Autopsy

Forensic Investigation

Original Author (s): *Vishva Vaghela & Jeenali Kothari*

Table of Contents

<u>Abstract</u>

Autopsy is an open-source forensic tool used to investigate disk images for evidence in computer crimes. It helps recover deleted data and analyze information through features like timeline analysis, keyword search, and email analysis. Widely used by law enforcement and corporations, it is built into Kali Linux for Linux users and available for Windows on its official website.

In this report, we will show how to use Autopsy on both Windows and Linux to analyze file metadata during a forensic investigation.

If you're interested in digital forensics, this report is for you—sit back, buckle up, and let's dive into the adventure!

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.
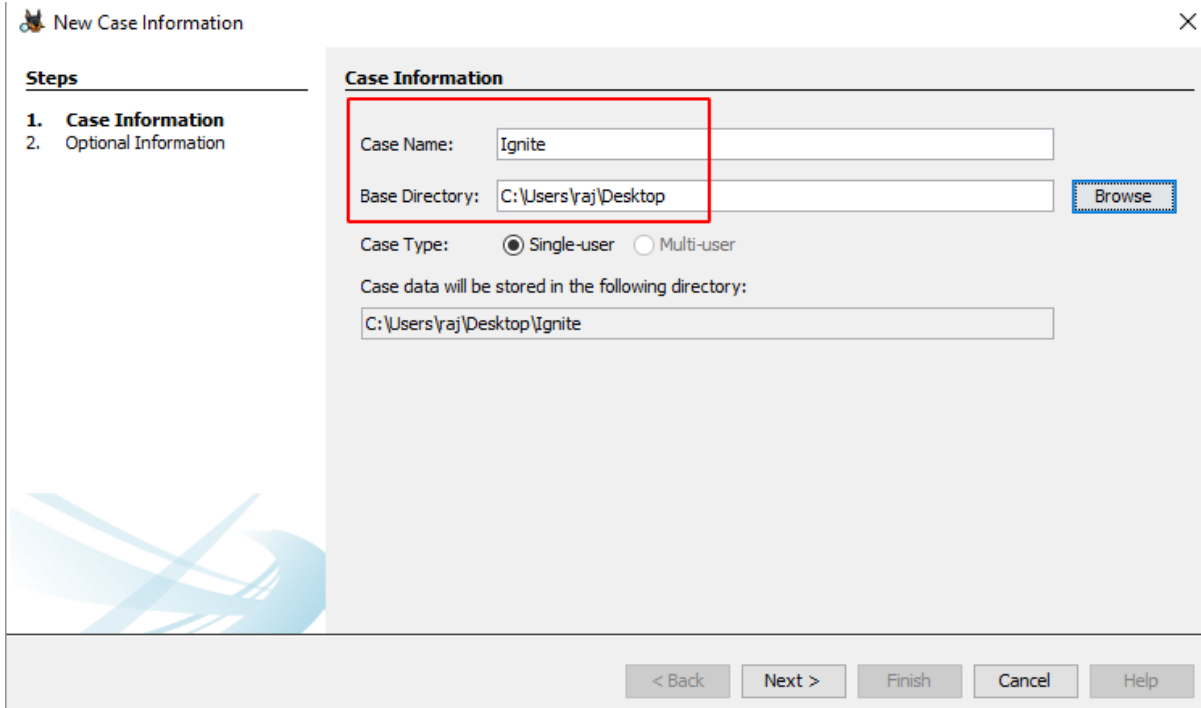
Windows Forensic Investigation

Creating a new Case

Run the Autopsy tool on your Windows Operating System and click on "New Case" to create a new case.
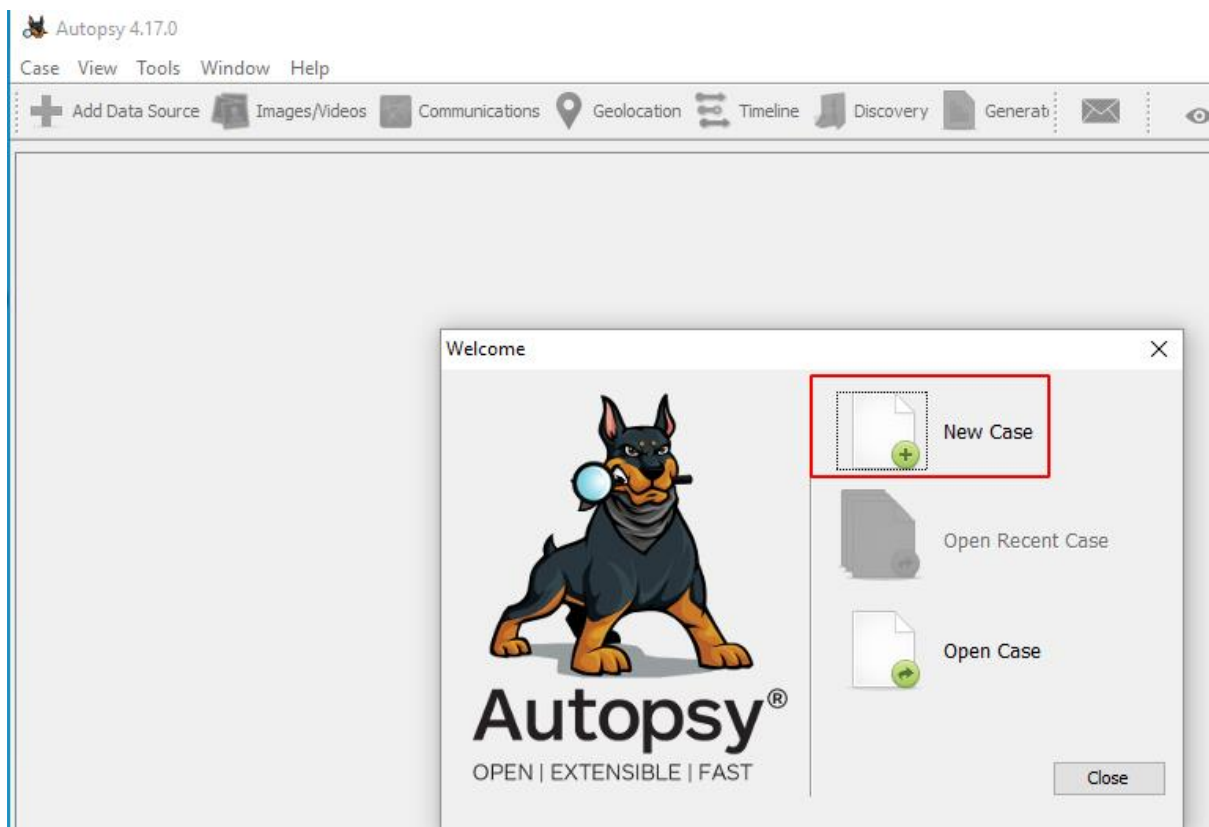
Then fill in all the necessary case information like the case name and choose a base directory to save all the case data in one place.

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.

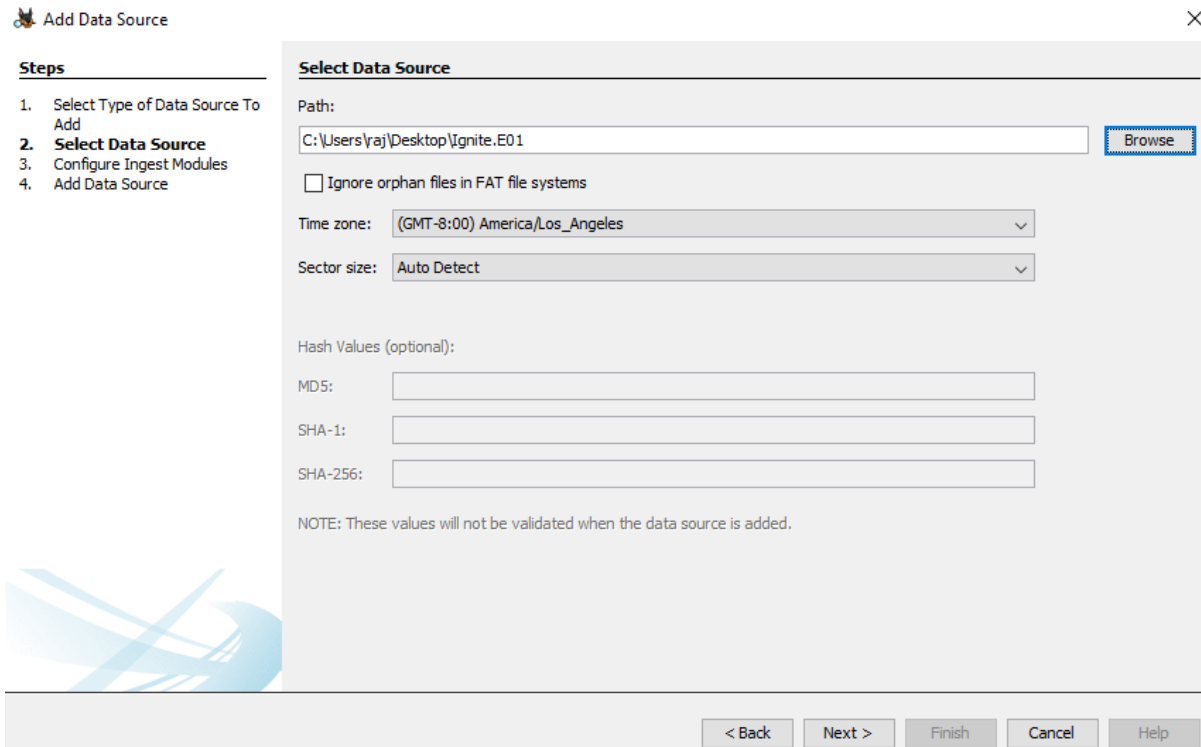**Logical Files**: It includes the image of any local folders or files.

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,
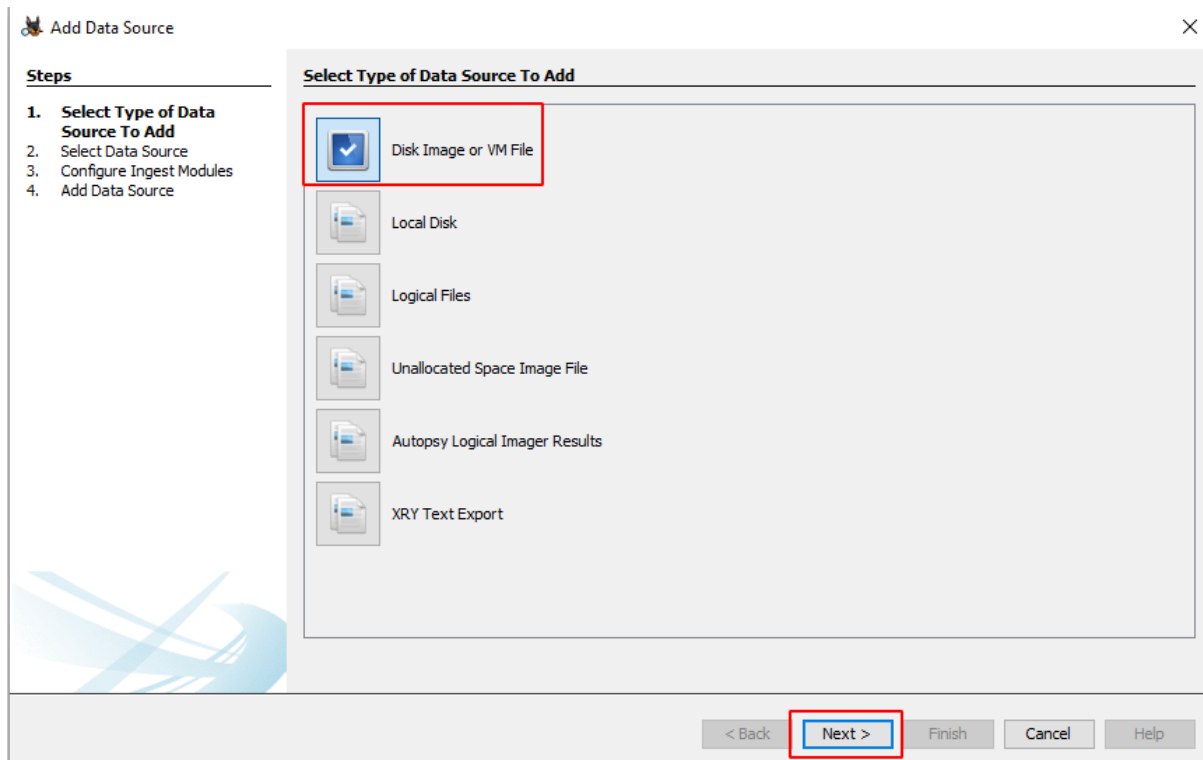
Now let us add the data source. Here we have a previously created image file, so we will add the location of that file.
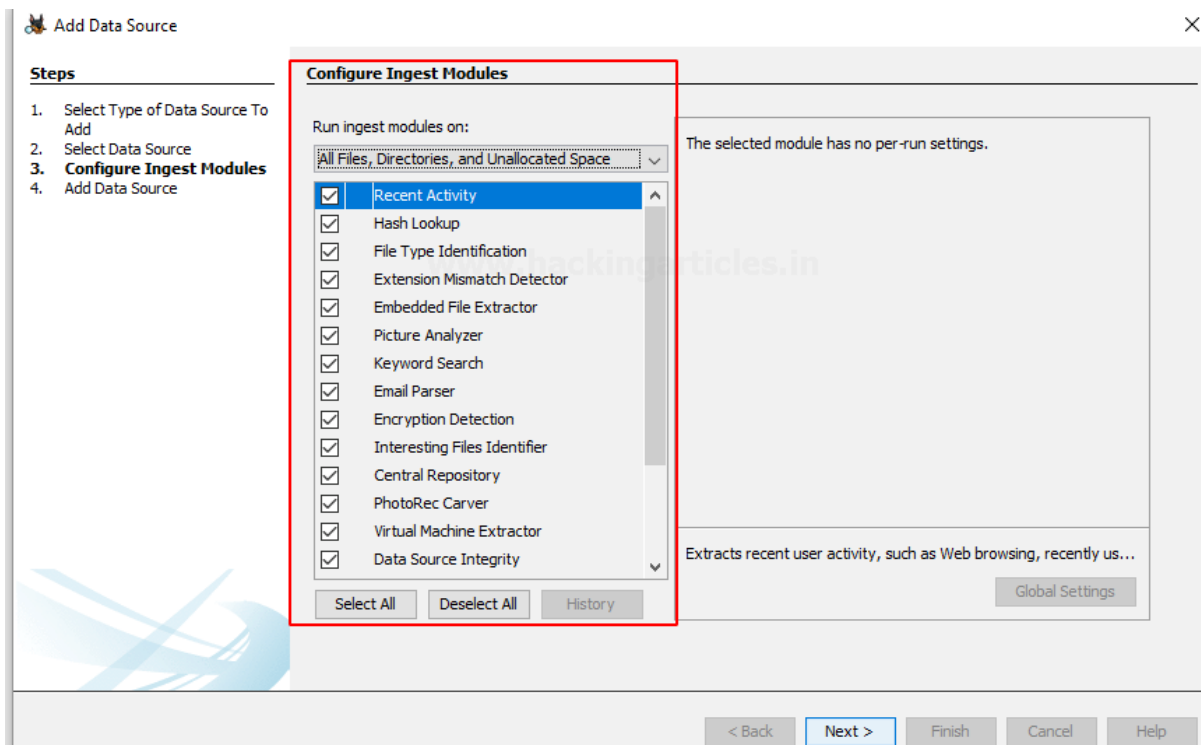
Next, you will be prompted to **Configure the Ingest Module.**

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.
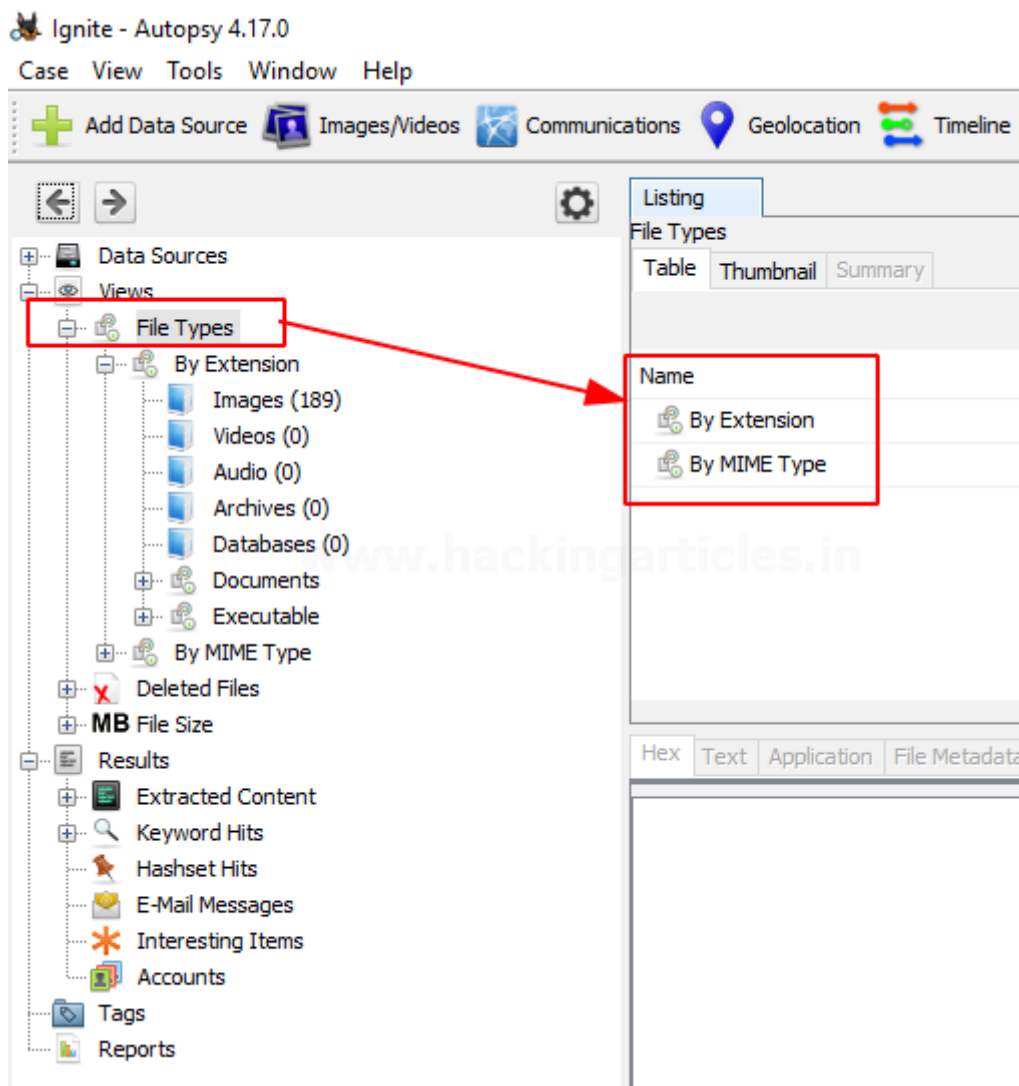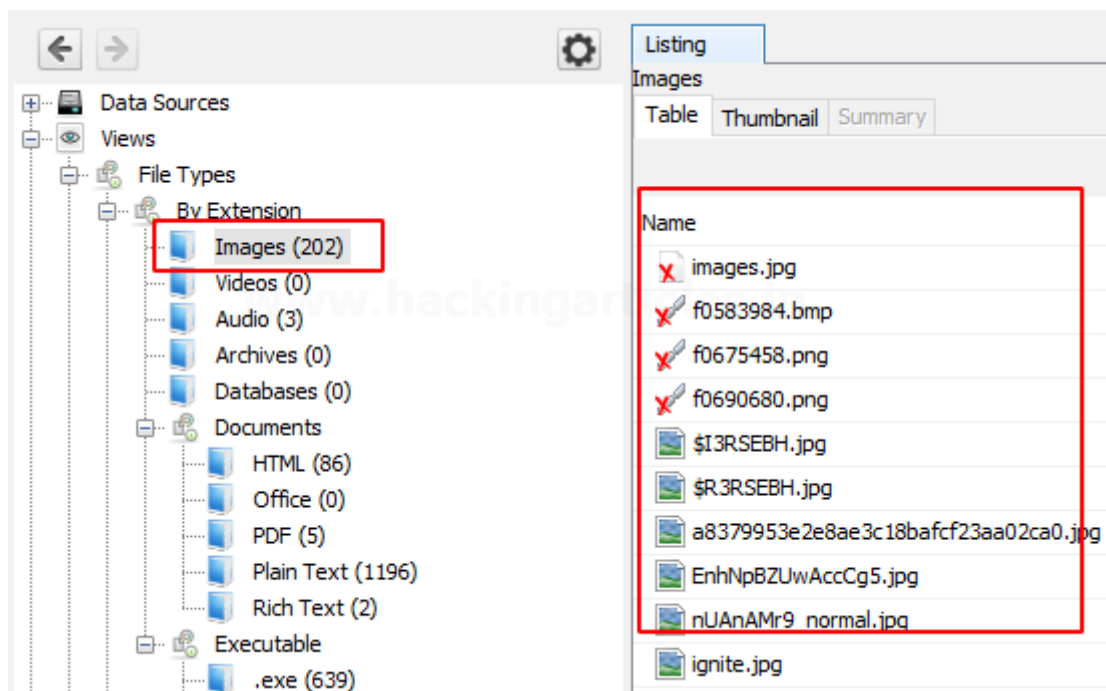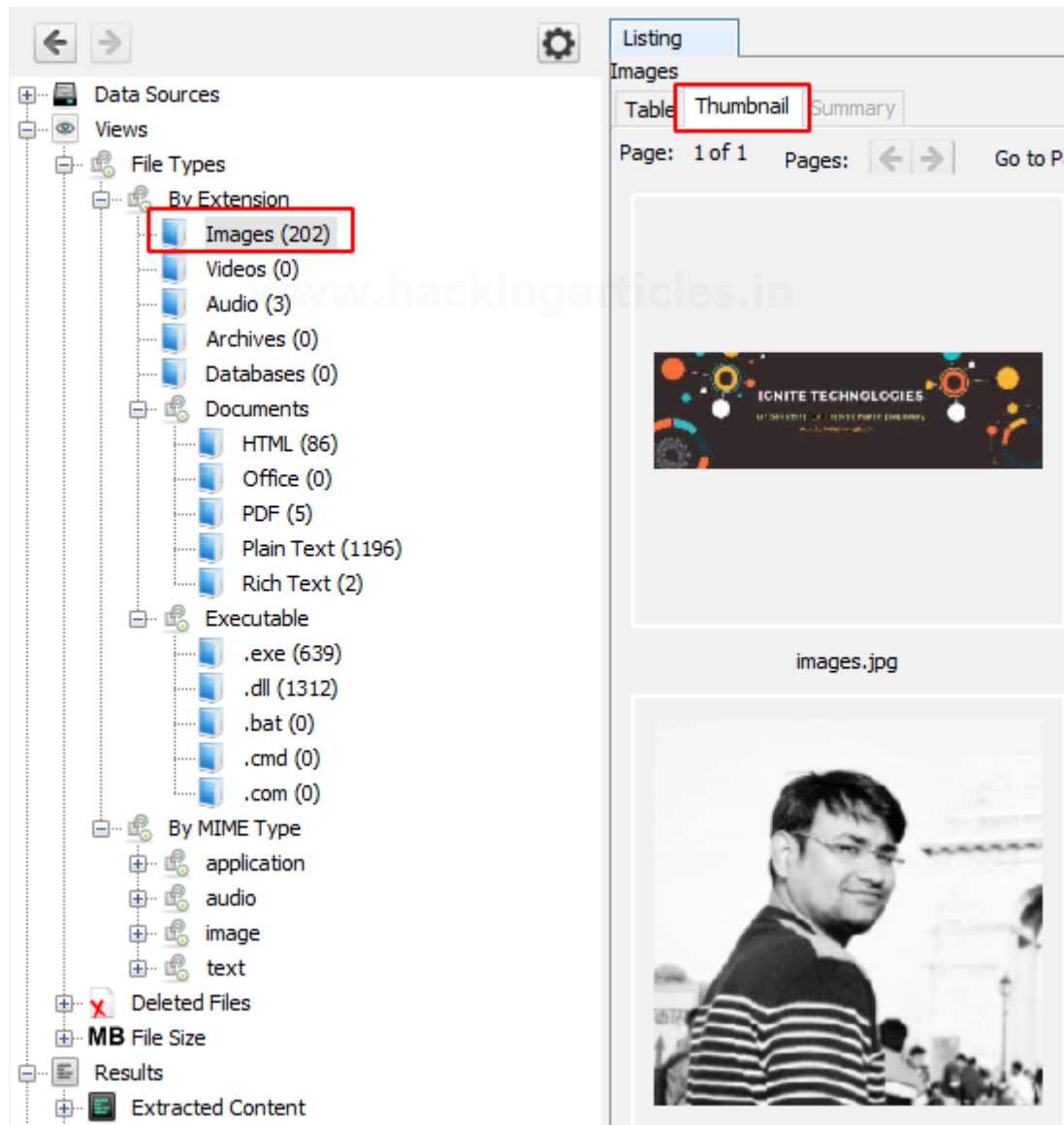
By Extension

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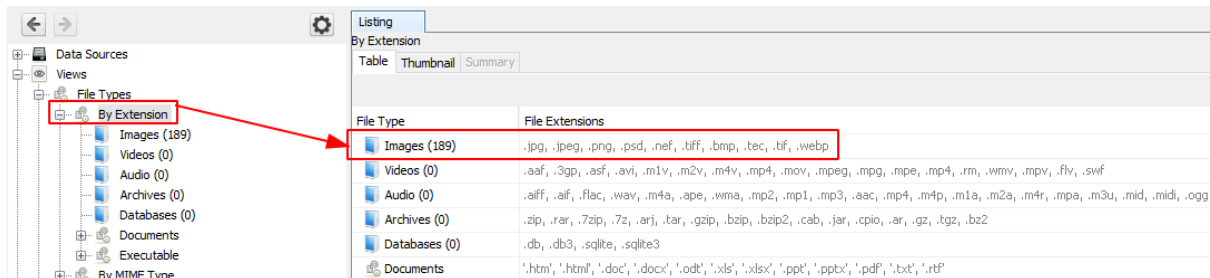
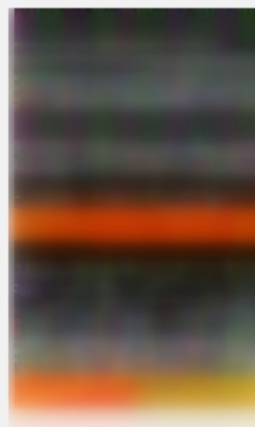Let us click on images and explore the images that have been recovered.

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.
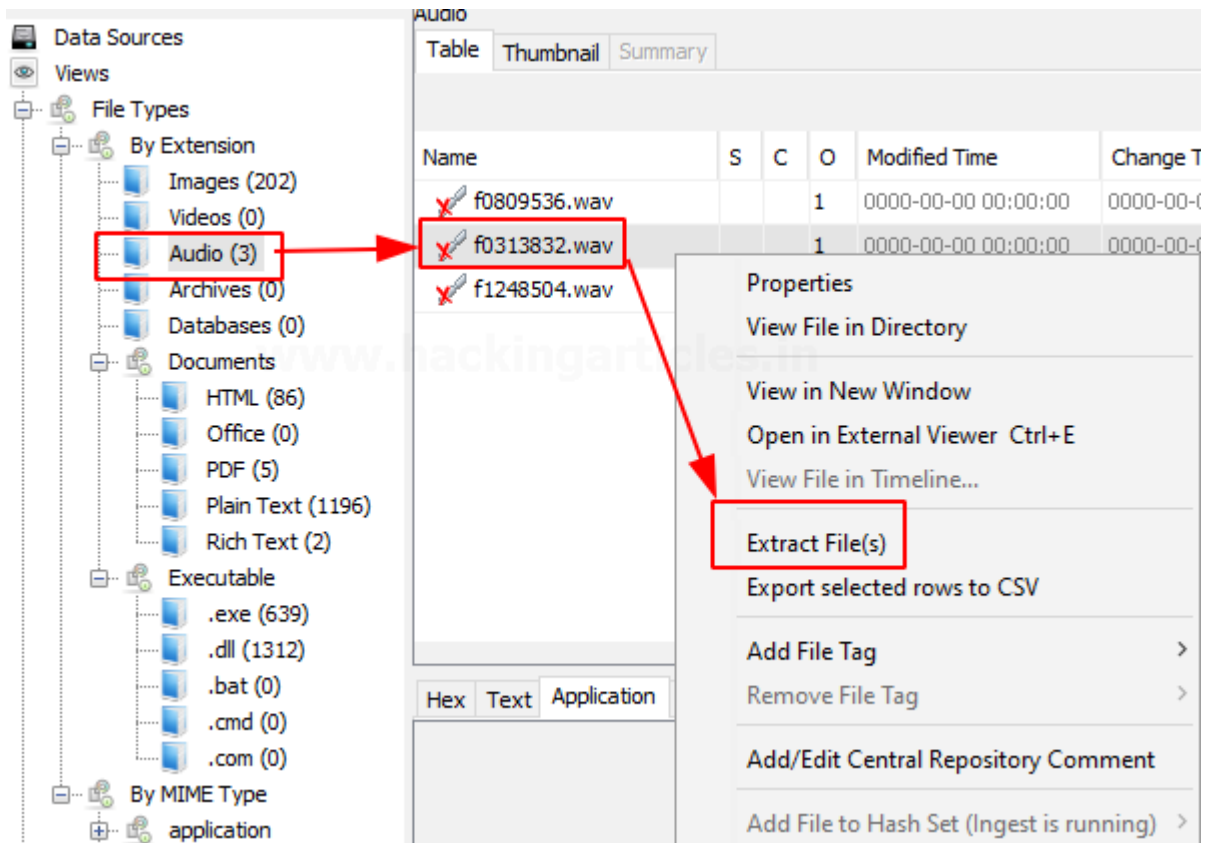
Documents

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.
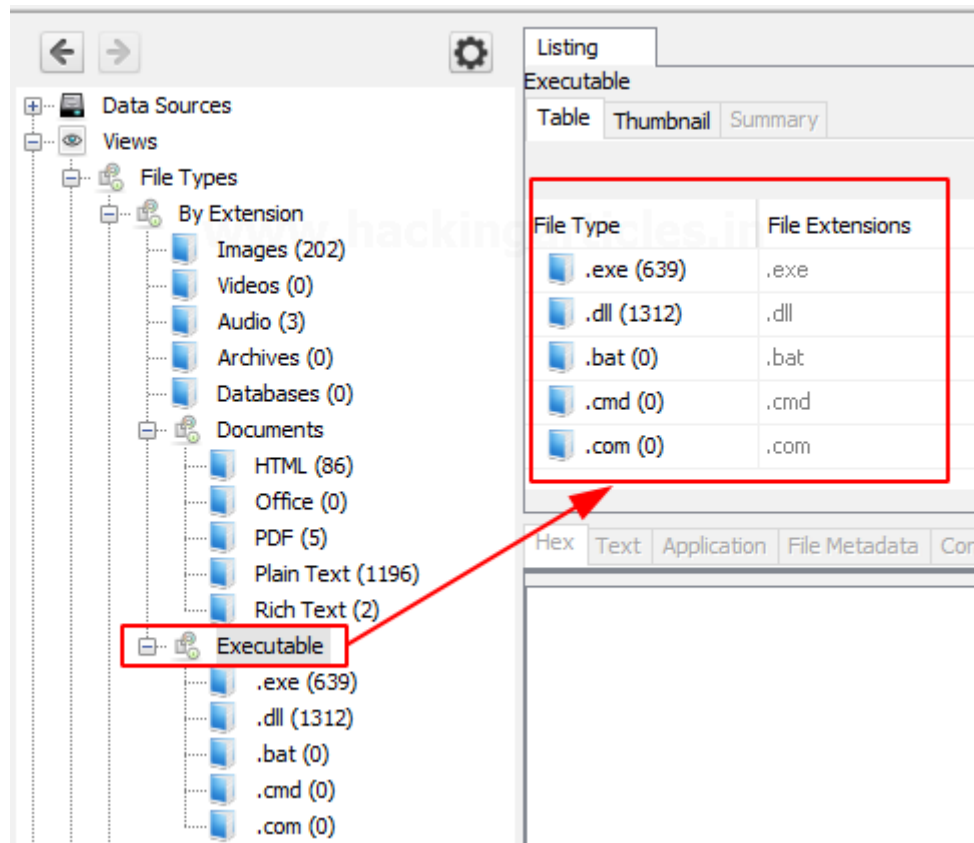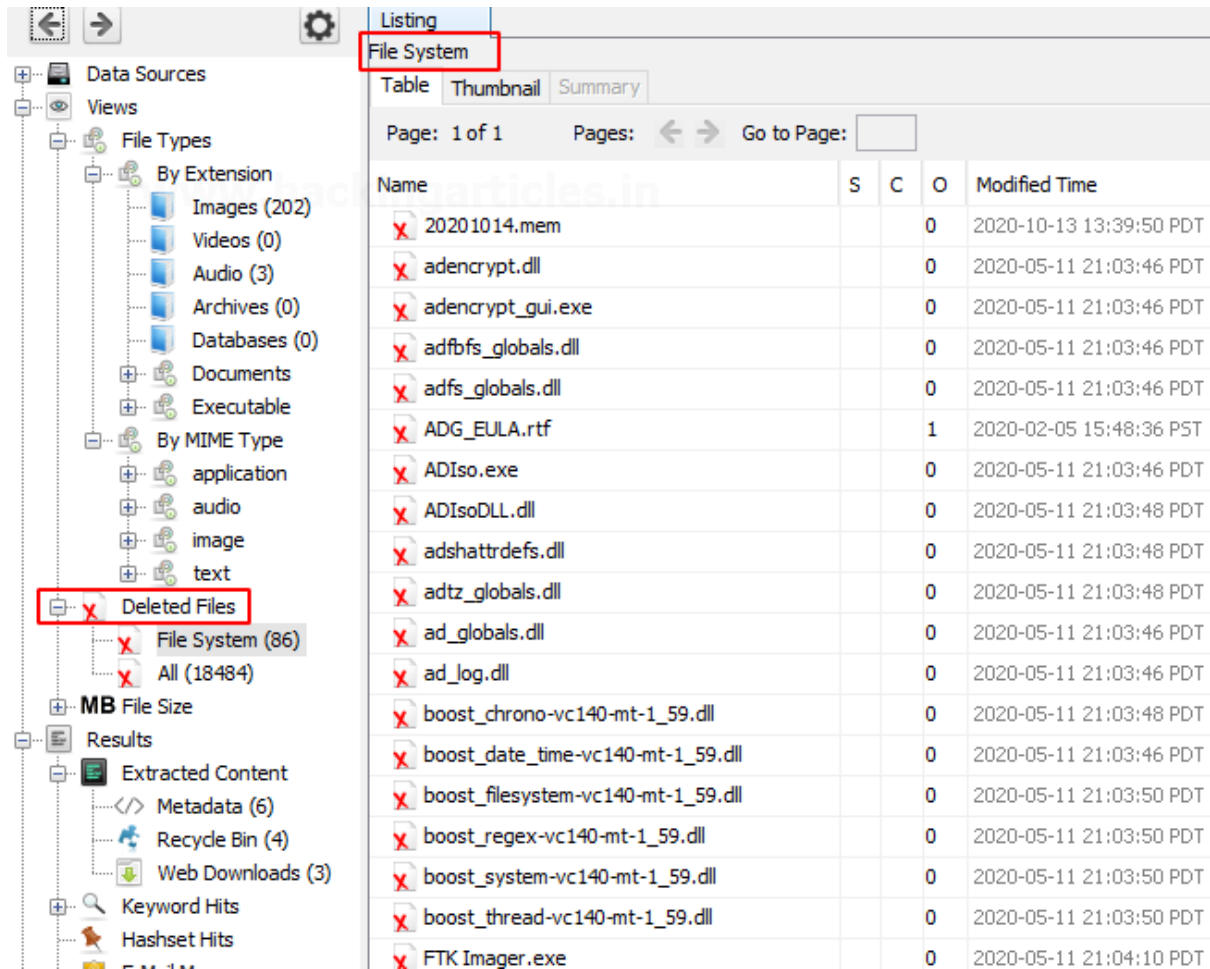
By MIME Type

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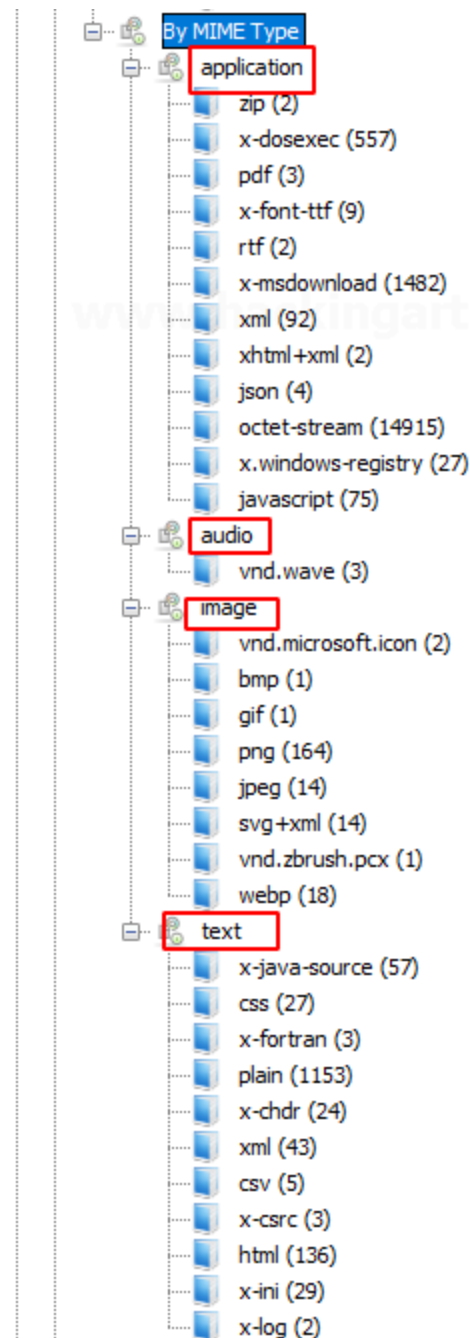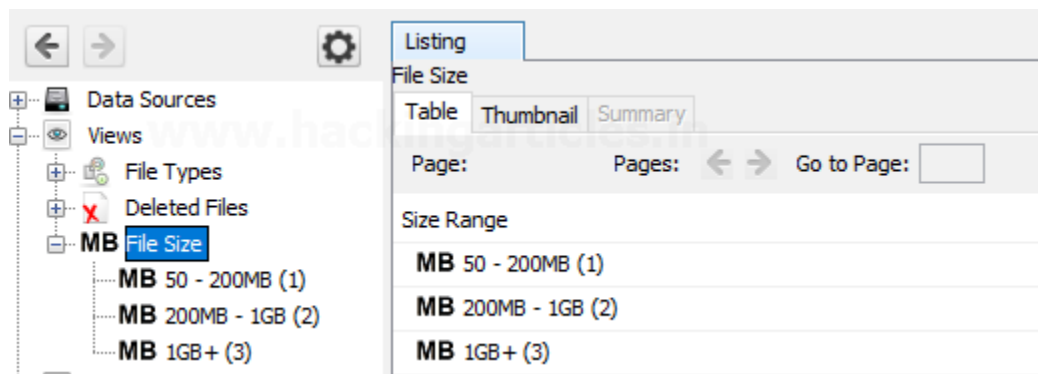
Deleted Files: It displays information about the deleted file which can be then recovered.

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.
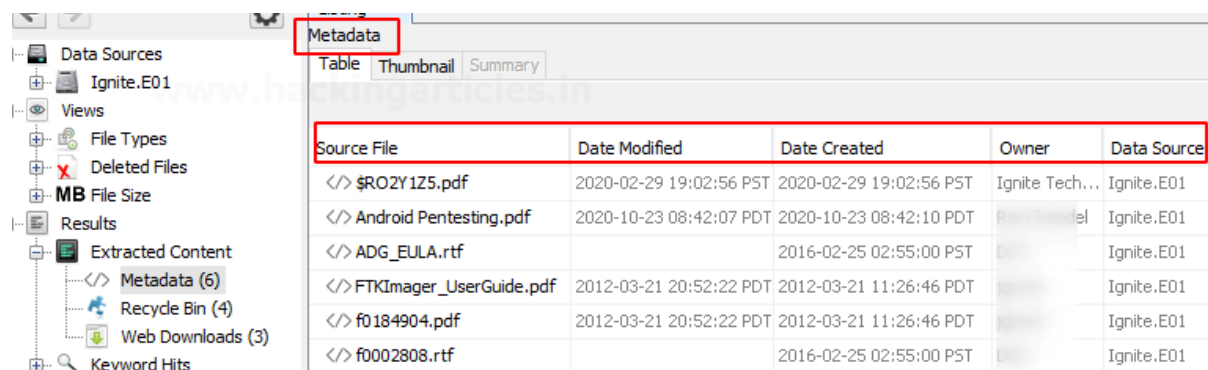
Results

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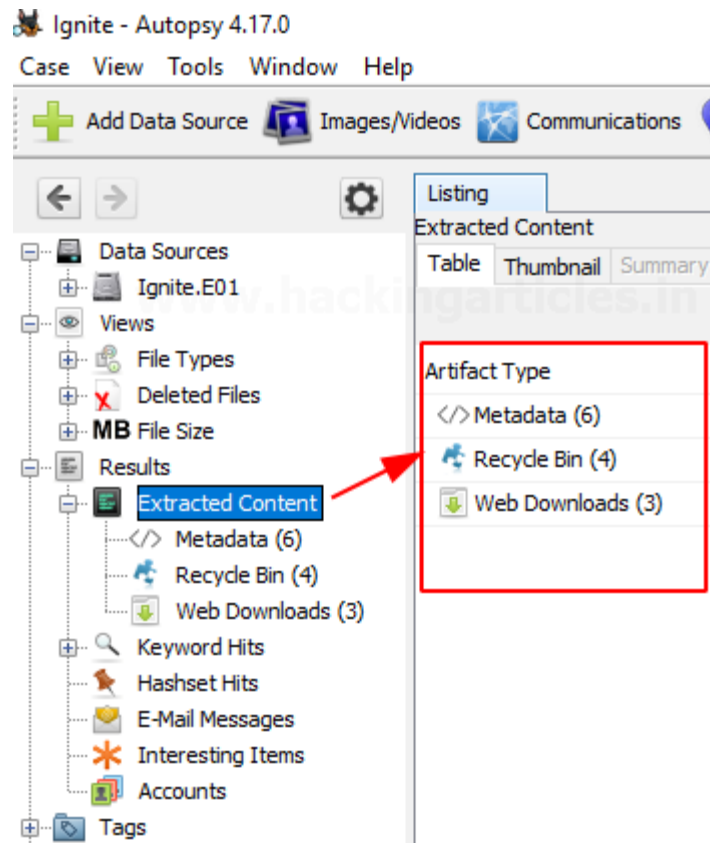
Metadata: Here we can view all the information about the files like the date it was created, to was modified, file's owner, etc.

Recycle Bin: The files that were put in the recycle bin are found in this category.
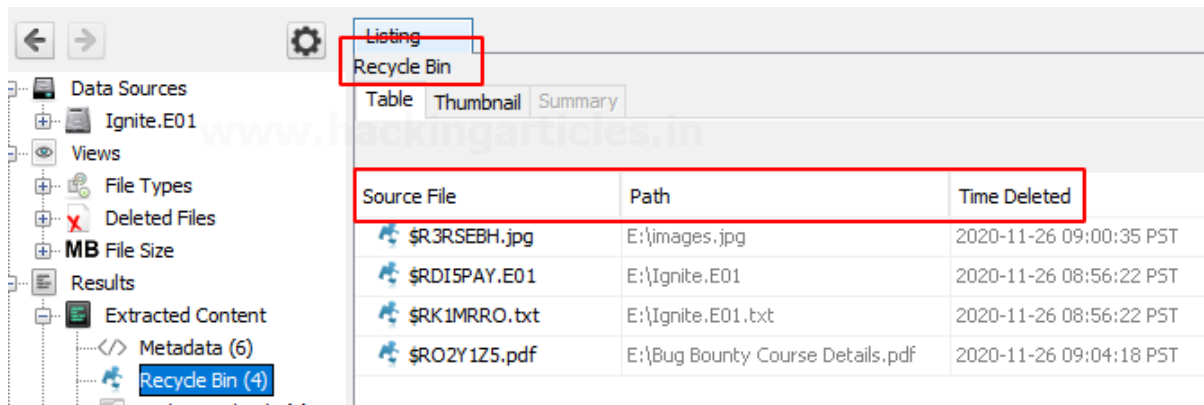
Web Downloads: Here you can see the files that were downloaded from the internet.
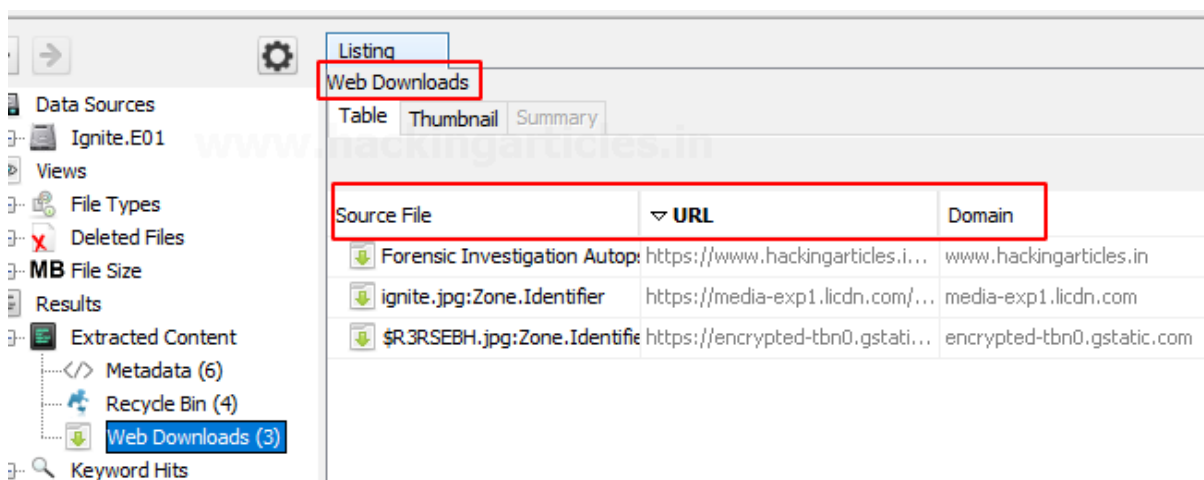
Keyword Hits: In this, any specific keywords can be looked up for in the disk image. The search can be conducted concerning the Exact match, Substring matches, Emails, Literal words, Regular expressions, etc.
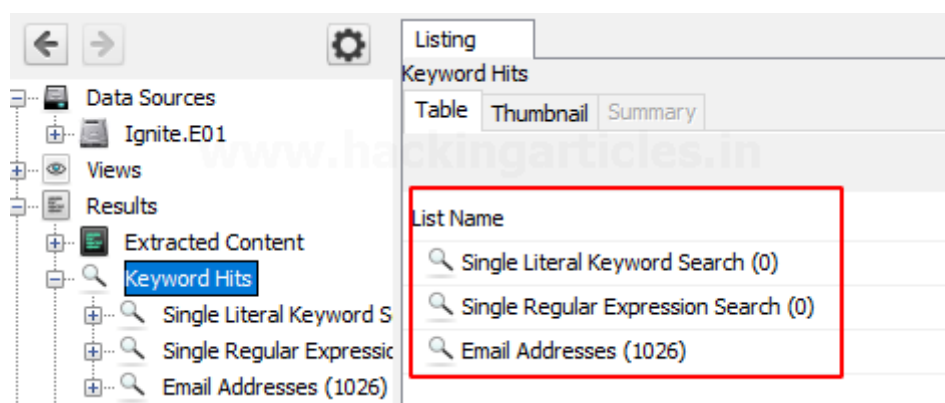
You can view the available email addresses.
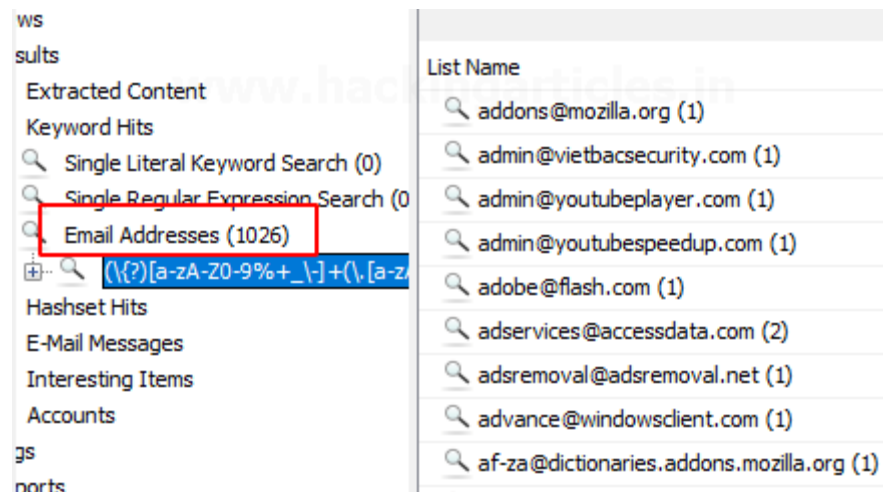
You can choose to export into a CSV format.
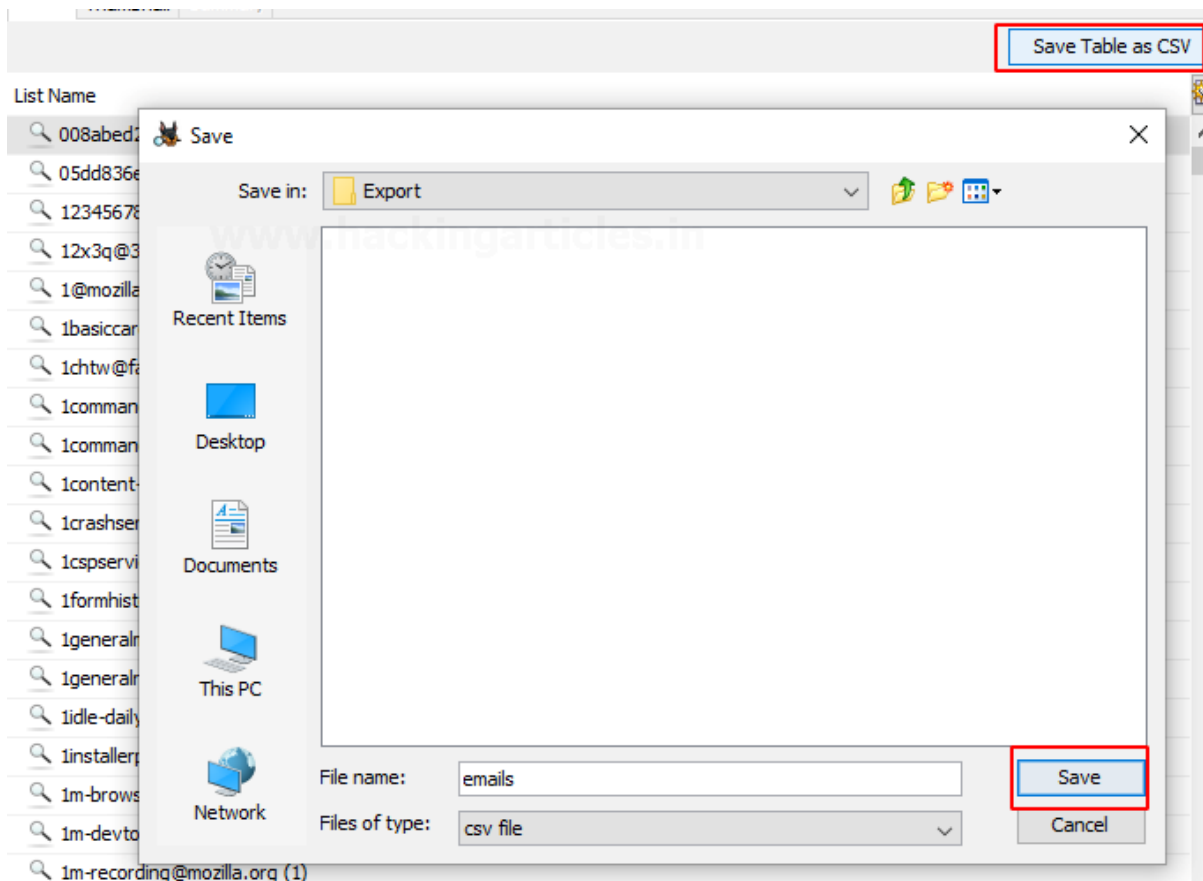
Timeline

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

Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: [Counts] [**Details**] [List] »
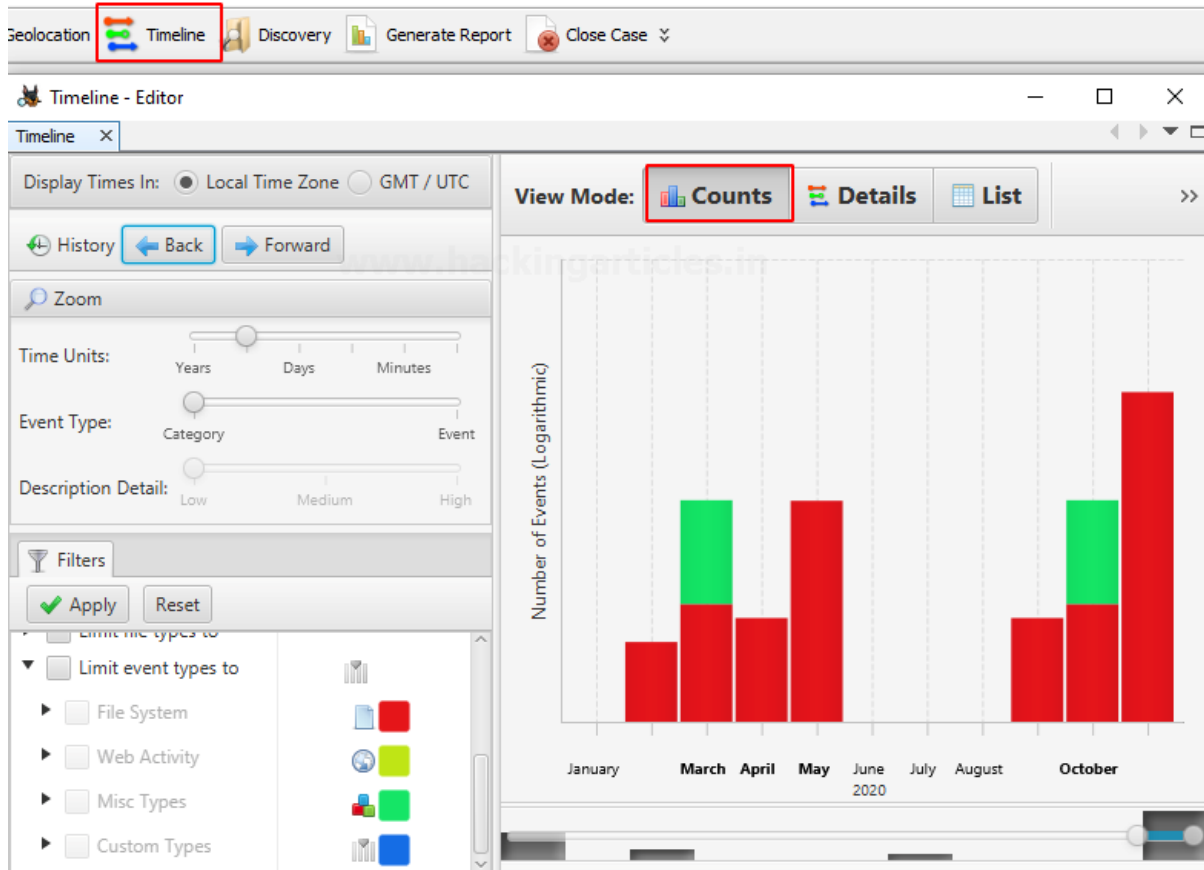
⊕ History | ← Back | → Forward

🔍 Zoom

Time Units: Years — Days — Minutes

Event Type: Category — Event

Description Detail: Low — Medium — High

▼ Filters

✔ Apply | Reset

▼ ☐ Limit event types to

▸ ☐ File System 📄 🟥

▸ ☐ Web Activity 🌐 🟩

▸ ☐ Misc Types 🧩 🟩

▸ ☐ Custom Types 📊 🟦

👁 Hidden Descriptions

.../S-1-5-21-1276730070-1850728493-30201559-1001/$RO2Y

.../S-1-5-21-1276730070-1850728493-30201559-1001/$I

46

🔒 Document Last Saved (2)
M ...: : M ...: :

🔒 Document Created (2)
B ...: : B ...: :

📄 /Bug Bounty Course Details.pdf (4)
... 3

/USB.txt (4)
2

2

/20201014.mem (4)

January April June August November
2020

Start: Jan 27, 2020 11:33:00 PM 🕐 🔍➖ 🔍➕ »

🦊 Timeline - Editor — ☐

Timeline ✕

Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: [Counts] [Details] [**List**]

⊕ History | ← Back | → Forward

▼ Filters

✔ Apply | Reset

☐ Must include text: [enter filter string]

☐ Must be tagged

☐ Must have hash hit

▸ ☐ Limit data sources to

▸ ☐ Limit file types to

▼ ☐ Limit event types to 📊

▸ ☐ File System 📄 🟥

▸ ☐ Web Activity 🌐 🟩

▸ ☐ Misc Types 🧩 🟩

▸ ☐ Custom Types 📊 🟦

👁 Hidden Descriptions

Date/Time	Event Type	Description	Tag
2020-02-06 05:18:36	📄 M___	/$Orpha ... LA.rtf	
2020-03-01 00:32:57	📄 M___	/$RECY ... Z5.pdf	
2020-03-01 08:32:56	M Document L...	Documen ... d : :	
2020-03-01 08:32:56	B Document ...	Documen ... d : :	
2020-03-10 09:42:02	📄 M___	/$Orpha ... gpl.txt	
2020-03-10 09:48:50	📄 M___	/$Orpha ... gpl.txt	
2020-04-10 21:12:08	📄 __B_	/$RECY ... Z5.pdf	
2020-04-10 21:12:08	📄 __B_	/Bug Bo ... ils.pdf	
2020-05-12 01:06:40	📄 M___	/$Orpha ... ter.dll	
2020-05-12 09:33:46	📄 M___	/$Orpha ... ui.exe	
2020-05-12 09:33:46	📄 M___	/$Orpha ... _59.dll	
2020-05-12 09:33:46	📄 M___	/$Orpha ... als.dll	
2020-05-12 09:33:46	📄 M___	/$Orpha ... log.dll	

Start: Jan 27, 2020 11:33:00 PM 🕐

Discovery

This option allows finding media using different filters that are present on the disk image.
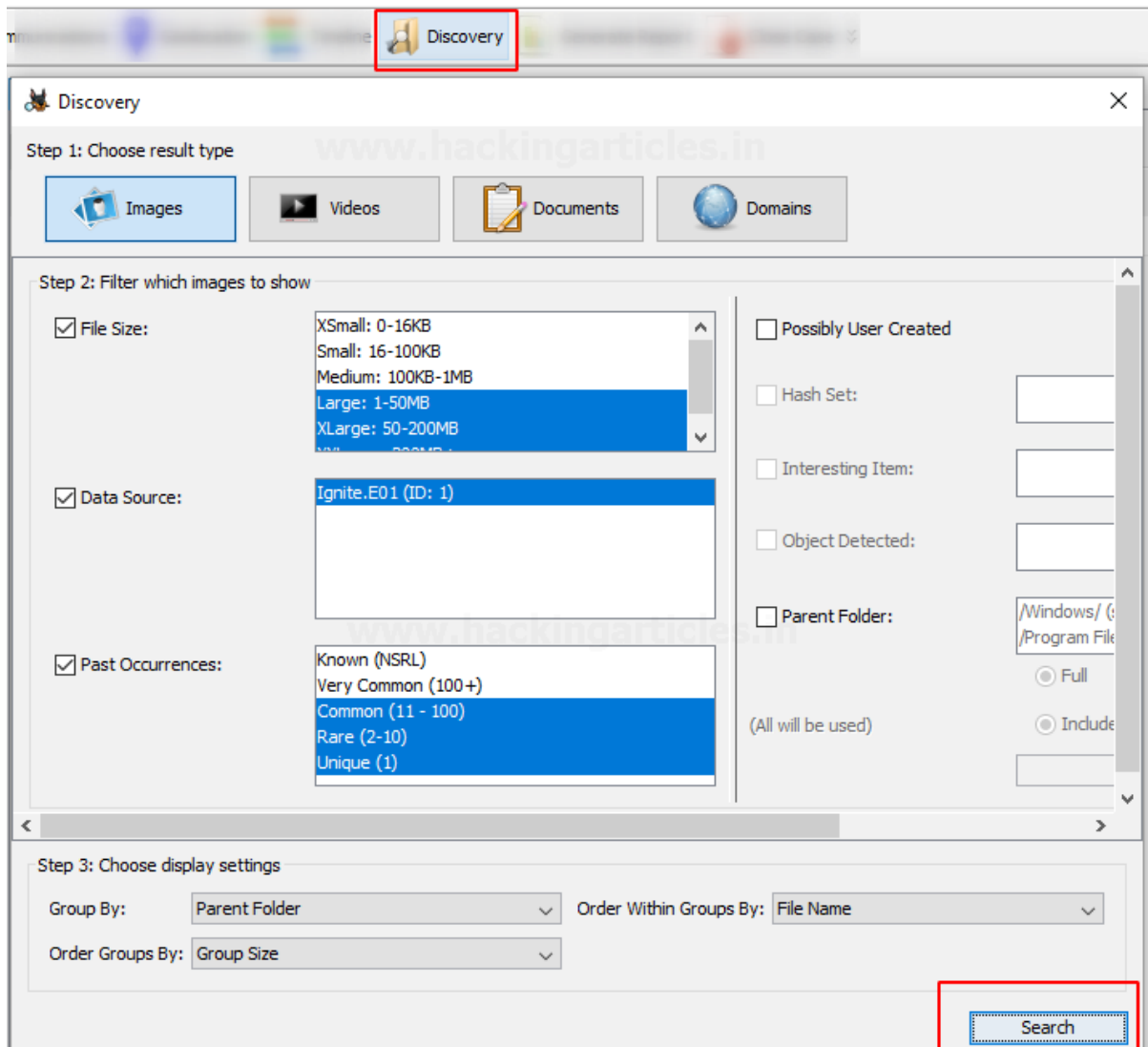
According to the selected options, you can get the desired results.
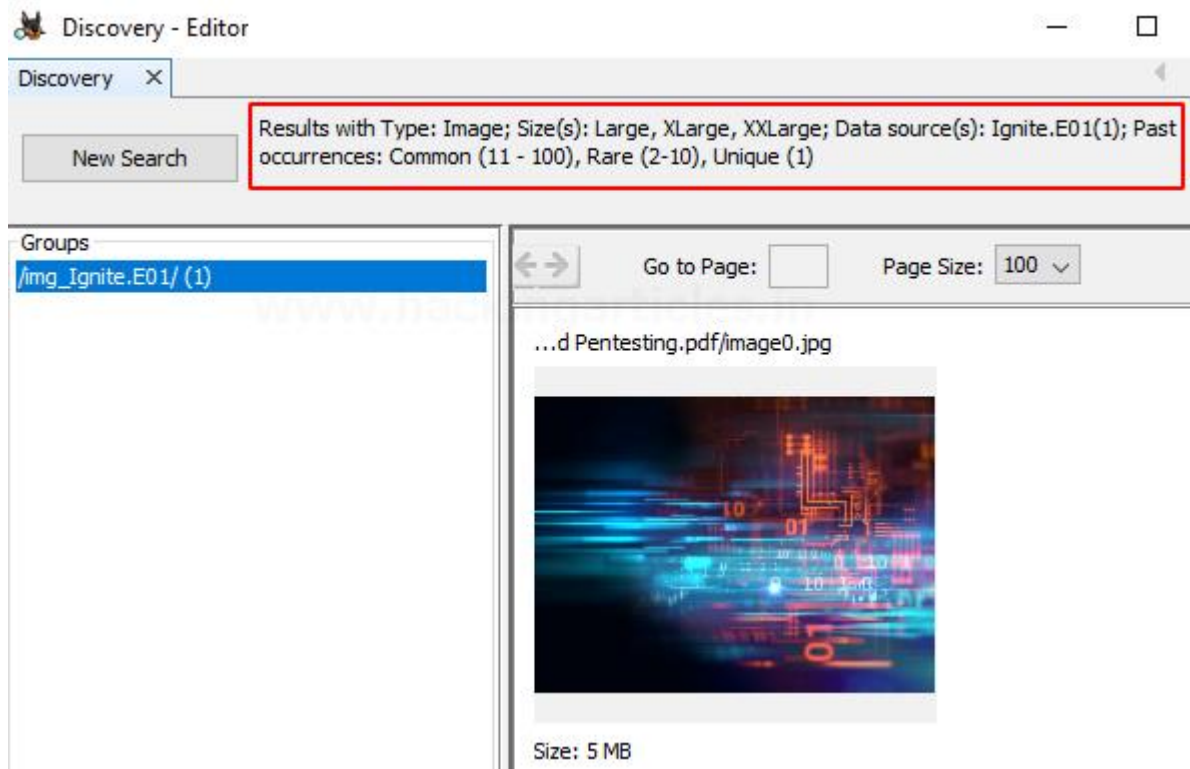
Images/Videos

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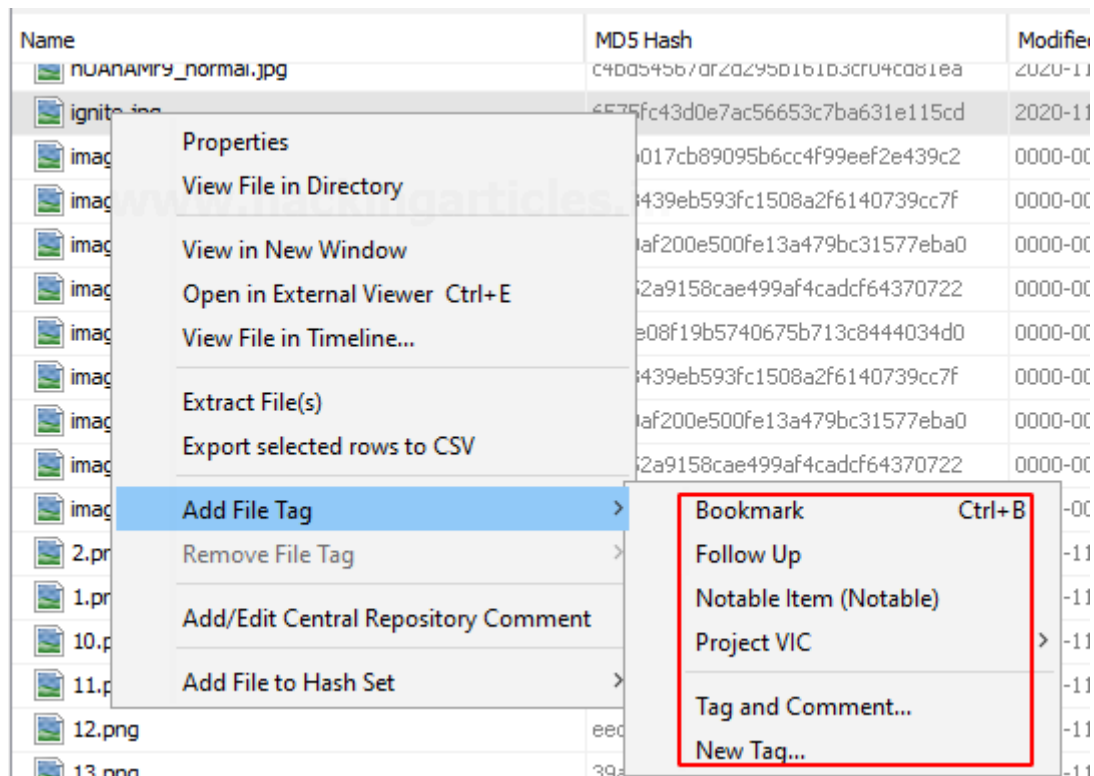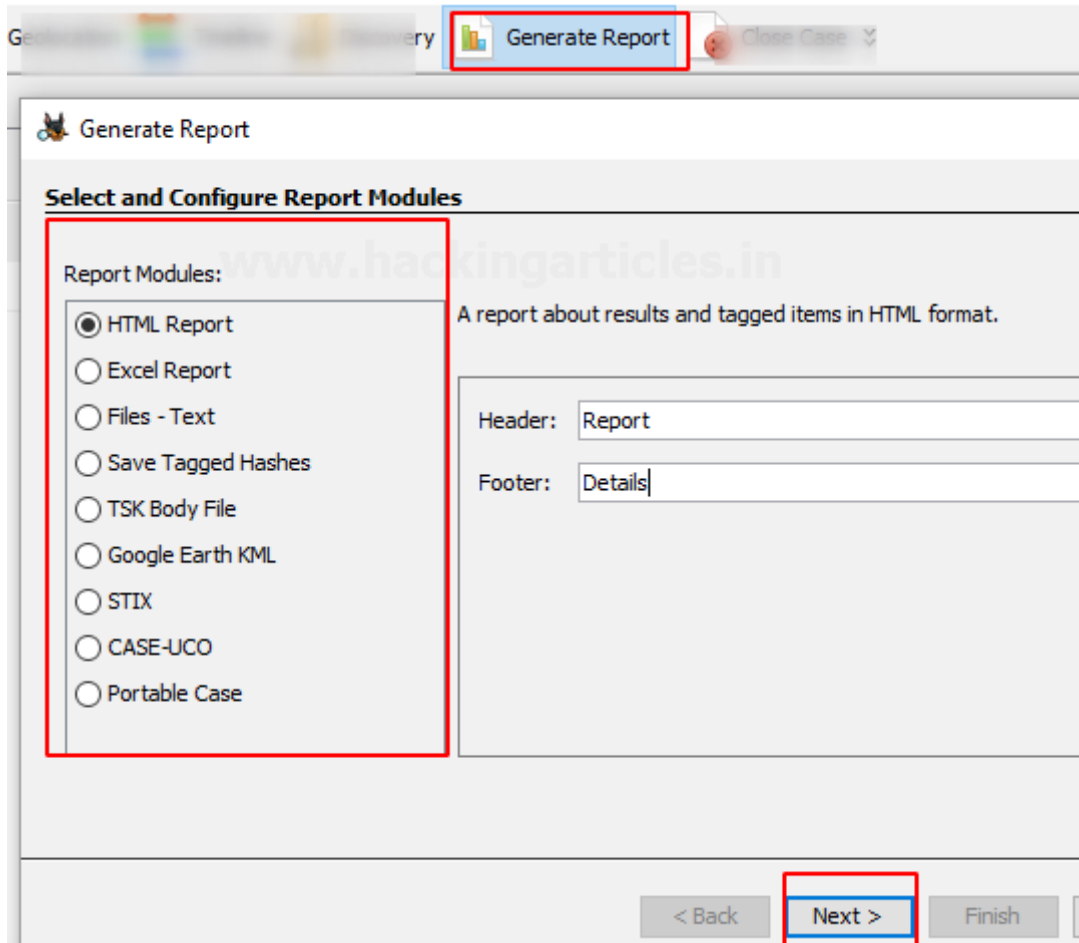
Now when you see the tags options, you will see that files were tagged according to various categories.
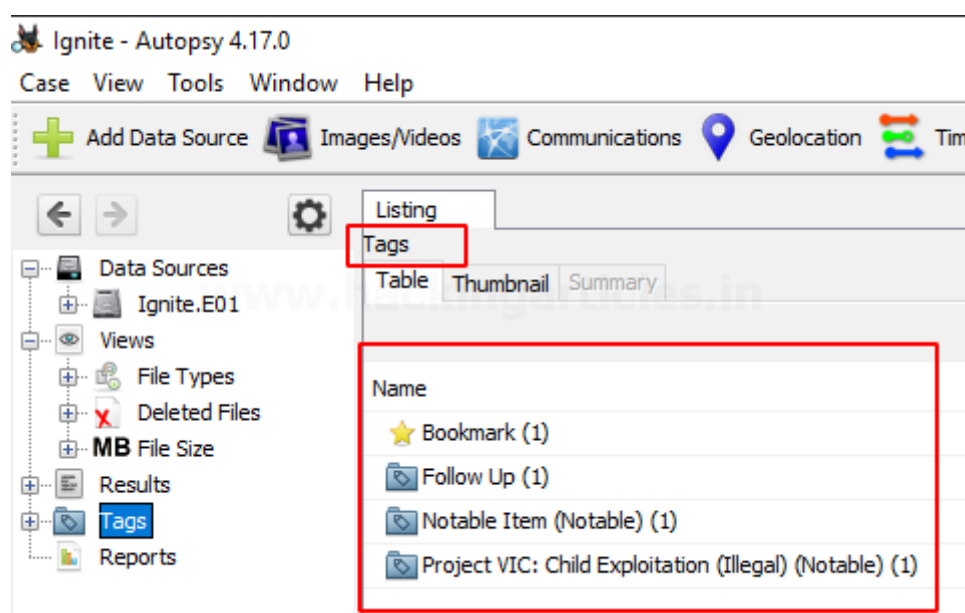
Generate Report

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.
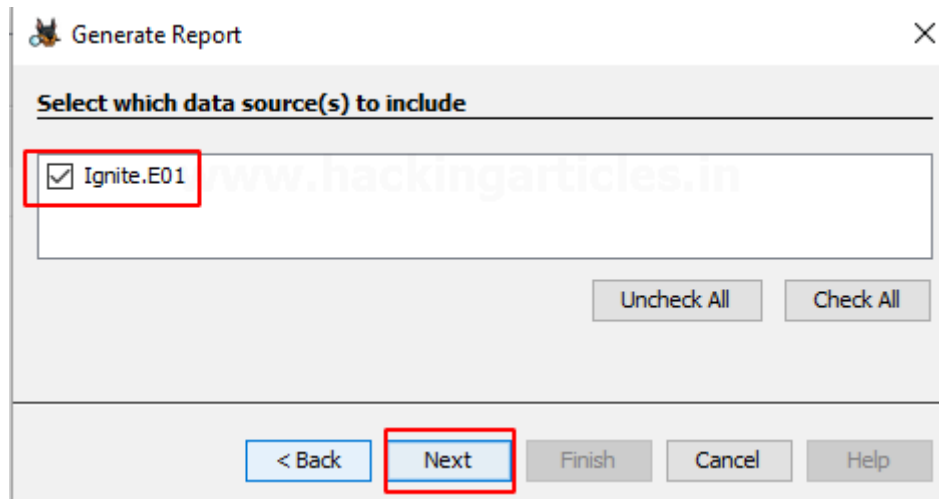
Here we chose to create the report in HTML format.
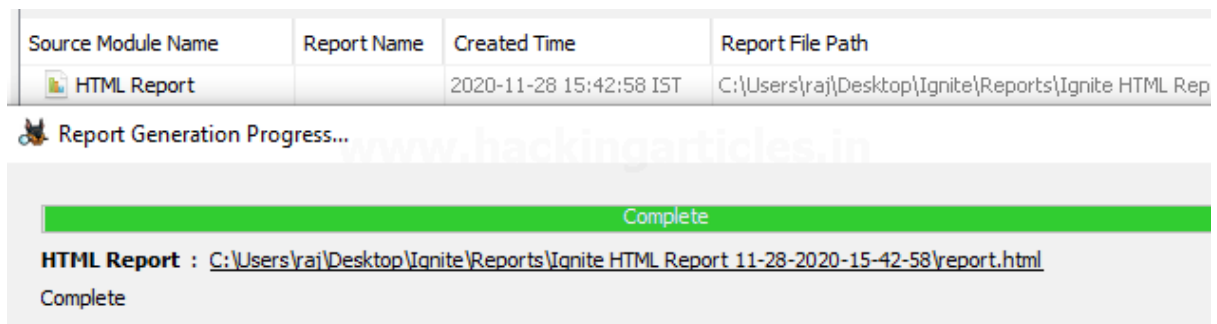
Kudos! Your Autopsy Forensic Report is ready!

Linux Forensic Investigation

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.
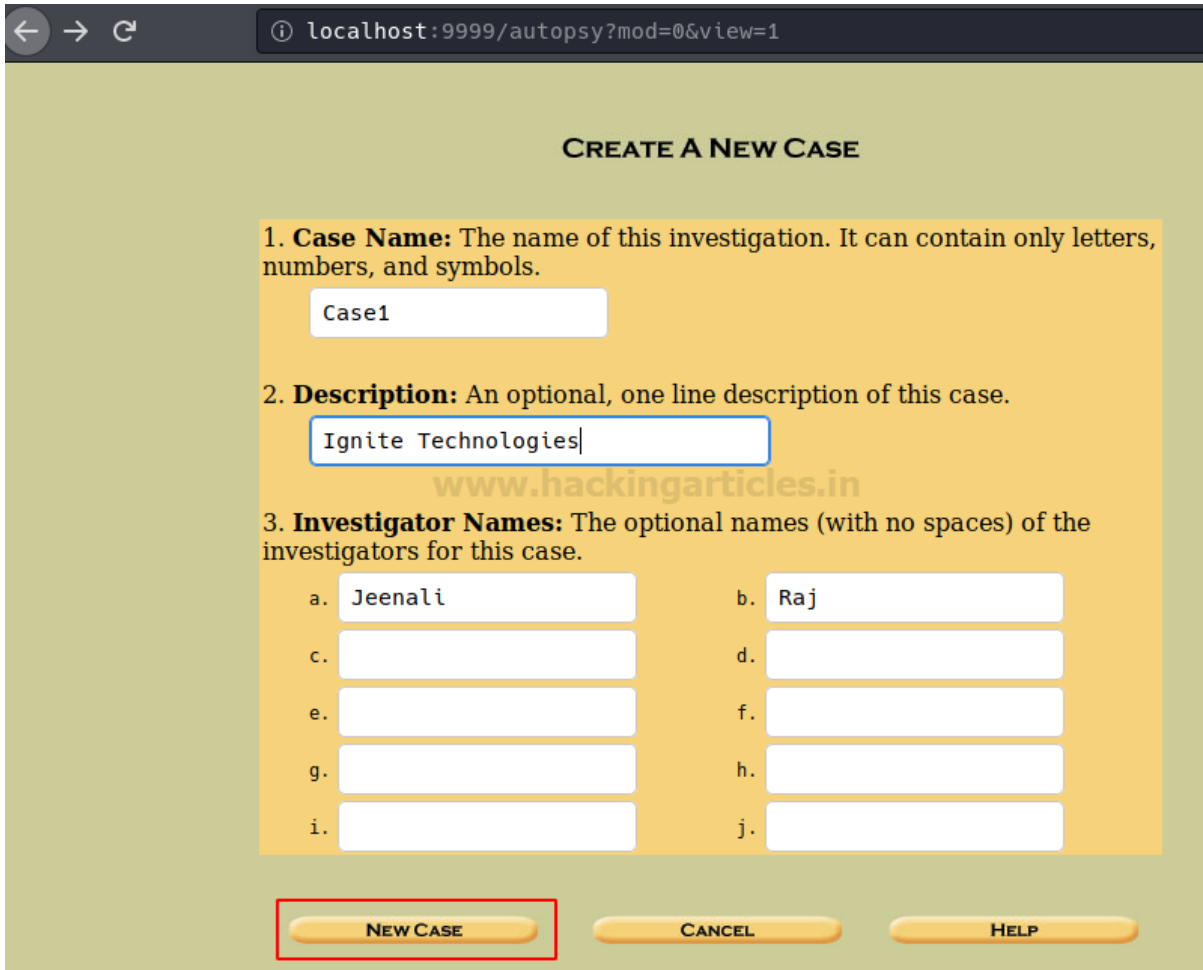
Now you will see three options on the home page.

- Open Case
- New Case
- Help

For the 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.
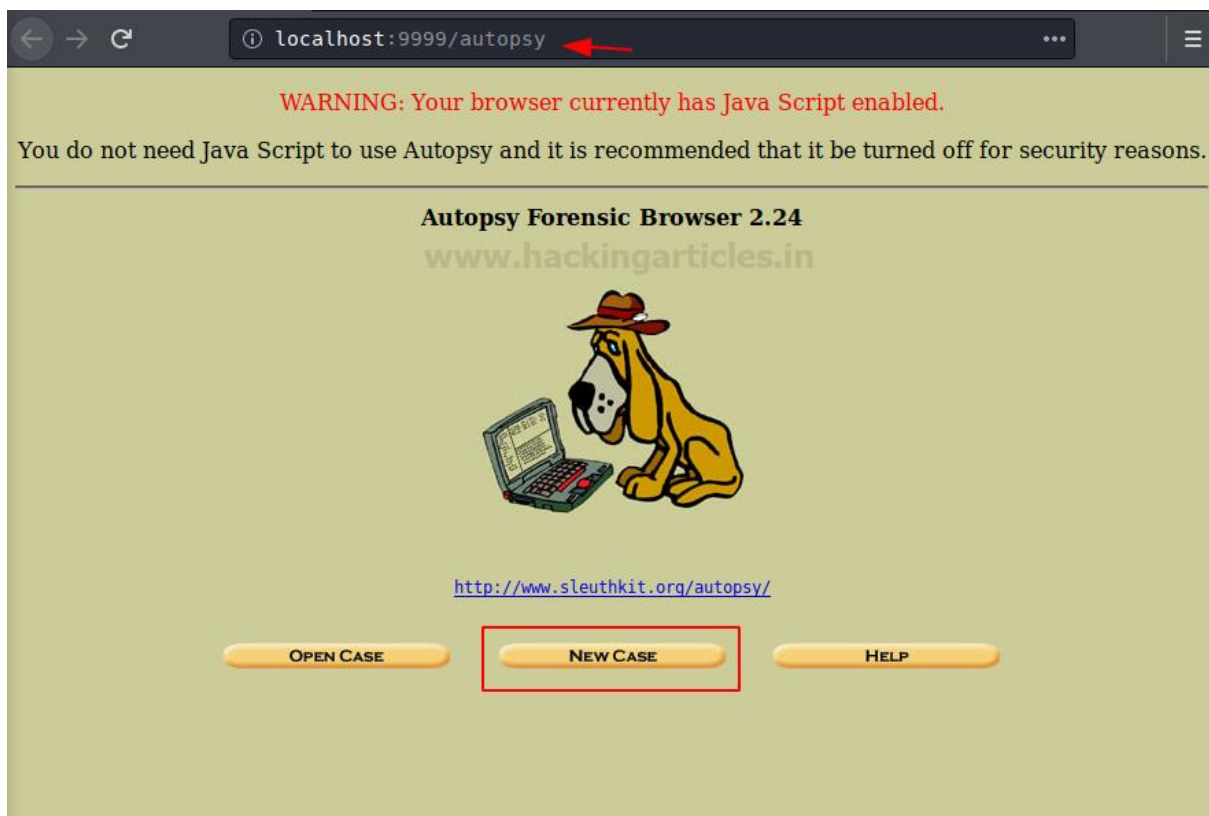
Now you will be directed to a new page, where it will require case details. You can Name the case and mention the description. You can also mention the names of multiple investigators working the case. After filling in these details, now you can select 'New case'
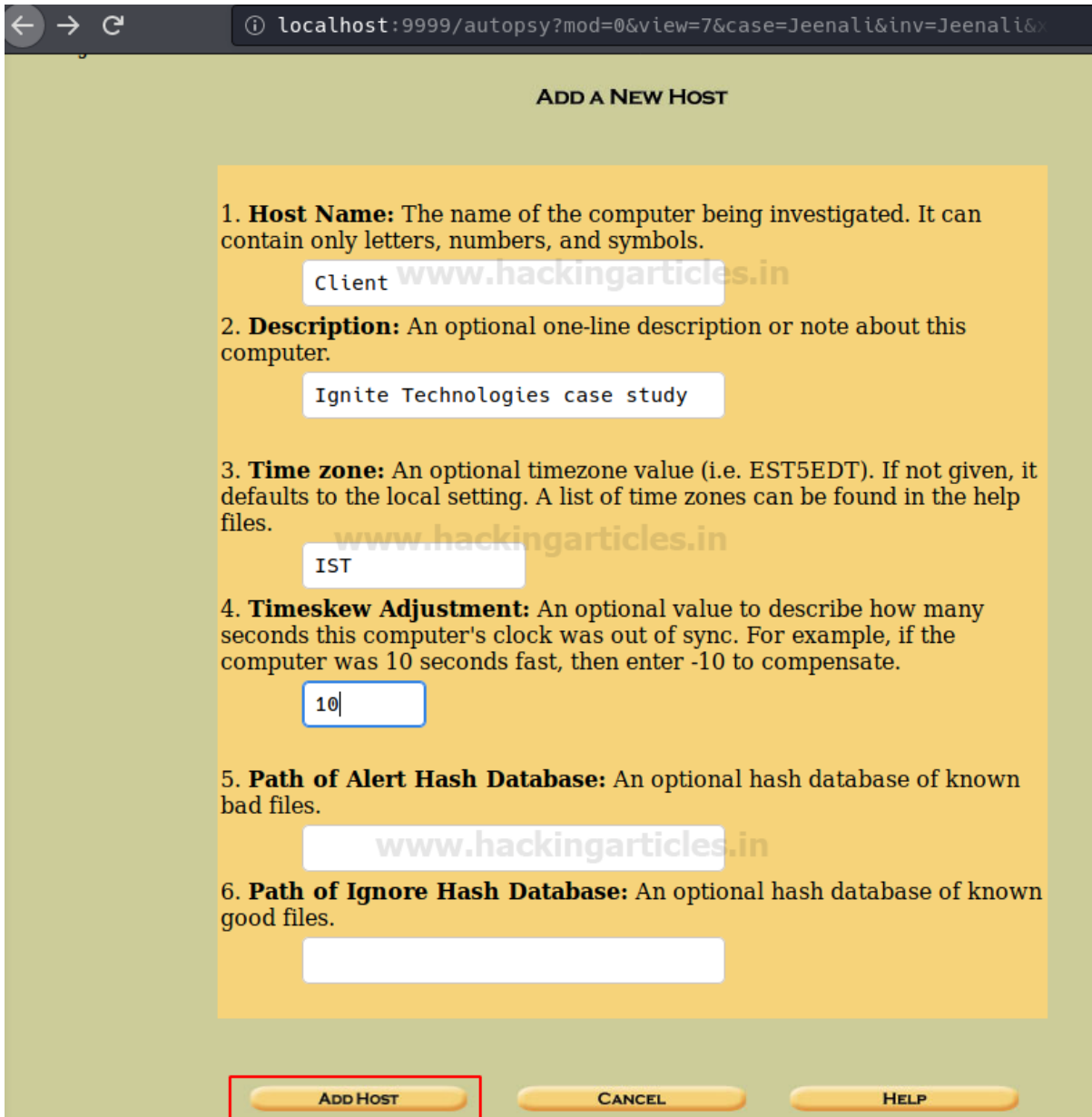
The new case will be stored in i.e. /var/lib/autopsy/case1/, and the configuration file will be stored in/var/lib/autopsy/case01/case.aut. Now , create the host for investigation and click on 'Add Host'.

Once you add 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'.

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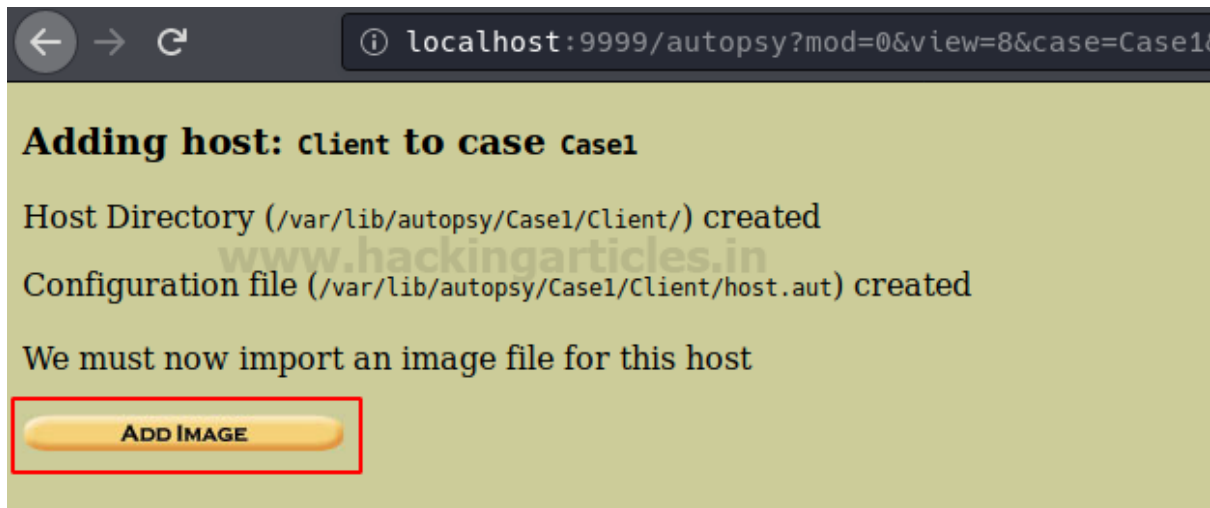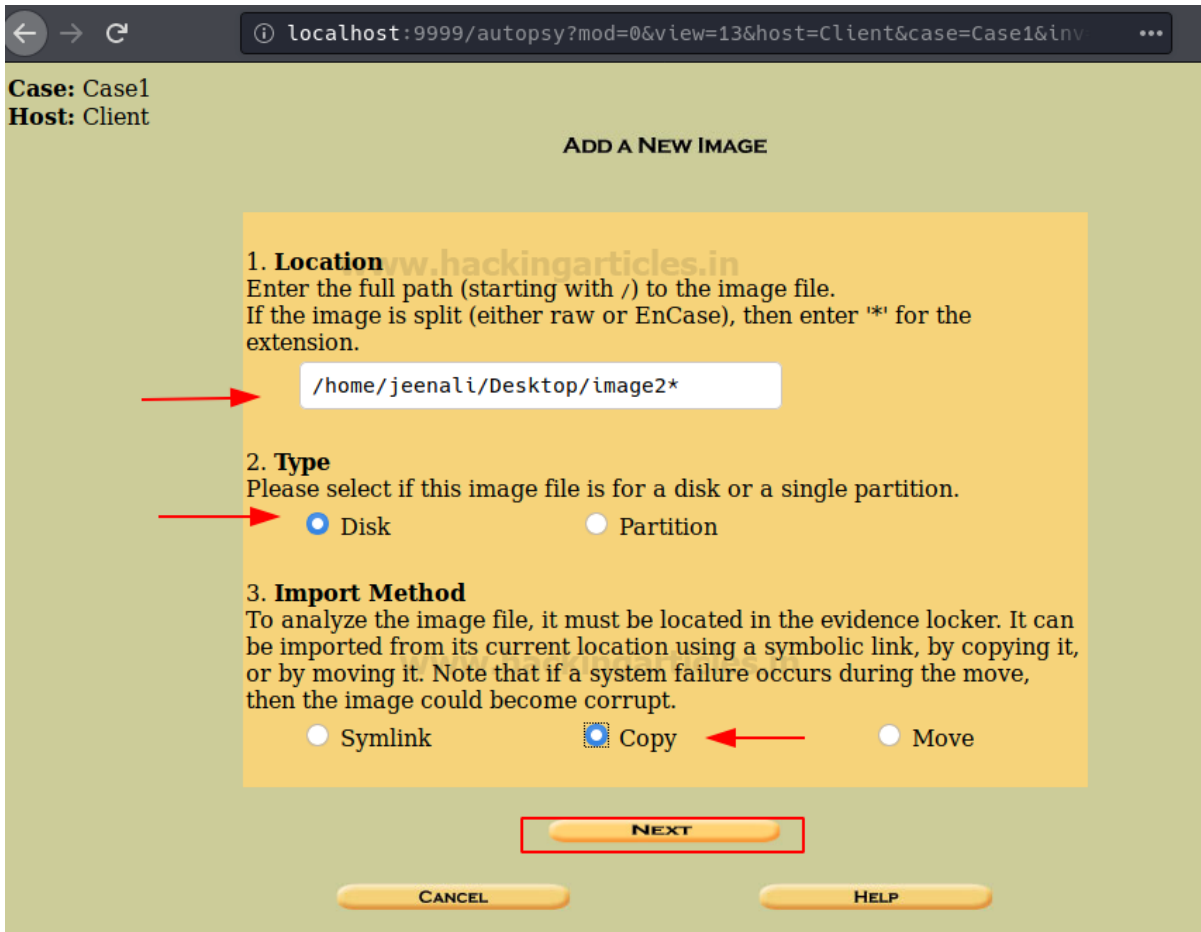
Adding Image File

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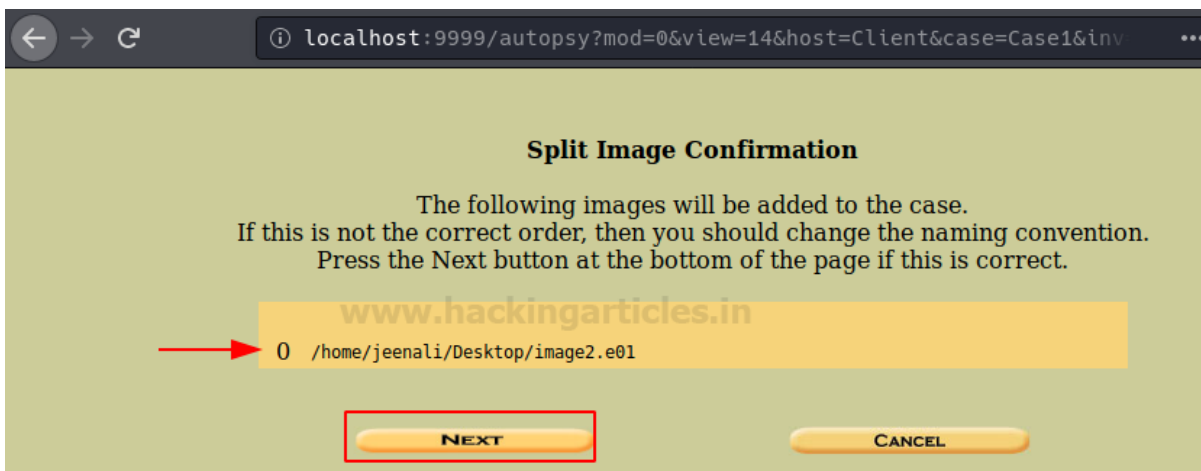
You can now confirm the Image file being added to the evidence locker and click on 'Next'.

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.

Image File Details

Local Name: "/home/jeenali/Desktop/image2.e01"

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: Basic data partition)
  Add to case? ☑
  Sector Range: 2048 to 1085439
  Mount Point: `C:`   File System Type: `ntfs ⌄`

Partition 2 (Type: EFI system partition)
  Add to case? ☑
  Sector Range: 1085440 to 1288191
  Mount Point: `D:`   File System Type: `fat32 ⌄`

Partition 3 (Type: Microsoft reserved partition)
  Add to case? ☑
  Sector Range: 1288192 to 1320959
  Mount Point: `/3/`   File System Type: `raw ⌄`

Partition 4 (Type: Basic data partition)
  Add to case? ☑
  Sector Range: 1320960 to 83884031
  Mount Point: `E:`   File System Type: `ntfs ⌄`

ADD   CANCEL   HELP

Now the Autopsy will test the partitions and links them to the evidence locker, then click on 'Ok' to proceed.
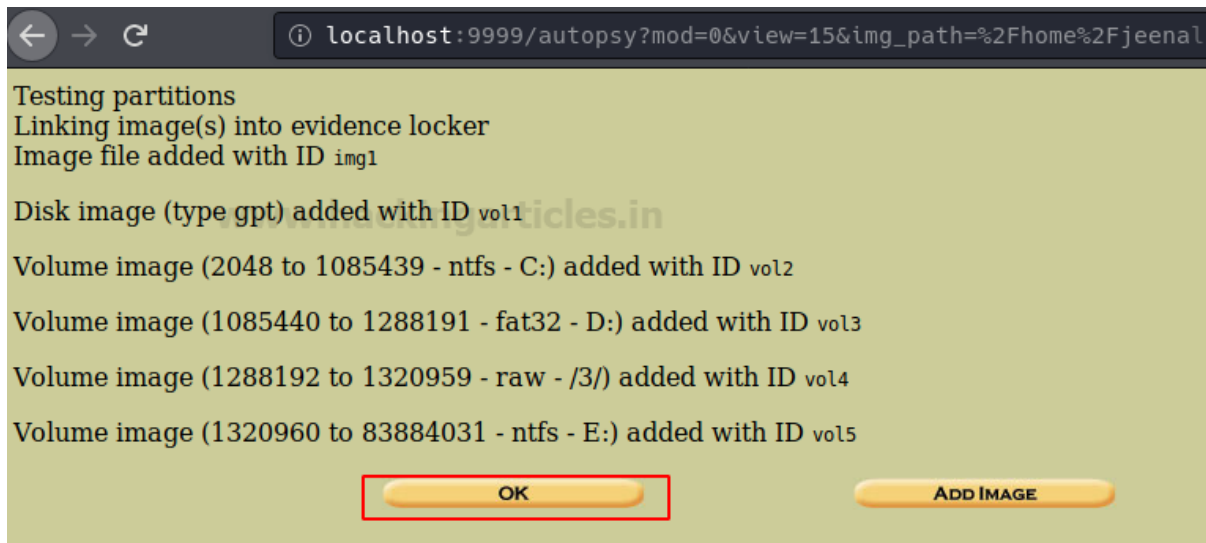
Now select the volume to be analyzed and click on 'Analyze'.
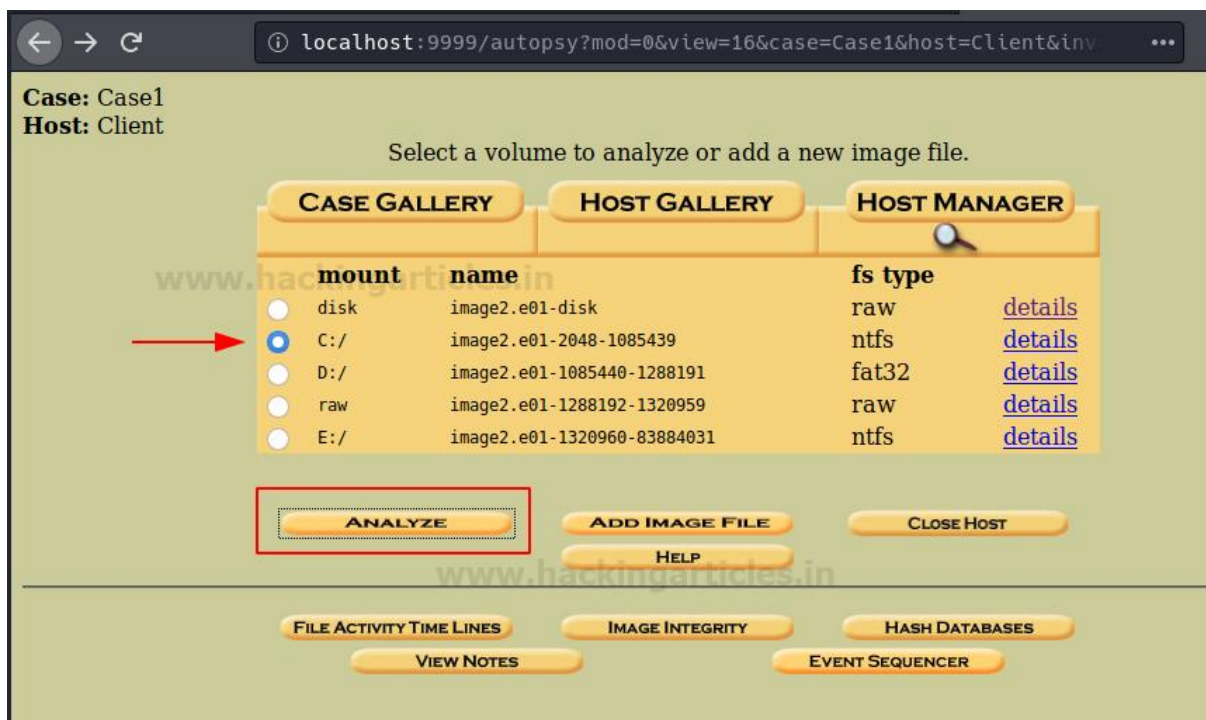
File Analysis-File and Metadata Analysis

Now, it will ask you to choose the mode of analysis that you want to conduct and here we are conducting an analysis of the file, therefore click on 'File Analysis'.
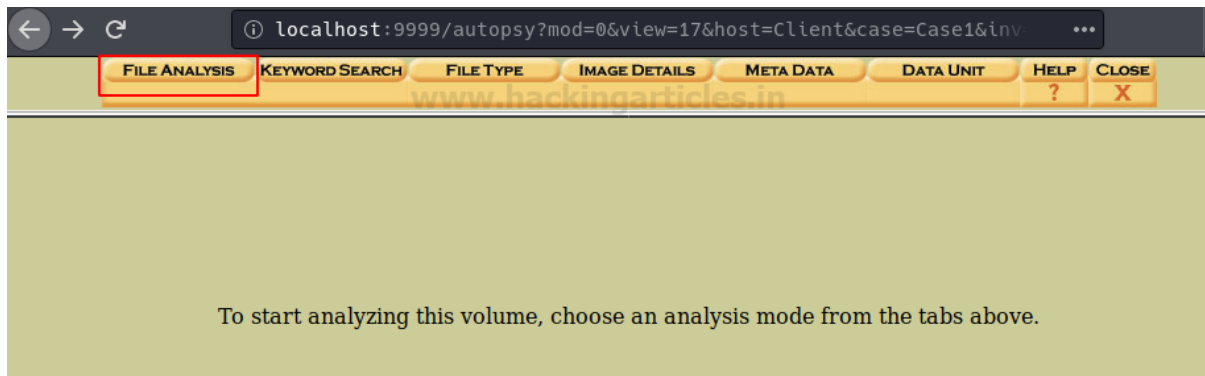
Now files will appear, which will give you the list of files and directories that are inside in this volume. From here you can analyze the content of the required image file and conduct the type of investigation you prefer. You can first generate an MD5 hash list of all the files present in this volume to maintain the integrity of the files, hence click on 'Generate MD5 List of Files'.
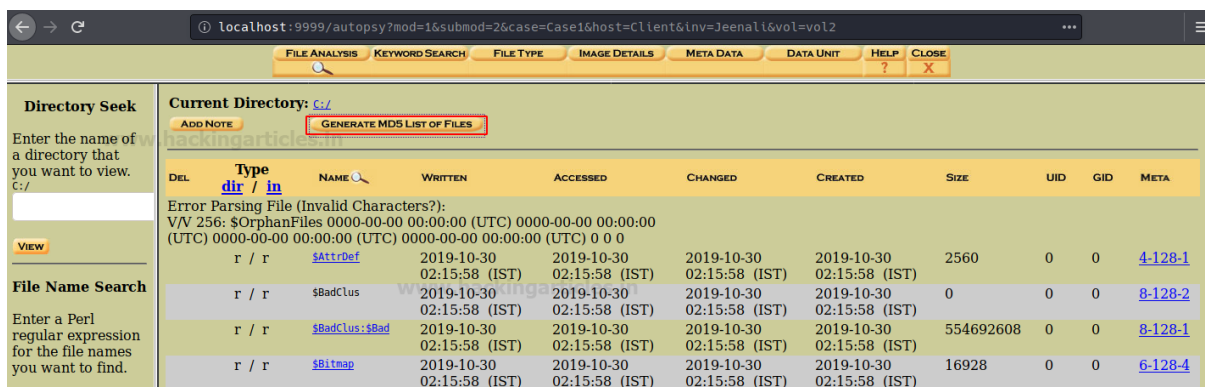
Now you can see the MD5 values of the files in volume C of the image file.
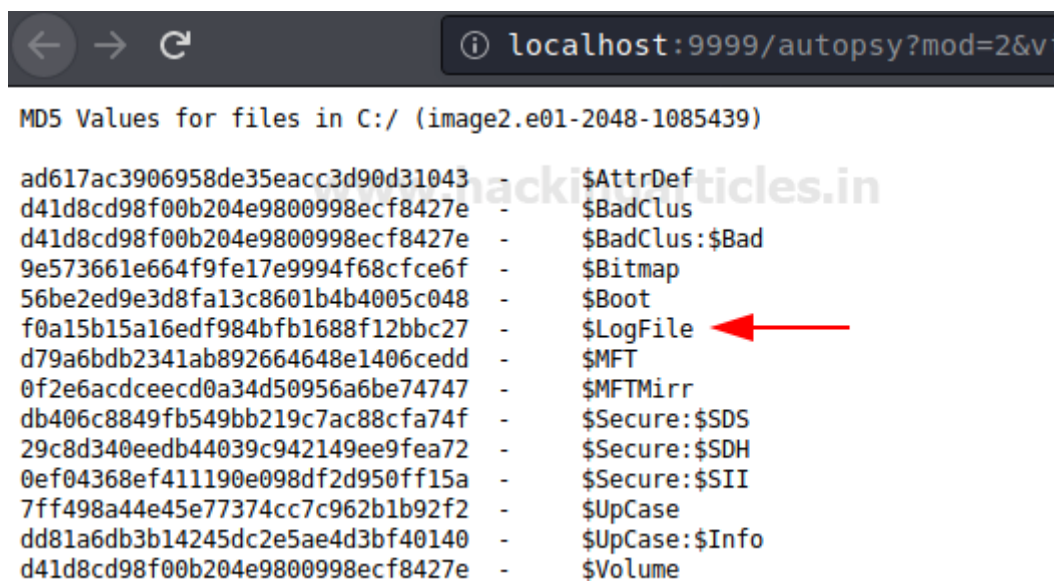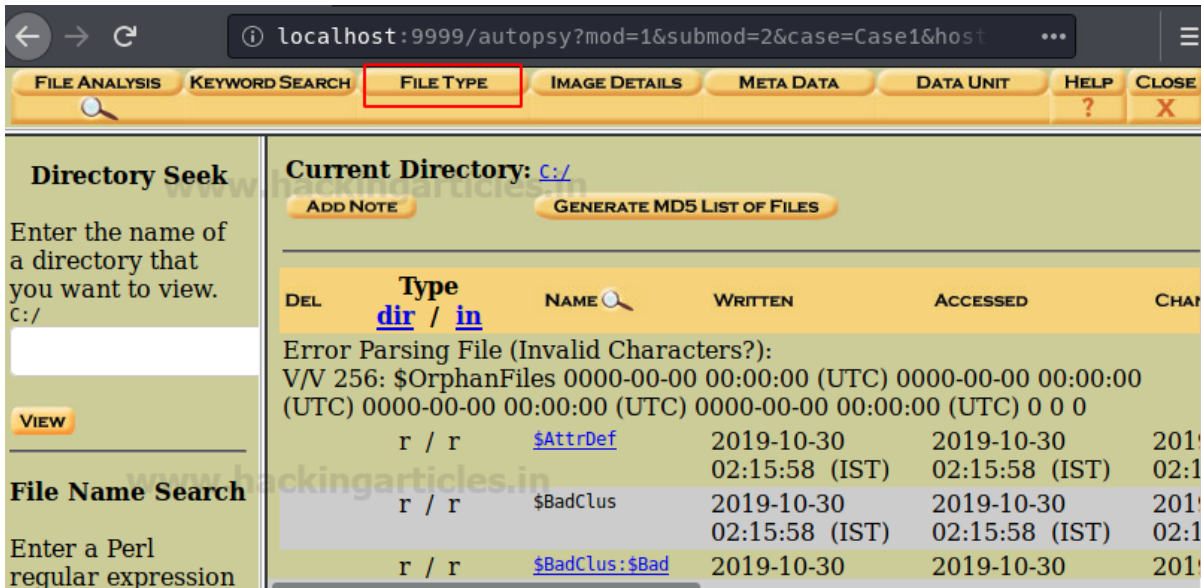
The file browsing mode consists of details of the directories that are shown below. The details include the time and date of the last time the directories were Written, Accessed, Changed and the time it was created with its size and also about its metadata. All the details are displayed in this, so in 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
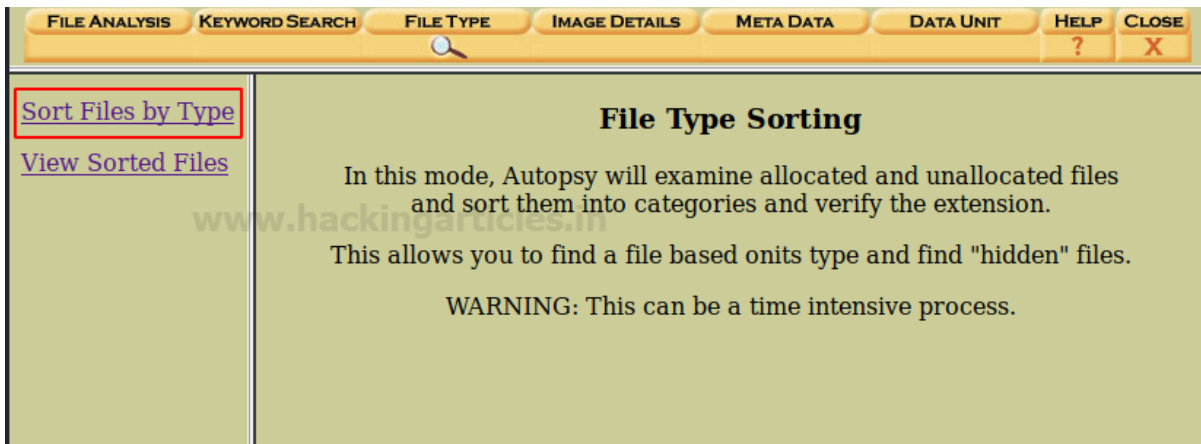
Here you can see the metadata information about the directory. In order to see more details, click on the first cluster '44067' in order to view its header information to find any relevant information to the case.

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'
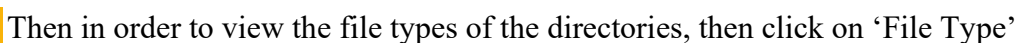
File Type

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.

| FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT |

Sort Files by
Type

View Sorted
Files

File Type Sortings

www.hackingarticles.in
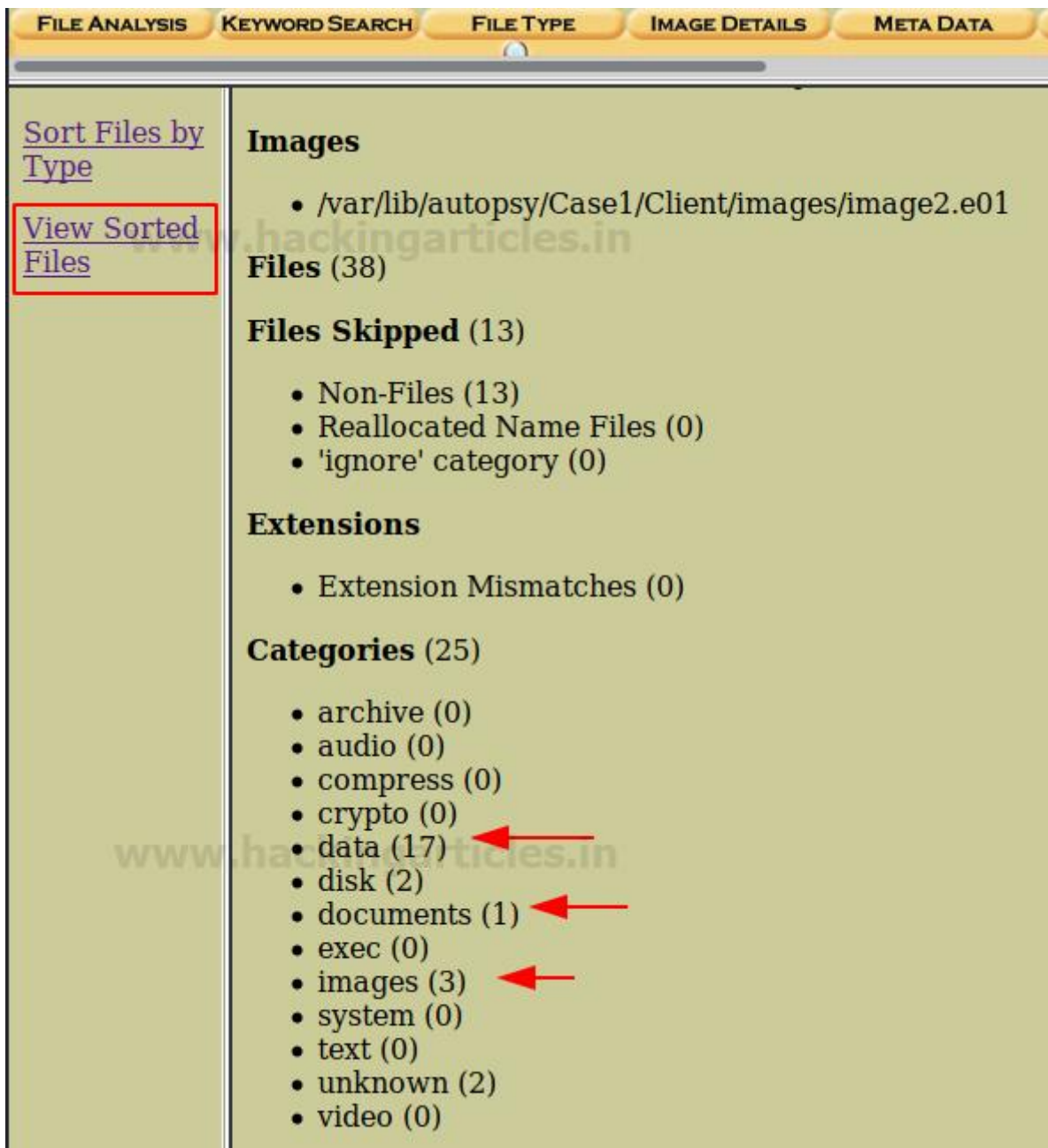
The **sorter** tool will process an image and organize the files based on their file type. The files are organized into categories that are defined in configuration files. The categories will be saved in the output directory.

WARNING: This will overwrite any existing data in:
    /var/lib/autopsy/Case1/Client/output/sorter-vol2/

☑ Sort files into categories by type

☐ Do not save data about unknown file types

☐ Save a copy of files in category directory (may require lots of disk space)

☐ Save ONLY graphic images and make thumbnails (may require lots of disk space and will save to a different directory than sorting all file types)

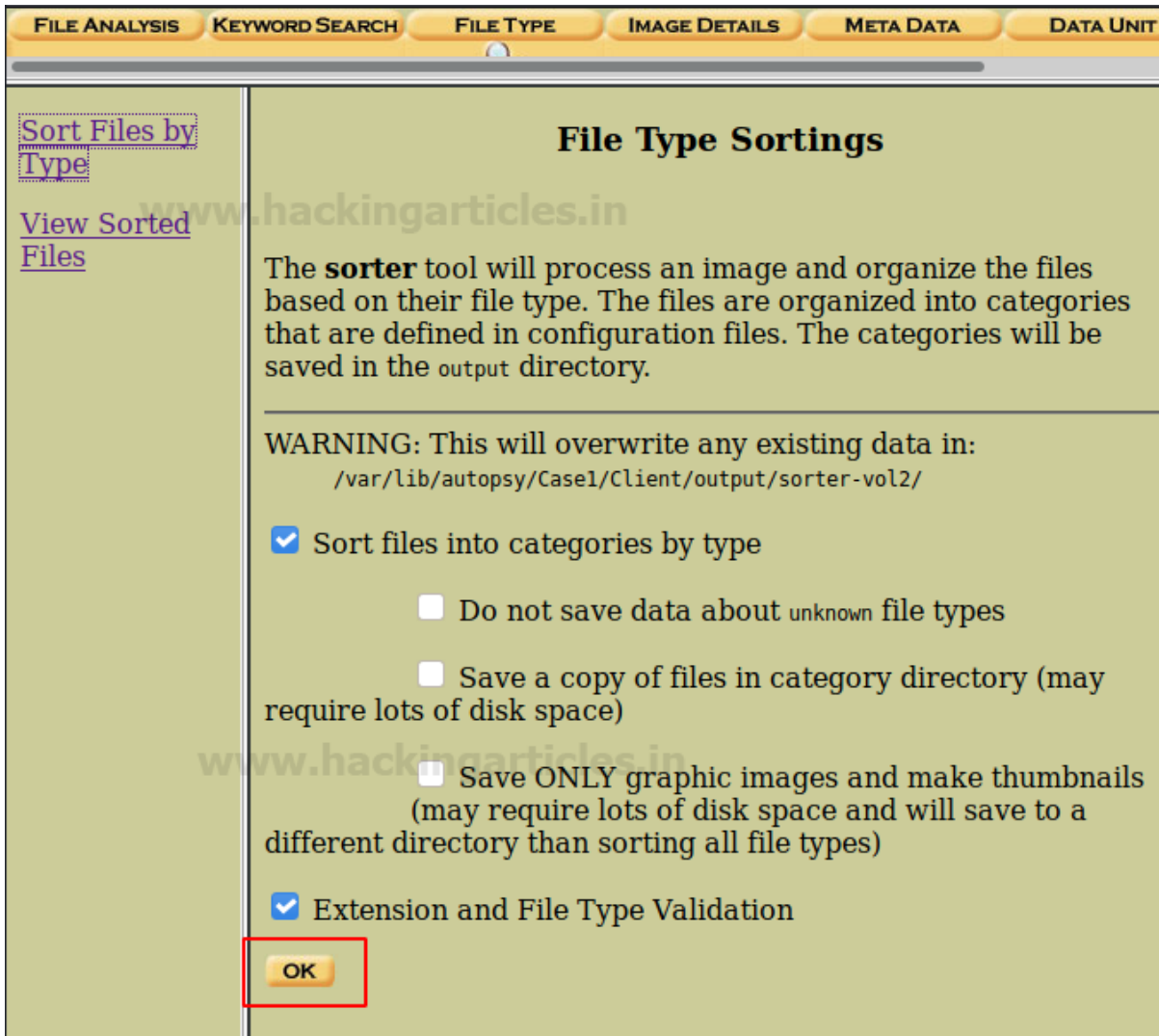☑ Extension and File Type Validation

OK

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.

| FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA |

Sort Files by Type

View Sorted Files

Images

- /var/lib/autopsy/Case1/Client/images/image2.e01

Files (38)

Files Skipped (13)

- Non-Files (13)
- Reallocated Name Files (0)
- 'ignore' category (0)

Extensions

- Extension Mismatches (0)

Categories (25)

- archive (0)
- audio (0)
- compress (0)
- crypto (0)
- data (17)
- disk (2)
- documents (1)
- exec (0)
- images (3)
- system (0)
- text (0)
- unknown (2)
- video (0)

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.
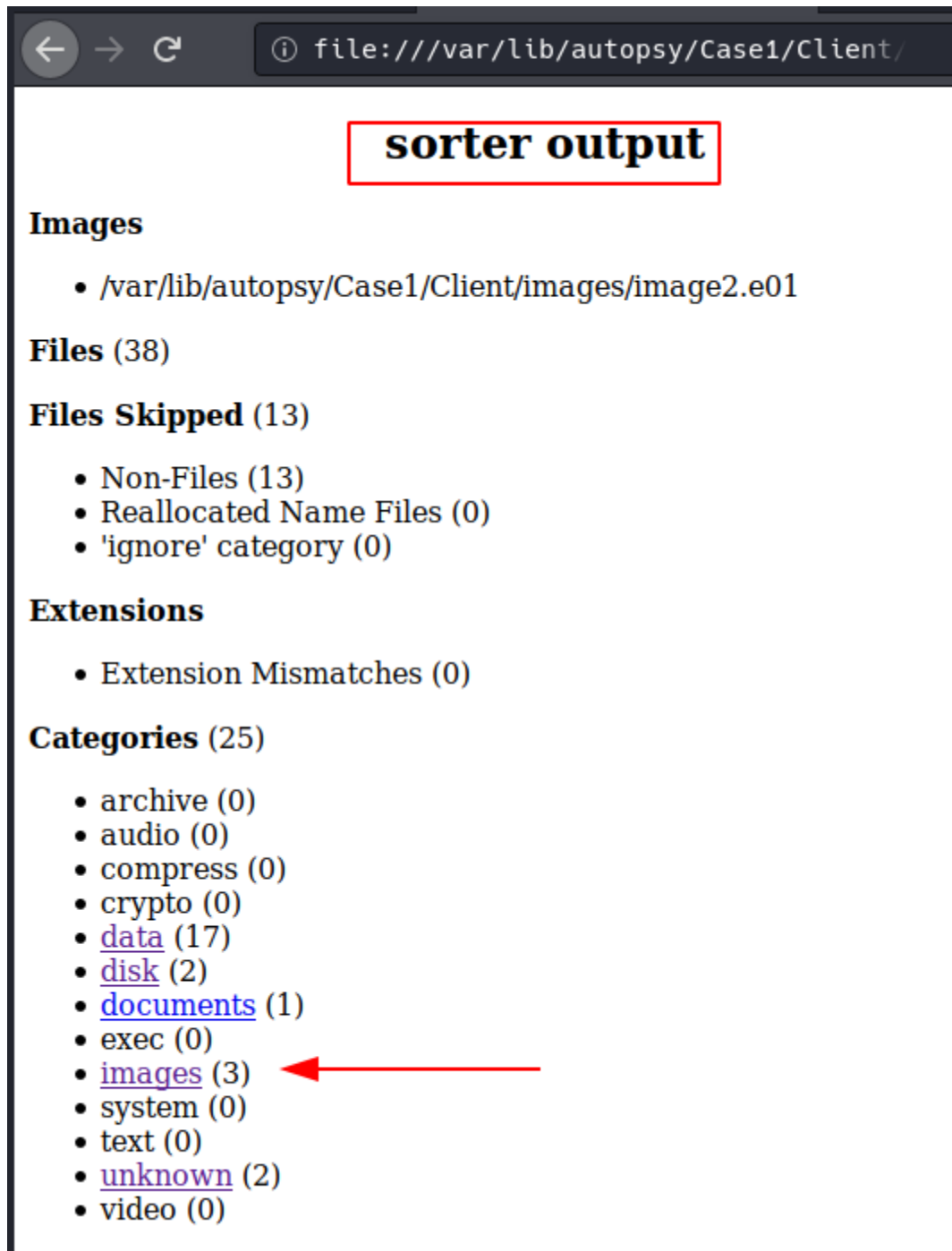
Now you can see Images categories and further investigate the files depending on the case requirement.
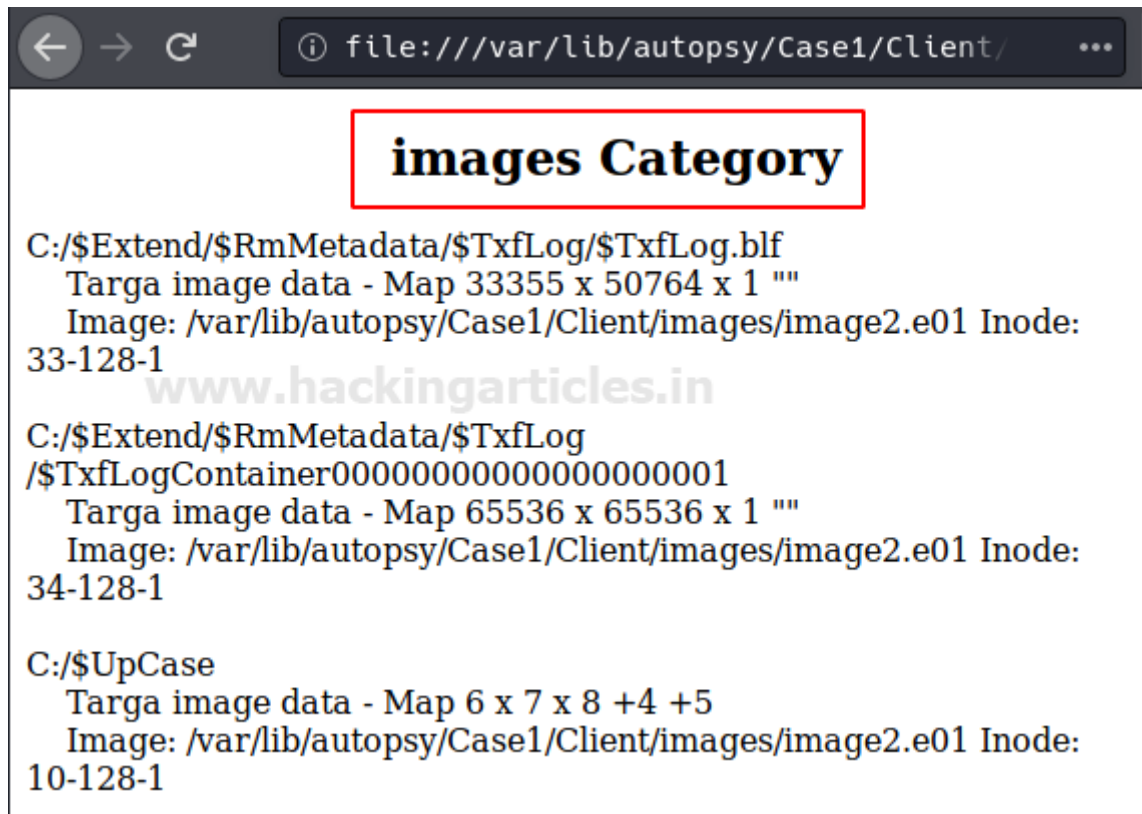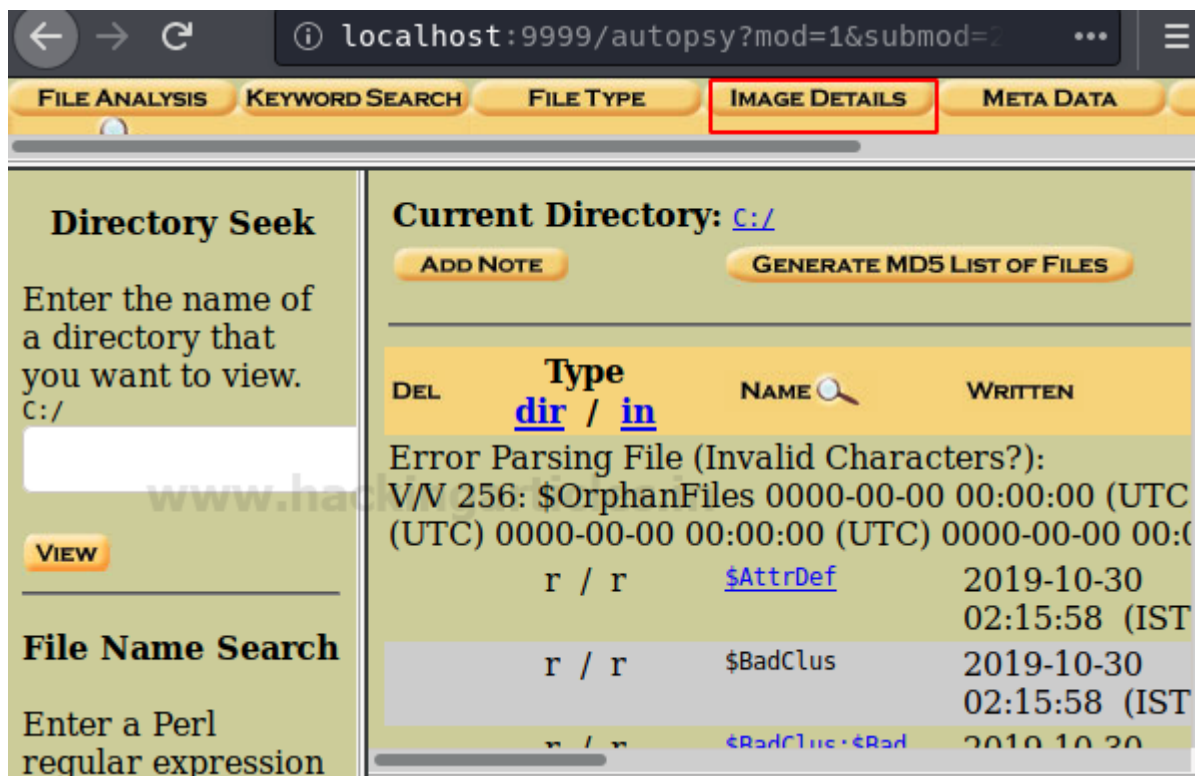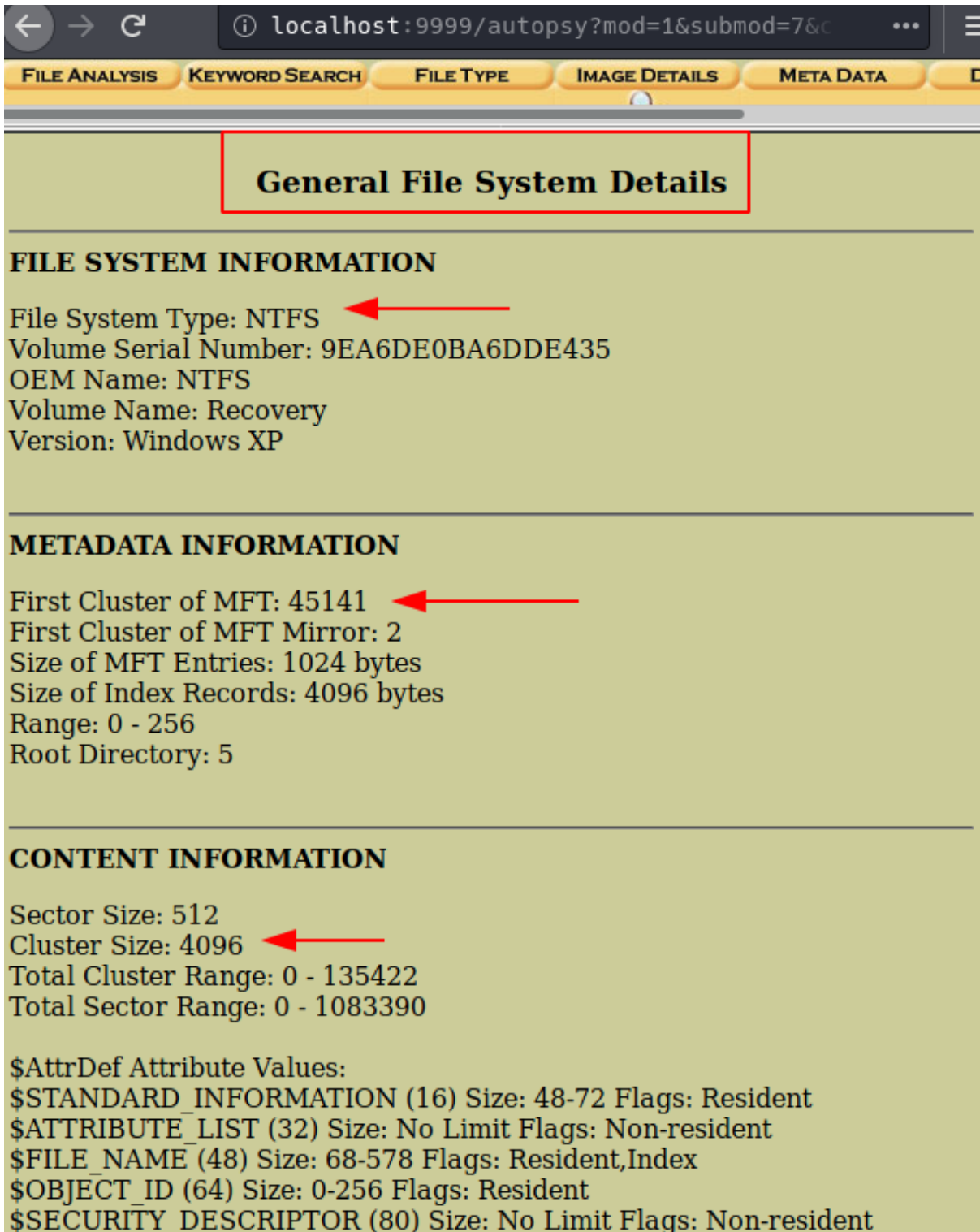
file:///var/lib/autopsy/Case1/Client/

images Category

C:/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
    Targa image data - Map 33355 x 50764 x 1 ""
    Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode:
33-128-1

C:/$Extend/$RmMetadata/$TxfLog
/$TxfLogContainer00000000000000000001
    Targa image data - Map 65536 x 65536 x 1 ""
    Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode:
34-128-1

C:/$UpCase
    Targa image data - Map 6 x 7 x 8 +4 +5
    Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode:
10-128-1

Image Details

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

localhost:9999/autopsy?mod=1&submod=

| FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA |

Directory Seek

Enter the name of
a directory that
you want to view.
C:/

VIEW

File Name Search

Enter a Perl
regular expression

Current Directory: C:/

ADD NOTE   GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN
	Error Parsing File (Invalid Characters?): V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:0		
r / r		$AttrDef	2019-10-30 02:15:58 (IST
r / r		$BadClus	2019-10-30 02:15:58 (IST
r / r		$BadClus:$Bad	2019-10-30

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

Keyword Search

To ease the search of a file or document you can make use of the 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.

Conclusion

Hence, you as a Digital Forensics Investigator can make use of these different options of tools in Autopsy. This collection of tools creates quite a powerful forensic analysis platform.

References

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