them.



On exploring the PDF option, you can also find the important PDF in the disk image.

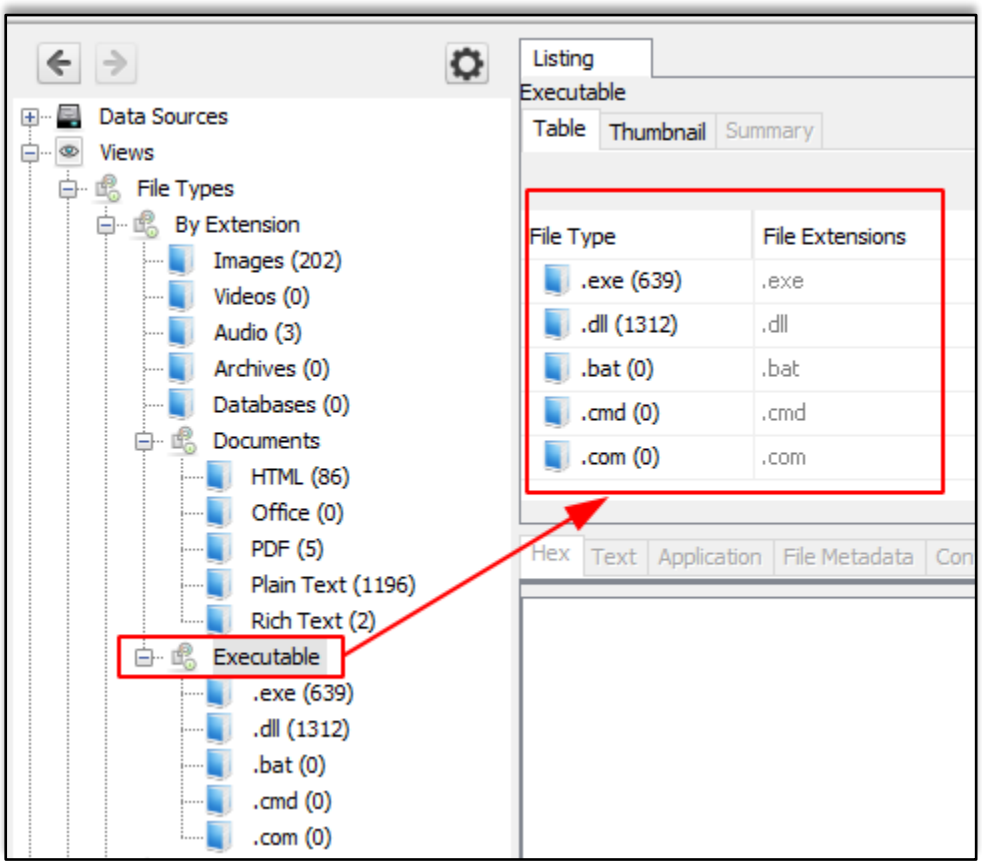


Similarly, the various Plain text files can also be viewed. You can also recover deleted plain text files.



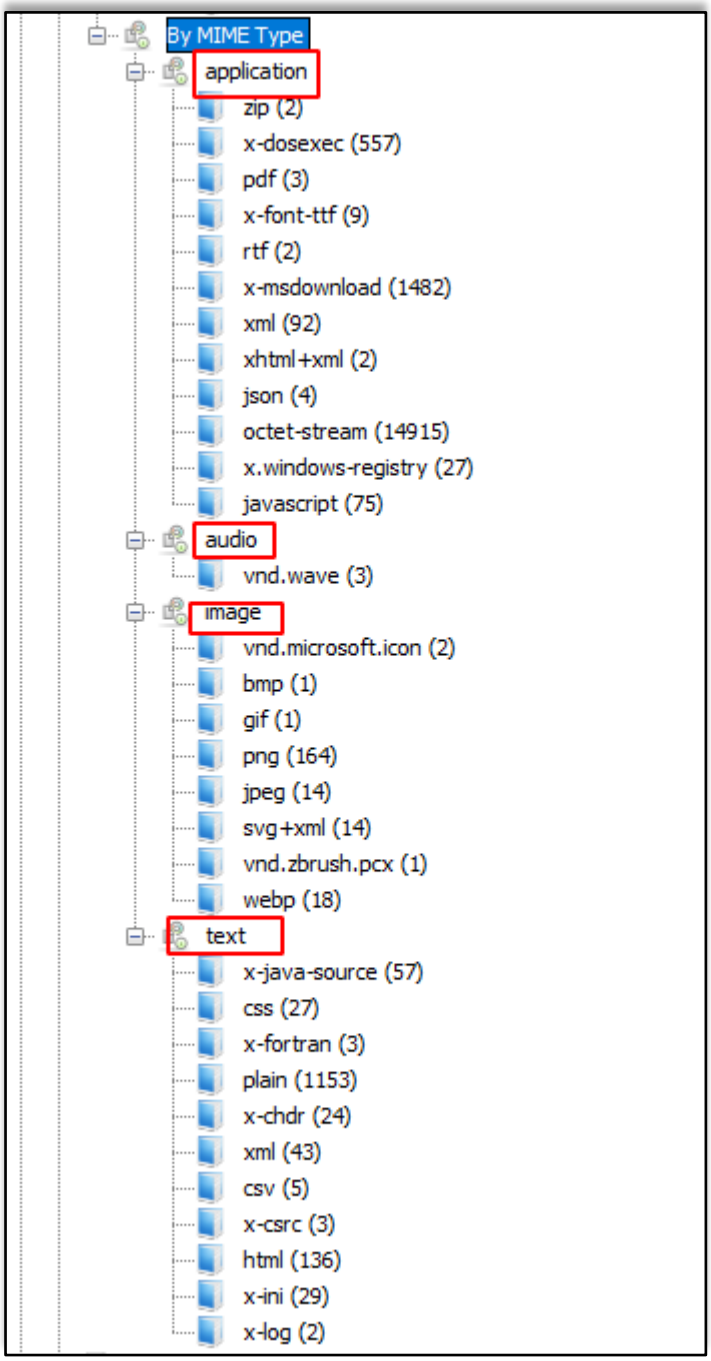
Executables

These file types are then sub-divided into .exe, .dll, .bat, .cmd and .com.



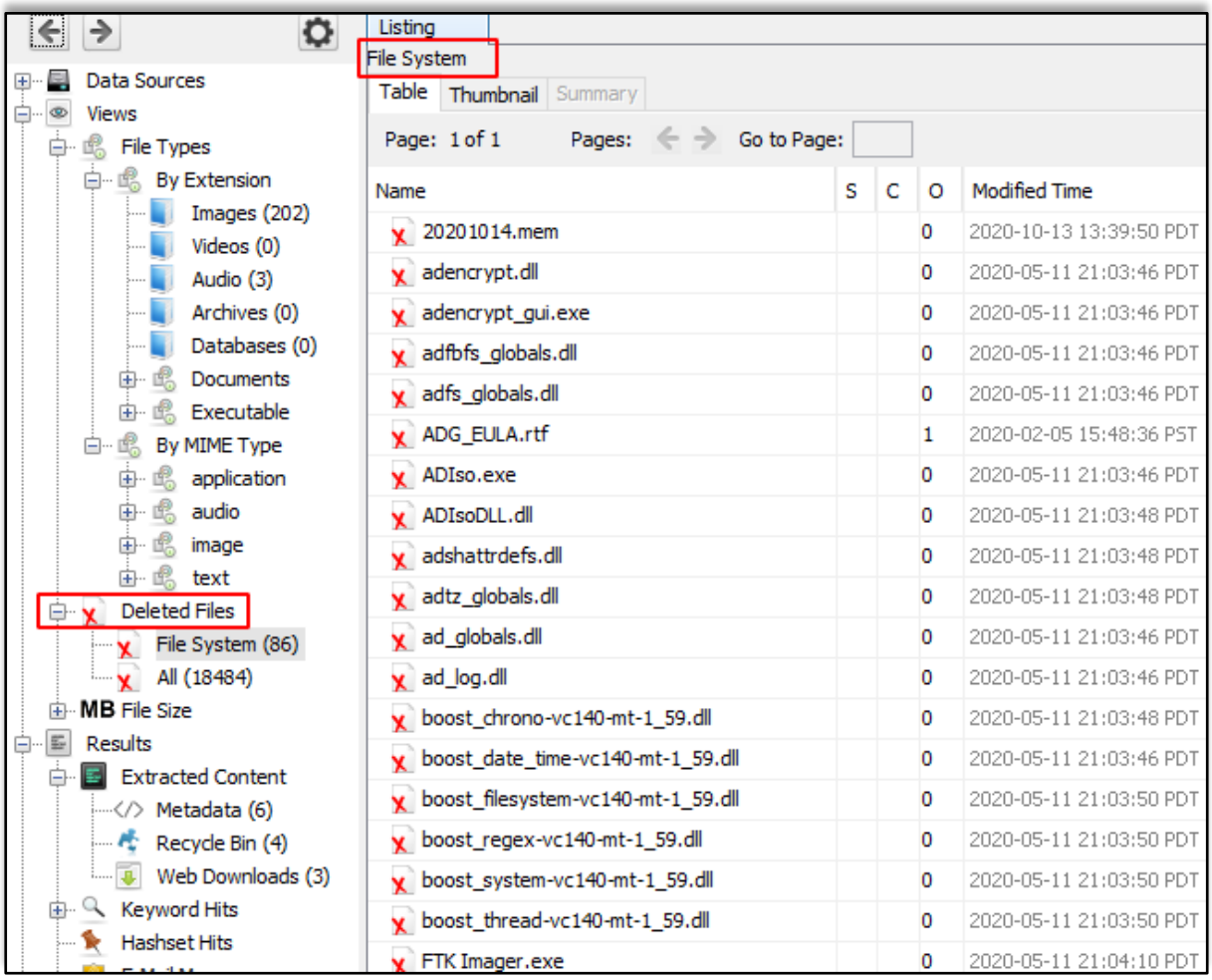
By Mime Type

In this type of category, there are four sub-categories like application, audio, image, and text. They are divided further into more sections and file types.



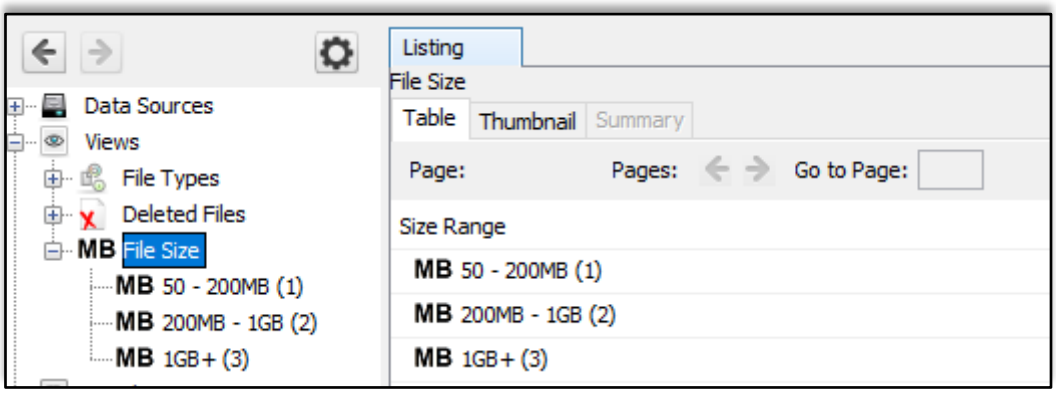
Deleted Files

It displays information about the deleted file which can be then recovered.



MB size Files

In this, the files are categorized based on their size starting from 50MB. This allows the examiner to look for large files.

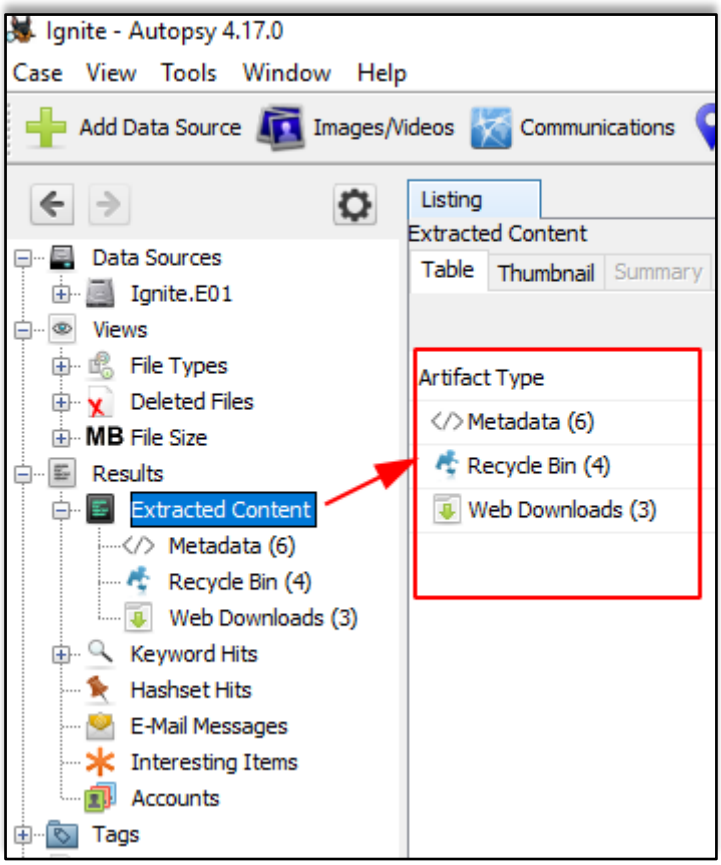


Results

In this section, we get information about the content that was extracted.

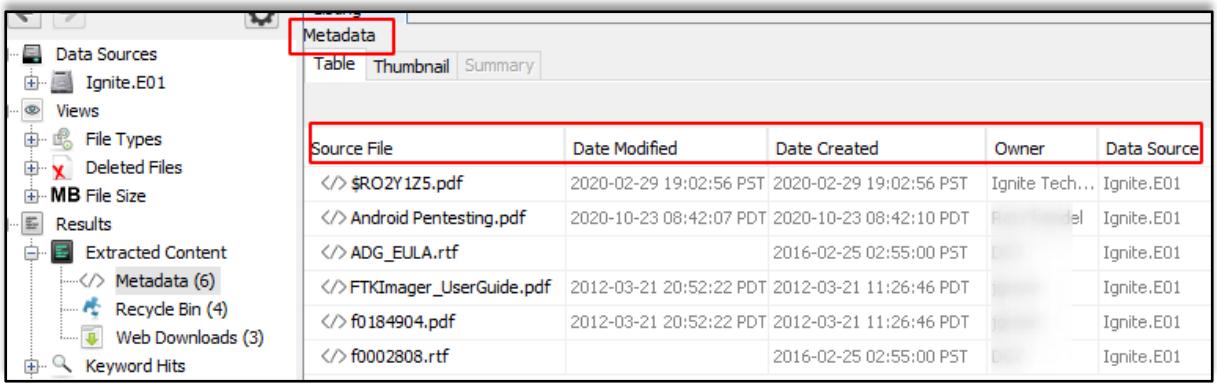
Extracted Content

All the content that was extracted, is segregated further in detail. Here we have found metadata, Recycle Bin, and web downloads. Let us further view each one of them.



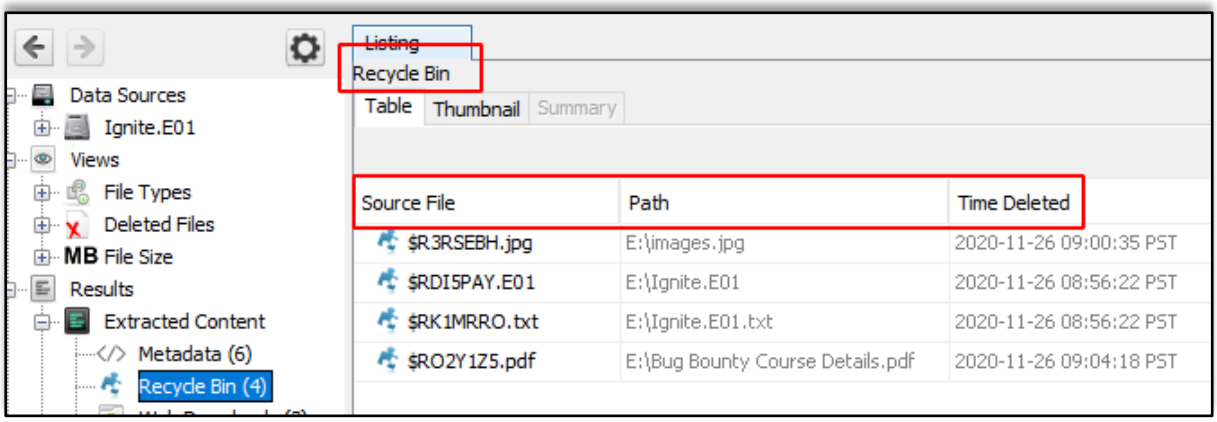
Metadata

Here we can view all the information about the files like the date it was created, to was modified, file's owner, etc.



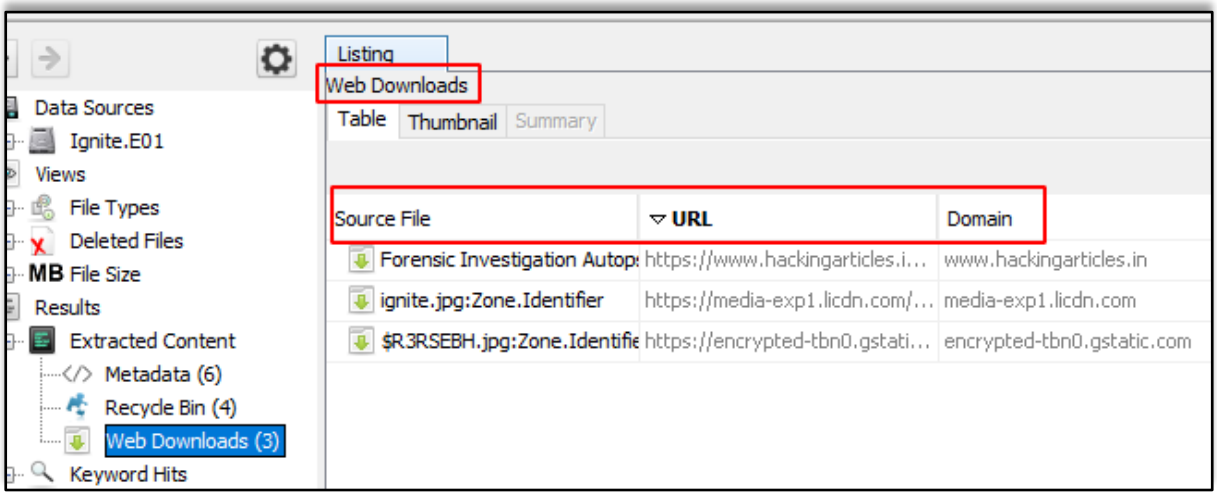
Recycle Bin

The files that were put in the recycle bin are found in this category.



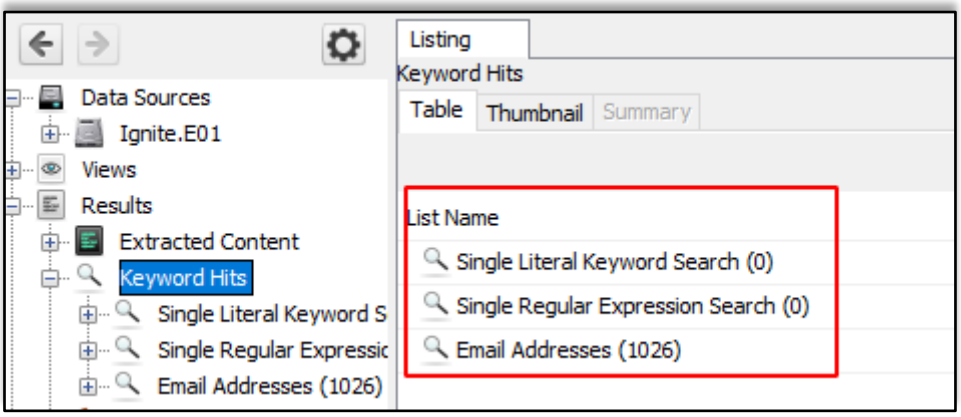
Web Downloads

Here you can see the files that were downloaded from the internet.

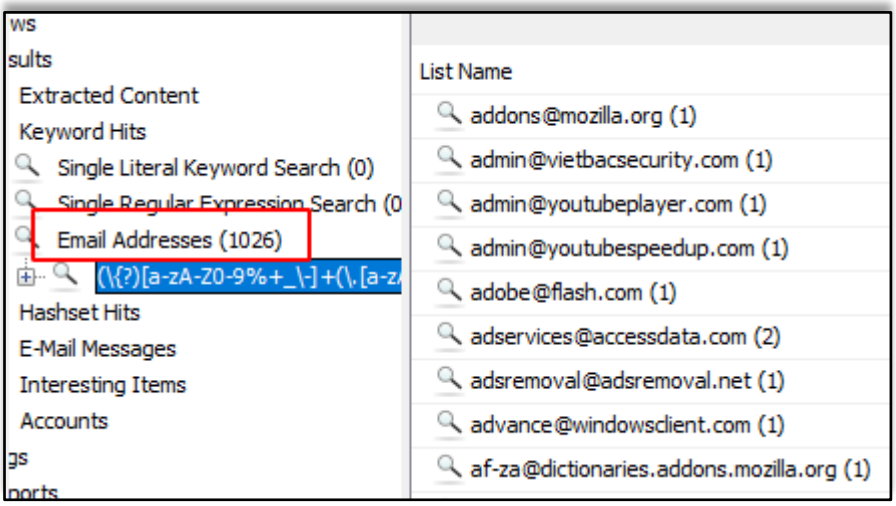


Keyword Hits

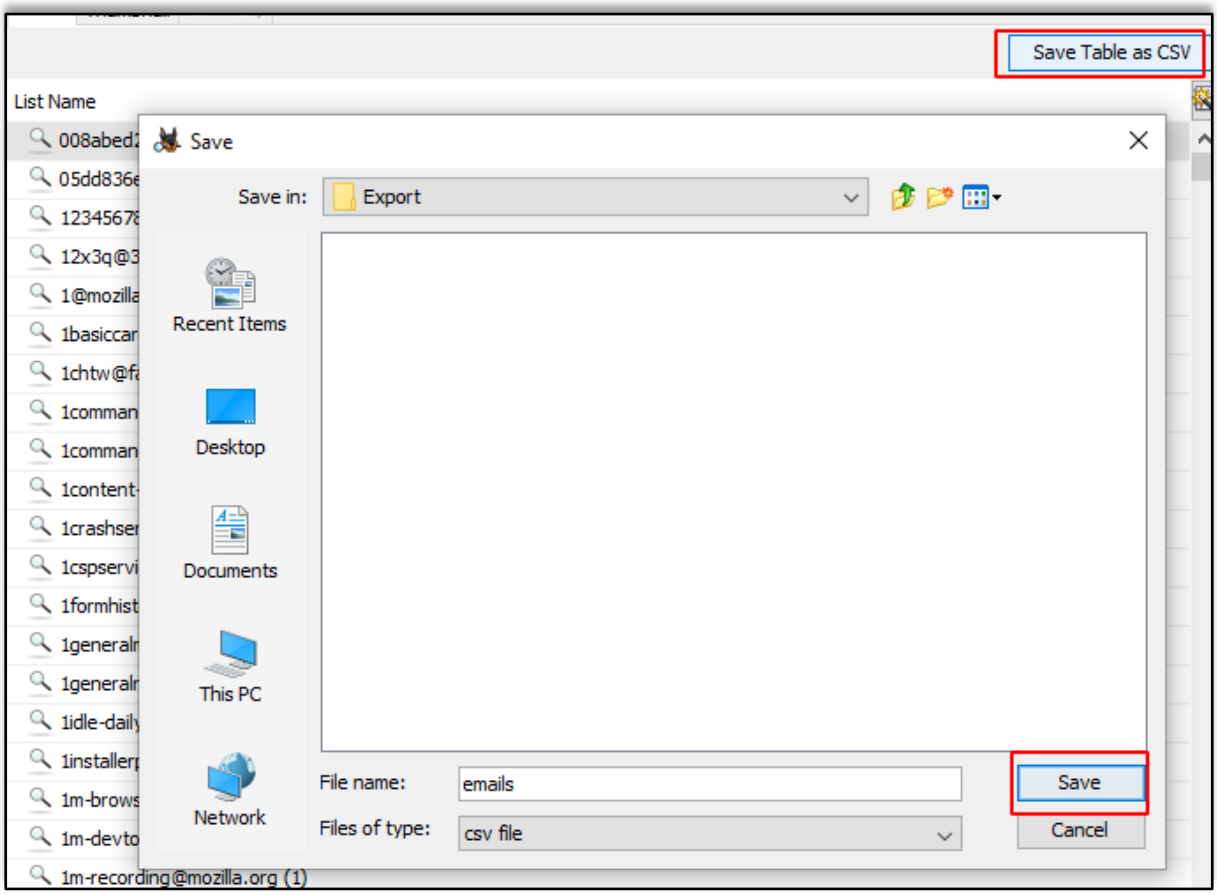
In this, any specific keywords can be looked up for in the disk image. The search can be conducted concerning the Exact match, Substring matches, Emails, Literal words, Regular expressions, etc.



You can view the available email addresses.

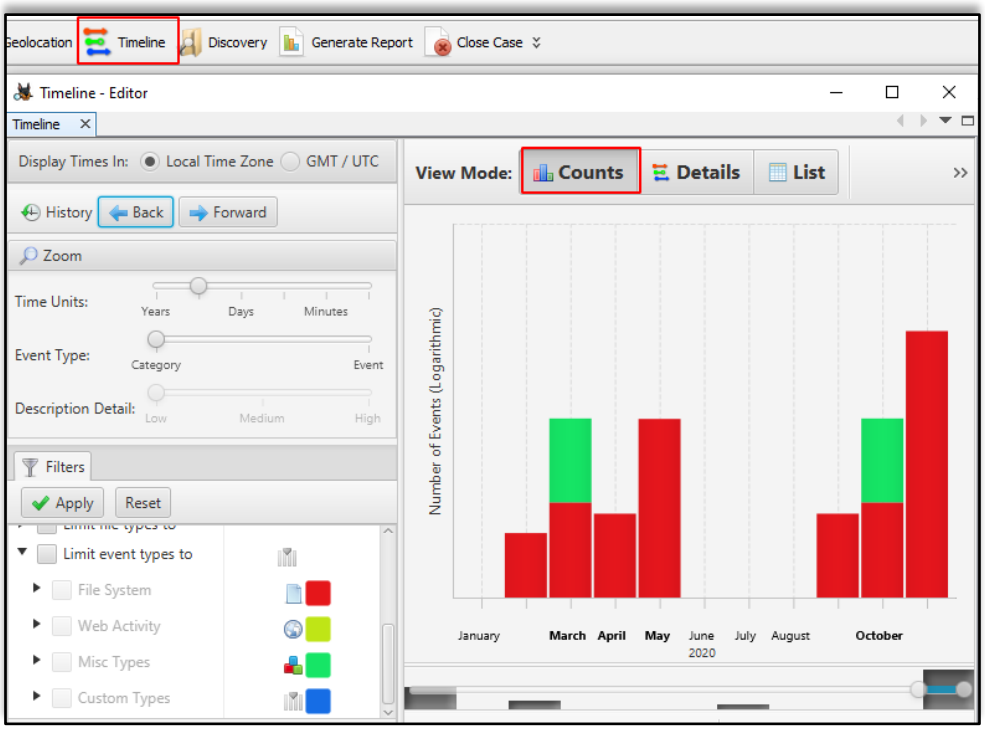


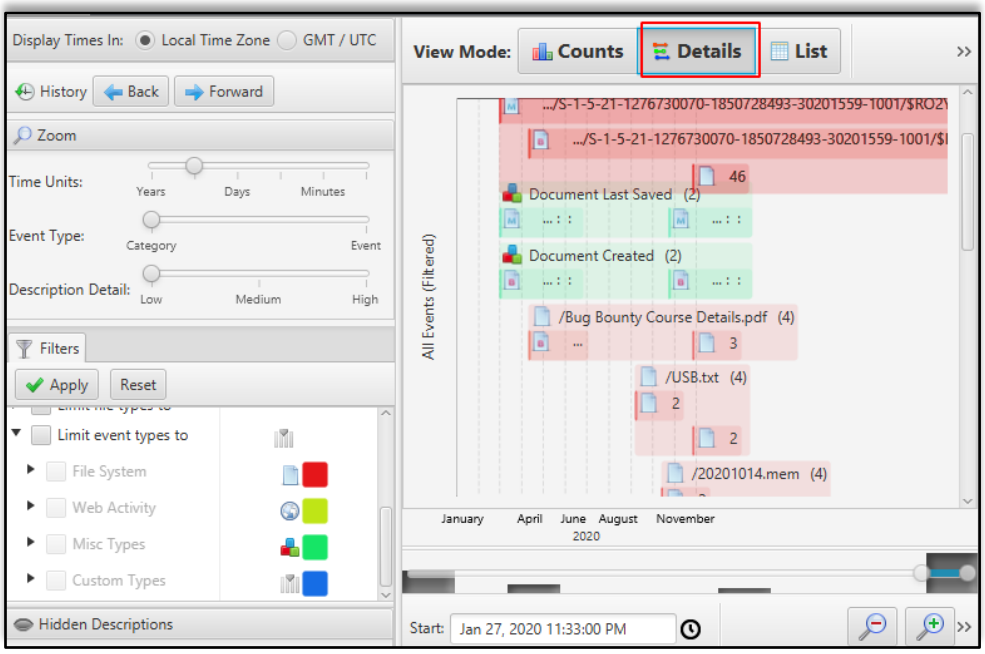
You can choose to export into a CSV format.

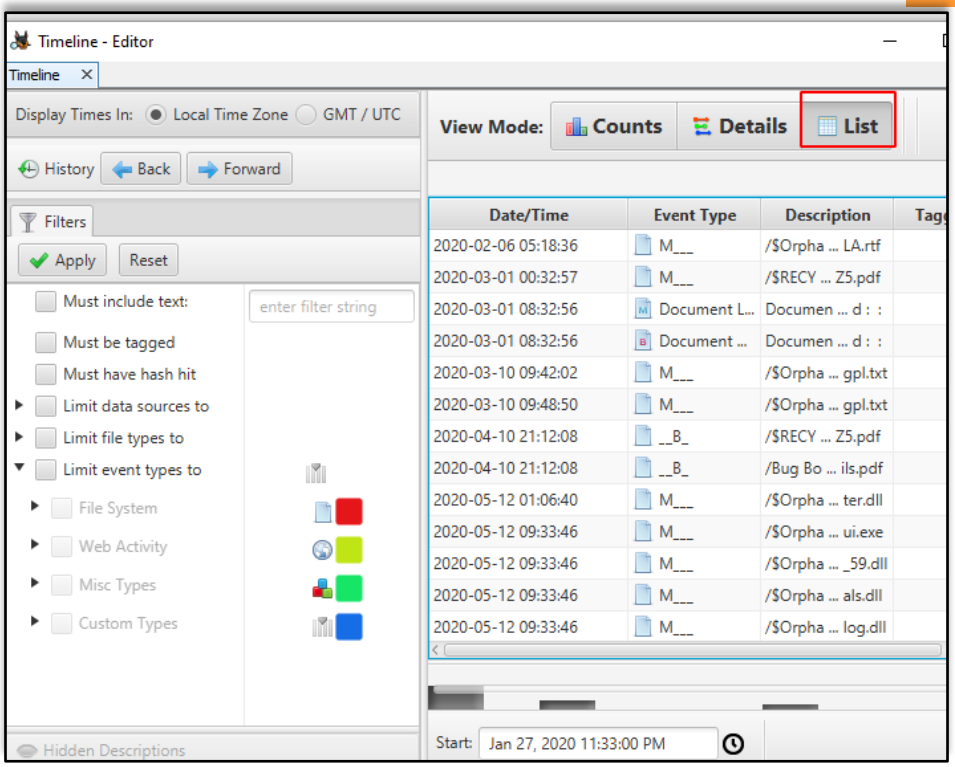


Timeline

By using this feature, you can get information on the usage of the system in a statistical, detailed, or list form.

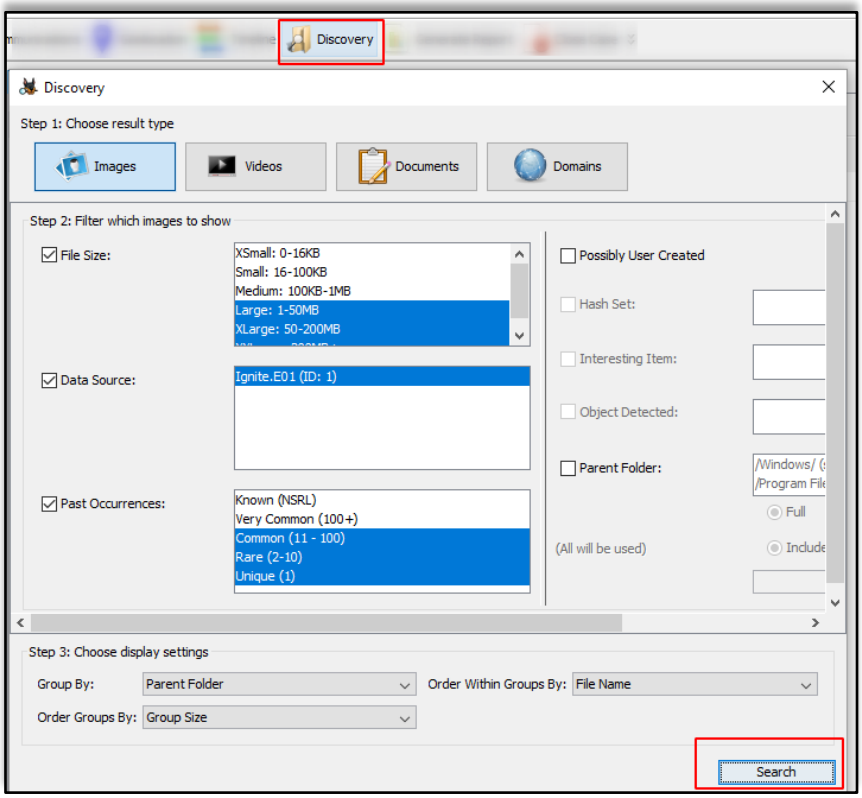




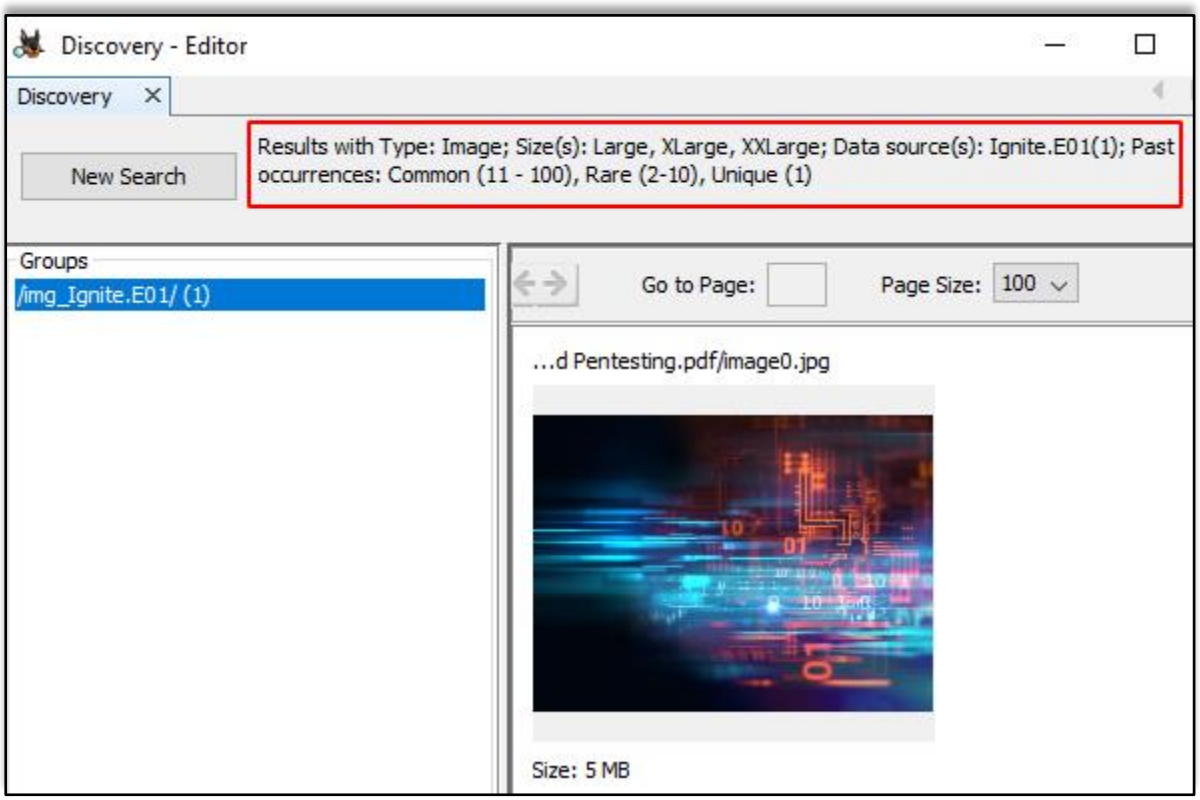


Discovery

This option allows finding media using different filters that are present on the disk image.

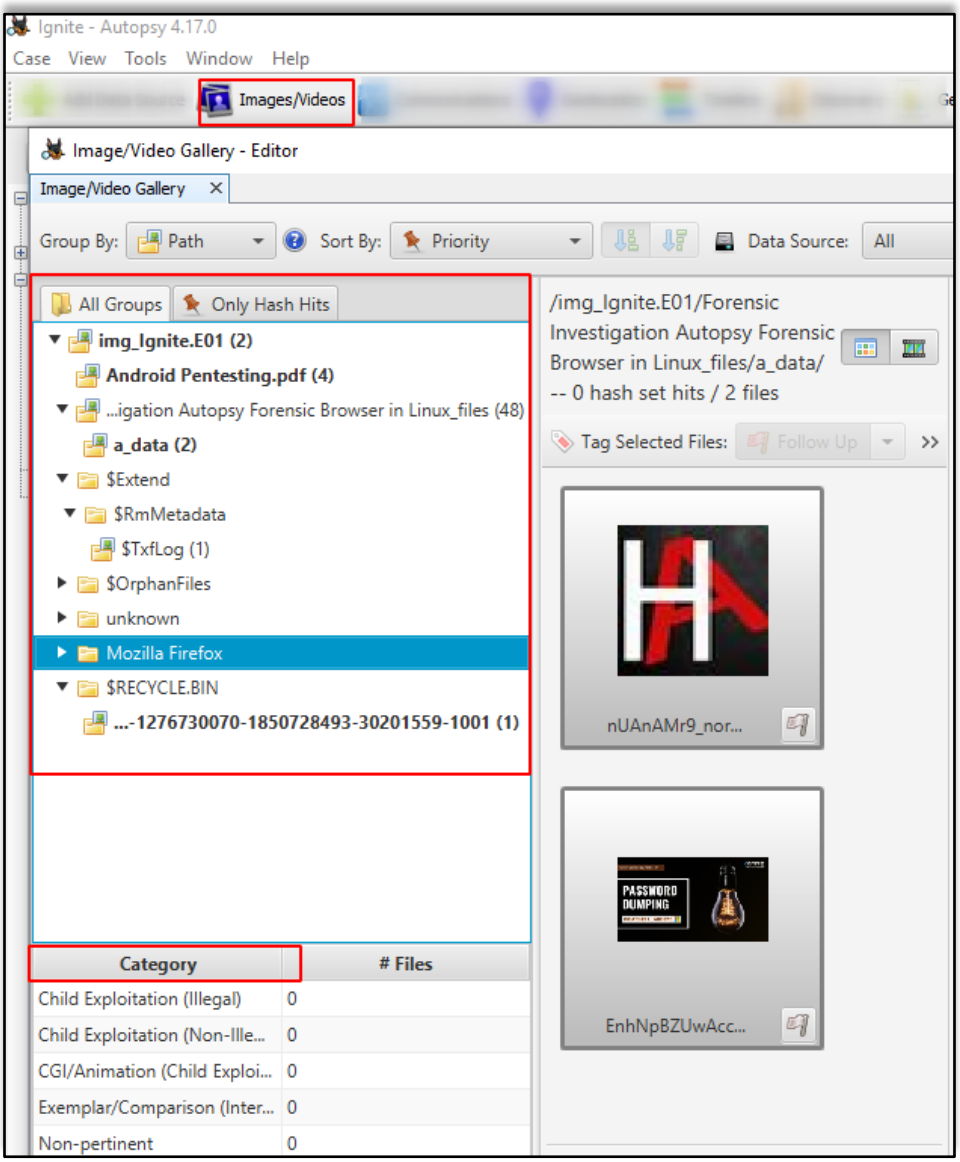


According to the selected options, you can get the desired results.



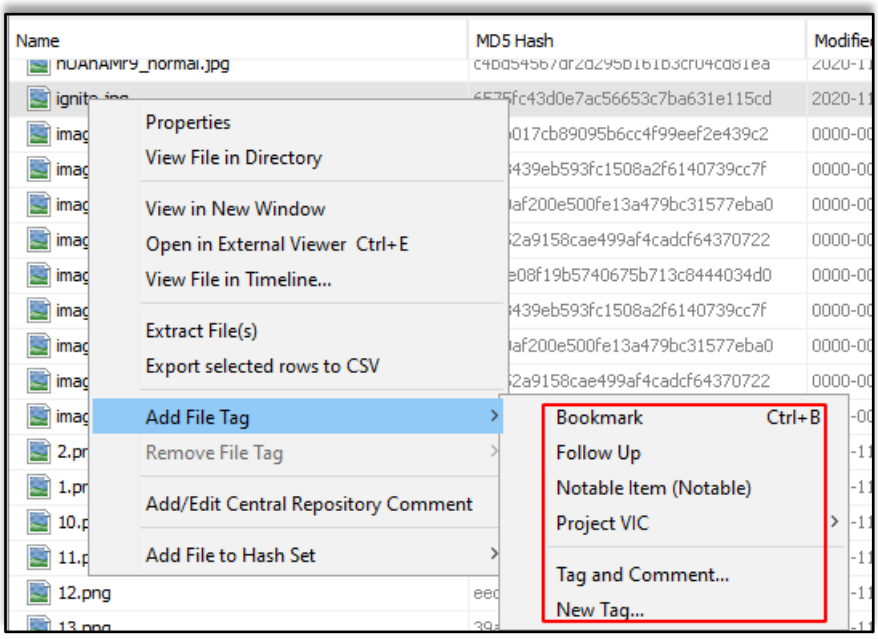
Images/Videos

This option is to find images and videos through various options and multiple categories

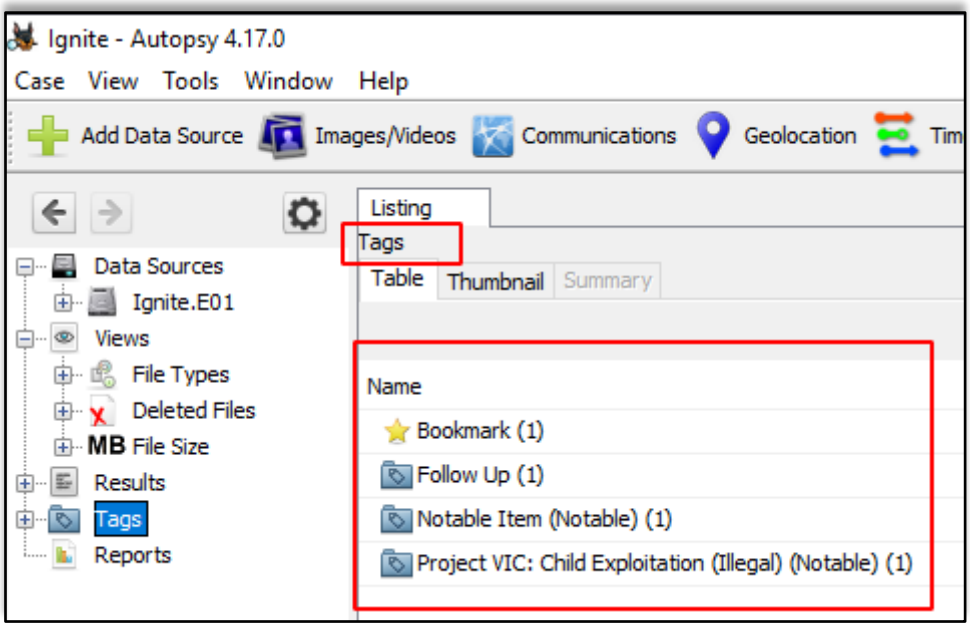


Add File Tag

Tagging can be used to create bookmarks, follow-up, mark as any notable item, etc.

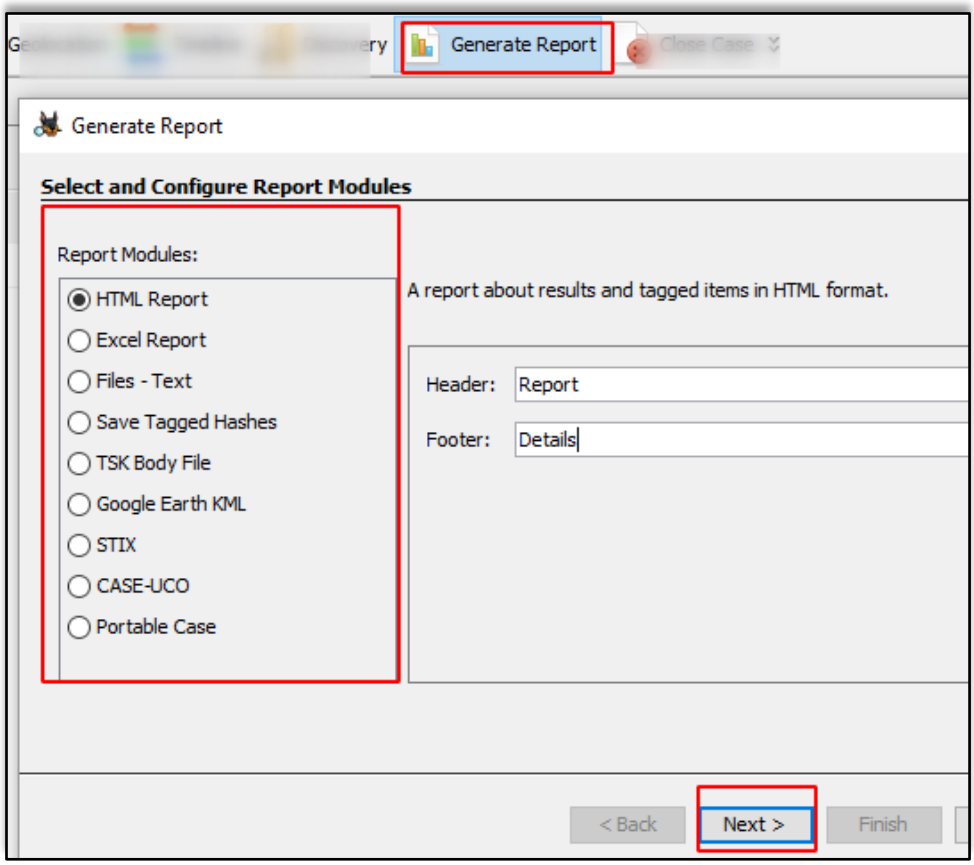


Now when you see the tags options, you will see that files were tagged according to various categories.

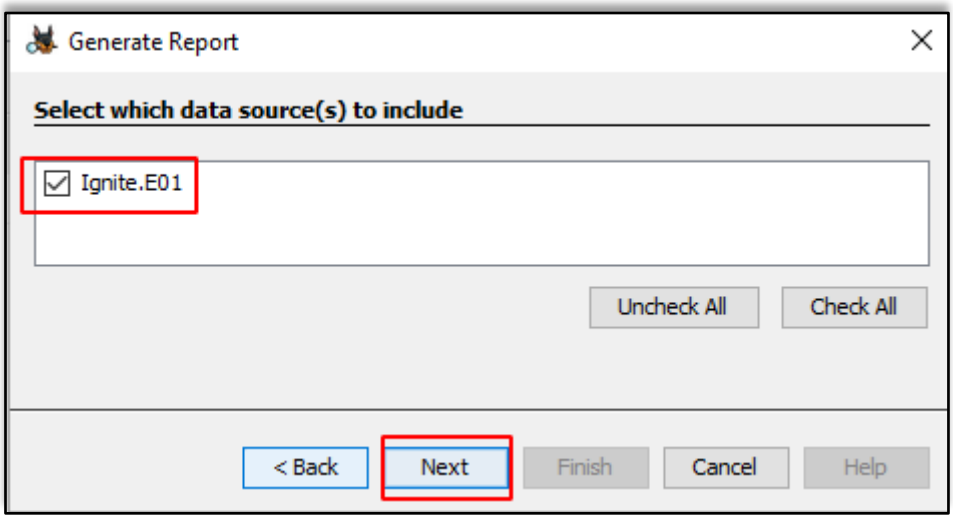


Generate Report

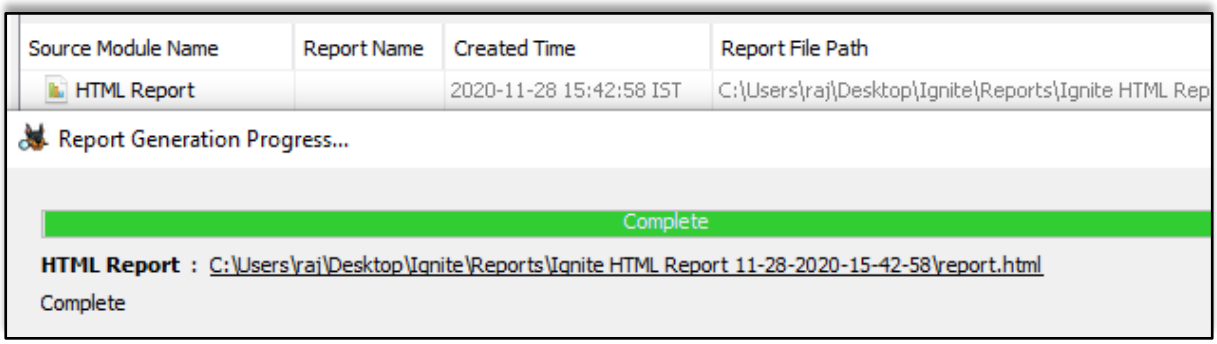
Once the investigation is done, the examiner can generate the report in various formats according to his preference.



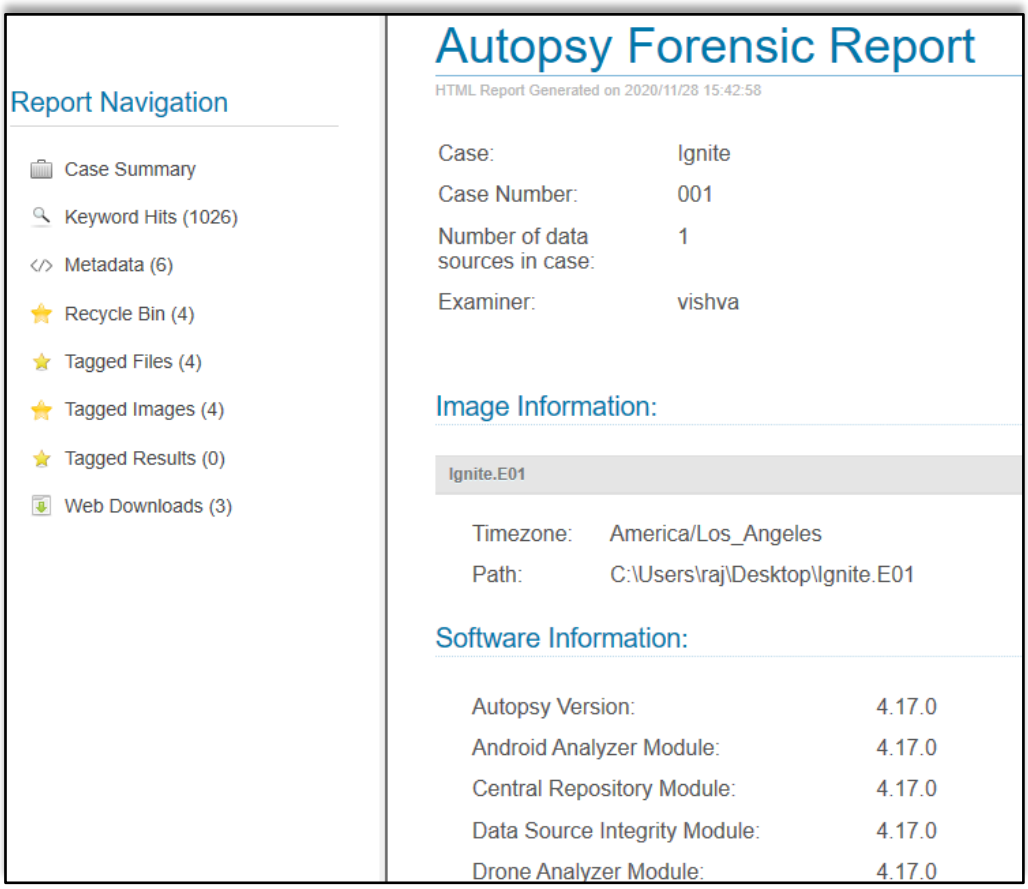
Check the data source whose report needs to be generated.



Here we chose to create the report in HTML format.



Kudos! Your Autopsy Forensic Report is ready!



References

- https://www.hackingarticles.in/comprehensive-guide-on-autopsy-tool-windows/
- https://www.hackingarticles.in/forensic-investigation-autopsy-forensic-browser-in-linux/

About Us

"Simple training makes Deep Learning"

"IGNITE" is a worldwide name in IT field. As we provide high-quality cybersecurity training and consulting services that fulfil students, government and corporate requirements.
We are working towards the vision to "Develop India as a Cyber Secured Country". With an outreach to over eighty thousand students and over a thousand major colleges, Ignite Technologies stood out to be a trusted brand in the Education and the Information Security structure.

We provide training and education in the field of Ethical Hacking & Information Security to the students of schools and colleges along with the corporate world. The training can be provided at the client's location or even at Ignite's Training Center.
We have trained over 10,000 + individuals across the globe, ranging from students to security experts from different fields. Our trainers are acknowledged as Security Researcher by the Top Companies like - Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more. Even the trained students are placed into a number of top MNC's all around the globe. Over with this, we are having International experience of training more than 400+ individuals.

The two brands, Ignite Technologies & Hacking Articles have been collaboratively working from past 10+ Years with about more than 100+ security researchers, who themselves have been recognized by several research paper publishing organizations, The Big 4 companies, Bug Bounty research programs and many more.

Along with all these things, all the major certification organizations recommend Ignite's training for its resources and guidance.
Ignite's research had been a part of number of global Institutes and colleges, and even a multitude of research papers shares Ignite's researchers in their reference.

iGNITE Technologies

What We Offer

Ethical Hacking

The Ethical Hacking course has been structured in such a way that a technical or a non-technical applicant can easily absorb its features and indulge his/her career in the field of IT security.

Bug Bounty 2.0

A bug bounty program is a pact offered by many websites and web developers by which folks can receive appreciation and reimbursement for reporting bugs, especially those affecting to exploits and vulnerabilities.
Over with this training, an indivisual is thus able to determine and report bugs to the authorized before the general public is aware of them, preventing incidents of widespread abuse.

Network Penetration Testing 2.0

The Network Penetration Testing training will build up the basic as well advance skills of an indivisual with the concept of Network Security & Organizational Infrastructure. Thereby this course will make the indivisual stand out of the crowd within just 45 days.

iGNITE Technologies

Red Teaming

This training will make you think like an "Adversary" with its systematic structure & real Environment Practice that contains more than 75 practicals on Windows Server 2016 & Windows 10. This course is especially designed for the professionals to enhance their Cyber Security Skills

CTF 2.0

The CTF 2.0 is the latest edition that provides more advance module connecting to real infrastructure organization as well as supporting other students preparing for global certification. This curriculum is very easily designed to allow a fresher or specialist to become familiar with the entire content of the course.

Infrastructure Penetration Testing

This course is designed for Professional and provides an hands-on experience in Vulnerability Assessment Penetration Testing & Secure configuration Testing for Applications Servers, Network Deivces, Container and etc.

Digital Forensic

Digital forensics provides a taster in the understanding of how to conduct investigations in order for business and legal audien ces to correctly gather and analyze digital evidence.