



Autopsy

Forensic Investigation

Prof. Abhishek Singh



Table of Contents

Abstract.....	3
Windows Forensic Investigation	4
Creating a new Case	4
Views	9
By Extension	10
Documents	13
Executables	16
By MIME Type	17
Results	20
Timeline	23
Discovery	25
Images/Videos	26
Add File Tag	28
Generate Report	29
Linux Forensic Investigation	31
Creating A New Case	31
Adding Image File	36
File Analysis-File and Metadata Analysis	39
File Type	43
Image Details	47
Keyword Search	49
Conclusion	50

Abstract

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.

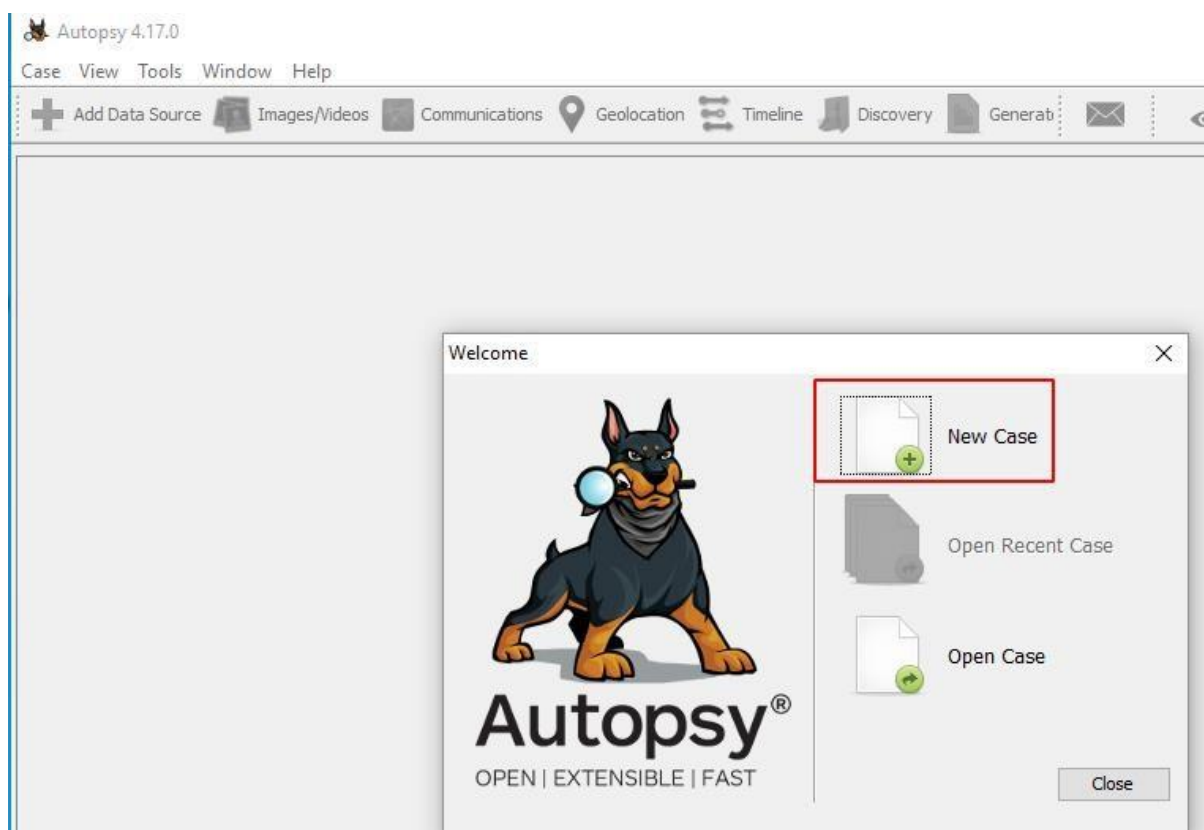
If you're interested in digital forensics, this report is for you—sit back, buckle up, and let's dive into the adventure!

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.

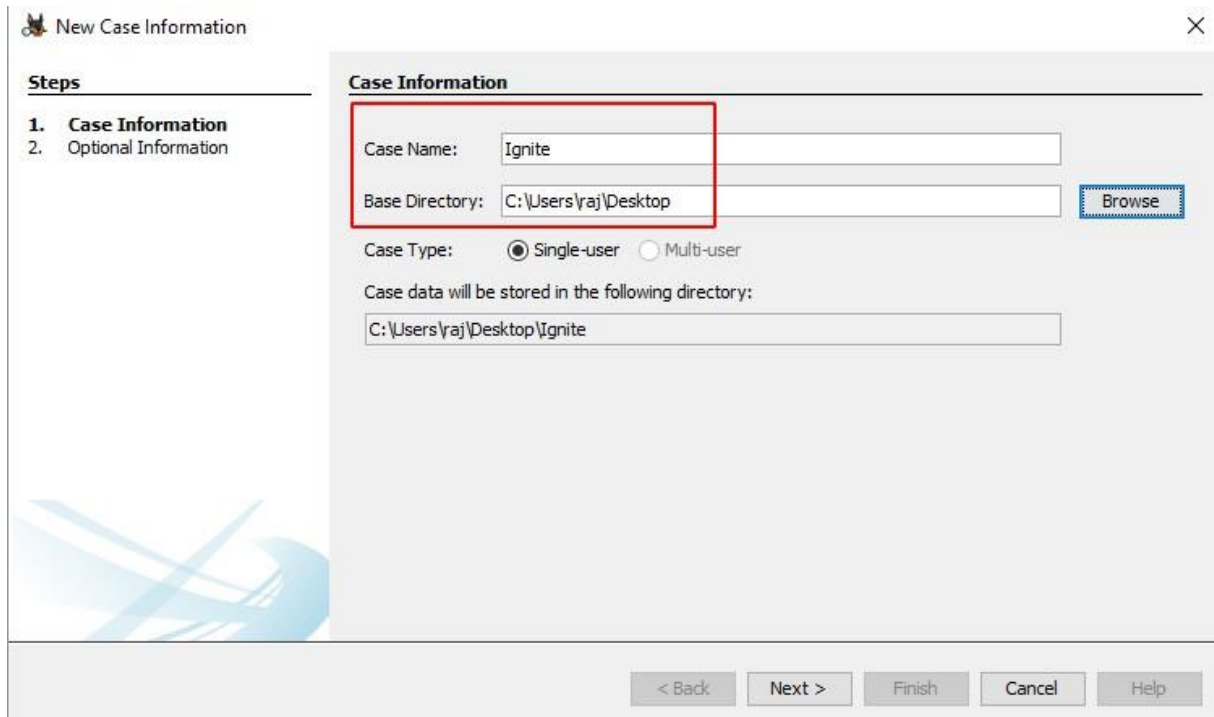
Windows Forensic Investigation

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.



New Case Information

Steps

- 1. Case Information**
- Optional Information

Case Information

Case Name:

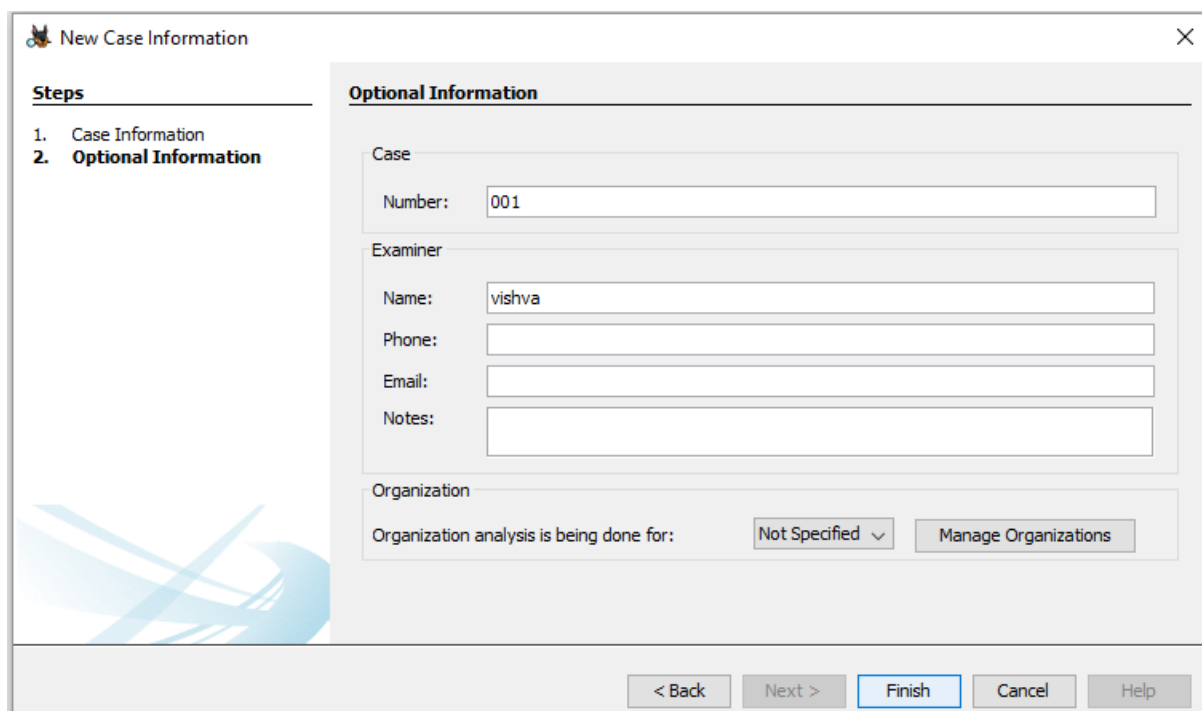
Base Directory: [Browse](#)

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

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



New Case Information

Steps

- Case Information
- 2. Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for: [Manage Organizations](#)

< Back Next > **Finish** Cancel Help

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.

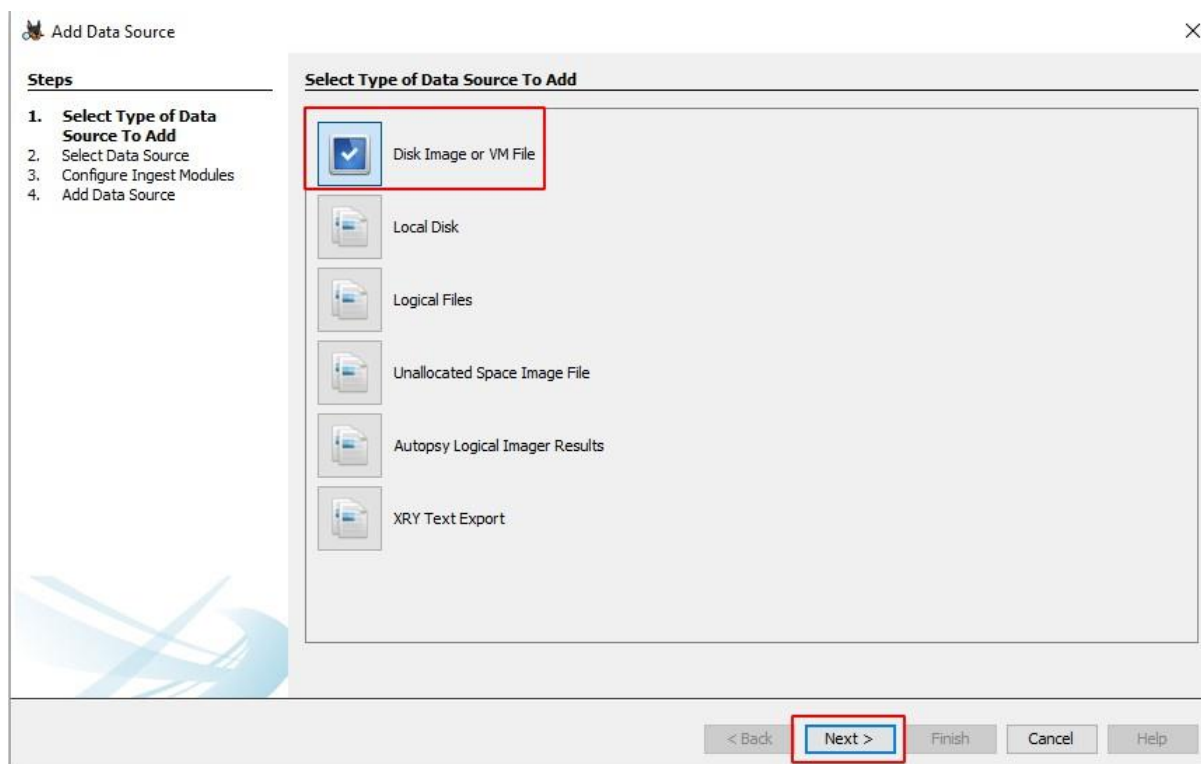
Local Disk: This option includes devices like Hard disk, Pen drives, memory cards, etc.

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.

Add Data Source

Steps

1. Select Type of Data Source To Add
- 2. Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

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

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
- 3. Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on:

☒ Recent Activity
☒ Hash Lookup
☒ File Type Identification
☒ Extension Mismatch Detector
☒ Embedded File Extractor
☒ Picture Analyzer
☒ Keyword Search
☒ Email Parser
☒ Encryption Detection
☒ Interesting Files Identifier
☒ Central Repository
☒ PhotoRec Carver
☒ Virtual Machine Extractor
☒ Data Source Integrity

Select All Deselect All History

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Global Settings

< Back Next > Finish Cancel Help

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.

Ignite - Autopsy 4.17.0
Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
Data Sources

Name	Type	Size (Bytes)
Ignite.E01	Image	64420392960

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Page: 1 of 3931909 Page Go to Page: Jump to Offset 0

```

0x00000000: EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 .R.NIFS .....
0x00000010: 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 58 E0 03 .....?....X..
0x00000020: 00 00 00 00 80 00 80 00 FF D7 1B 01 00 00 00 00 .....
0x00000030: 00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00 .....
0x00000040: FE 00 00 00 01 00 00 00 17 59 BE 64 56 BE 64 76 .....Y.d..dv
0x00000050: 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 .....3.....h..
0x00000060: 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.....f>..N
0x00000070: 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB TFSu..A..U..r..
0x00000080: 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC U.u.....u.....

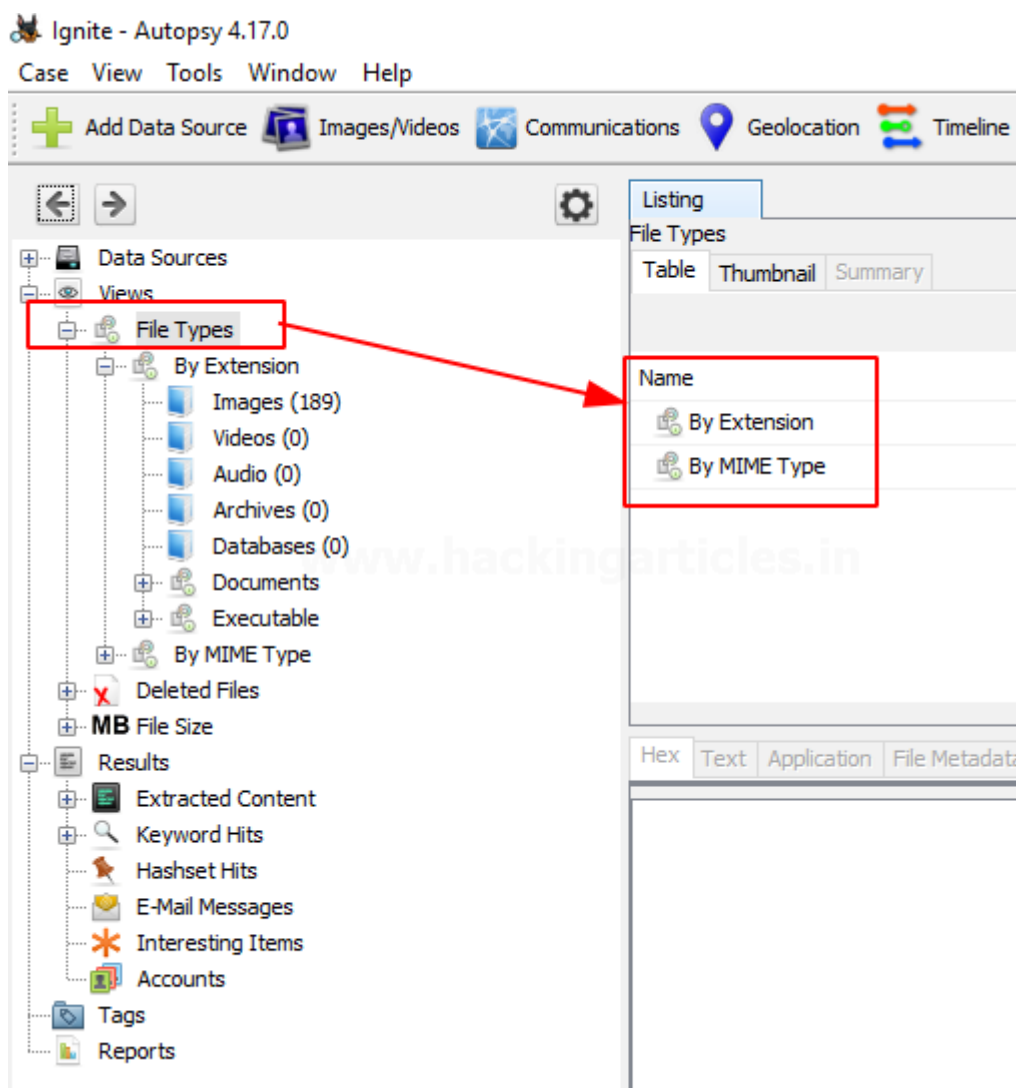
```


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.

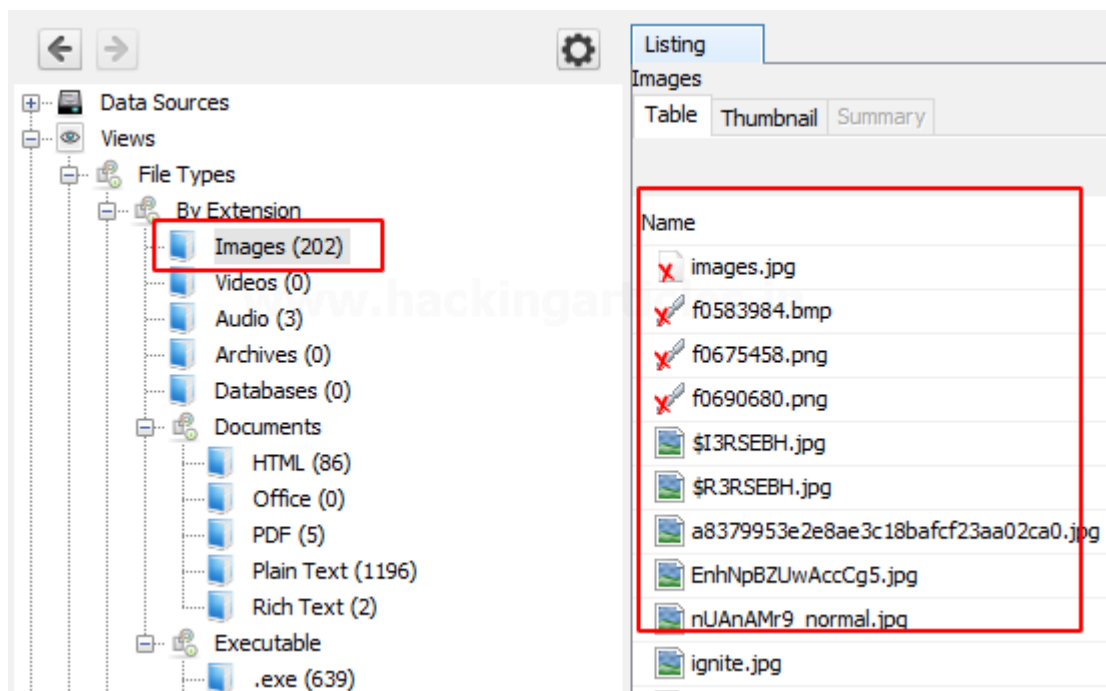


By Extension

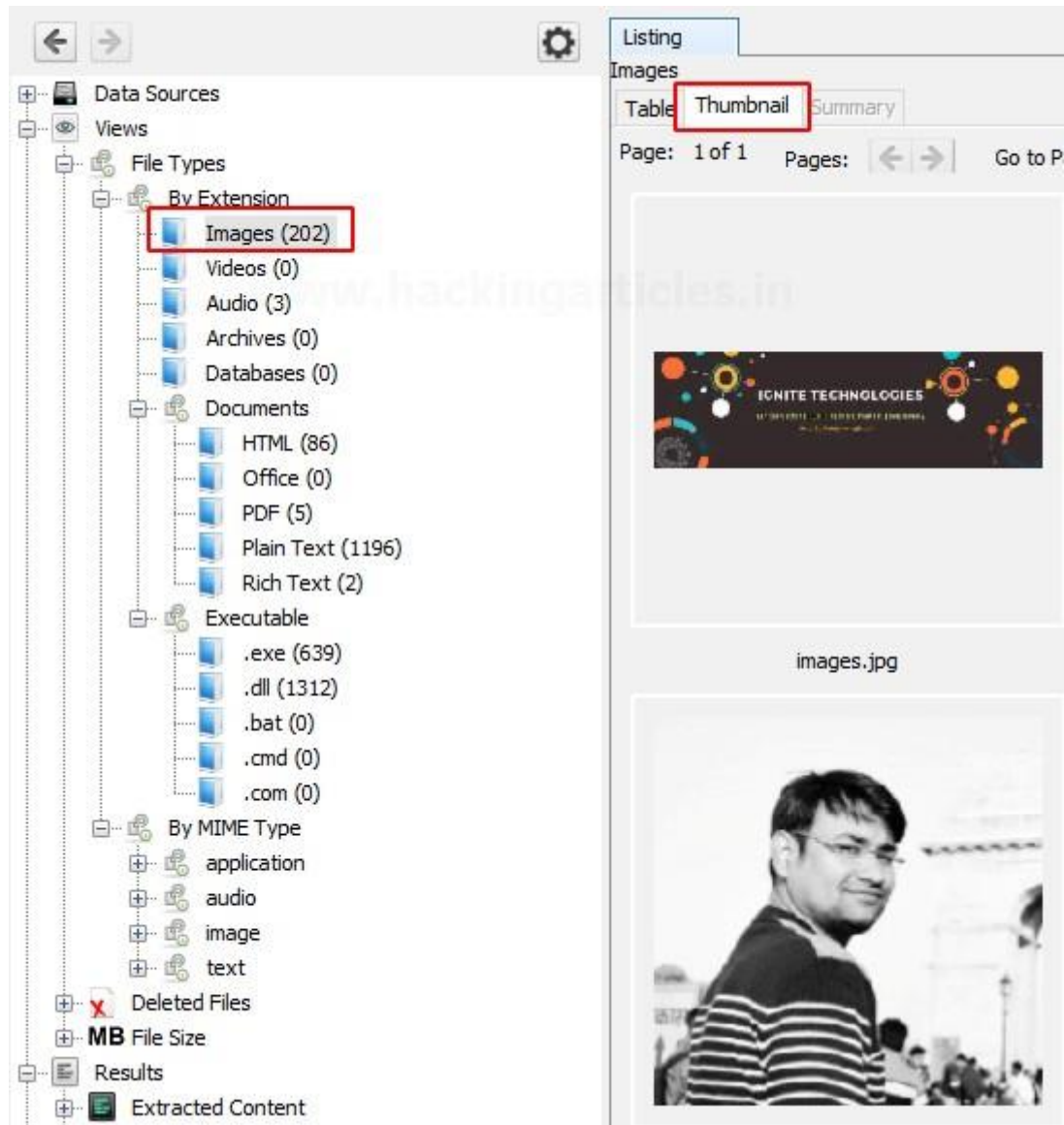
In the category Filetypes by extension and you can see that this has been sub-divided into file types like images, video, audio, archives, databases, etc.



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.

Table Thumbnail Summary

Page: 1 of 1 Pages: < > Go to Page: Image



images.jpg

/img_Ignite.E01/images.jpg

Hex Text Application **File Metadata** Context Results Annotations Ot

From The Sleuth Kit istat Tool:

MFT Entry Header Values:
 Entry: 49 Sequence: 1
 \$LogFile Sequence Number: 16885331
 Allocated File
 Links: 1

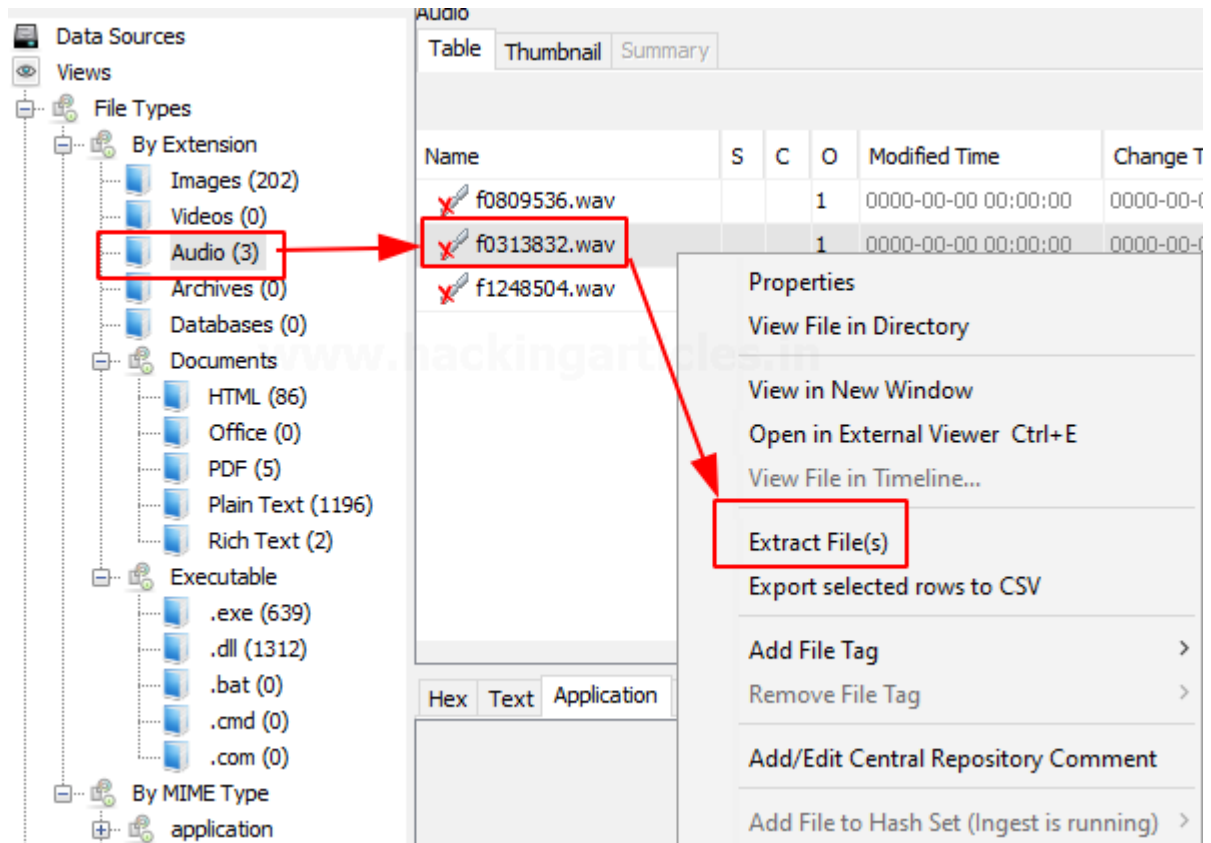
\$STANDARD_INFORMATION Attribute Values:
 Flags: Archive
 Owner ID: 0

Security ID: 271 (S-1-5-21-1276730070-1850728493-30201
 Created: 2020-11-26 08:20:24.482672700 (PST)
 File Modified: 2020-11-26 08:20:24.667704200 (PST)
 MFT Modified: 2020-11-26 09:00:35.829441300 (PST)
 Accessed: 2020-11-26 08:59:53.860554000 (PST)

\$FILE_NAME Attribute Values:
 Flags: Archive
 Name: \$R3RSEBH.jpg
 Parent MFT Entry: 40 Sequence: 1
 Allocated Size: 8192 Actual Size: 7641
 Created: 2020-11-26 08:20:24.482672700 (PST)
 File Modified: 2020-11-26 08:20:24.667704200 (PST)
 MFT Modified: 2020-11-26 08:59:01.714957400 (PST)
 Accessed: 2020-11-26 08:59:01.704974100 (PST)

\$OBJECT_ID Attribute Values:
 Object Id: 3fd39b21-2f45-11eb-ala0-001b10002aec

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.

The screenshot shows a file explorer interface with a sidebar on the left and a main pane on the right. The sidebar lists various file types, including 'HTML (86)', which is highlighted with a red box. The main pane displays a table of files with columns 'Name', 'S', 'C', and 'O'. The file 'Forensic Investigation Autopsy Forensic Browser in Linux.html' is highlighted with a red box. Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occ'. The 'Text' tab is selected, showing the content of the selected file. The content includes a header 'Hacking Articles', a sub-header 'Raj Chandel's Blog', and a list of topics: CTF Challenges, Penetration Testing, Web Penetration Testing, Red Teaming, Donate us, and Courses We Offer. The footer of the preview area contains the text 'Forensic Investigation: Autopsy Forensic Browser in Linux', 'posted inCyber Forensics on August 13, 2020 by Raj Chandel', 'SHARE', and 'Save'.

Name	S	C	O
Forensic Investigation Autopsy Forensic Browser in Linux.html			1
a.html			1
a_002.html			1
fastbutton.html			1
like.html			1

Page: 1 of 3 Page Matches on page: - of - Match 10

Hacking Articles

Raj Chandel's Blog

- * CTF Challenges
- * Penetration Testing
- * Web Penetration Testing
- * Red Teaming
- * Donate us
- * Courses We Offer
 - o Bug Bounty
 - o Computer Forensics
 - o Ethical Hacking
 - o Red Teaming

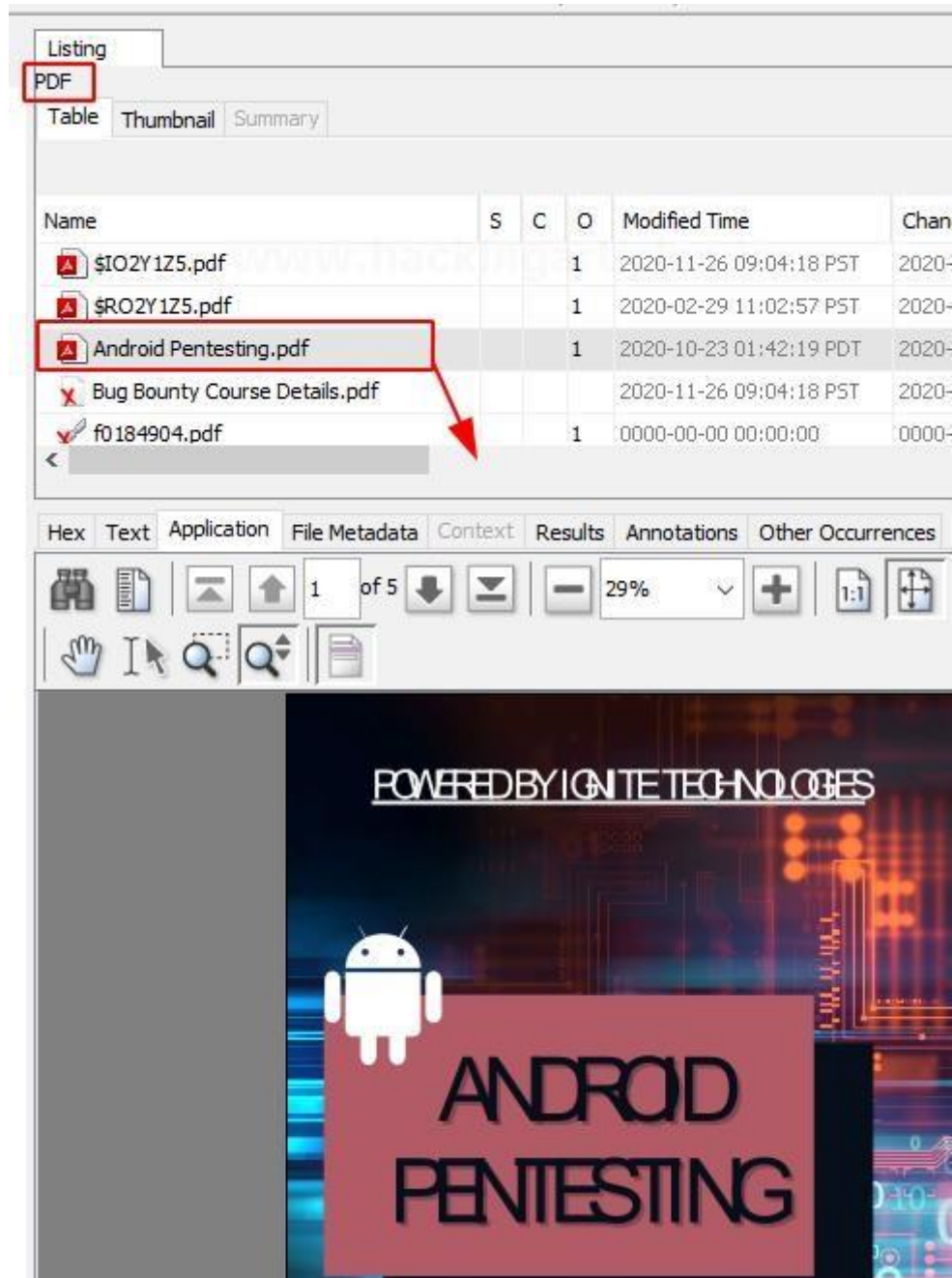
Forensic Investigation: Autopsy Forensic Browser in Linux

posted inCyber Forensics on August 13, 2020 by Raj Chandel

SHARE

Save

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.

The screenshot shows a file explorer on the left with a tree view. The 'Plain Text (1196)' folder is selected, and a red box highlights it. A red arrow points from this folder to a file named '\$RK1MRRO.txt' in the main pane. The file is highlighted with a red box. Below the file list, the 'Text' tab is active in the hex editor, showing the content of the selected file. The content is a text file with the following information:

Name	S	C	O	Modified Time
\$IK1MRRO.txt			1	2020-11-26 08:56:
\$RK1MRRO.txt			1	2020-11-26 08:55:
USB.txt			1	2020-09-09 07:15:
Ignite.E01.txt				2020-11-26 08:56:
f0484218.txt			1	0000-00-00 00:00:

Hex Text Application File Metadata Context Results An

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Mat

NOTICE: The imaging operation was cancelled!

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:

Acquired using: ADI4.3.1.1

Case Number: 001

Evidence Number: AU001

Unique description: Hacking Articles

Examiner: Vishva

Notes:

Information for E:\Ignite:

Physical Evidentiary Item (Source) Information

[Device Info]

Source Type: Logical

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 125,821,080

[Physical Drive Information]

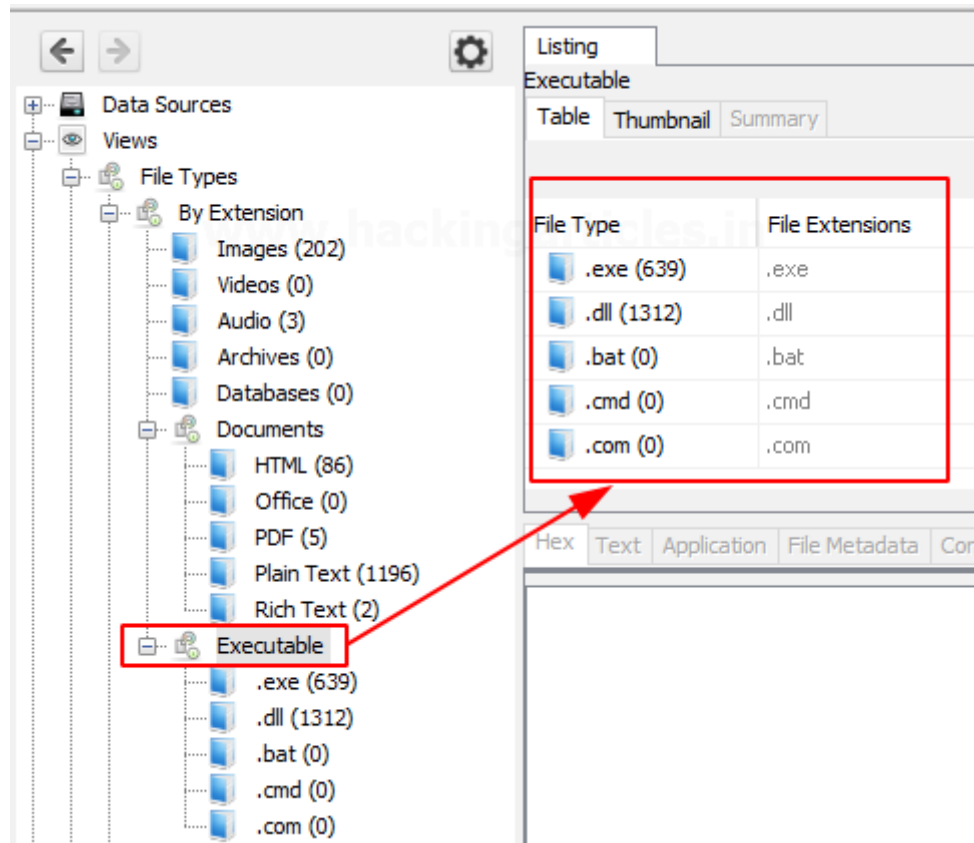
Removable drive: False

Source data size: 61436 MB

Sector count: 125821080

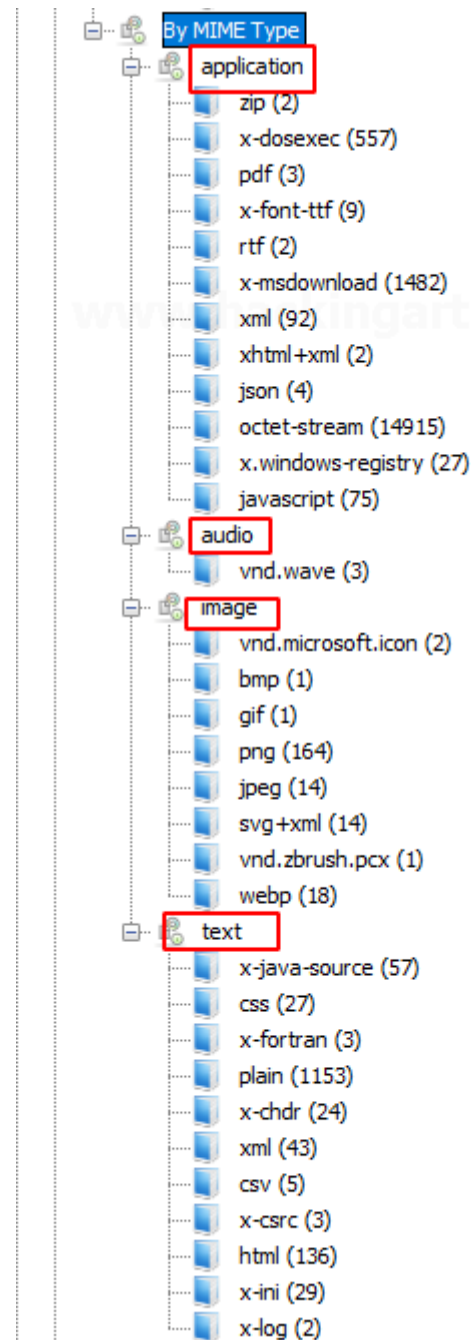
Executables

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.

File System

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Modified Time
20201014.mem			0	2020-10-13 13:39:50 PDT
adencrypt.dll			0	2020-05-11 21:03:46 PDT
adencrypt_gui.exe			0	2020-05-11 21:03:46 PDT
adfbs_globals.dll			0	2020-05-11 21:03:46 PDT
adfs_globals.dll			0	2020-05-11 21:03:46 PDT
ADG_EULA.rtf			1	2020-02-05 15:48:36 PST
ADIso.exe			0	2020-05-11 21:03:46 PDT
ADIsoDLL.dll			0	2020-05-11 21:03:48 PDT
adshattrdefs.dll			0	2020-05-11 21:03:48 PDT
adtz_globals.dll			0	2020-05-11 21:03:48 PDT
ad_globals.dll			0	2020-05-11 21:03:46 PDT
ad_log.dll			0	2020-05-11 21:03:46 PDT
boost_chrono-vc140-mt-1_59.dll			0	2020-05-11 21:03:48 PDT
boost_date_time-vc140-mt-1_59.dll			0	2020-05-11 21:03:46 PDT
boost_filesystem-vc140-mt-1_59.dll			0	2020-05-11 21:03:50 PDT
boost_regex-vc140-mt-1_59.dll			0	2020-05-11 21:03:50 PDT
boost_system-vc140-mt-1_59.dll			0	2020-05-11 21:03:50 PDT
boost_thread-vc140-mt-1_59.dll			0	2020-05-11 21:03:50 PDT
FTK Imager.exe			0	2020-05-11 21:04:10 PDT

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.

MB File Size

Table Thumbnail Summary

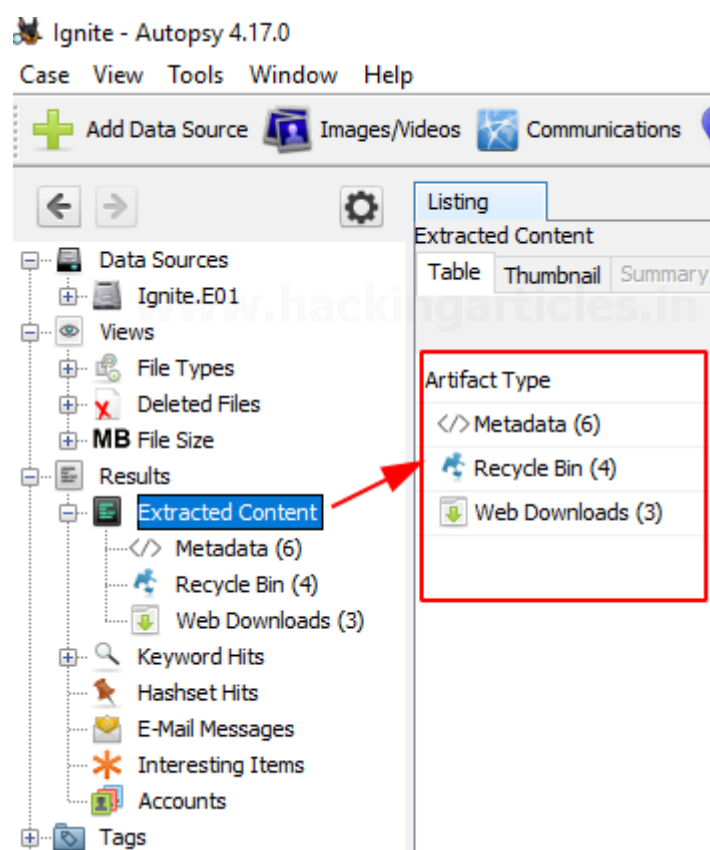
Page: Pages: Go to Page:

Size Range	MB 50 - 200MB (1)	MB 200MB - 1GB (2)	MB 1GB+ (3)
MB 50 - 200MB (1)			
MB 200MB - 1GB (2)			
MB 1GB+ (3)			

Results

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

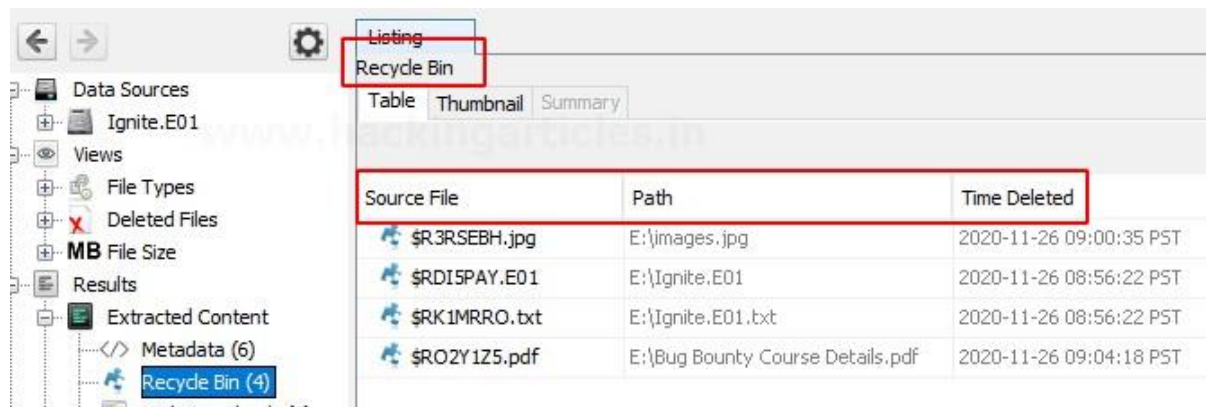
Extracted Content: All the content that was extracted, is segregated further in detail. Here we have found metadata, Recycle Bin, and web downloads. Let us further view each one of them.



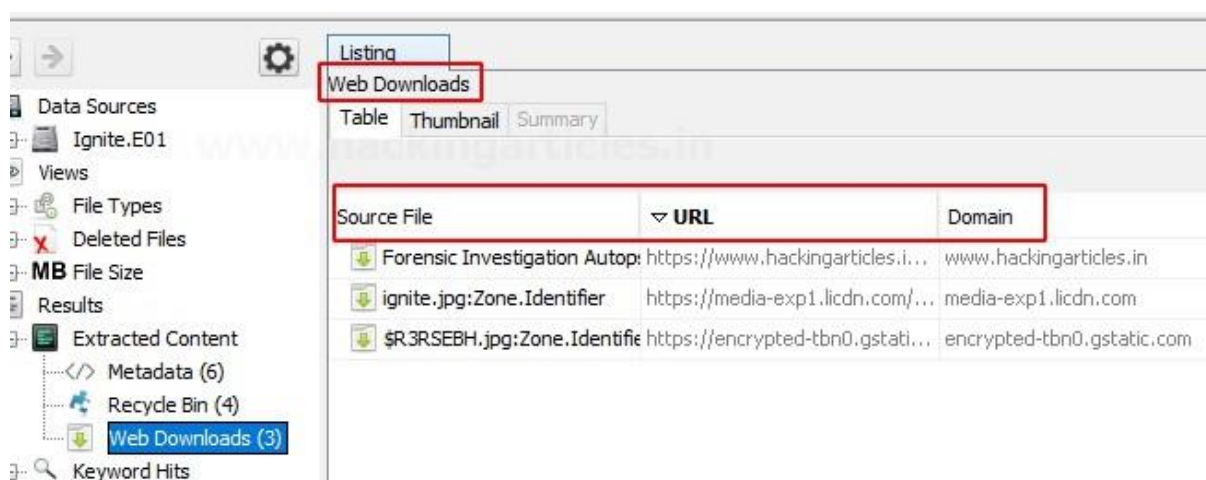
Metadata: Here we can view all the information about the files like the date it was created, to was modified, file's owner, etc.

Source File	Date Modified	Date Created	Owner	Data Source
</> \$ROZY1Z5.pdf	2020-02-29 19:02:56 PST	2020-02-29 19:02:56 PST	Ignite Tech...	Ignite.E01
</> Android Pentesting.pdf	2020-10-23 08:42:07 PDT	2020-10-23 08:42:10 PDT	...	Ignite.E01
</> ADG_EULA.rtf		2016-02-25 02:55:00 PST	...	Ignite.E01
</> FTKImager_UserGuide.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	...	Ignite.E01
</> f0184904.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	...	Ignite.E01
</> f0002808.rtf		2016-02-25 02:55:00 PST	...	Ignite.E01

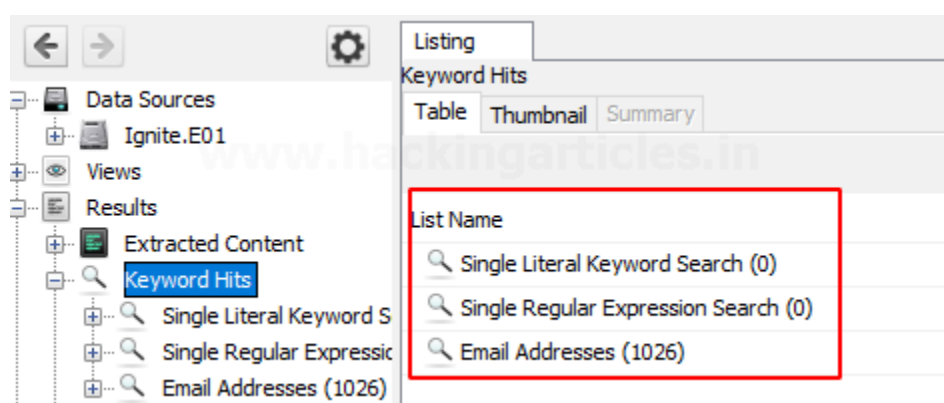
Recycle Bin: The files that were put in the recycle bin are found in this category.



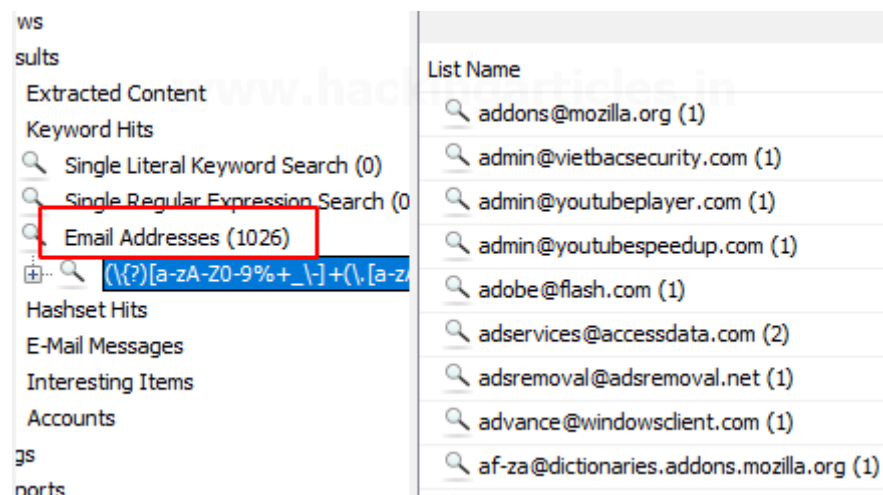
Web Downloads: Here you can see the files that were downloaded from the internet.



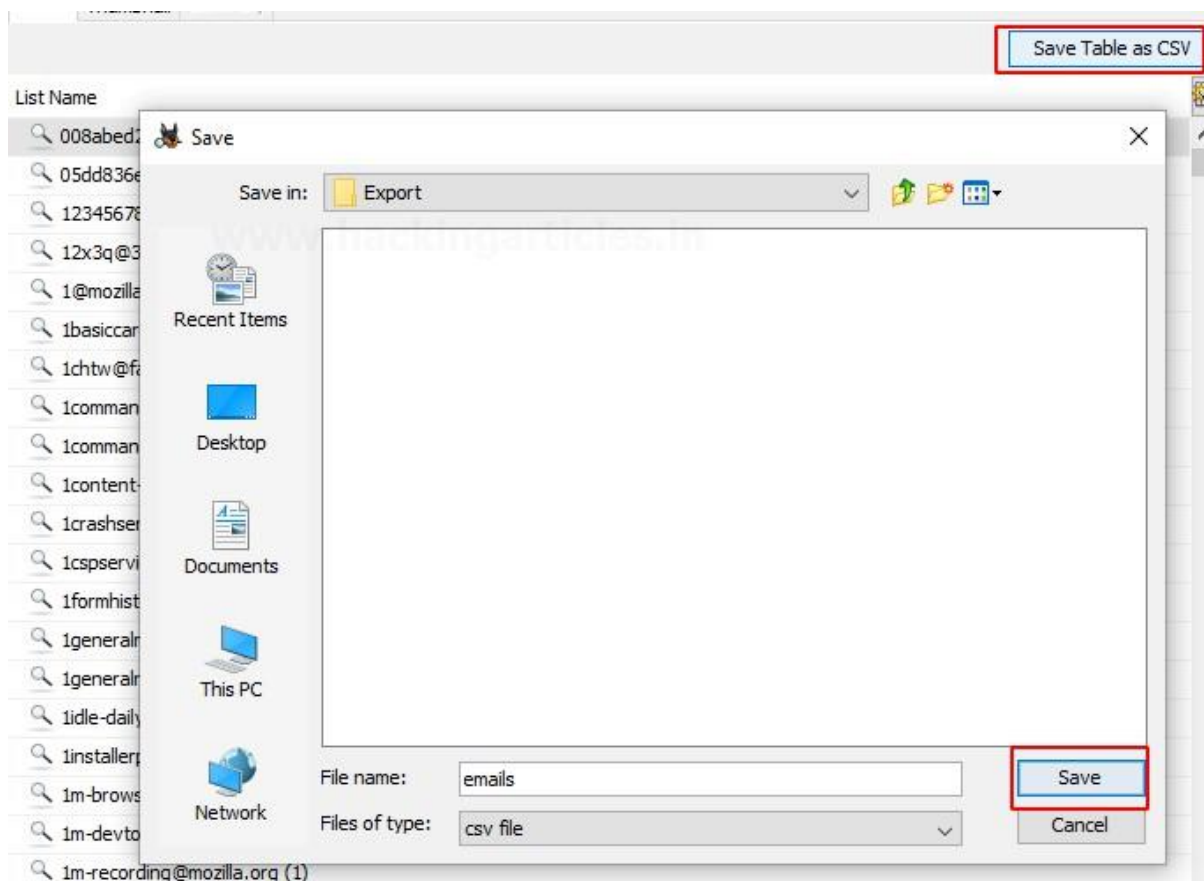
Keyword Hits: In this, any specific keywords can be looked up for in the disk image. The search can be conducted concerning the Exact match, Substring matches, Emails, Literal words, Regular expressions, etc.



You can view the available email addresses.

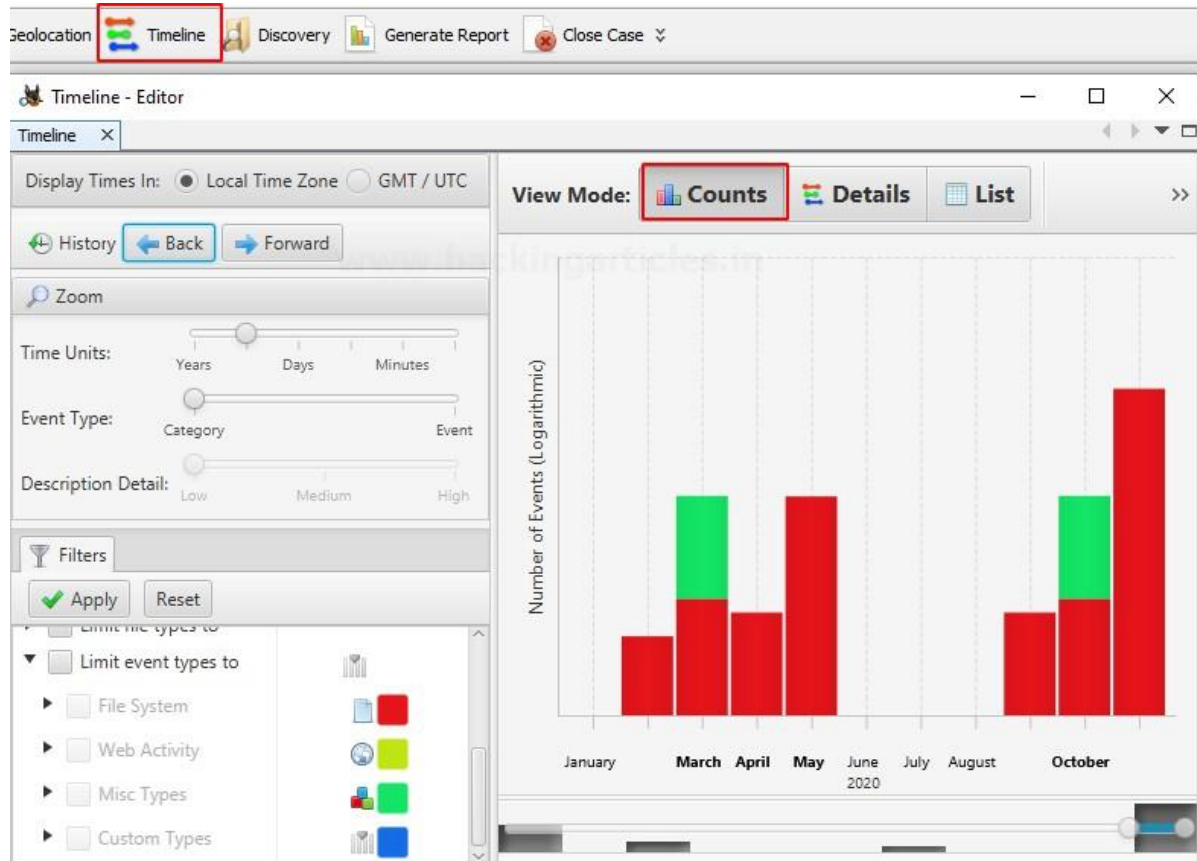


You can choose to export into a CSV format.



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

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

View Mode: ☒ Counts ☐ Details ☐ List

All Events (Filtered)

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

History [Back](#) [Forward](#)

Filters

☒ Apply ☐ Reset

☐ Must include text:

☐ 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

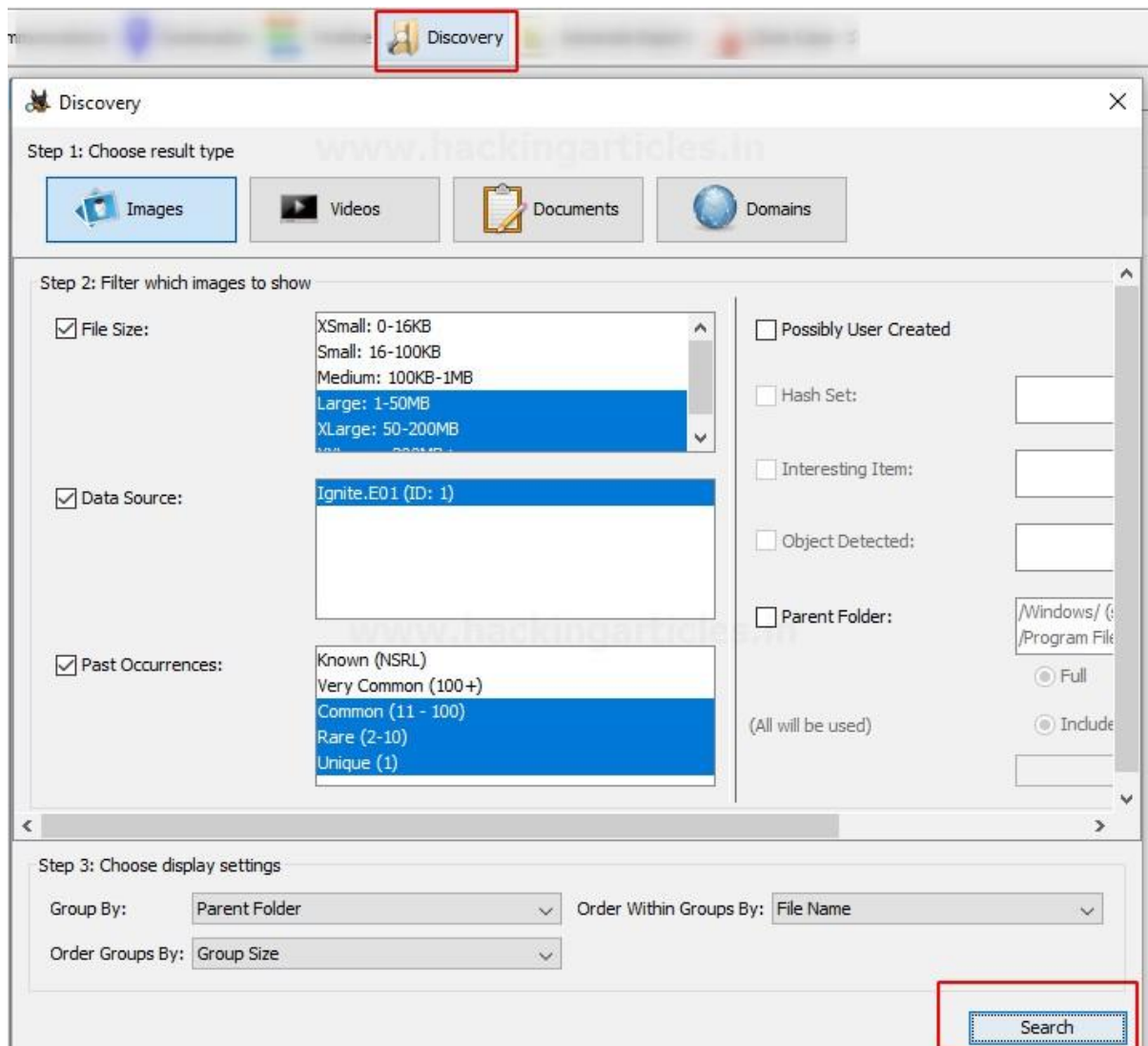
View Mode: ☒ Counts ☐ Details ☐ List

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

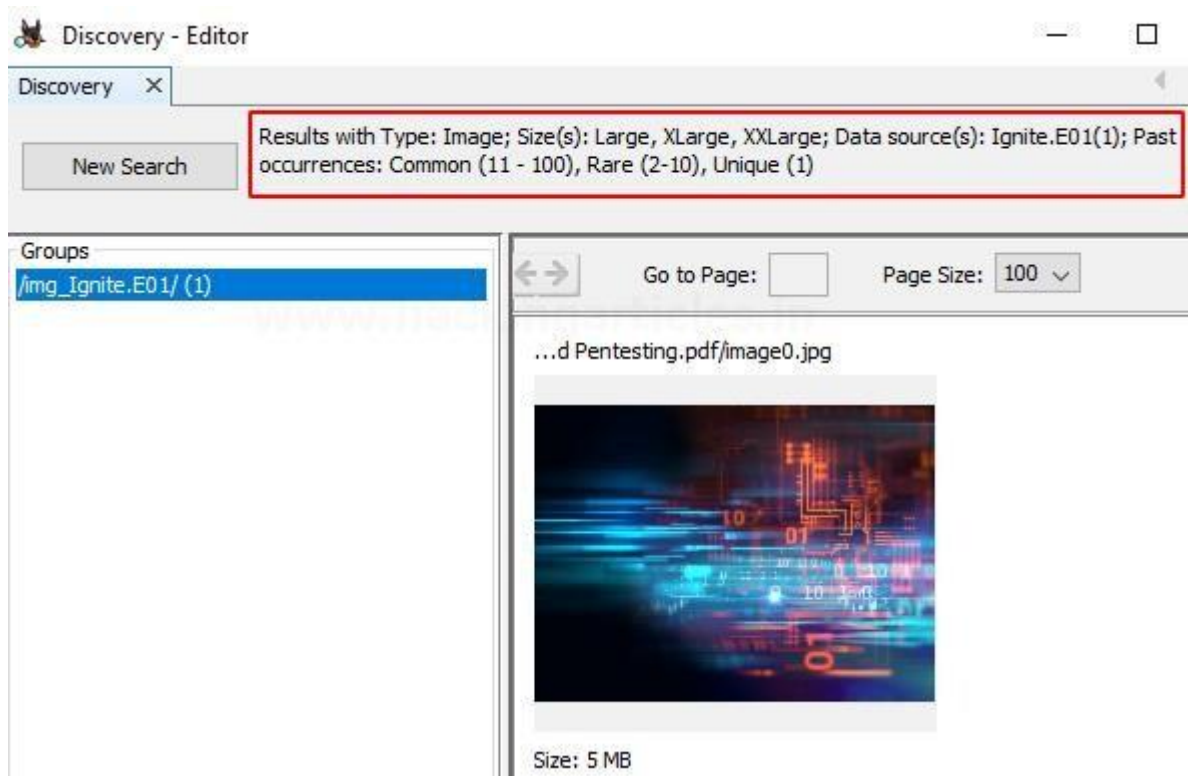
Start: Jan 27, 2020 11:33:00 PM

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

Ignite - Autopsy 4.17.0

Case View Tools Window Help

Images/Videos

Image/Video Gallery - Editor

Image/Video Gallery

Group By: Path

Sort By: Priority

Data Source: All

All Groups

Only Hash Hits

img_Ignite.E01 (2)

Android Pentesting.pdf (4)

...igation Autopsy Forensic Browser in Linux_files (48)

a_data (2)

\$Extend

\$RmMetadata

\$TxfLog (1)

\$OrphanFiles

unknown

Mozilla Firefox

\$RECYCLE.BIN

...-1276730070-1850728493-30201559-1001 (1)

/img_Ignite.E01/Forensic Investigation Autopsy Forensic Browser in Linux_files/a_data/ -- 0 hash set hits / 2 files

Tag Selected Files: Follow Up

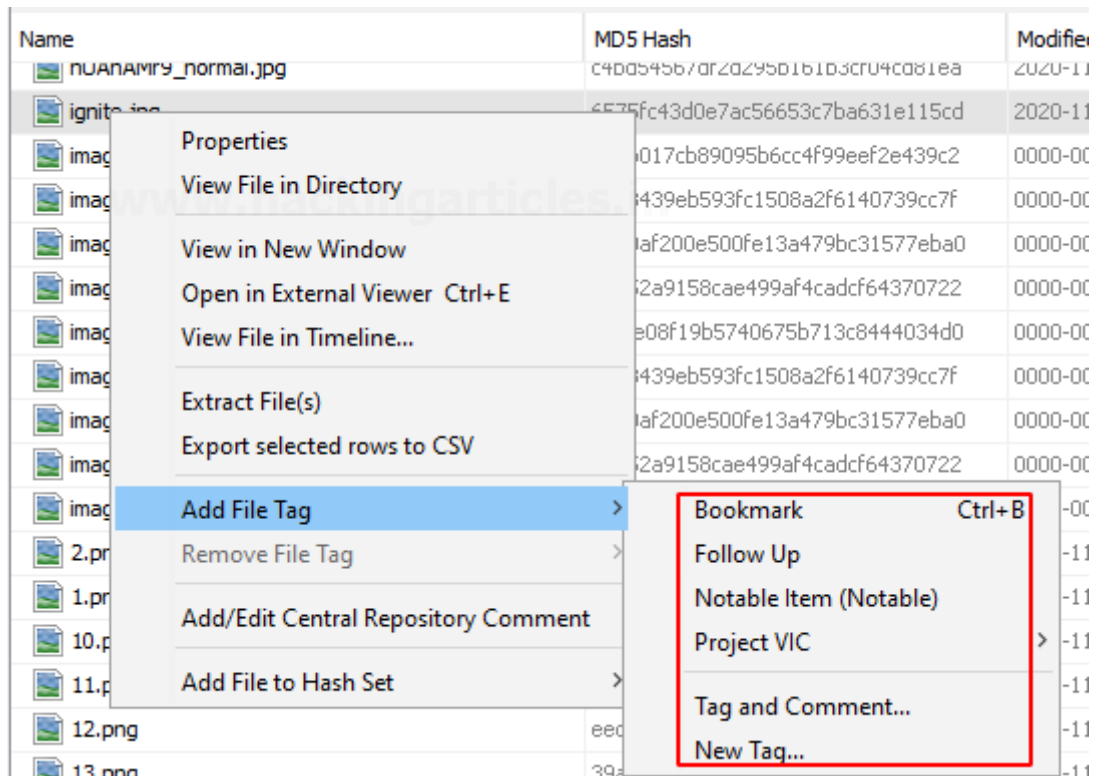
nUAnAMr9_nor...

EnhNpBZUwAcc...

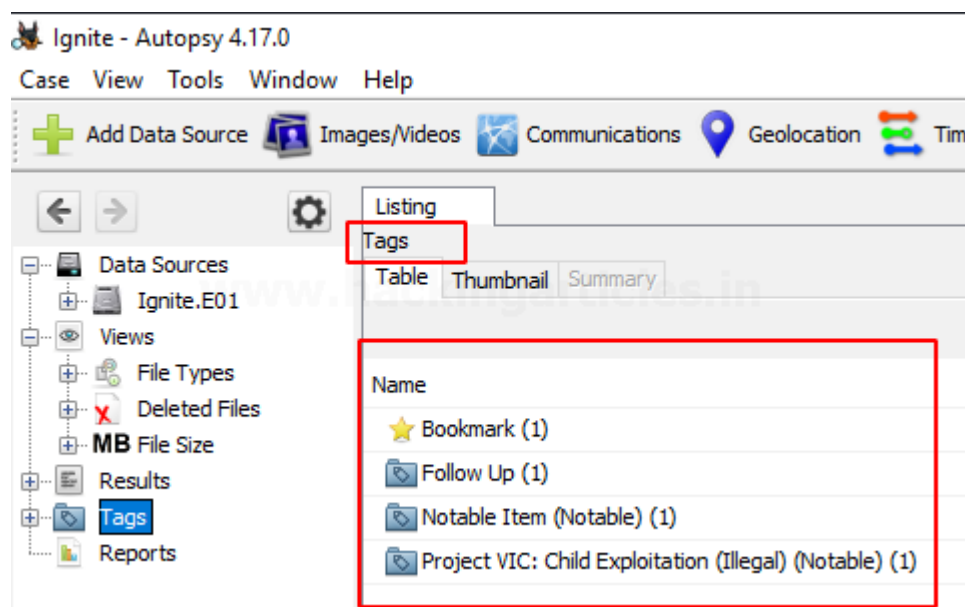
Category	# Files
Child Exploitation (Illegal)	0
Child Exploitation (Non-Ille...	0
CGI/Animation (Child Exploi...	0
Exemplar/Comparison (Inter...	0
Non-pertinent	0

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.

Generate Report

Close Case

Generate Report

Select and Configure Report Modules

Report Modules:

- ☒ HTML Report
- ☐ Excel Report
- ☐ Files - Text
- ☐ Save Tagged Hashes
- ☐ TSK Body File
- ☐ Google Earth KML
- ☐ STIX
- ☐ CASE-UCO
- ☐ Portable Case

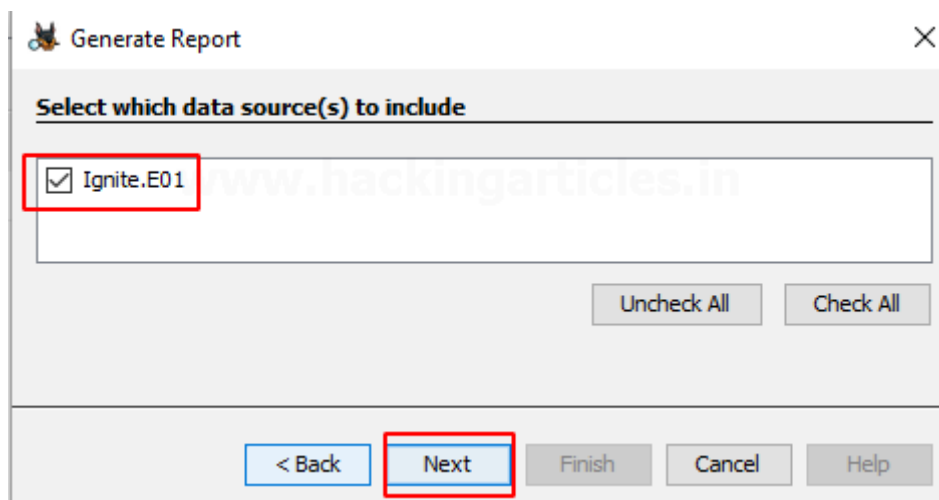
A report about results and tagged items in HTML format.

Header: Report

Footer: Details

< Back Next > Finish

Check the data source whose report needs to be generated.



Here we chose to create the report in HTML format.

Source Module Name	Report Name	Created Time	Report File Path
HTML Report		2020-11-28 15:42:58 IST	C:\Users\raj\Desktop\Ignite\Reports\Ignite HTML Rep

Report Generation Progress...









Complete

HTML Report : C:\Users\raj\Desktop\Ignite\Reports\Ignite HTML Report 11-28-2020-15-42-58\report.html

Complete

Kudos! Your Autopsy Forensic Report is ready!

Report Navigation

-  Case Summary
-  Keyword Hits (1026)
-  Metadata (6)
-  Recycle Bin (4)
-  Tagged Files (4)
-  Tagged Images (4)
-  Tagged Results (0)
-  Web Downloads (3)

Autopsy Forensic Report

HTML Report Generated on 2020/11/28 15:42:58

Case: Ignite
 Case Number: 001
 Number of data sources in case: 1
 Examiner: vishva

Image Information:

Ignite.E01

Timezone: America/Los_Angeles
 Path: C:\Users\raj\Desktop\Ignite.E01

Software Information:

Autopsy Version: 4.17.0
 Android Analyzer Module: 4.17.0
 Central Repository Module: 4.17.0
 Data Source Integrity Module: 4.17.0
 Drone Analyzer Module: 4.17.0

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.

```
root@Jeenali:~# autopsy
```

Autopsy Forensic Browser
<http://www.sleuthkit.org/autopsy/>
ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Wed Aug 12 20:37:30 2020
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

<http://localhost:9999/autopsy>

Keep this process running and use <ctrl-c> to exit

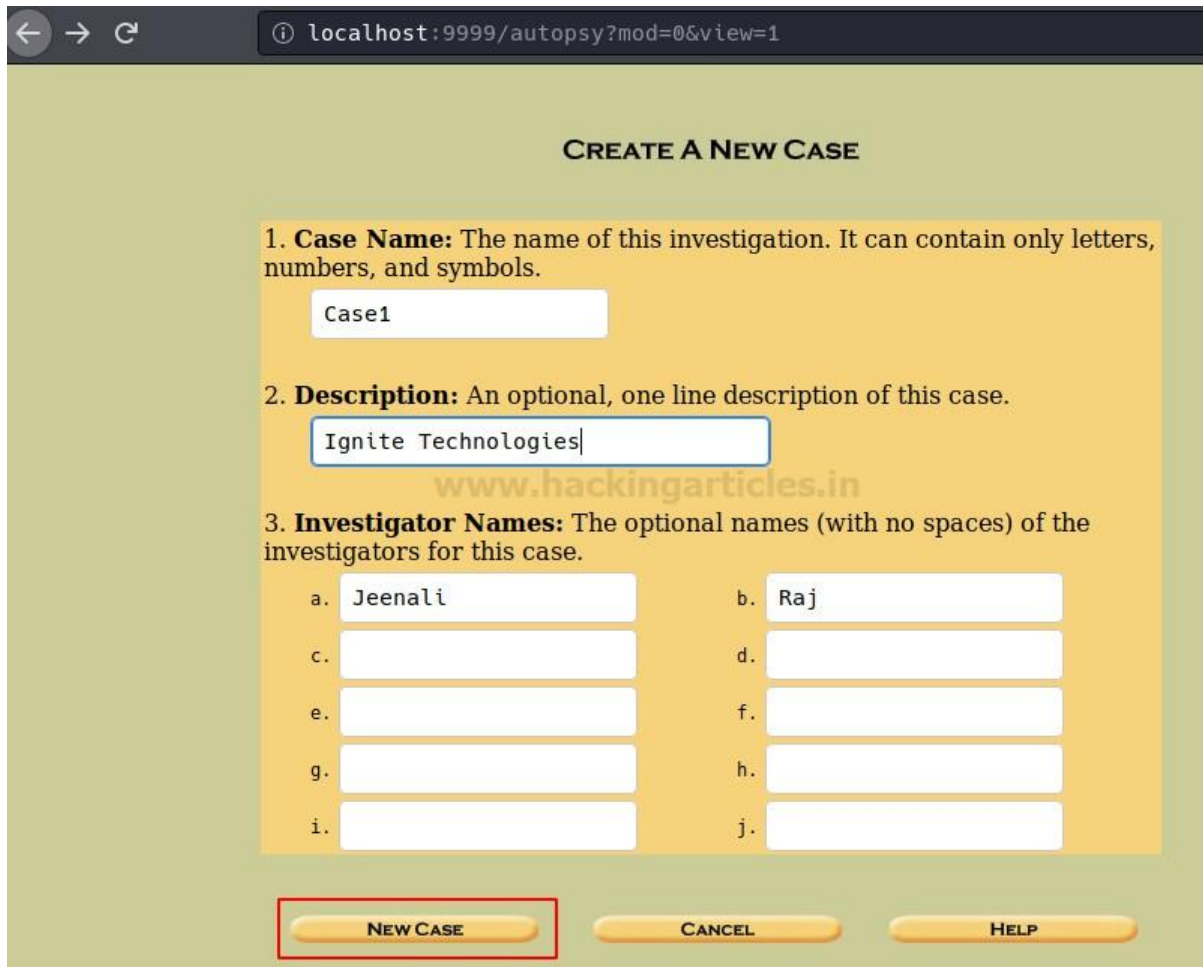
Now you will see three options on the home page.

- 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 screenshot shows a web browser window with the address bar displaying `localhost:9999/autopsy?mod=0&view=1`. The page title is "CREATE A NEW CASE". The form contains three main sections:

- 1. Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols. The input field contains "Case1".
- 2. Description:** An optional, one line description of this case. The input field contains "Ignite Technologies".
- 3. Investigator Names:** The optional names (with no spaces) of the investigators for this case. There are ten input fields labeled a. through j. Field 'a.' contains "Jeenali" and field 'b.' contains "Raj".

At the bottom of the form, there are three buttons: "NEW CASE" (highlighted with a red rectangle), "CANCEL", and "HELP". A watermark "www.hackingarticles.in" is visible in the background of the form area.

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'.

← → ↻ ⓘ localhost:9999/autopsy?mod=0&view=7&case=Jeenali&inv=Jeenali&

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

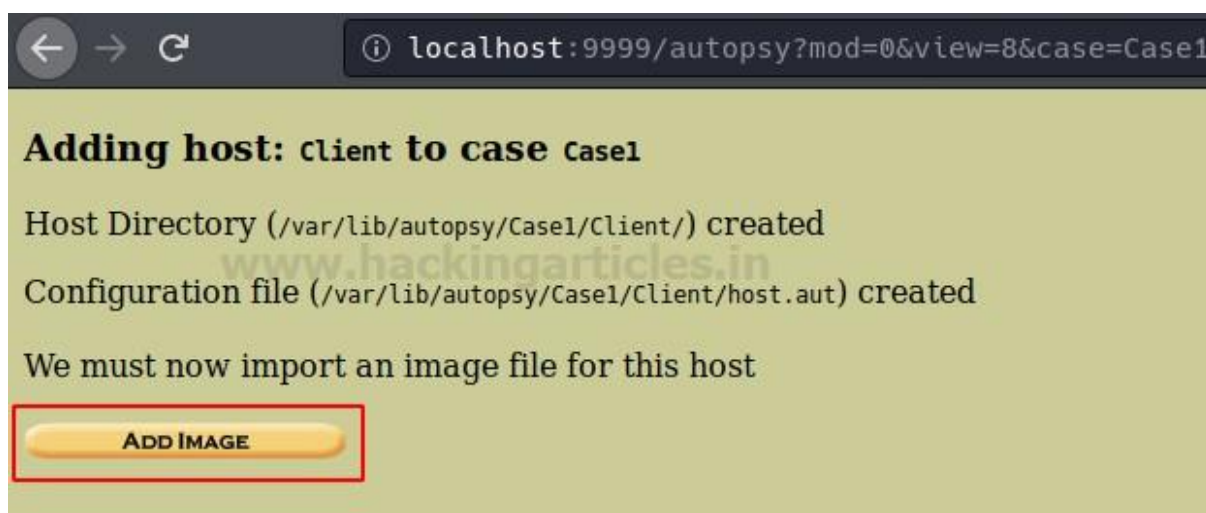
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

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'.

← → ↻ **localhost:9999/autopsy?mod=0&view=13&host=Client&case=Case1&inv** ...

Case: Case1
Host: Client

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

→ /home/jeenali/Desktop/image2*

2. Type
Please select if this image file is for a disk or a single partition.

→ ☒ Disk ☐ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☐ Symlink ☒ Copy → ☐ Move

NEXT

CANCEL **HELP**

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

← → ↻ **localhost:9999/autopsy?mod=0&view=14&host=Client&case=Case1&inv** ...

Split Image Confirmation

The following images will be added to the case.
If this is not the correct order, then you should change the naming convention.
Press the Next button at the bottom of the page if this is correct.

→ 0 /home/jeenali/Desktop/image2.e01

NEXT **CANCEL**

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.

localhost:9999/autopsy?case=Case1&host=Client&inv=Jeenali&mod=@

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: File System Type:

Partition 2 (Type: EFI system partition)

Add to case? ☒

Sector Range: 1085440 to 1288191

Mount Point: File System Type:

Partition 3 (Type: Microsoft reserved partition)

Add to case? ☒

Sector Range: 1288192 to 1320959

Mount Point: File System Type:

Partition 4 (Type: Basic data partition)

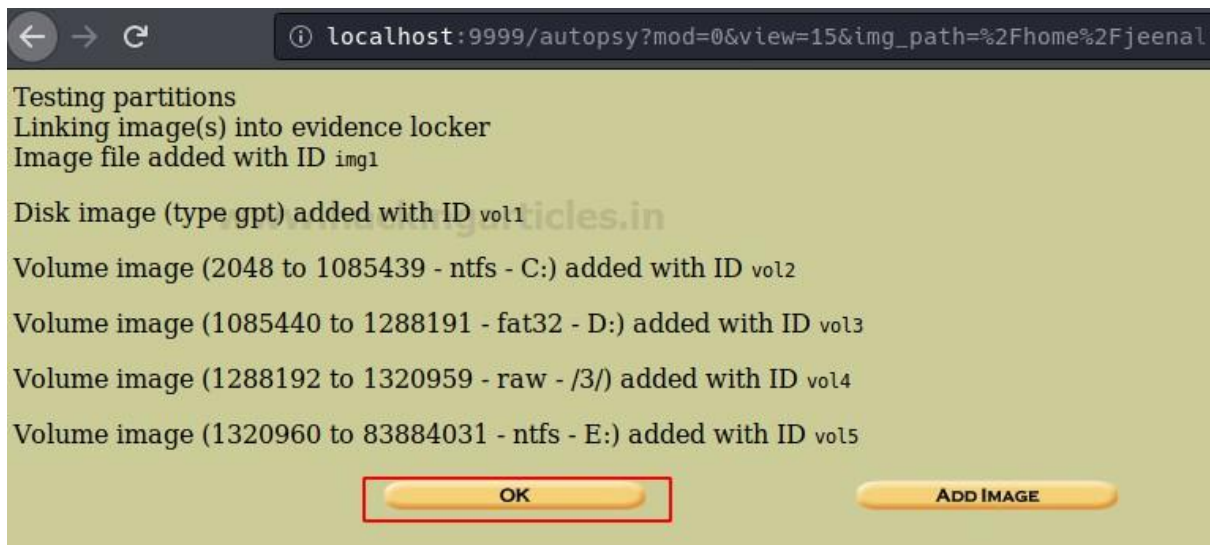
Add to case? ☒

Sector Range: 1320960 to 83884031

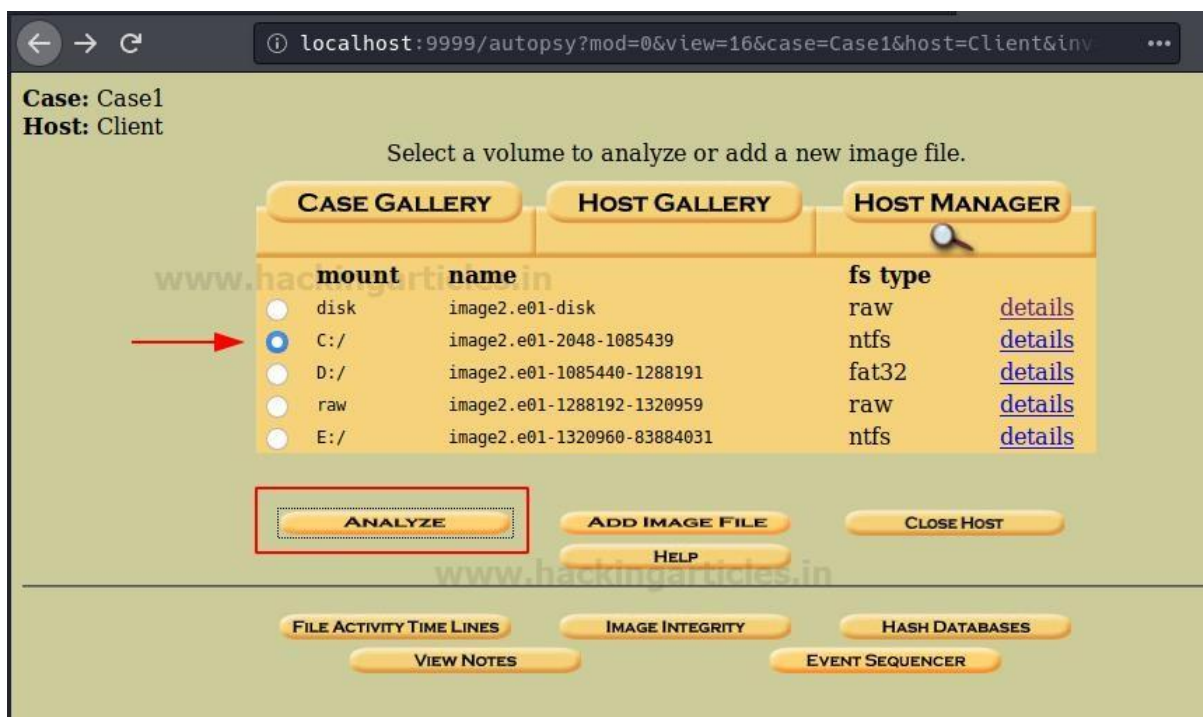
Mount Point: File System Type:

ADD **CANCEL** **HELP**

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

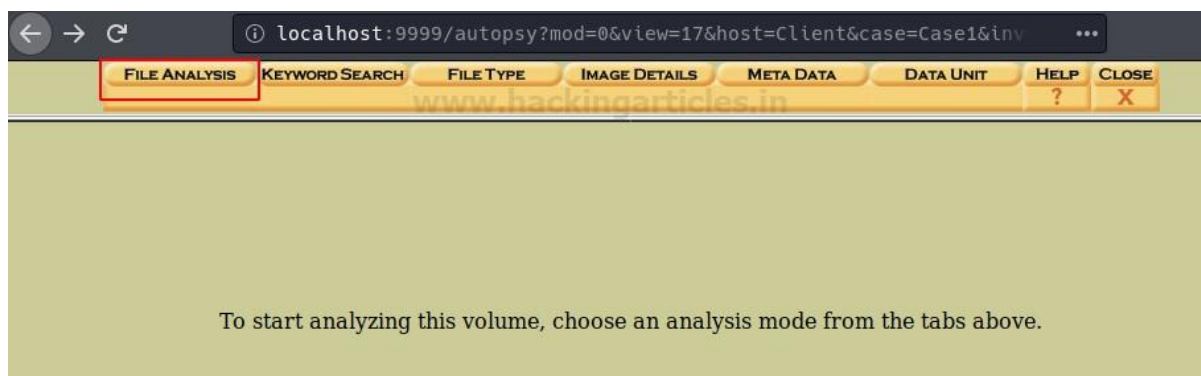


Now select the volume to be analyzed and click on 'Analyze'.

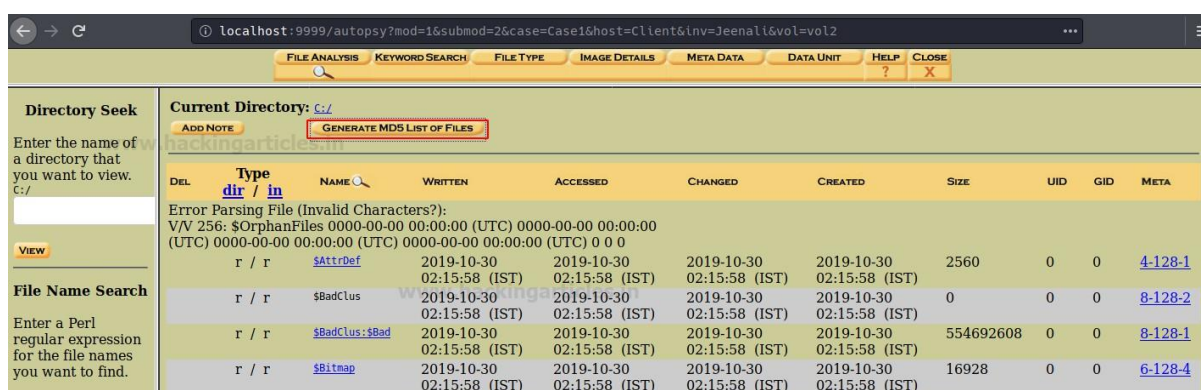


File Analysis-File and Metadata Analysis

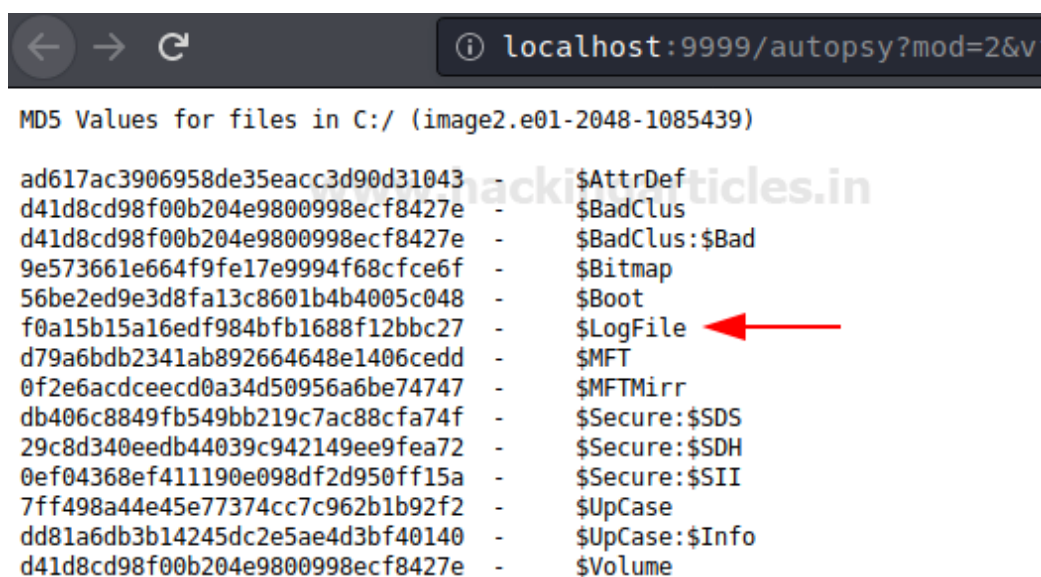
Now, it will ask you to choose the mode of analysis that you want to conduct and here we are conducting an analysis of the file, therefore click on 'File Analysis'.



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) 0 0 0 (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.

The screenshot shows the 'FILE ANALYSIS' tab of a tool. On the left, 'MFT Entry Number:' is set to '2-128-1'. The main pane displays details for this entry:

Accessed: 2019-10-30 02:15:58.098799200 (IST)

\$FILE_NAME Attribute Values:
 Flags: Hidden, System
 Name: \$LogFile
 Parent MFT Entry: 5 Sequence: 5
 Allocated Size: 4374528 Actual Size: 4374528
 Created: 2019-10-30 02:15:58.098799200 (IST)
 File Modified: 2019-10-30 02:15:58.098799200 (IST)
 MFT Modified: 2019-10-30 02:15:58.098799200 (IST)
 Accessed: 2019-10-30 02:15:58.098799200 (IST)

Attributes:
 \$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
 \$FILE_NAME (48-2) Name: N/A Resident size: 82
 \$DATA (128-1) Name: N/A Non-Resident size: 4374528 init_size: 4374528

A list of cluster numbers is shown, with 44067 highlighted in red. The list includes: 44067, 44068, 44069, 44070, 44071, 44072, 44073, 44074, 44075, 44076, 44077, 44078, 44079, 44080, 44081, 44082, 44083, 44084, 44085, 44086, 44087, 44088, 44089, 44090, 44091, 44092, 44093, 44094, 44095, 44096, 44097, 44098, 44099, 44100, 44101, 44102, 44103, 44104, 44105, 44106, 44107, 44108, 44109, 44110, 44111, 44112, 44113, 44114, 44115, 44116, 44117, 44118, 44119, 44120, 44121, 44122, 44123, 44124, 44125, 44126, 44127, 44128, 44129, 44130, 44131, 44132, 44133, 44134, 44135, 44136, 44137, 44138, 44139, 44140, 44141, 44142, 44143, 44144, 44145, 44146, 44147, 44148, 44149, 44150, 44151, 44152, 44153, 44154, 44155, 44156, 44157, 44158, 44159, 44160, 44161, 44162, 44163, 44164, 44165, 44166, 44167, 44168, 44169, 44170, 44171, 44172, 44173, 44174, 44175, 44176, 44177, 44178, 44179, 44180, 44181, 44182, 44183, 44184, 44185, 44186, 44187, 44188, 44189, 44190, 44191, 44192, 44193, 44194, 44195, 44196, 44197, 44198, 44199, 44200, 44201, 44202.

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

The screenshot shows the 'FILE ANALYSIS' tab. On the left, 'Cluster Number:' is set to '44067'. The main pane displays details for this cluster:

Cluster: 44067
 Status: Allocated
[Find Meta Data Address](#)

ASCII Contents of Cluster 44067 in image2.e01-2048-1085439

A list of cluster numbers is shown, with 44067 highlighted in red. The list includes: 44067, 44068, 44069, 44070, 44071, 44072, 44073, 44074, 44075, 44076, 44077, 44078, 44079, 44080, 44081, 44082, 44083, 44084, 44085, 44086, 44087, 44088, 44089, 44090, 44091, 44092, 44093, 44094, 44095, 44096, 44097, 44098, 44099, 44100, 44101, 44102, 44103, 44104, 44105, 44106, 44107, 44108, 44109, 44110, 44111, 44112, 44113, 44114, 44115, 44116, 44117, 44118, 44119, 44120, 44121, 44122, 44123, 44124, 44125, 44126, 44127, 44128, 44129, 44130, 44131, 44132, 44133, 44134, 44135, 44136, 44137, 44138, 44139, 44140, 44141, 44142, 44143, 44144, 44145, 44146, 44147, 44148, 44149, 44150, 44151, 44152, 44153, 44154, 44155, 44156, 44157, 44158, 44159, 44160, 44161, 44162, 44163, 44164, 44165, 44166, 44167, 44168, 44169, 44170, 44171, 44172, 44173, 44174, 44175, 44176, 44177, 44178, 44179, 44180, 44181, 44182, 44183, 44184, 44185, 44186, 44187, 44188, 44189, 44190, 44191, 44192, 44193, 44194, 44195, 44196, 44197, 44198, 44199, 44200, 44201, 44202.

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

Directory Seek

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

File Name Search

Enter a Perl regular expression

Current Directory: [C:/](#)

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type	NAME	WRITTEN	ACCESSED	CHAP
	dir / in				
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) 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)
r / r	\$BadClus		2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)
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)

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'.

Sort Files by Type

[View Sorted Files](#)

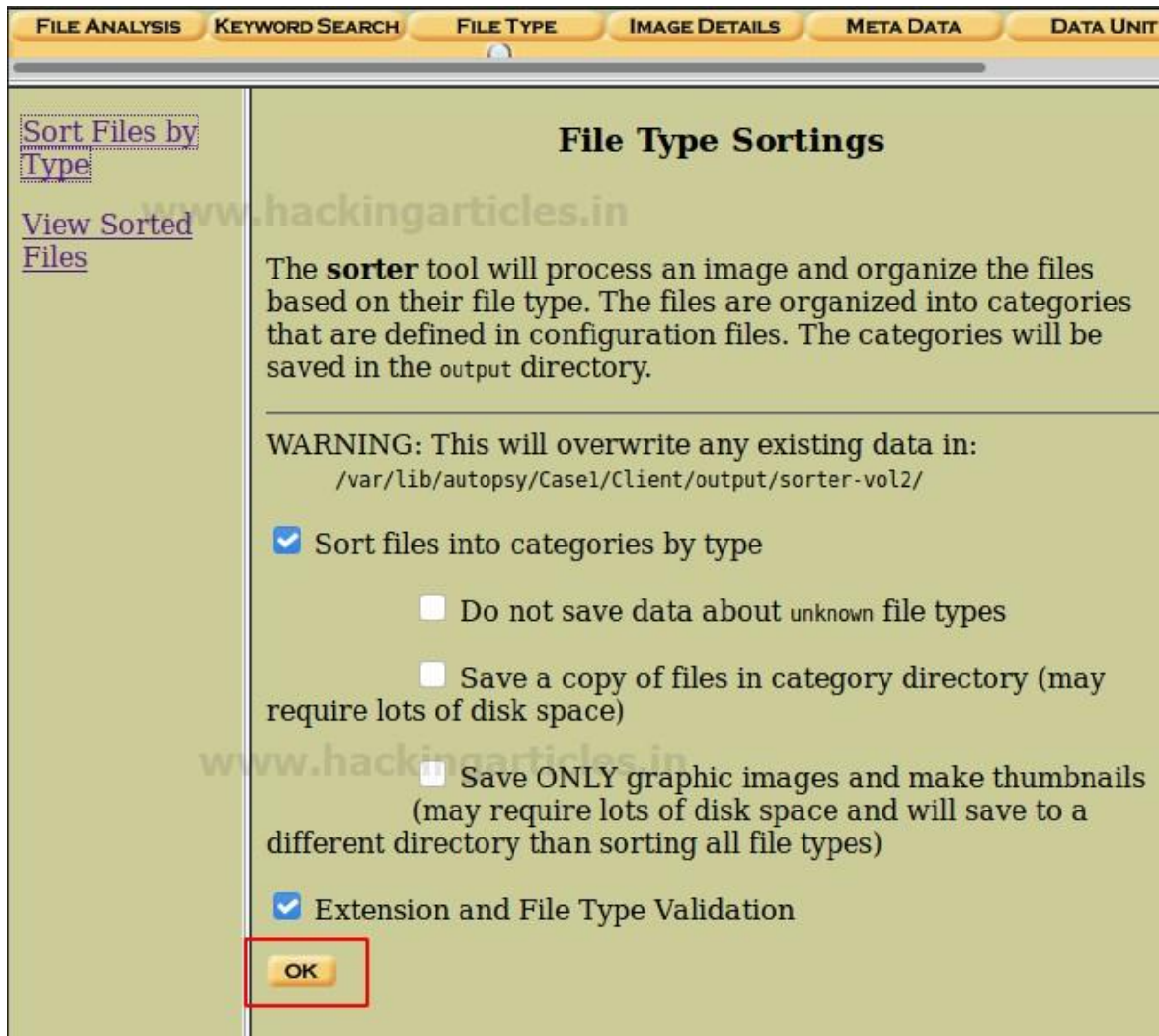
File Type Sorting

In this mode, Autopsy will examine allocated and unallocated files and sort them into categories and verify the extension.

This allows you to find a file based on its type and find "hidden" files.

WARNING: This can be a time intensive process.

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



The screenshot shows a web-based interface for file analysis. At the top, there is a navigation bar with tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, and DATA UNIT. The 'FILE TYPE' tab is currently selected. On the left side, there is a sidebar with two links: 'Sort Files by Type' and 'View Sorted Files'. The main content area is titled 'File Type Sortings'. It contains a paragraph explaining the 'sorter' tool, a warning message about overwriting data, and several configuration options with checkboxes. The 'OK' button at the bottom is highlighted with a red rectangle.

File Type Sortings

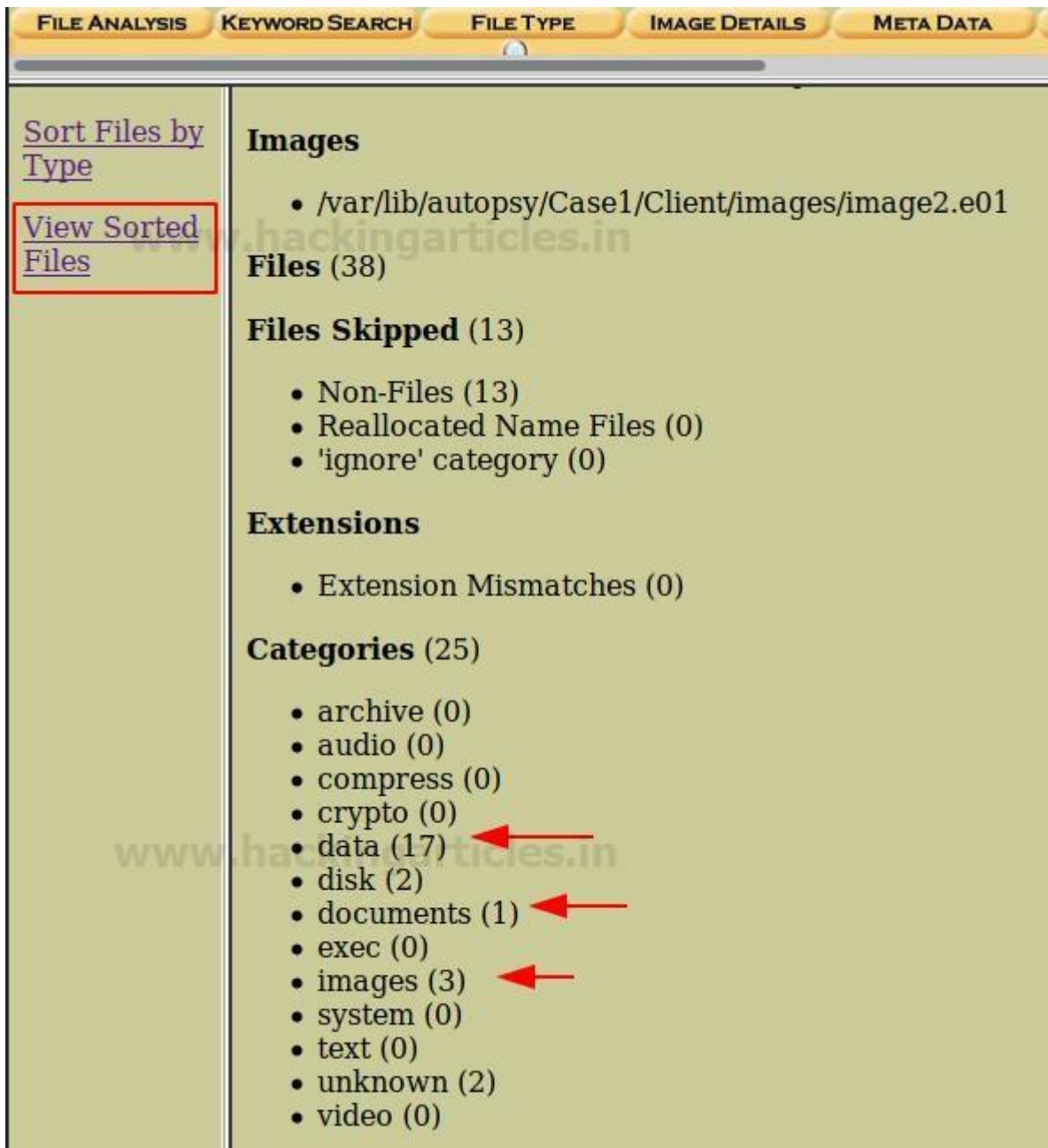
The **sorter** tool will process an image and organize the files based on their file type. The files are organized into categories that are defined in configuration files. The categories will be saved in the output directory.

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

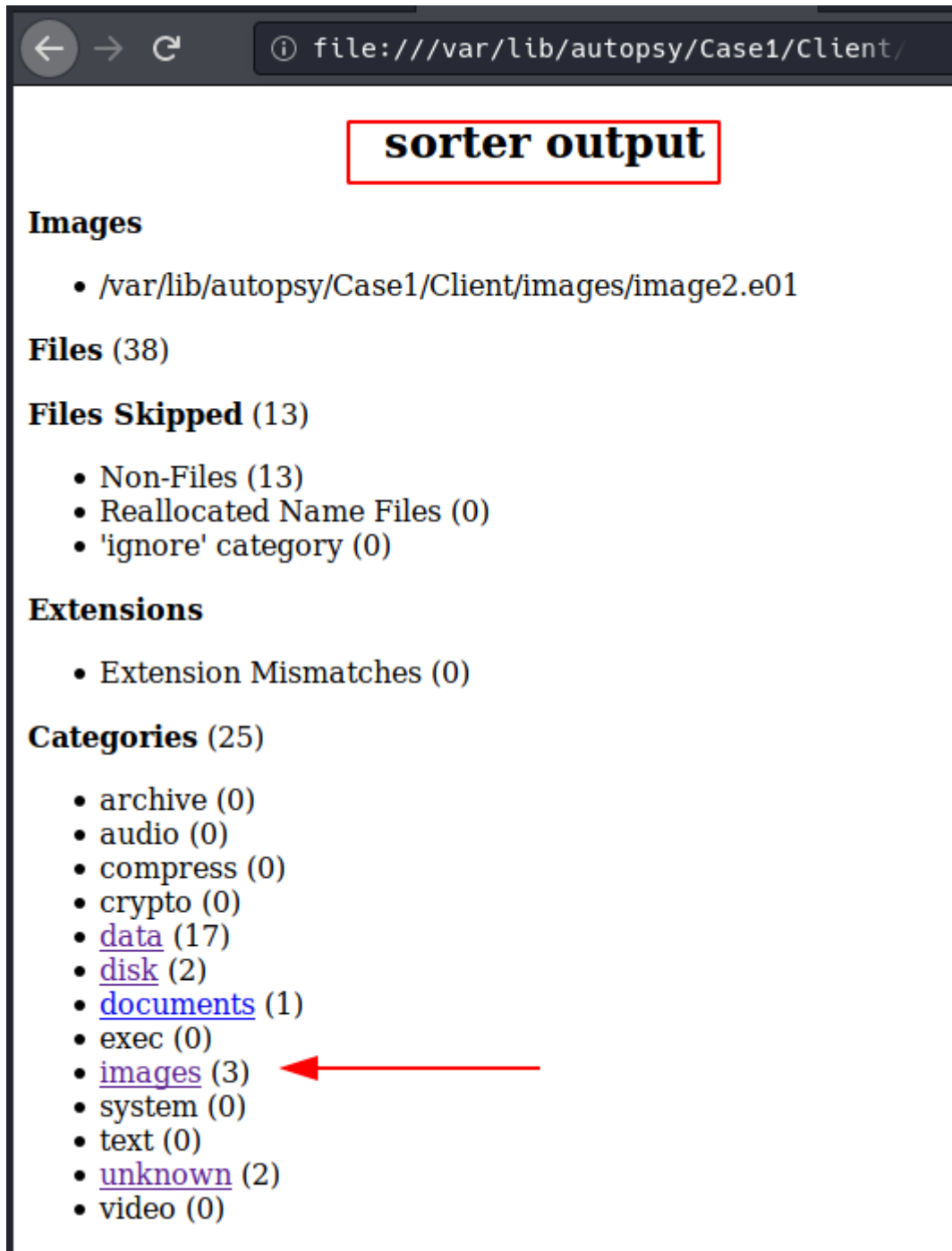
- ☒ Sort files into categories by type
 - ☐ Do not save data about unknown file types
 - ☐ Save a copy of files in category directory (may require lots of disk space)
 - ☐ Save ONLY graphic images and make thumbnails (may require lots of disk space and will save to a different directory than sorting 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.



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.

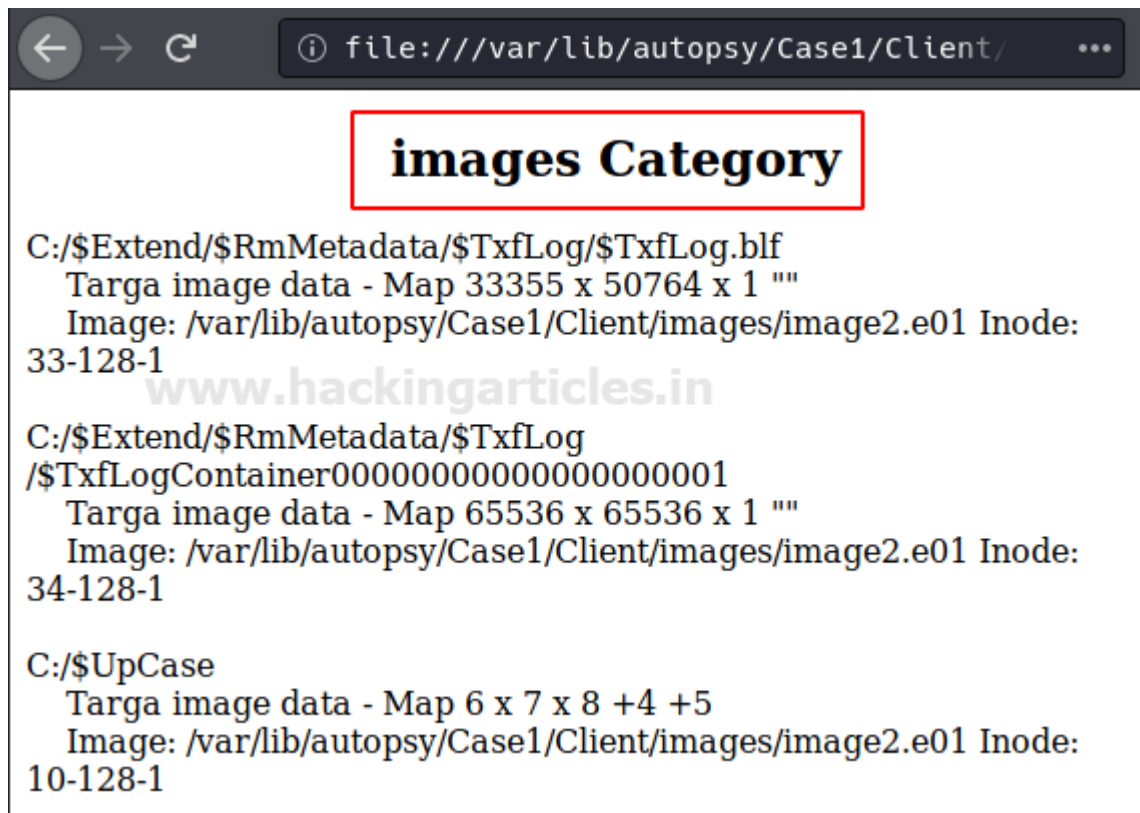
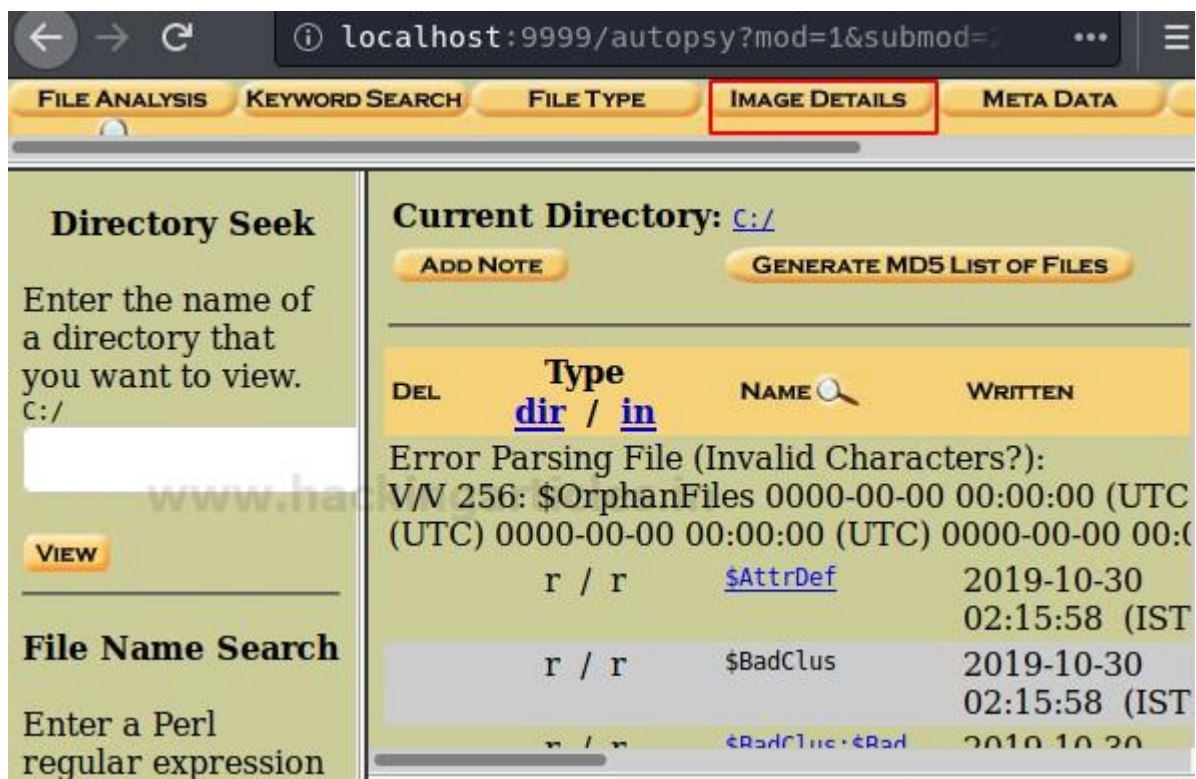
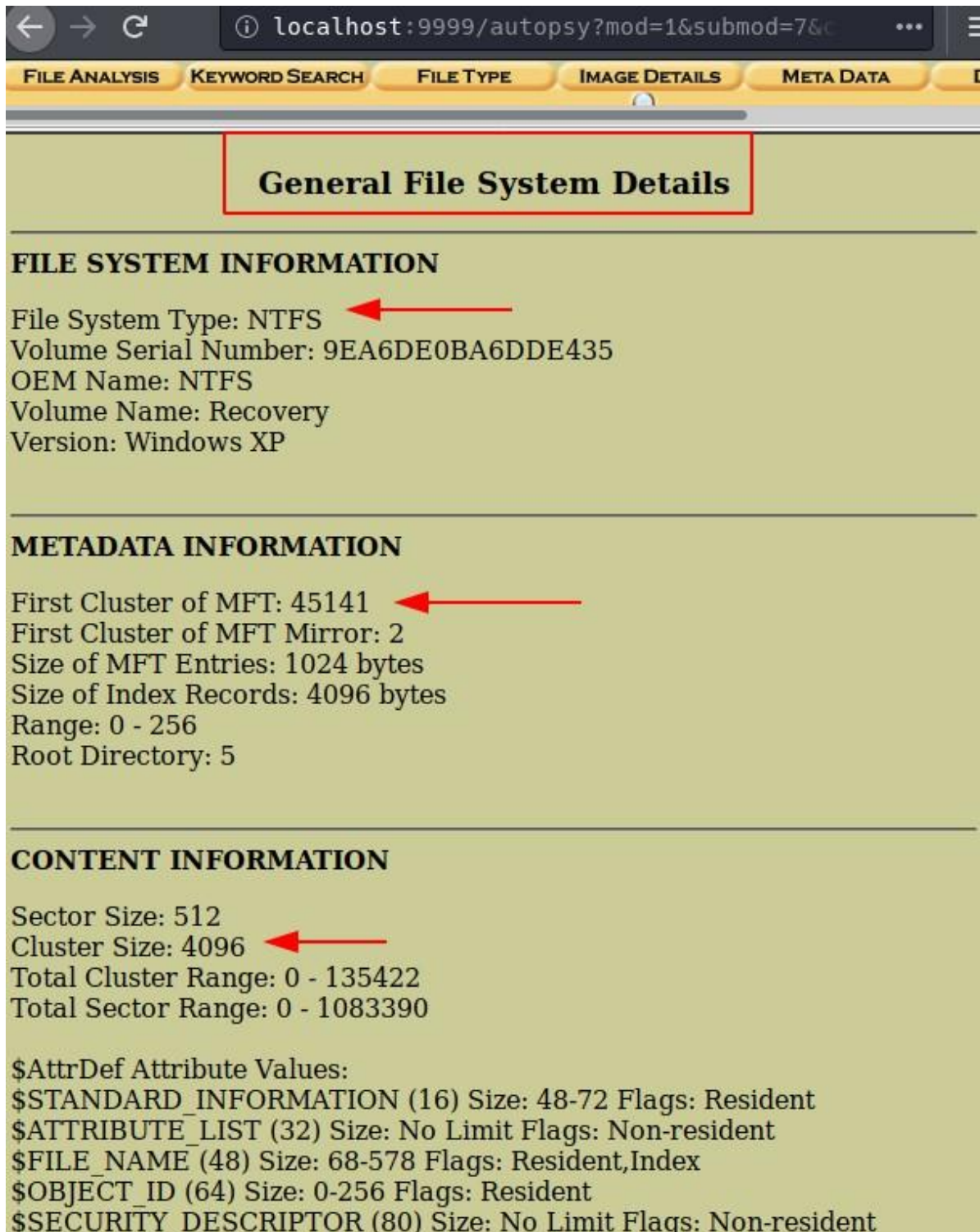


Image Details

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, the first cluster of MFT, cluster size etc.



The screenshot shows the Autopsy web interface at localhost:9999/autopsy?mod=1&submod=7&c. The 'FILE ANALYSIS' tab is selected. A red box highlights the 'General File System Details' section. Below this, three sections are visible: 'FILE SYSTEM INFORMATION', 'METADATA INFORMATION', and 'CONTENT INFORMATION'. Red arrows point to specific values: 'File System Type: NTFS', 'First Cluster of MFT: 45141', and 'Cluster Size: 4096'.

General File System Details

FILE SYSTEM INFORMATION

File System Type: NTFS
Volume Serial Number: 9EA6DE0BA6DDE435
OEM Name: NTFS
Volume Name: Recovery
Version: Windows XP

METADATA INFORMATION

First Cluster of MFT: 45141
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

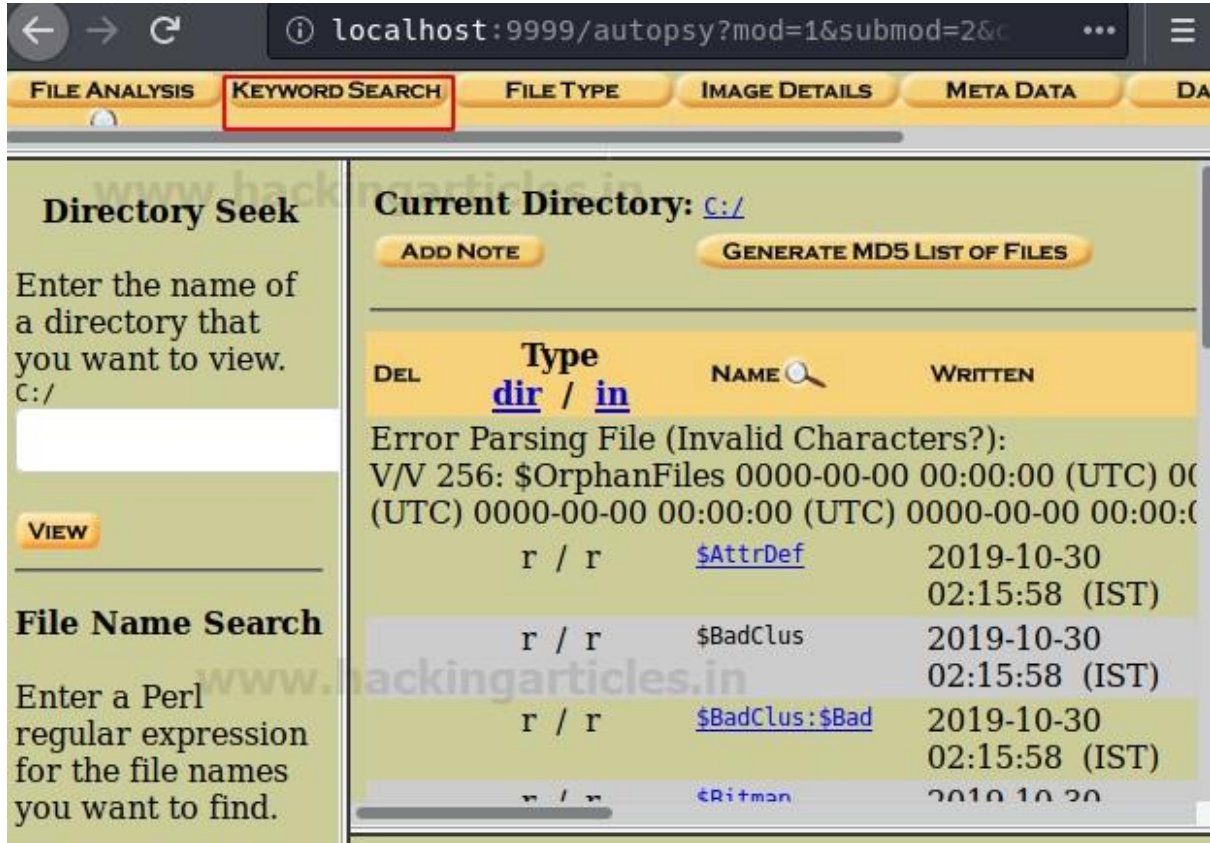
CONTENT INFORMATION

Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 135422
Total Sector Range: 0 - 1083390

\$AttrDef Attribute Values:
\$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
\$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
\$FILE_NAME (48) Size: 68-578 Flags: Resident, Index
\$OBJECT_ID (64) Size: 0-256 Flags: Resident
\$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident

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.



Directory Seek

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

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

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) 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC)	
	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 02:15:58 (IST)
	r / r	\$Ritman	2019-10-30 02:15:58 (IST)

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

The screenshot shows the Autopsy web interface at `localhost:9999/autopsy?mod=1&submod=4&c`. The 'KEYWORD SEARCH' tab is selected. The main heading is 'Keyword Search of Allocated and Unallocated Space'. Below it, a prompt says 'Enter the keyword string or expression to search for:'. A text input field contains 'Jeenali', with a red arrow pointing to it. Below the input field are four checkboxes: 'ASCII' (checked), 'Unicode' (checked), 'Case Insensitive' (unchecked), and 'grep Regular Expression' (unchecked). A red rectangle highlights the 'SEARCH' button. Below the buttons are two orange buttons: 'EXTRACT STRINGS' and 'EXTRACT UNALLOCATED'. A link 'Regular Expression Cheat Sheet' is visible. At the bottom, a note states: 'NOTE: The keyword search runs grep on the image. A list of what will and what will not be found is available [here](#).'

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.