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.

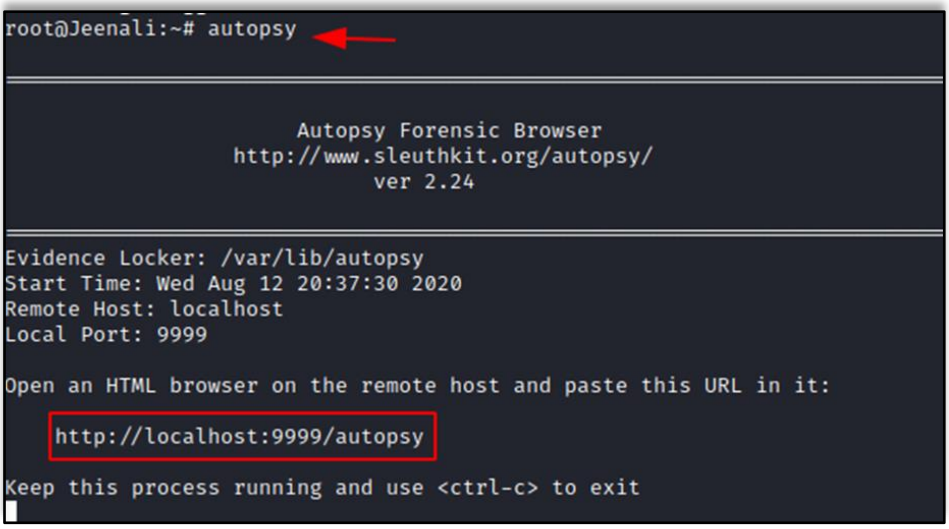
Autopsy Forensic Browser is a built-in application in Kali Linux operating system, so let’s power on the Kali in a Virtual Machine.

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.

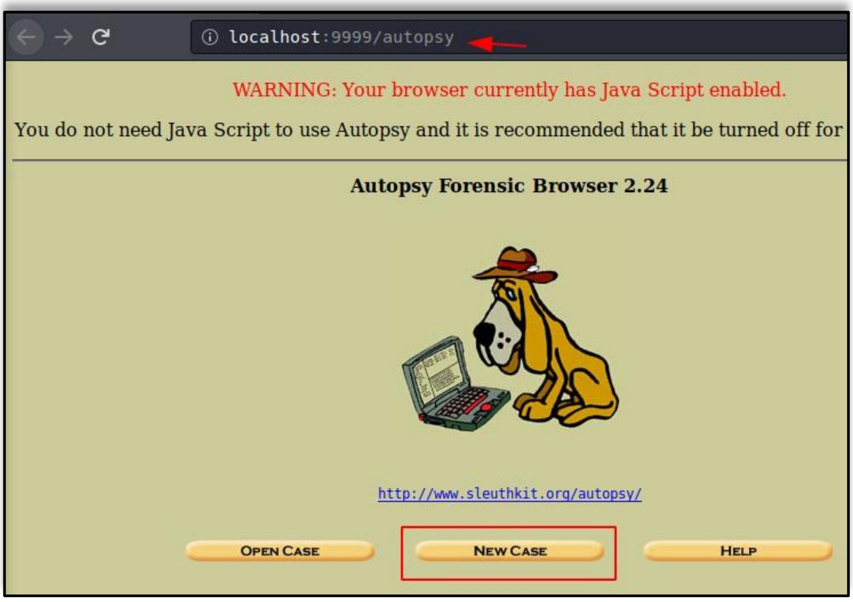


```
root@Jeenali:~# autopsy

============================================================================

                         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 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.



localhost:9999/autopsy

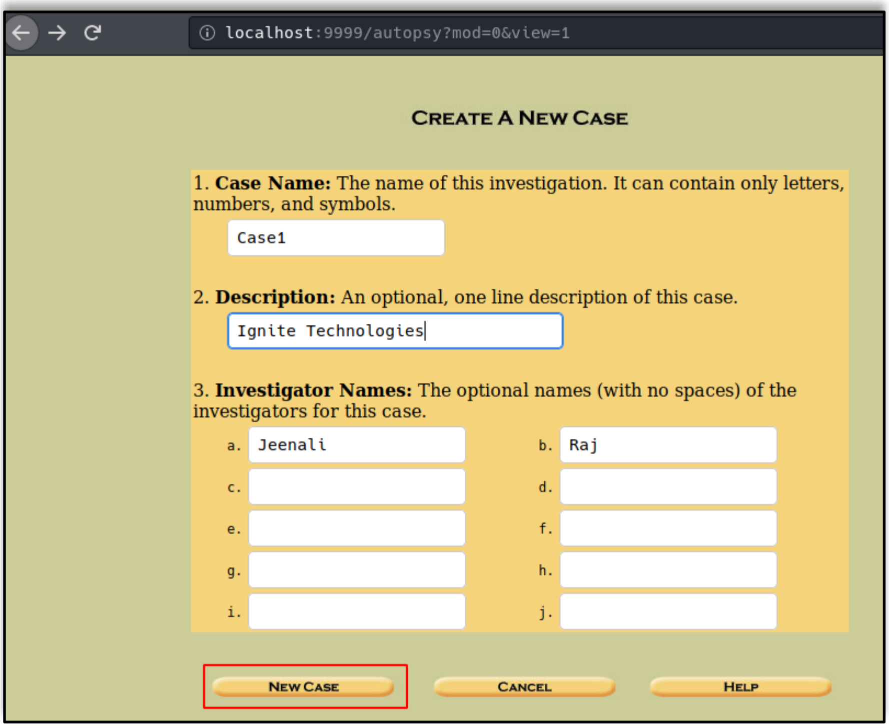
WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

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'.**



localhost:9999/autopsy?mod=0&view=1

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Case1

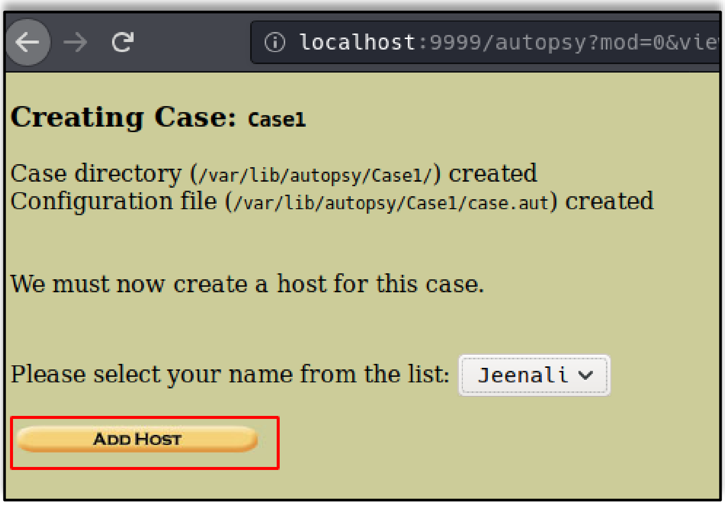
2. **Description:** An optional, one line description of this case.

Ignite Technologies

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Jeenali b. Raj

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'.



localhost:9999/autopsy?mod=0&vie

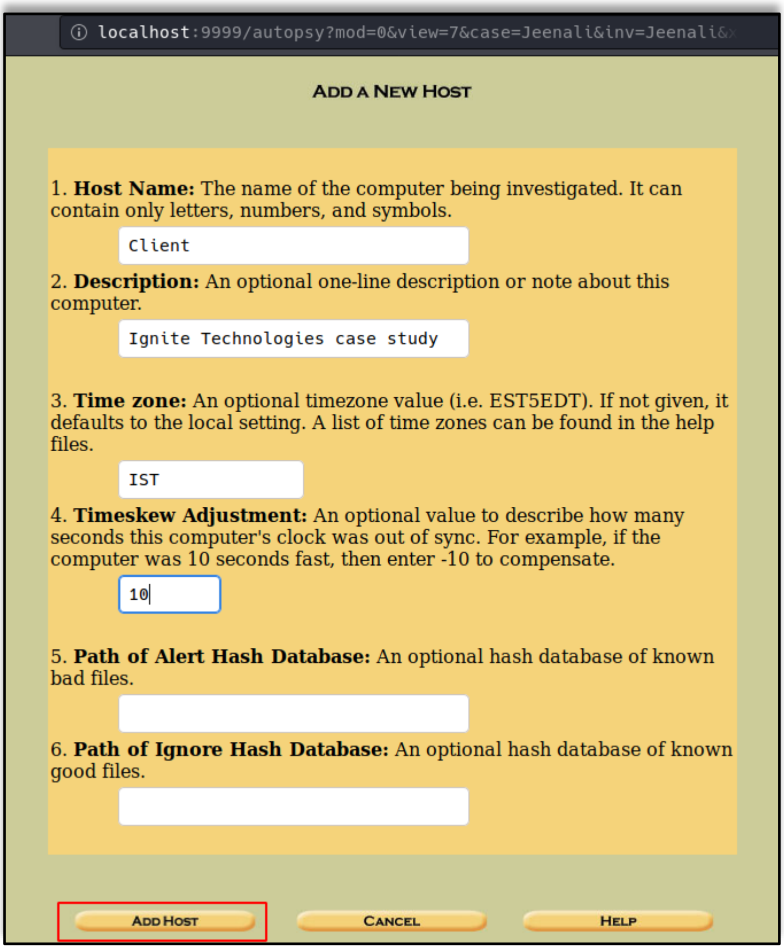
Creating Case: Case1

Case directory (/var/lib/autopsy/Case1/) created
Configuration file (/var/lib/autopsy/Case1/case.aut) created

We must now create a host for this case.

Please select your name from the list: Jeenali

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'**.



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.

Client

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

Ignite Technologies case study

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.

IST

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.

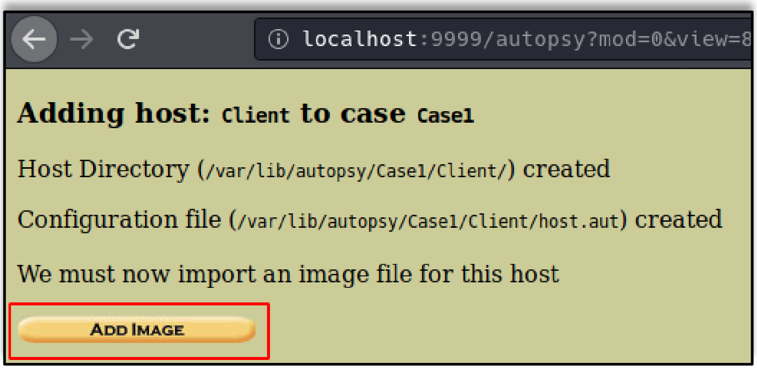
10

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.

Add Image File

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



localhost:9999/autopsy?mod=0&view=8

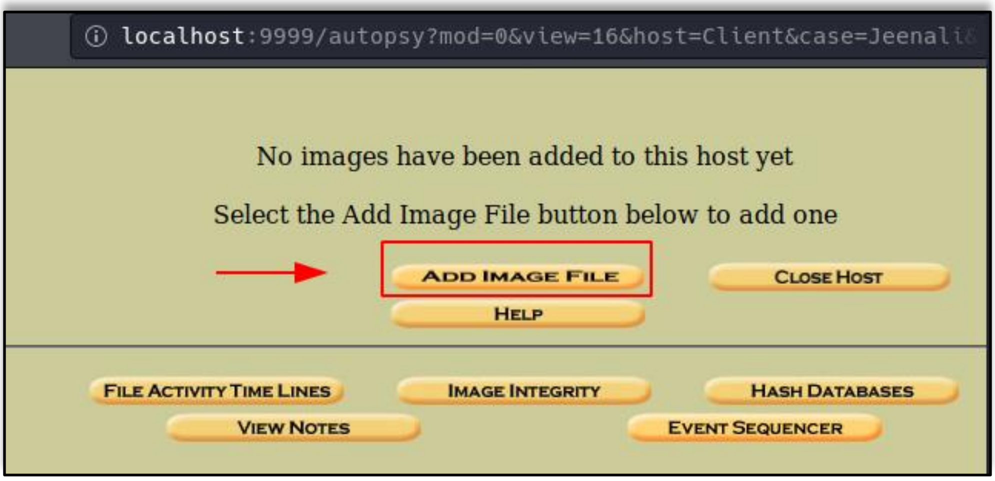
Adding host: Client to case Case1

Host Directory (/var/lib/autopsy/Case1/Client/) created

Configuration file (/var/lib/autopsy/Case1/Client/host.aut) created

We must now import an image file for this host

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.

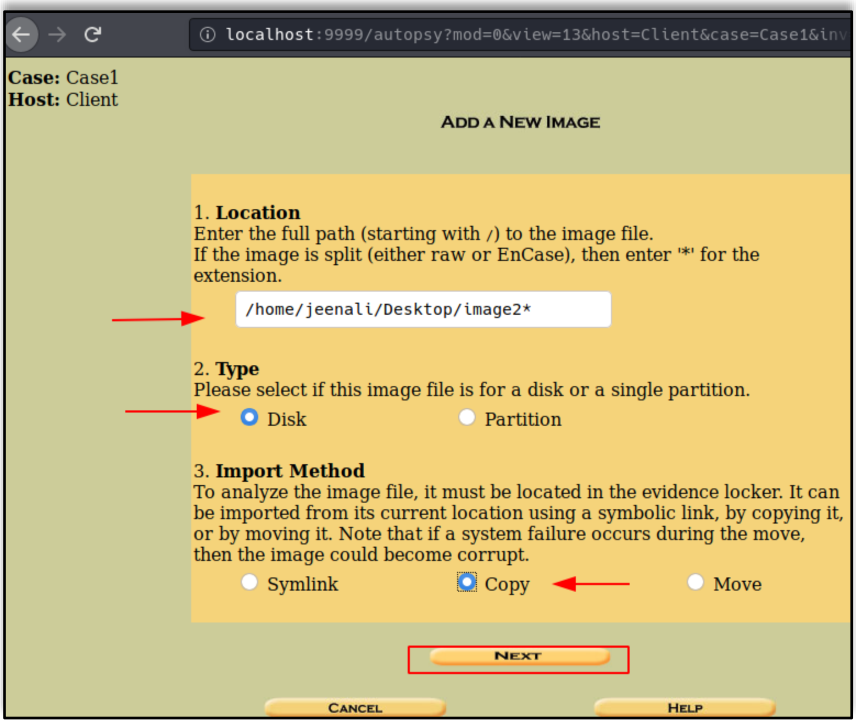


localhost:9999/autopsy?mod=0&view=16&host=Client&case=Jeenali

No images have been added to this host yet

Select the Add Image File button below to add one

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

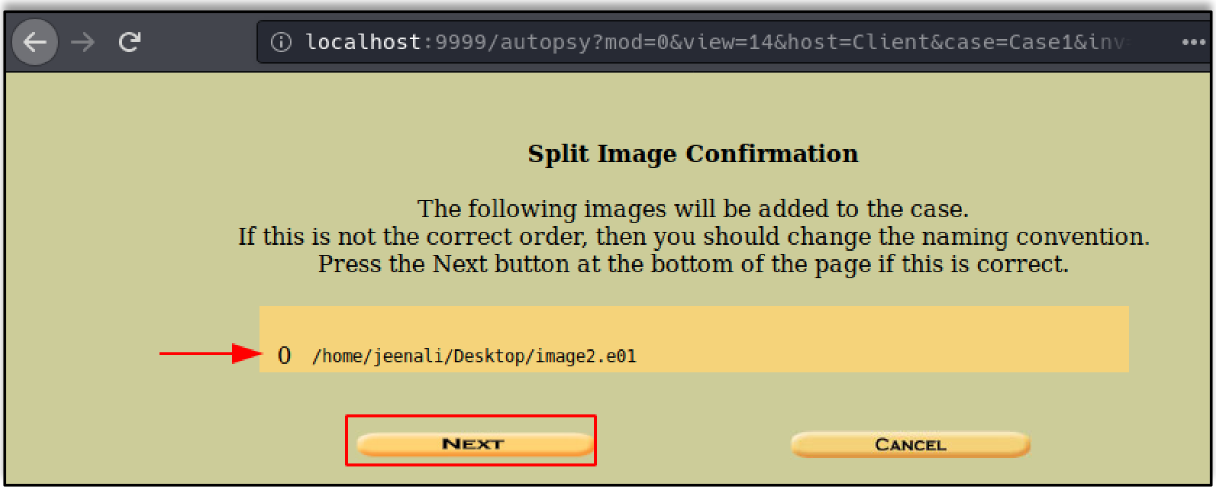
1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/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

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



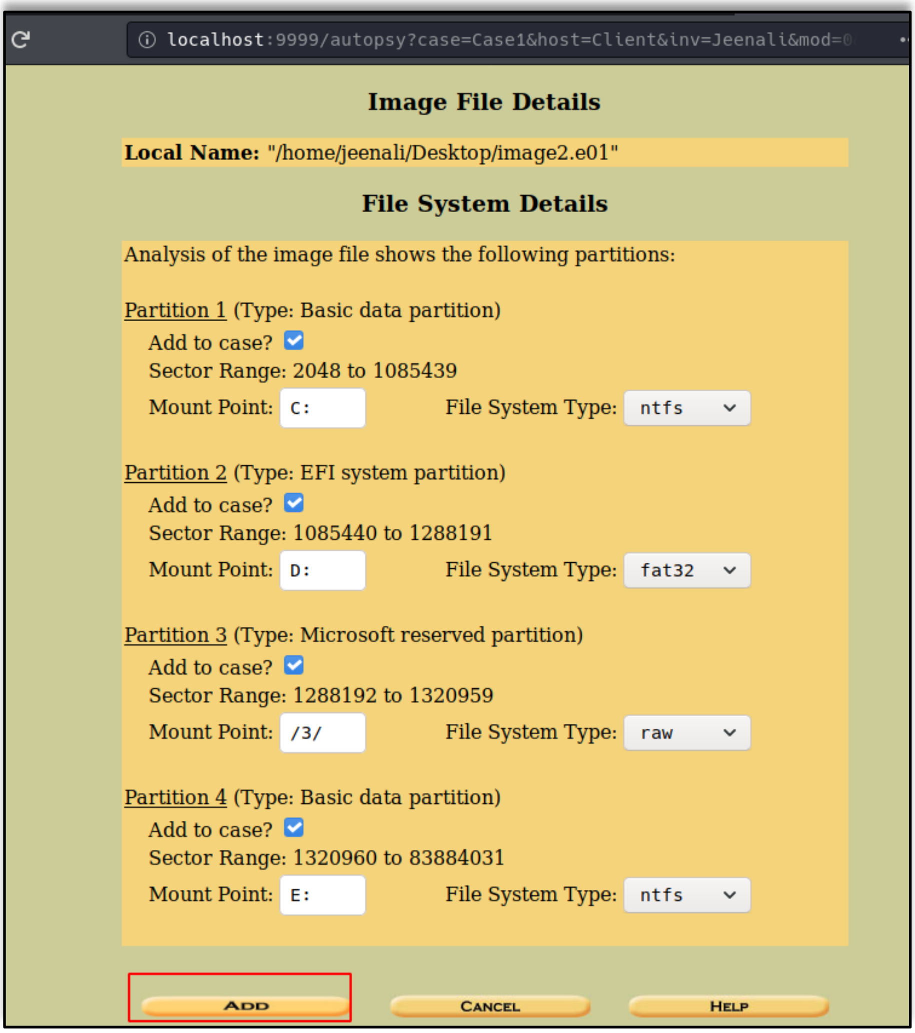
localhost:9999/autopsy?mod=0&view=14&host=Client&case=Case1&inv

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

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=0

Image File Details

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

File System Details

Analysis of the image file shows the following partitions:

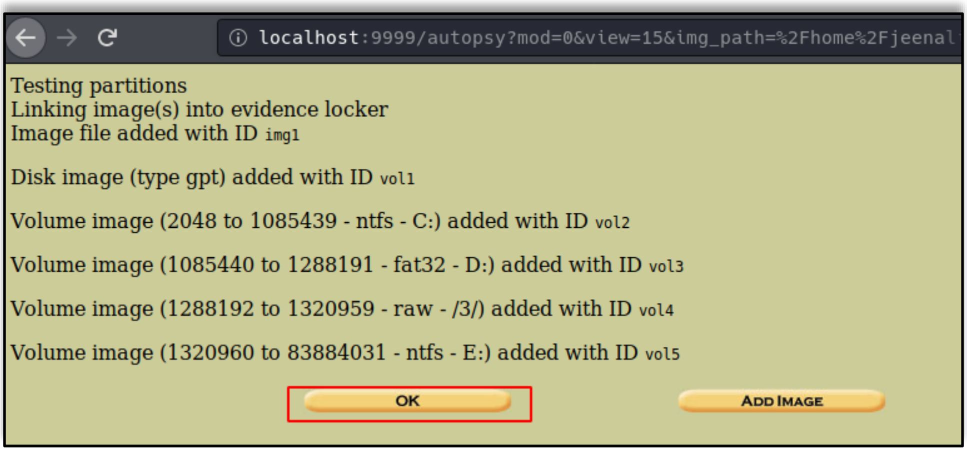
Partition 1 (Type: Basic data partition)
Add to case? ☑
Sector Range: 2048 to 1085439
Mount Point: C: File System Type: ntfs

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

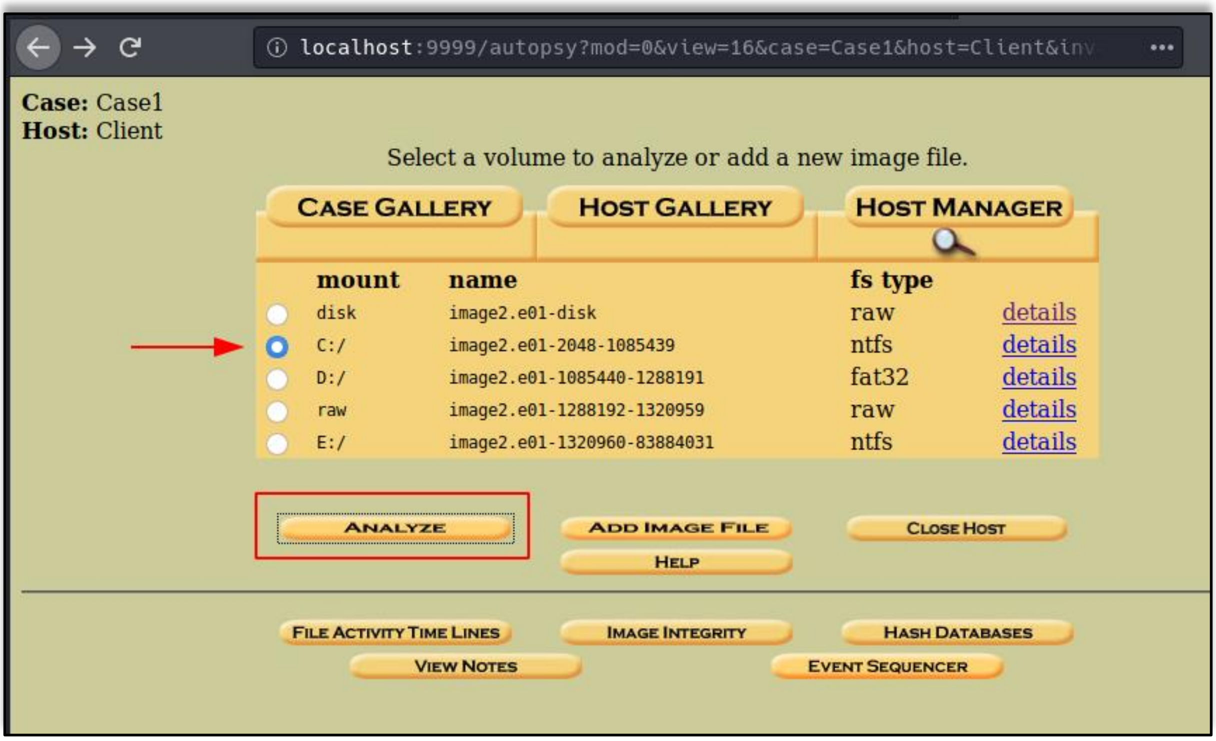
Now the Autopsy will test the partitions and links them to the evidence locker, then click on 'Ok' to proceed.



localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fjeenal

```
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Disk image (type gpt) added with ID vol1

Volume image (2048 to 1085439 - ntfs - C:) added with ID vol2

Volume image (1085440 to 1288191 - fat32 - D:) added with ID vol3

Volume image (1288192 to 1320959 - raw - /3/) added with ID vol4

Volume image (1320960 to 83884031 - ntfs - E:) added with ID vol5
```

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



localhost:9999/autopsy?mod=0&view=16&case=Case1&host=Client&inv

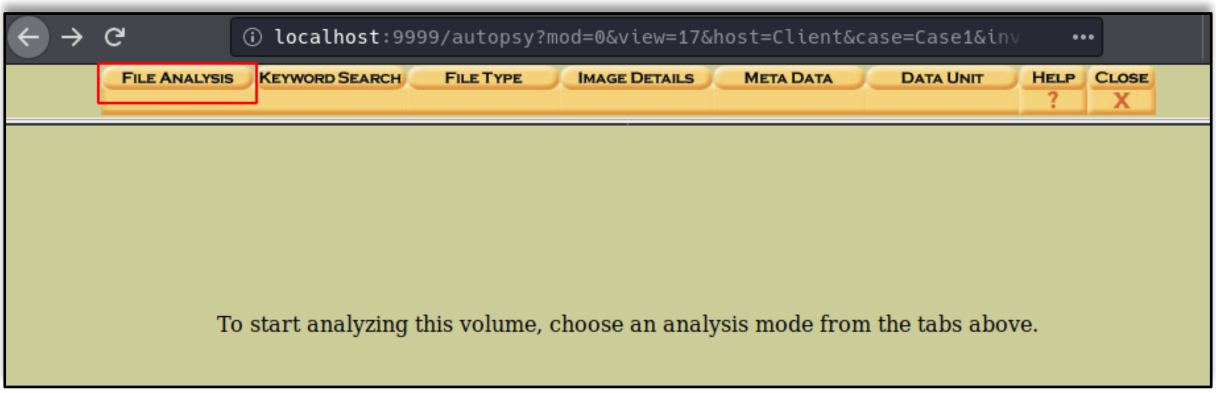
Case: Case1
Host: Client

Select a volume to analyze or add a new image file.

	mount	name	fs type	
○	disk	image2.e01-disk	raw	details
●	C:/	image2.e01-2048-1085439	ntfs	details
○	D:/	image2.e01-1085440-1288191	fat32	details
○	raw	image2.e01-1288192-1320959	raw	details
○	E:/	image2.e01-1320960-83884031	ntfs	details

File Analysis

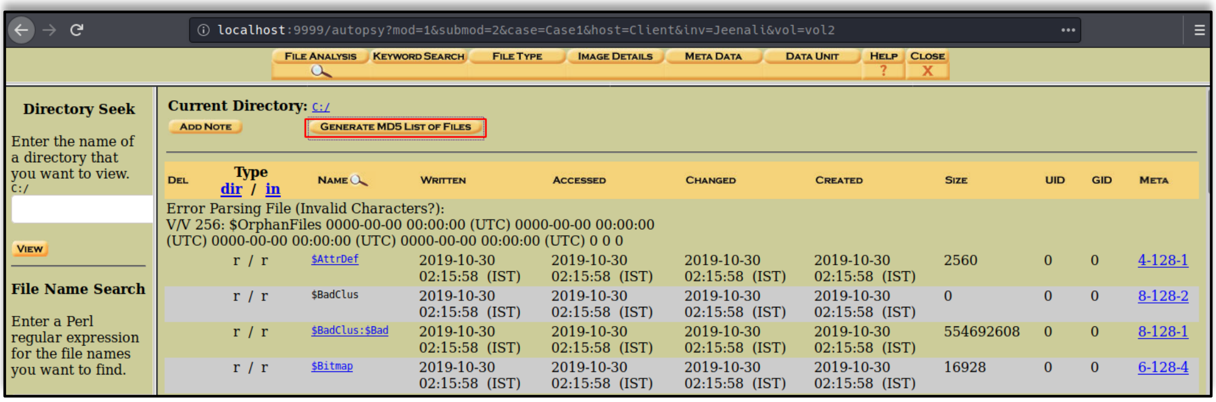
Now, it will ask you to choose the mode of analysis that you want to conduct and here we are conducting analysis of file, therefore click on 'File Analysis'.



localhost:9999/autopsy?mod=0&view=17&host=Client&case=Case1&inv

To start analyzing this volume, choose an analysis mode from the tabs above.

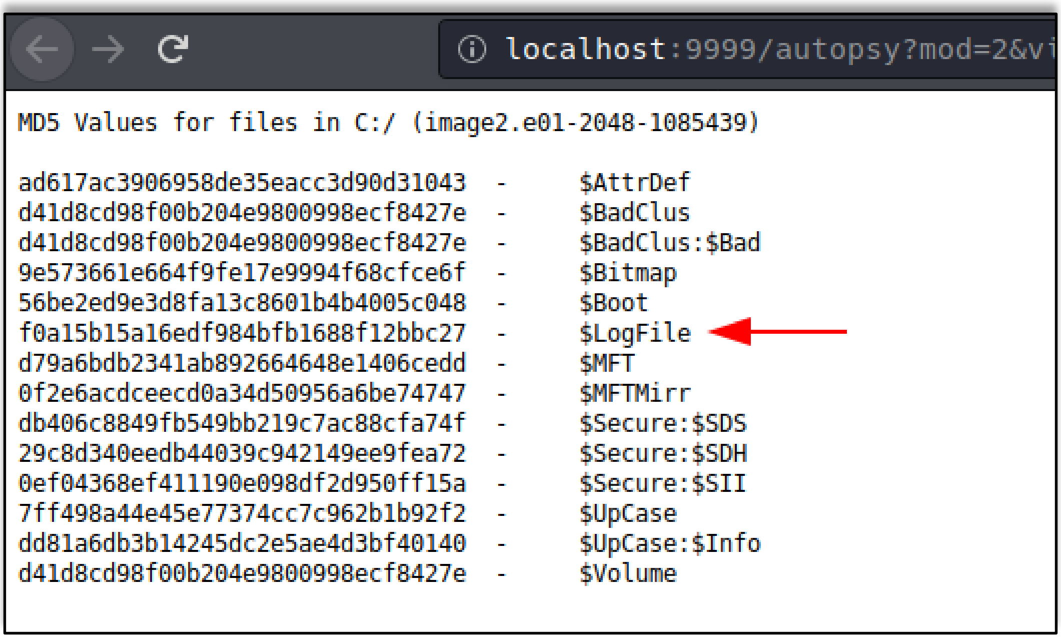
Now files will appear, which will give you the list of files and directories that are inside in this volume. From here you can analyze the content of the required image file and conduct the type of investigation you prefer. You can first generate a MD5 hash list of all the files present in this volume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


localhost:9999/autopsy?mod=1&submod=2&case=Case1&host=Client&inv=Jeenali&vol=vol2
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
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.
Add Note
Generate MD5 List of Files

Current Directory: C:/

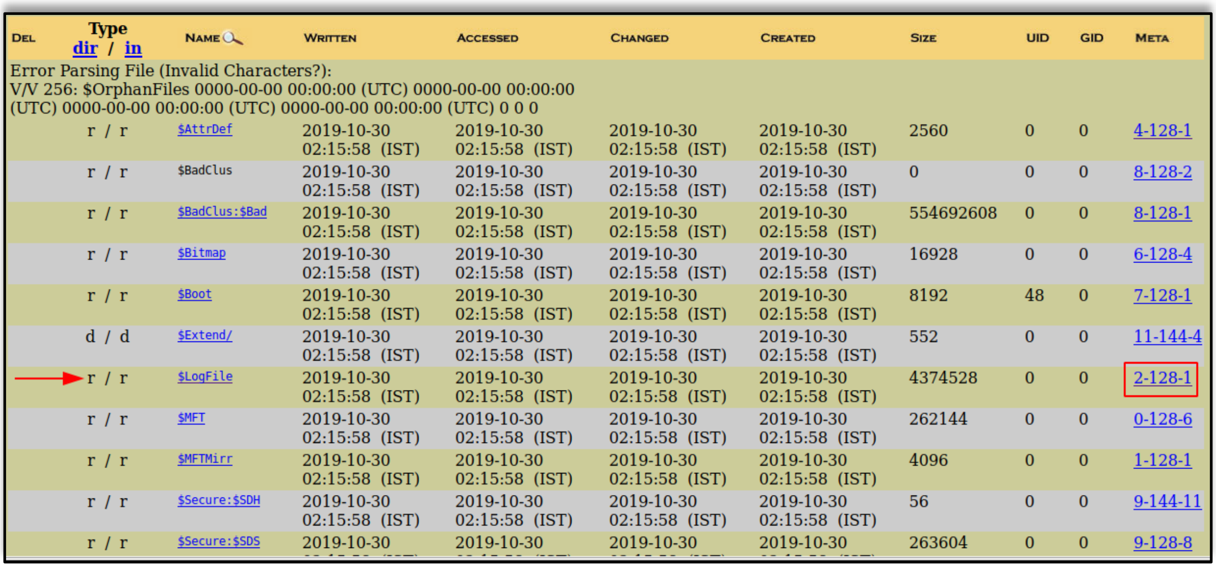
Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
Error Parsing File (Invalid Characters?): V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	r / r	$AttrDef	2019-10-30 02:15:58 (IST)	2019-10-30 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

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



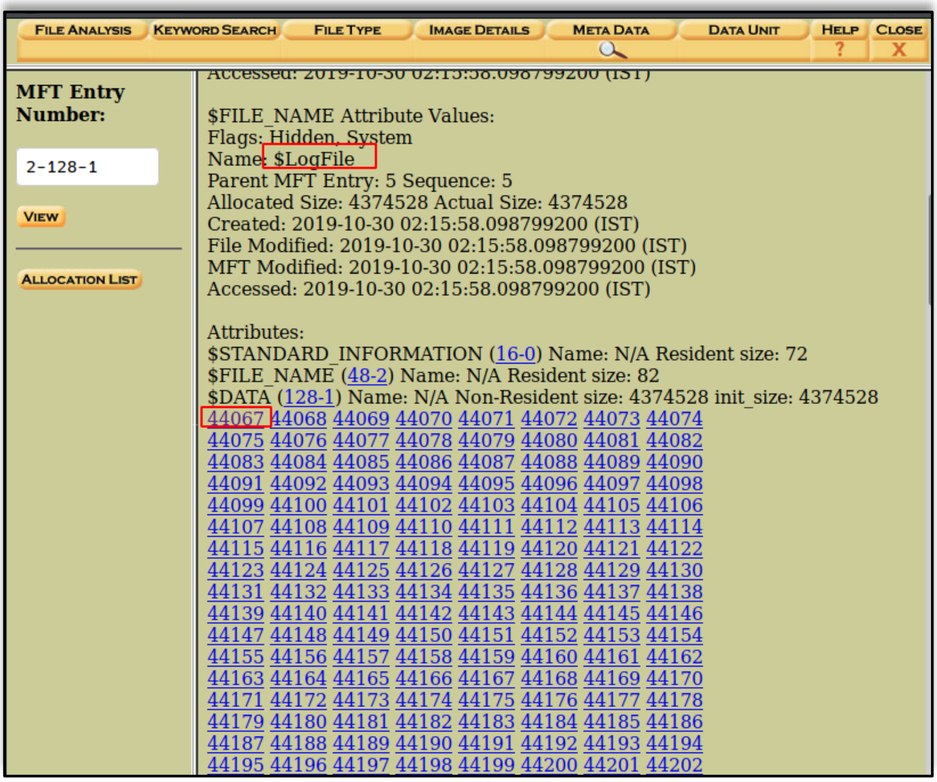
```
MD5 Values for files in C:/ (image2.e01-2048-1085439)

ad617ac3906958de35eacc3d90d31043  -    $AttrDef
d41d8cd98f00b204e9800998ecf8427e  -    $BadClus
d41d8cd98f00b204e9800998ecf8427e  -    $BadClus:$Bad
9e573661e664f9fe17e9994f68cfce6f  -    $Bitmap
56be2ed9e3d8fa13c8601b4b4005c048  -    $Boot
f0a15b15a16edf984bfb1688f12bbc27  -    $LogFile
d79a6bdb2341ab892664648e1406cedd  -    $MFT
0f2e6acdceecd0a34d50956a6be74747  -    $MFTMirr
db406c8849fb549bb219c7ac88cfa74f  -    $Secure:$SDS
29c8d340eedb44039c942149ee9fea72  -    $Secure:$SDH
0ef04368ef411190e098df2d950ff15a  -    $Secure:$SII
7ff498a44e45e77374cc7c962b1b92f2  -    $UpCase
dd81a6db3b14245dc2e5ae4d3bf40140  -    $UpCase:$Info
d41d8cd98f00b204e9800998ecf8427e  -    $Volume
```

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

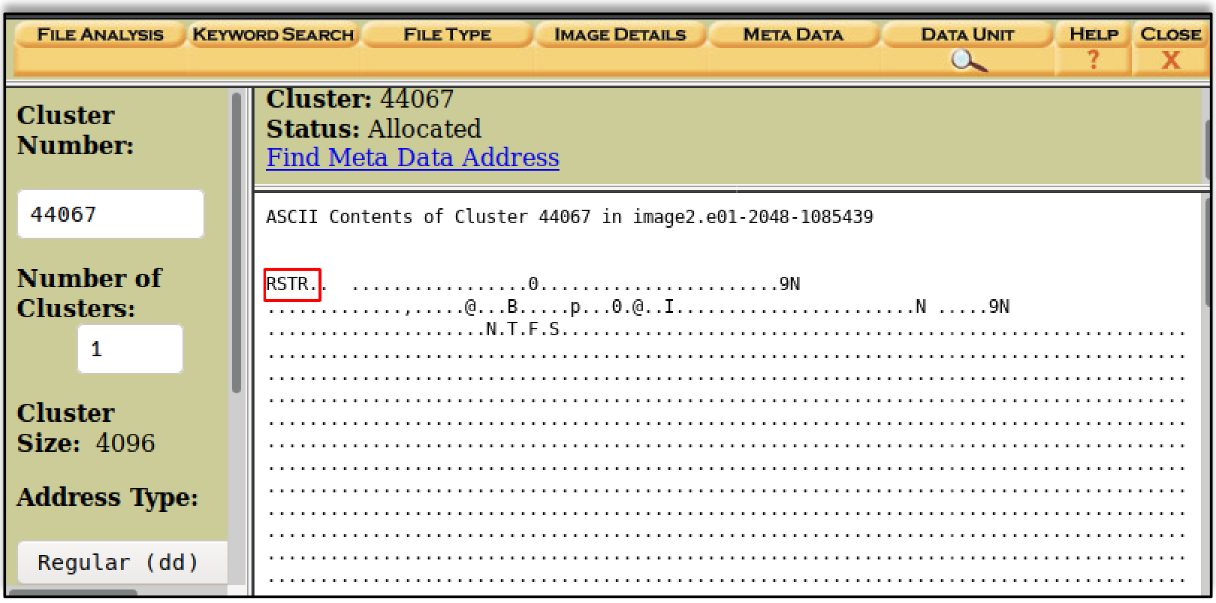
Here you can see the metadata information about the directory. In order to see more details, click on the first cluster '44067' in order to view its header information to find any relevant information to the case.



MFT Entry Number: 2-128-1

```
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
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.



Cluster Number: 44067

Number of Clusters: 1

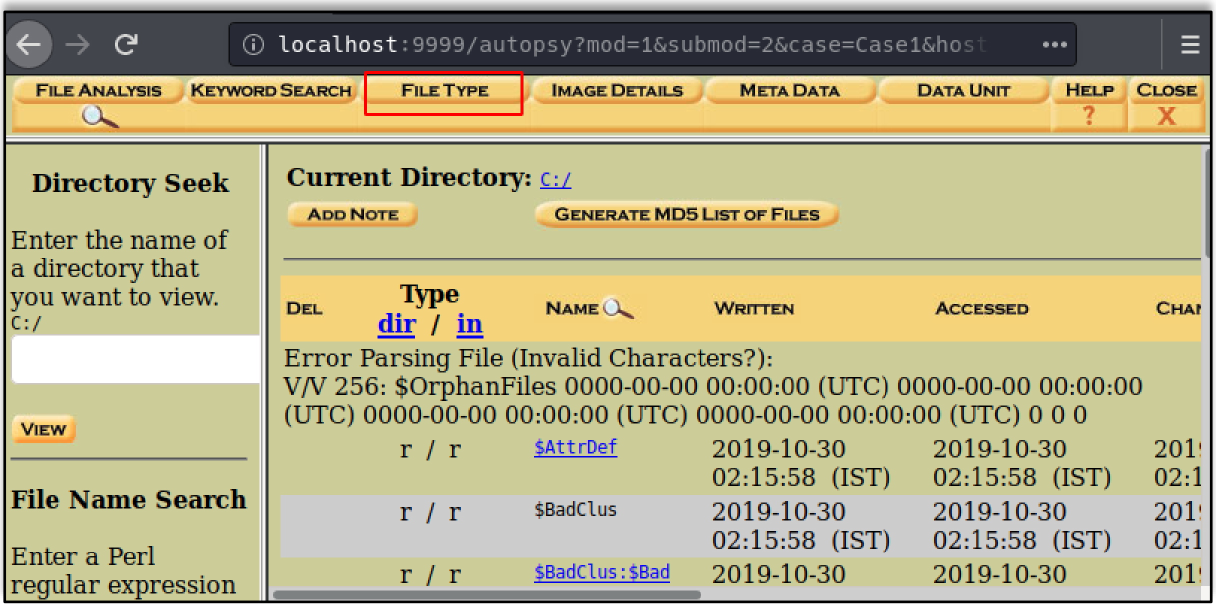
Cluster Size: 4096

Address Type: Regular (dd)

Cluster: 44067
Status: Allocated
Find Meta Data Address

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


RSTR..  ..................0.........................9N
..............,.....@...B.....p...0.@..I......................N .....9N
....................N.T.F.S..........................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
.......................................................................................
```

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

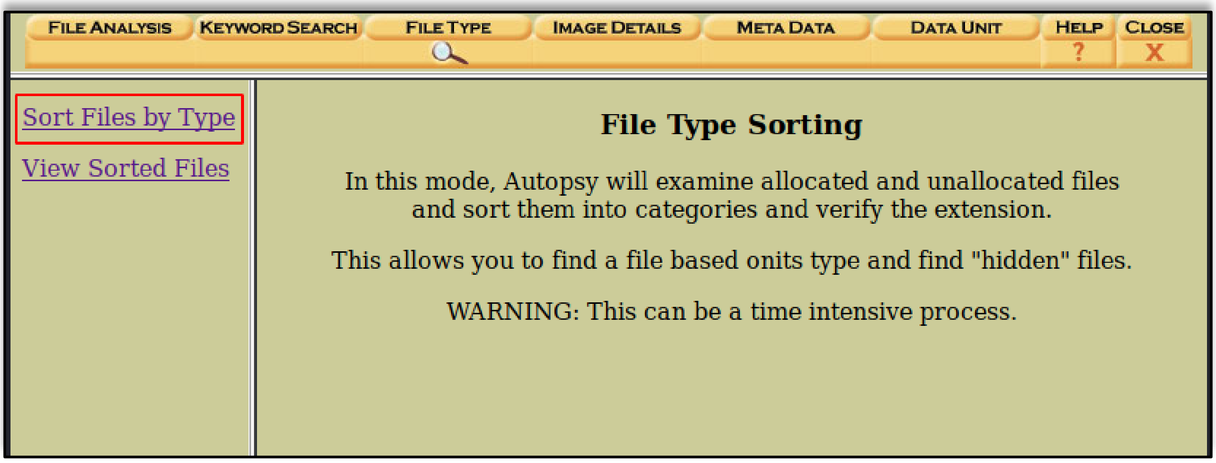
Enter a Perl regular expression

Current Directory: C:/

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHA
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)	201 02:1
	r / r	$BadClus	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	201 02:1
	r / r	$BadClus:$Bad	2019-10-30	2019-10-30	201

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'**.



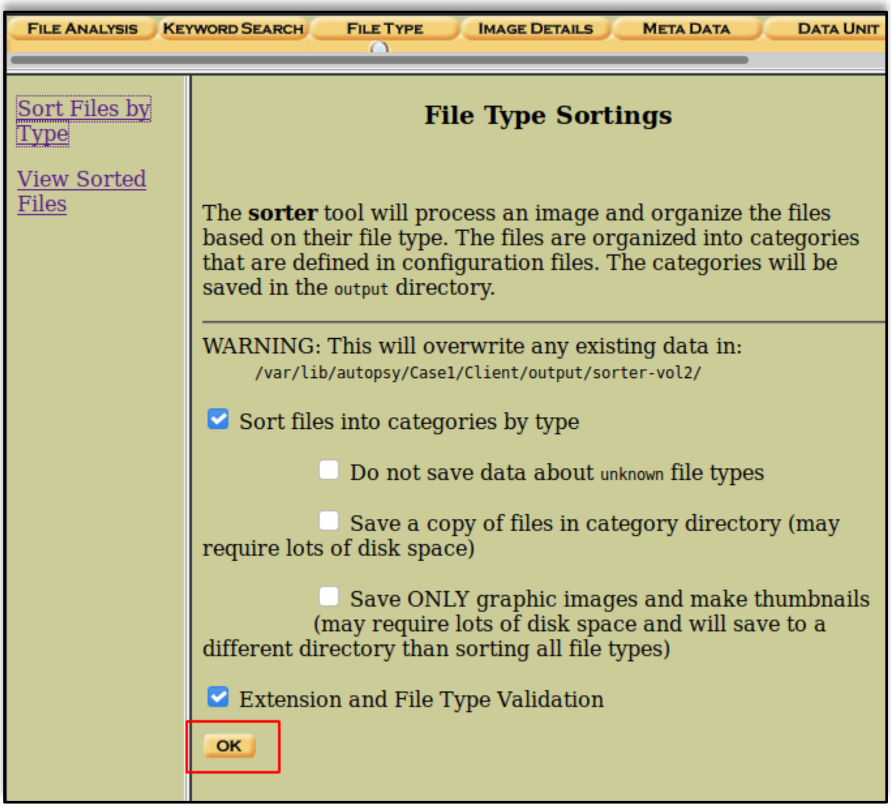
File Type Sorting

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 onits 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.



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

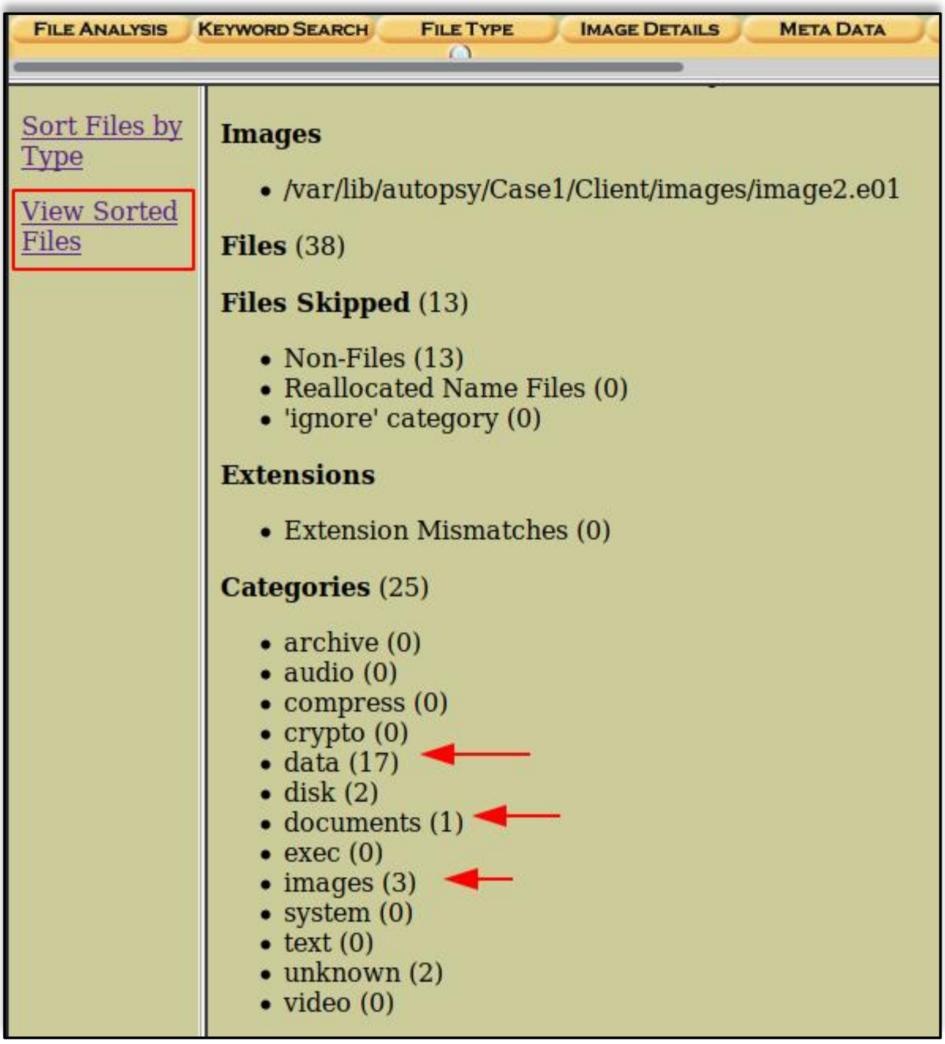
□ Do not save data about unknown file types

□ 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

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.



Images

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

Files (38)

Files Skipped (13)

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

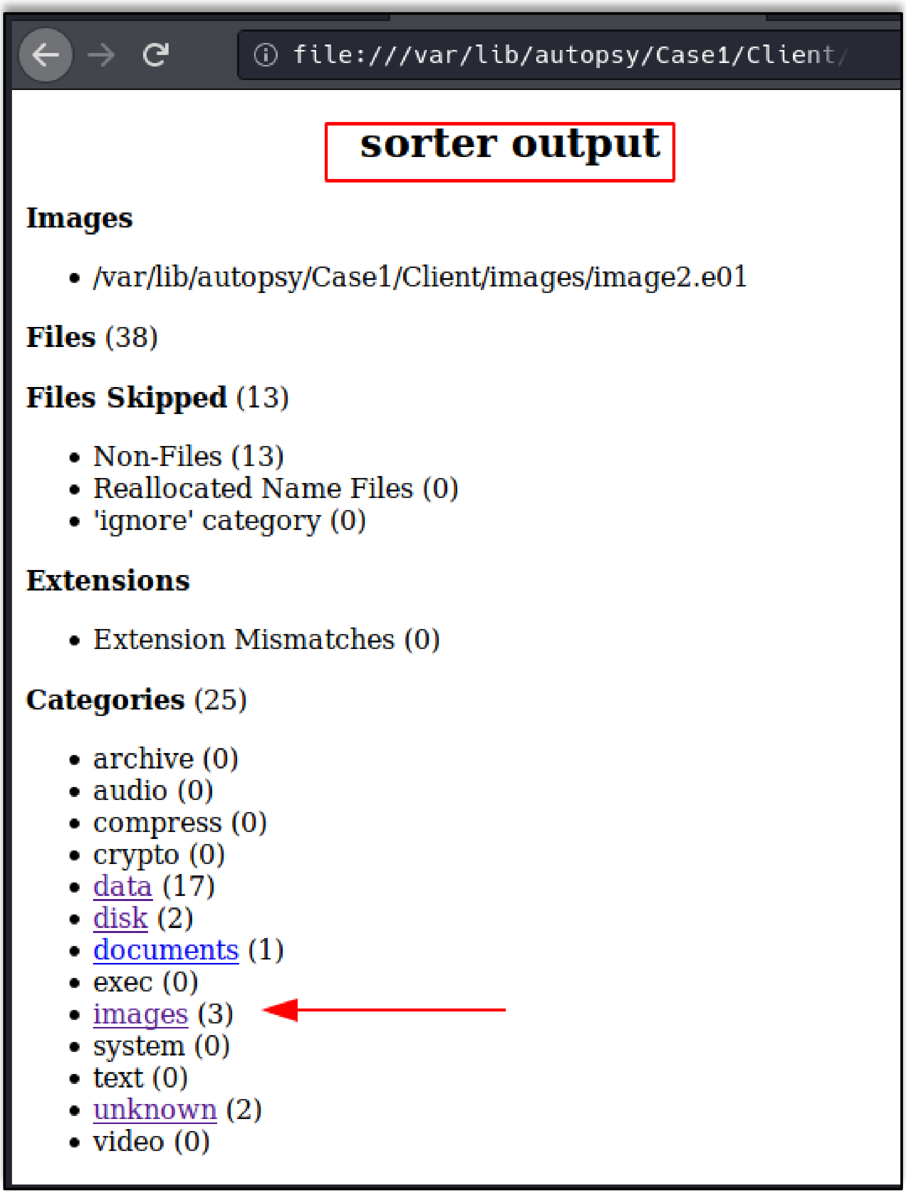
Extensions

- 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.



sorter output

Images

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

Files (38)

Files Skipped (13)

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

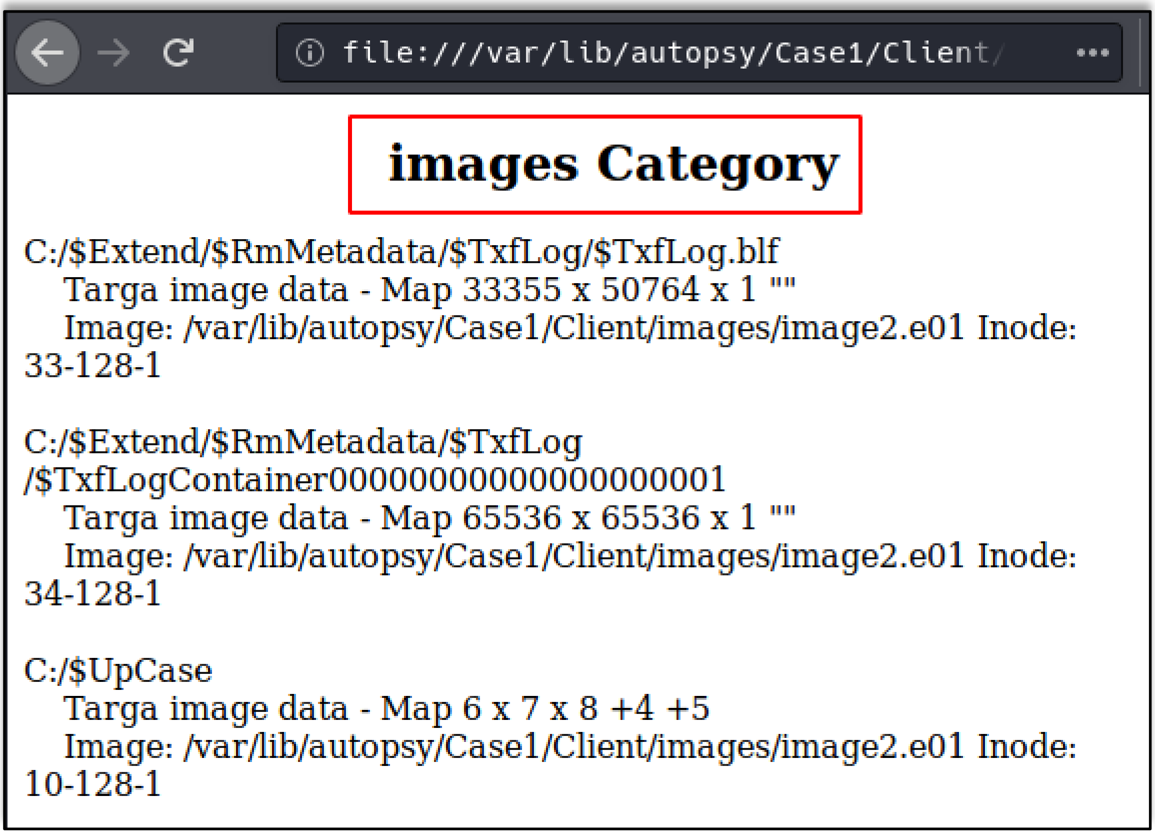
Extensions

- 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)

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



images Category

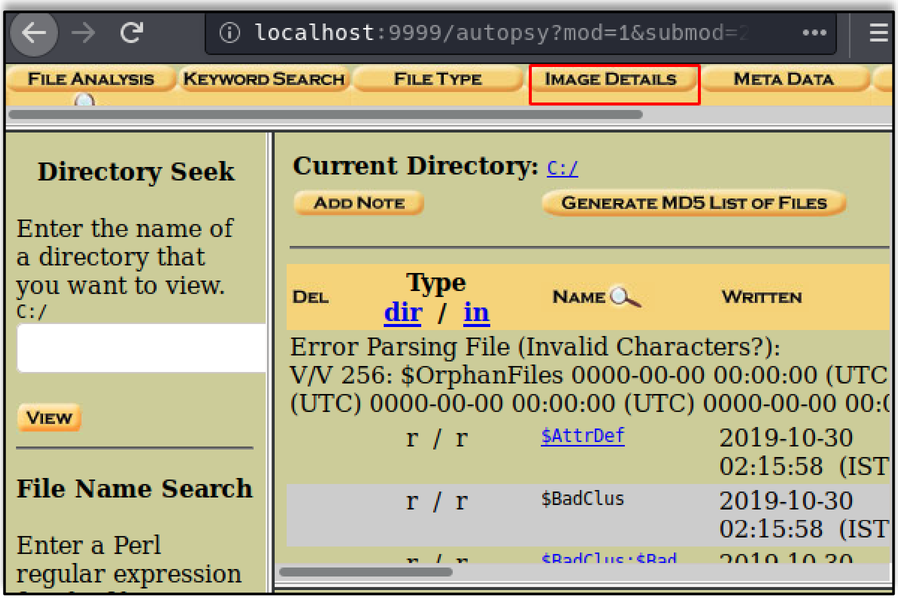
C:/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
Targa image data - Map 33355 x 50764 x 1 ""
Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode: 33-128-1

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

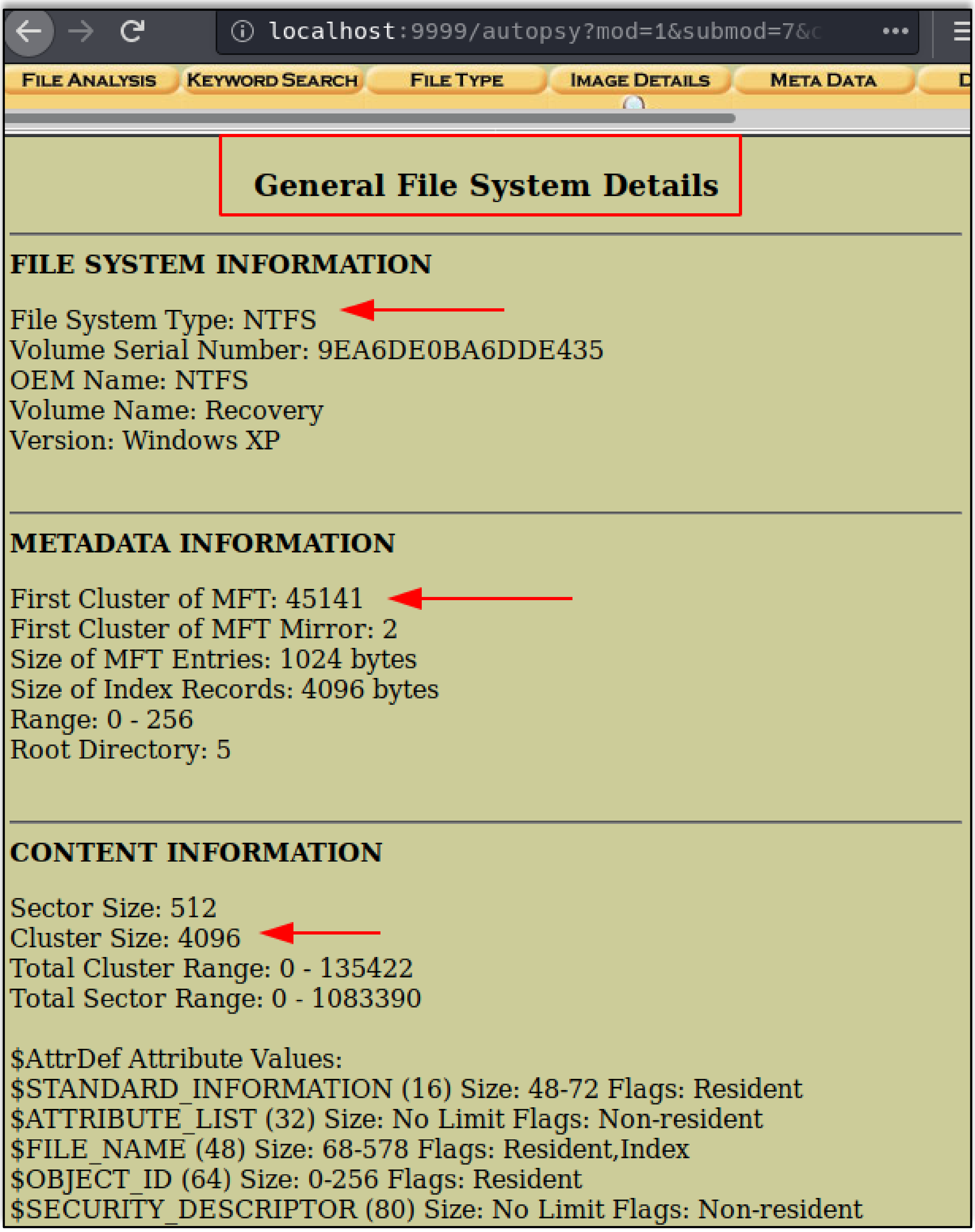
Image Details

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



```
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:(
        r / r    $AttrDef    2019-10-30
                             02:15:58  (IST
        r / r    $BadClus    2019-10-30
                             02:15:58  (IST
```

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



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

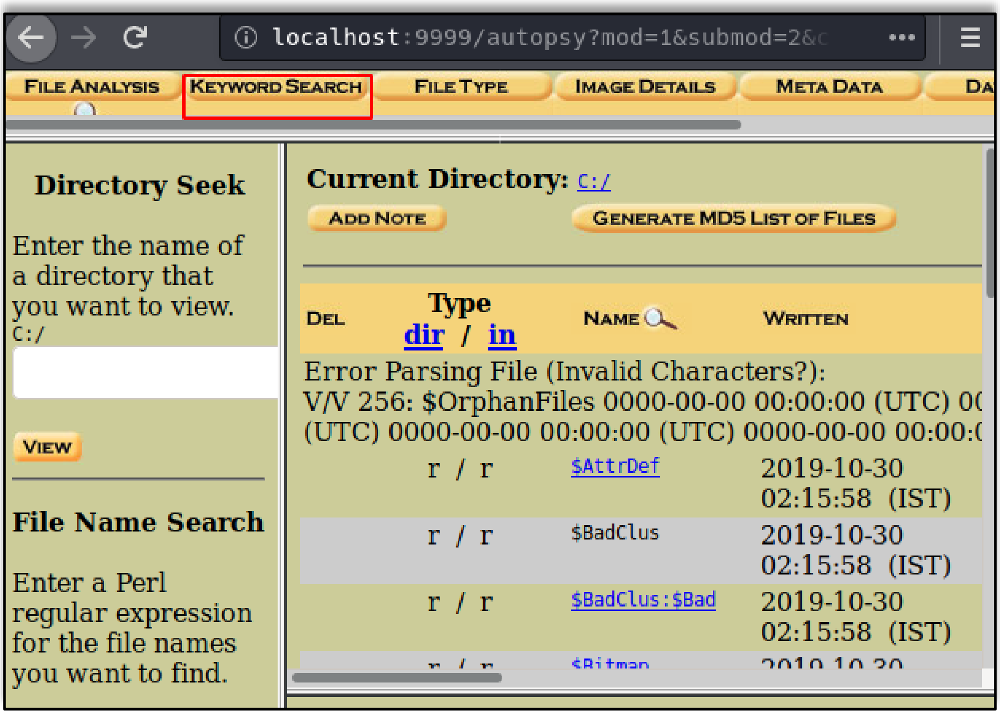
CONTENT INFORMATION

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

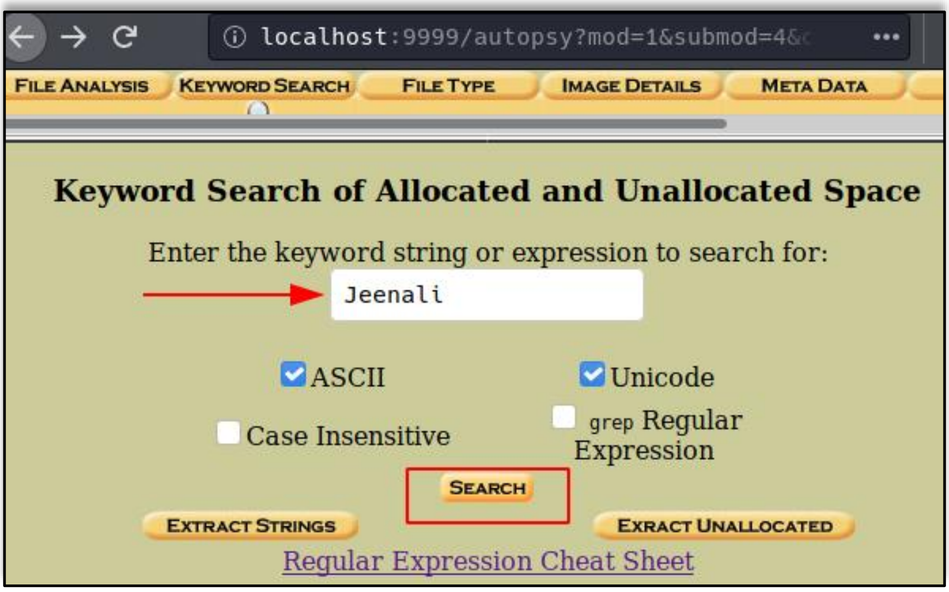
Keyword Search

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


localhost:9999/autopsy?mod=1&submod=2&
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Da
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
(UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 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 02:15:58 (IST)
r / r    $Bitmap         2019-10-30
```

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


localhost:9999/autopsy?mod=1&submod=4&
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Keyword Search of Allocated and Unallocated Space
Enter the keyword string or expression to search for:
☑ ASCII
☑ Unicode
□ Case Insensitive
□ grep Regular Expression
Search
Extract Strings
Exract Unallocated
Regular Expression Cheat Sheet

Jeenali

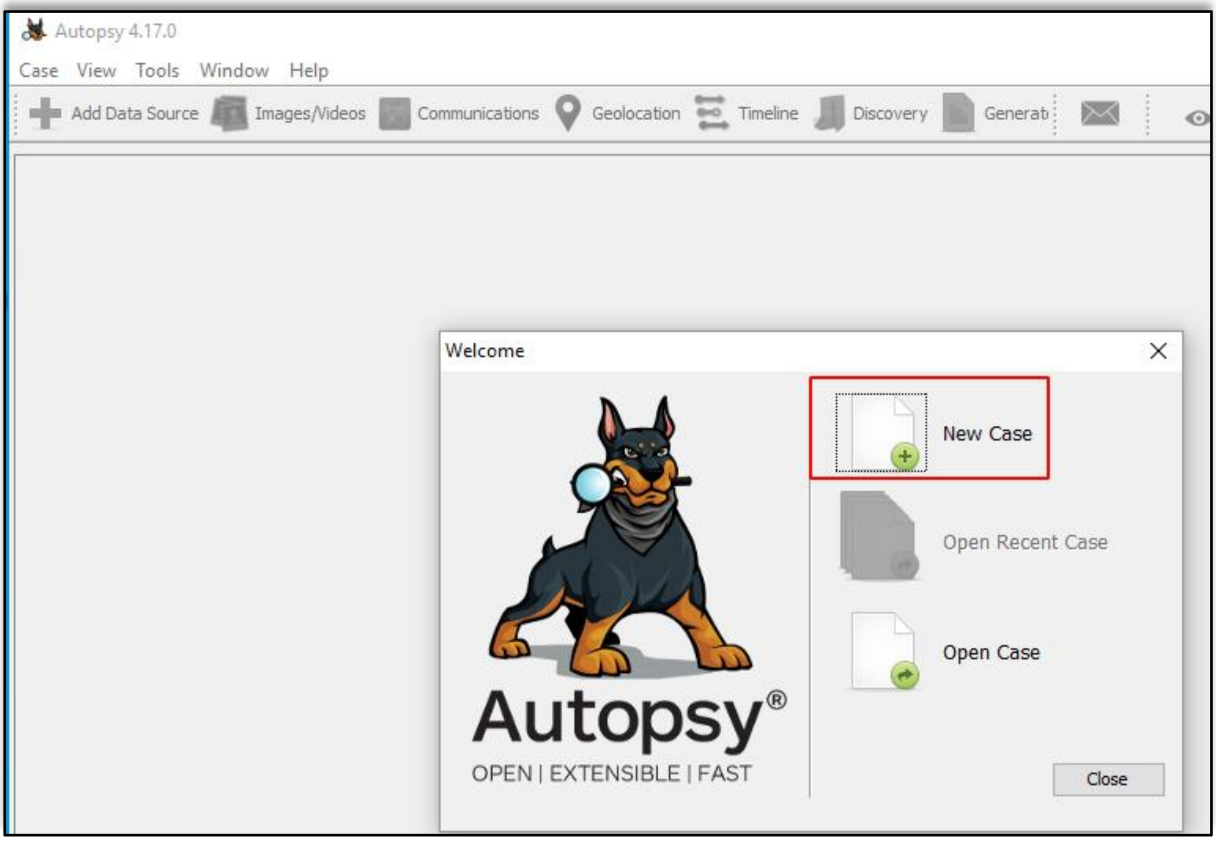
AUTOPSY WINDOWS

Autopsy for Windows

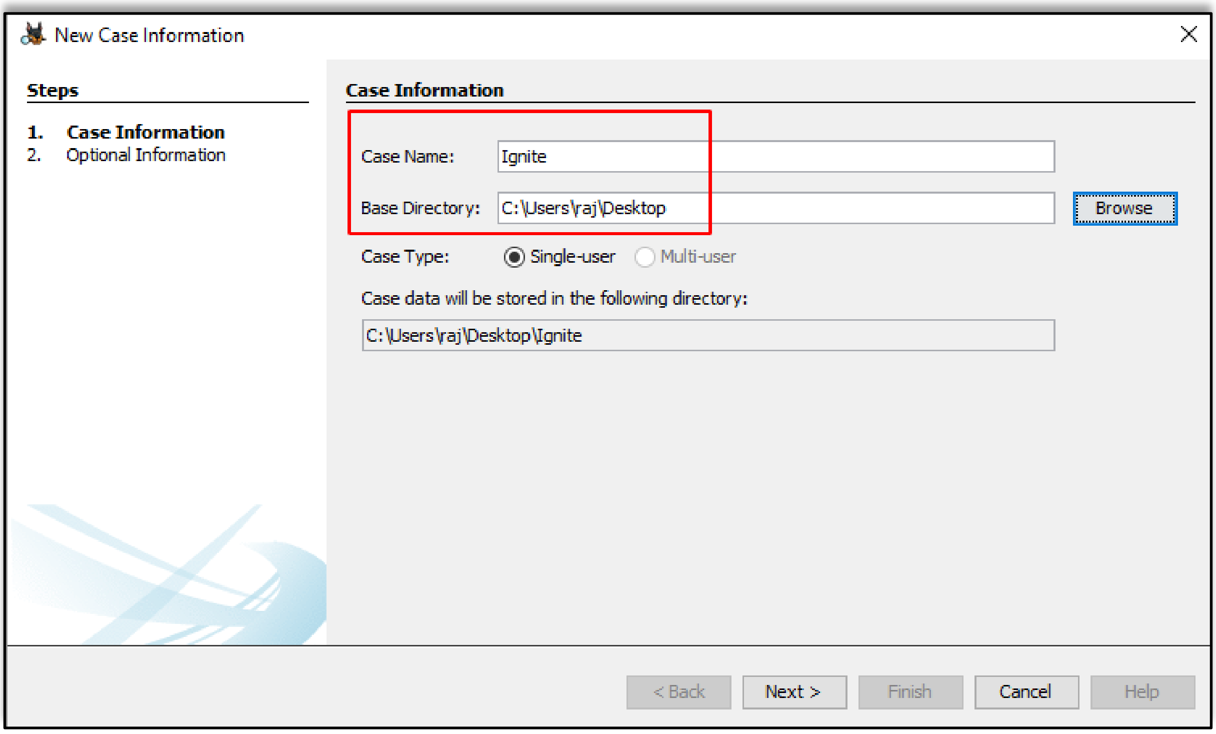
You can download the Autopsy Tool for Windows from here.

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.



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name: Ignite

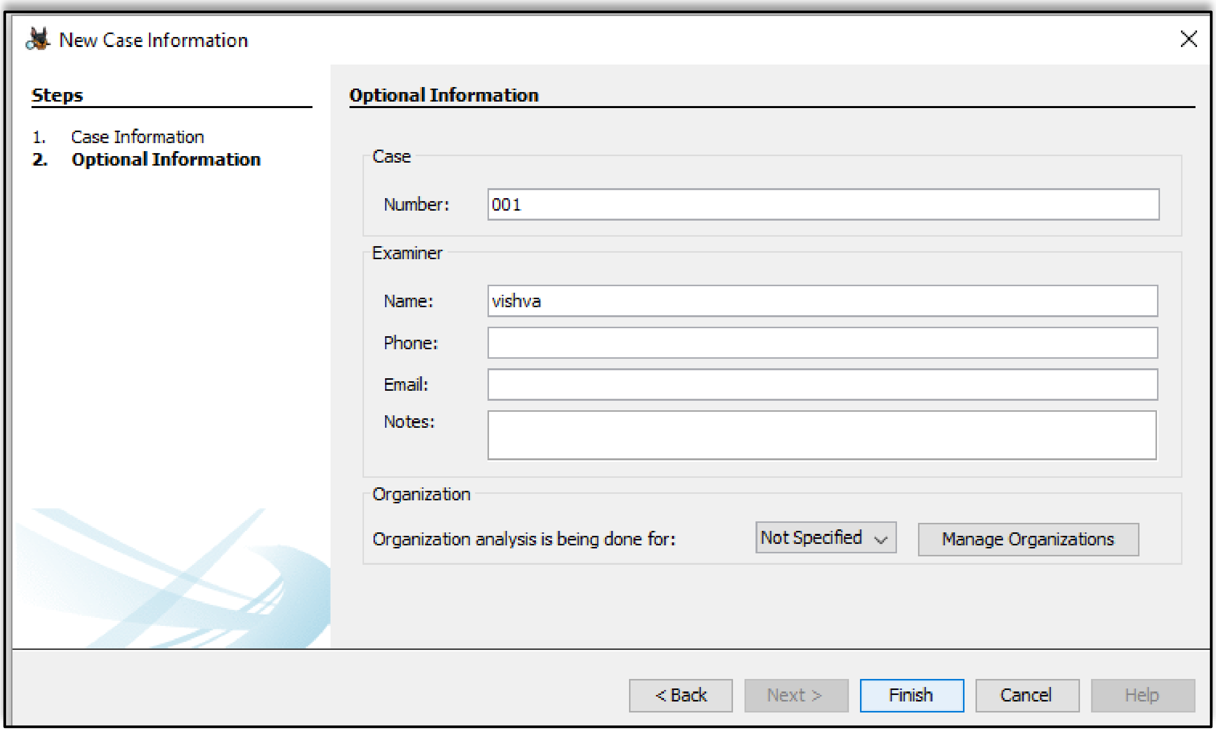
Base Directory: C:\Users\raj\Desktop

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\raj\Desktop\Ignite

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



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 001

Examiner

Name: vishva

Phone:

Email:

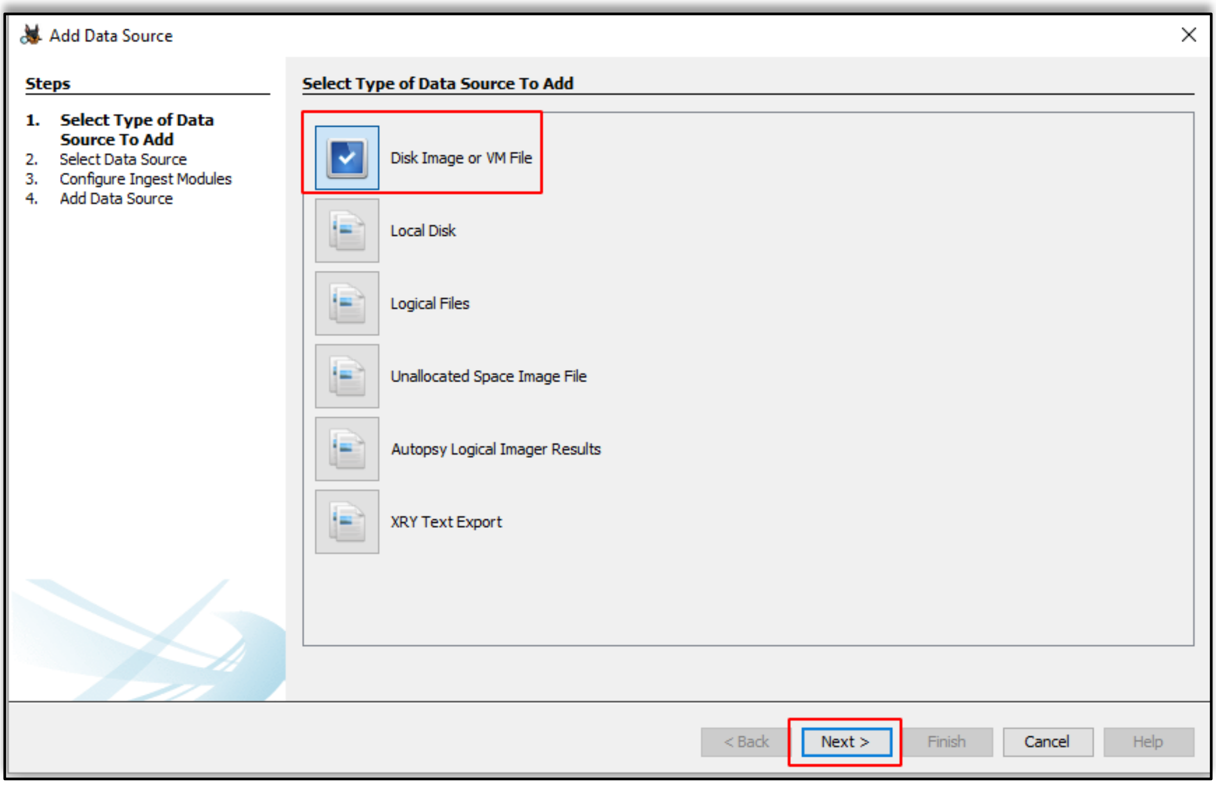
Notes:

Organization

Organization analysis is being done for: Not Specified

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.

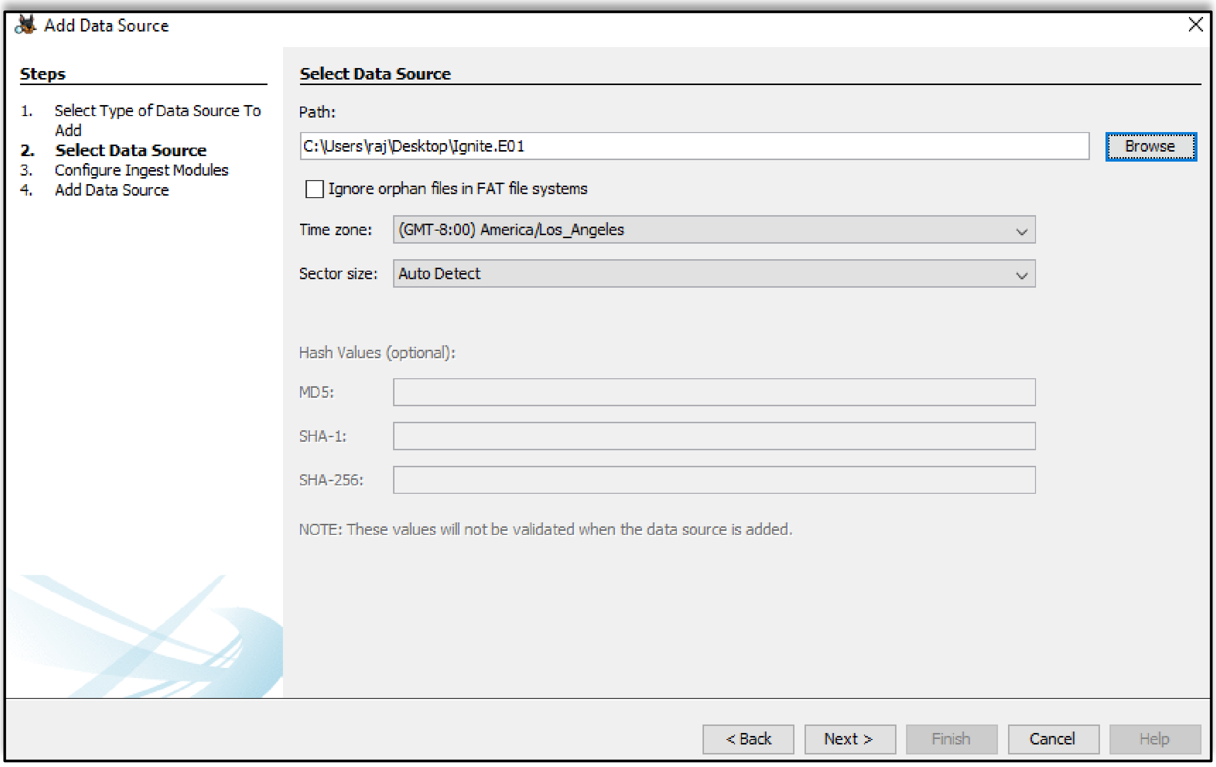

Add Data Source

Steps

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

Select Type of Data Source To Add

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: C:\Users\raj\Desktop\Ignite.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

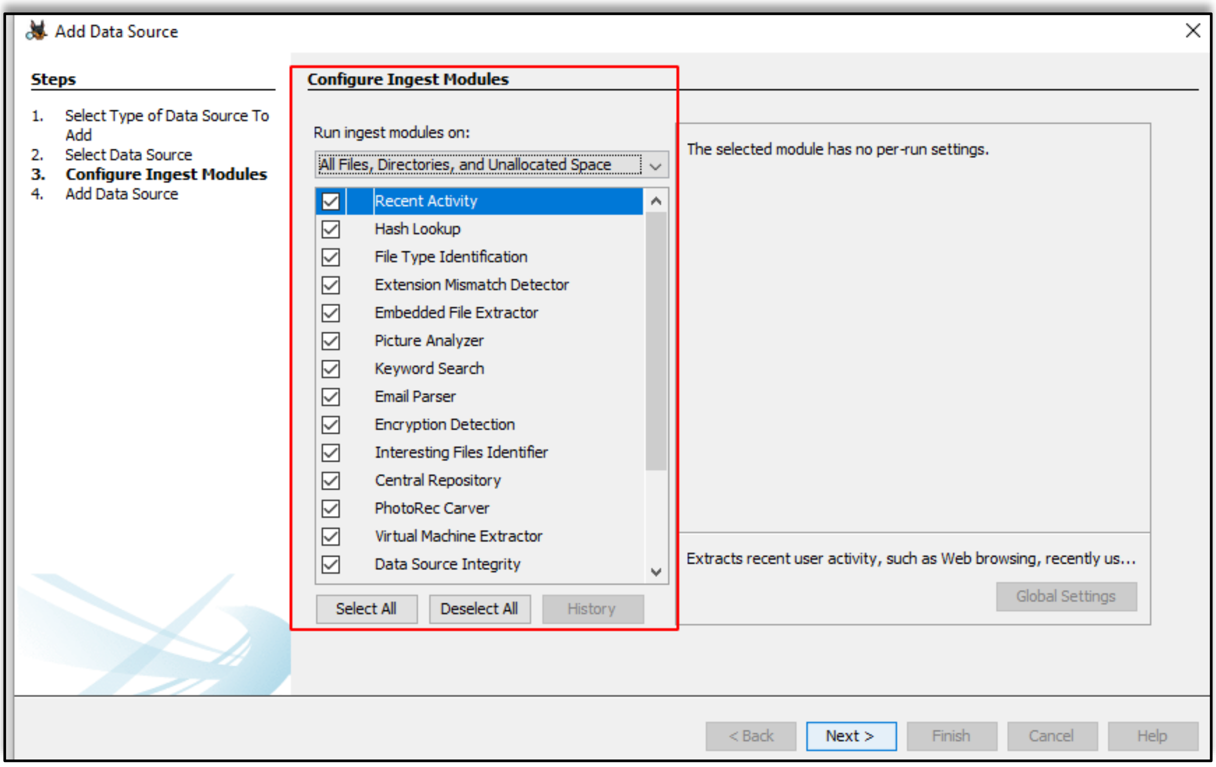
MD5:

SHA-1:

SHA-256:

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

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

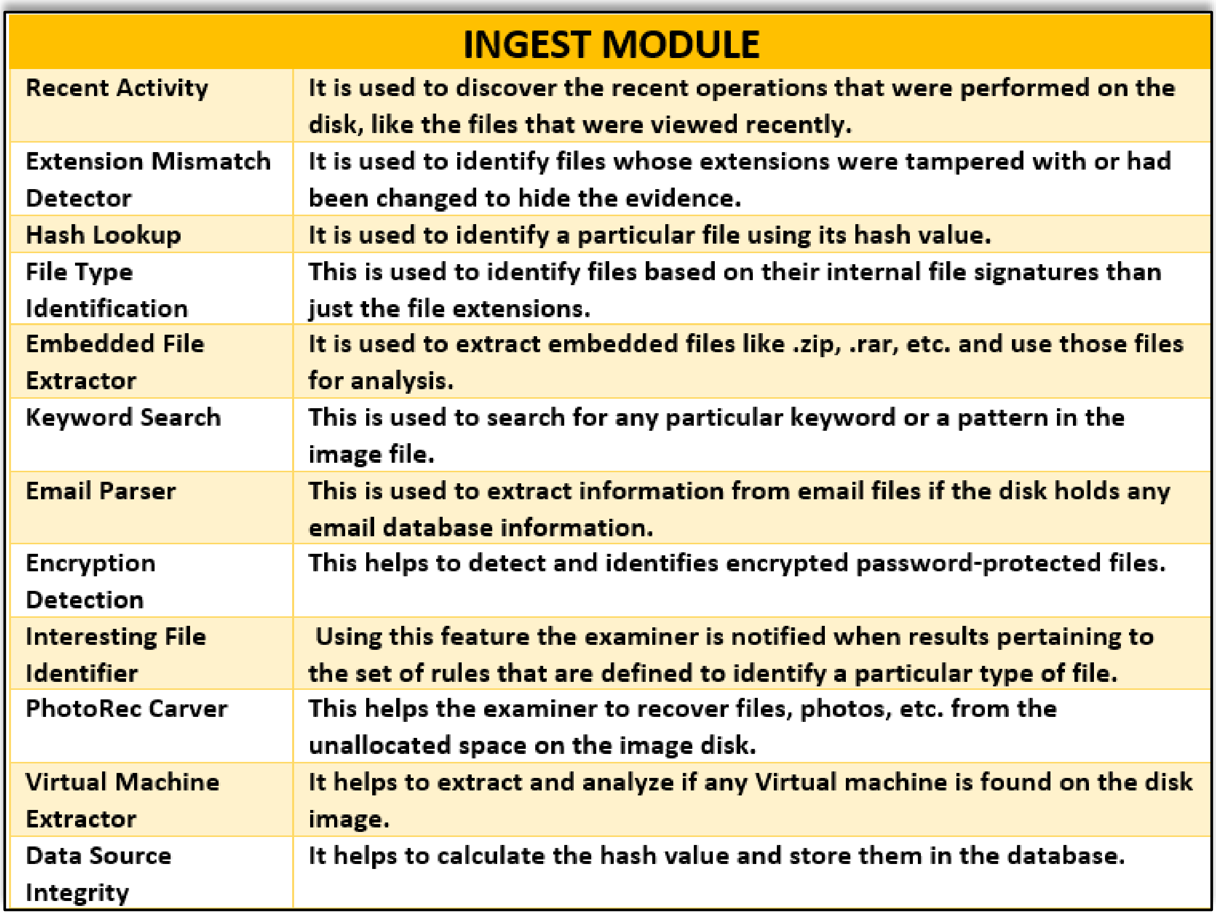
Run ingest modules on: All Files, Directories, and Unallocated Space

☑ 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

The selected module has no per-run settings.

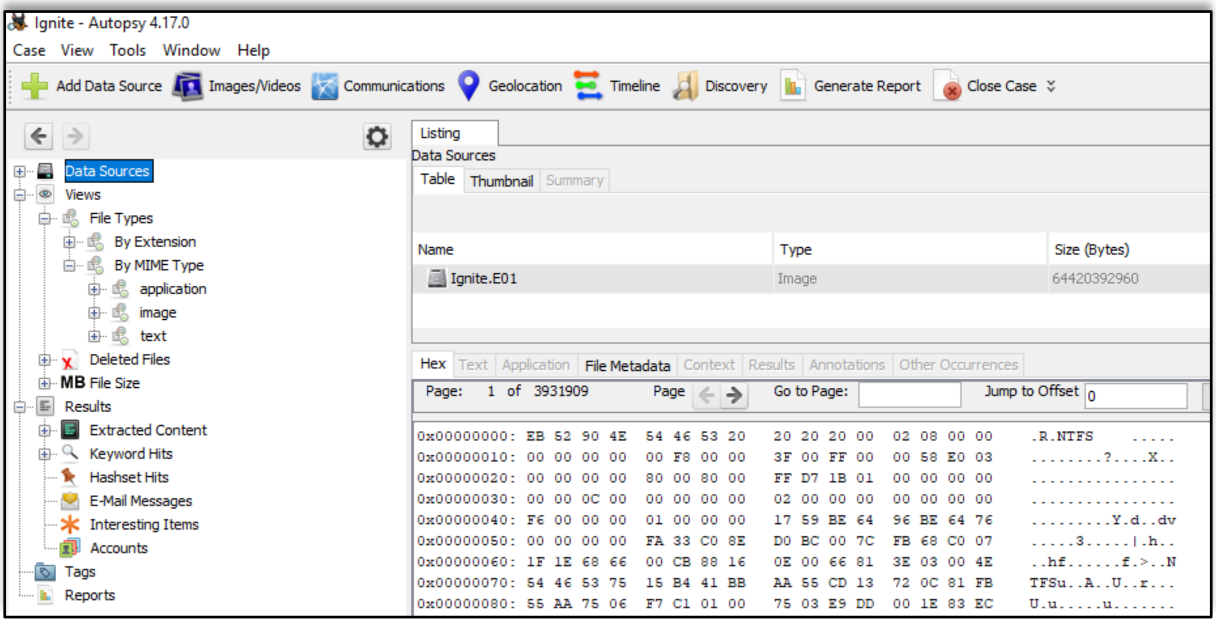
Extracts recent user activity, such as Web browsing, recently us...

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.



Name	Type	Size (Bytes)
Ignite.E01	Image	64420392960

Page: 1 of 3931909 Page

Jump to Offset 0

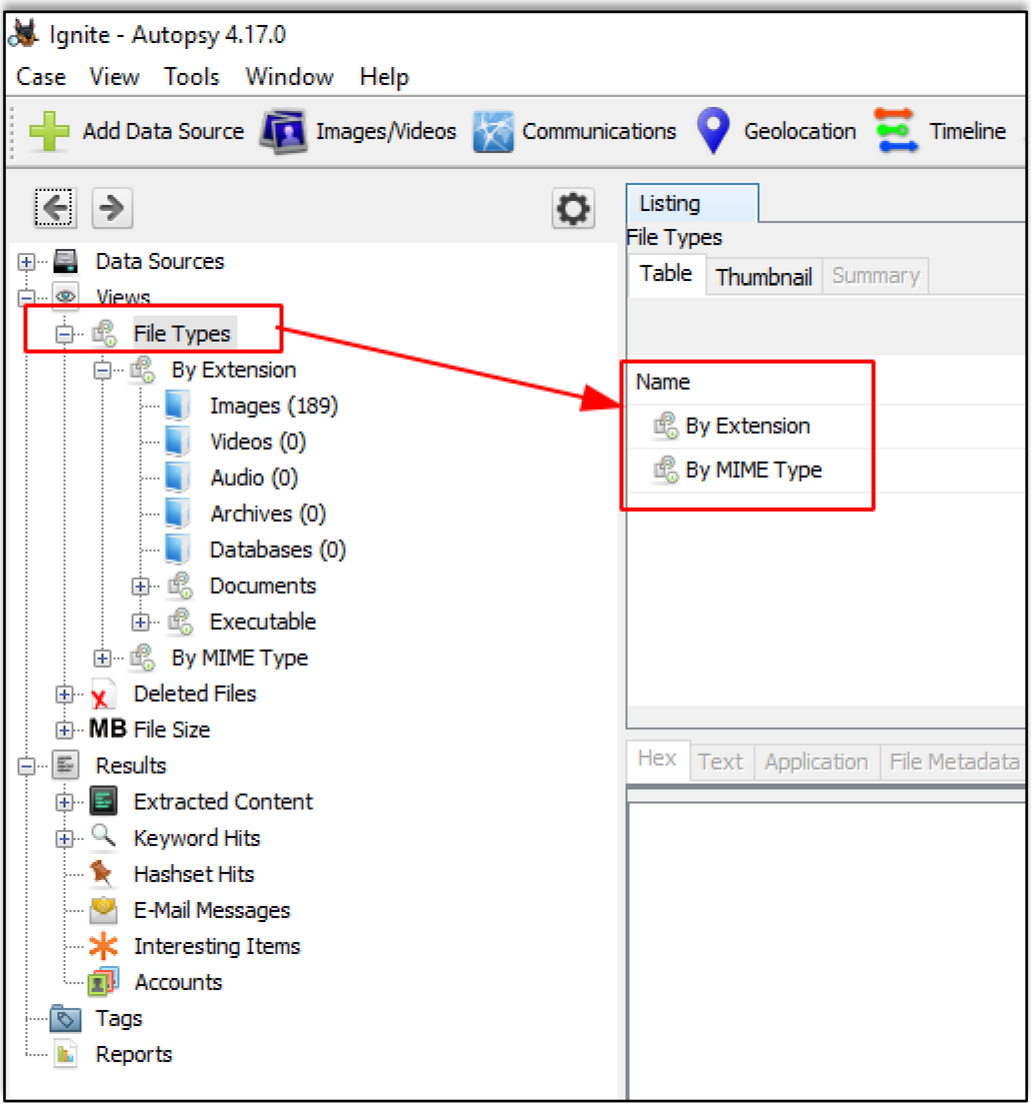
```
0x00000000: EB 52 90 4E  54 46 53 20   20 20 20 00  02 08 00 00    .R.NTFS    .....
0x00000010: 00 00 00 00  00 F8 00 00   3F 00 FF 00  00 58 E0 03    ........?....X..
0x00000020: 00 00 00 00  80 00 80 00   FF D7 1B 01  00 00 00 00    ................
0x00000030: 00 00 0C 00  00 00 00 00   02 00 00 00  00 00 00 00    ................
0x00000040: F6 00 00 00  01 00 00 00   17 59 BE 64  96 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

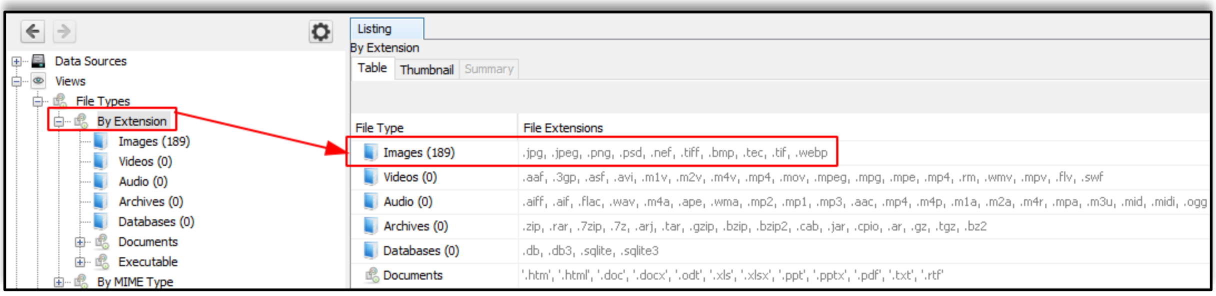
It can be classified in the form of File extension or MIME type.
It provides information on file extensions that are commonly used by the OS whereas MIME types are used by the browser to decide what data to represent. It also displays deleted files.

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



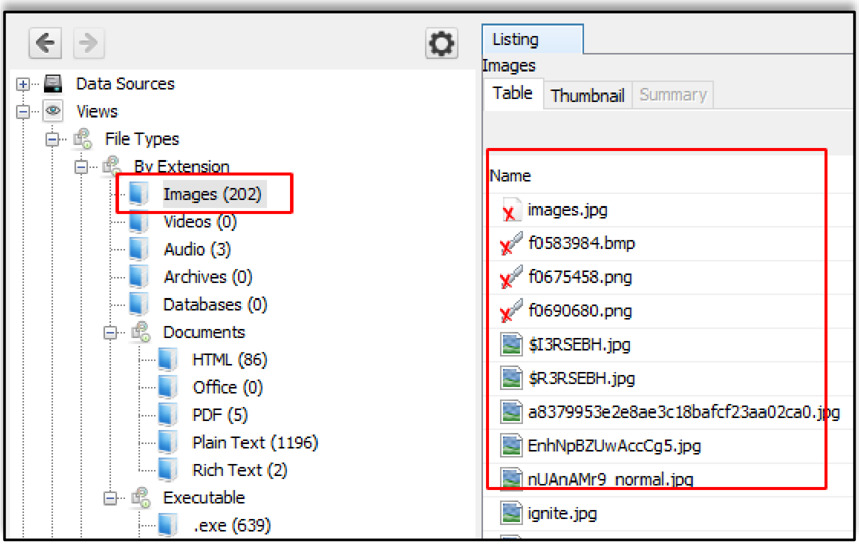
By Extension

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.



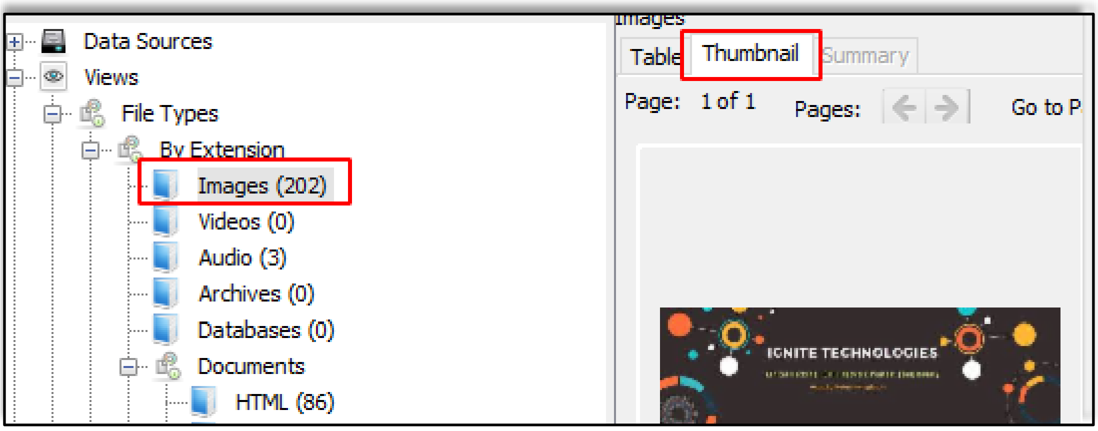
File Type	File Extensions
Images (189)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (0)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (0)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (0)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (0)	.db, .db3, .sqlite, .sqlite3
Documents	'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'

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

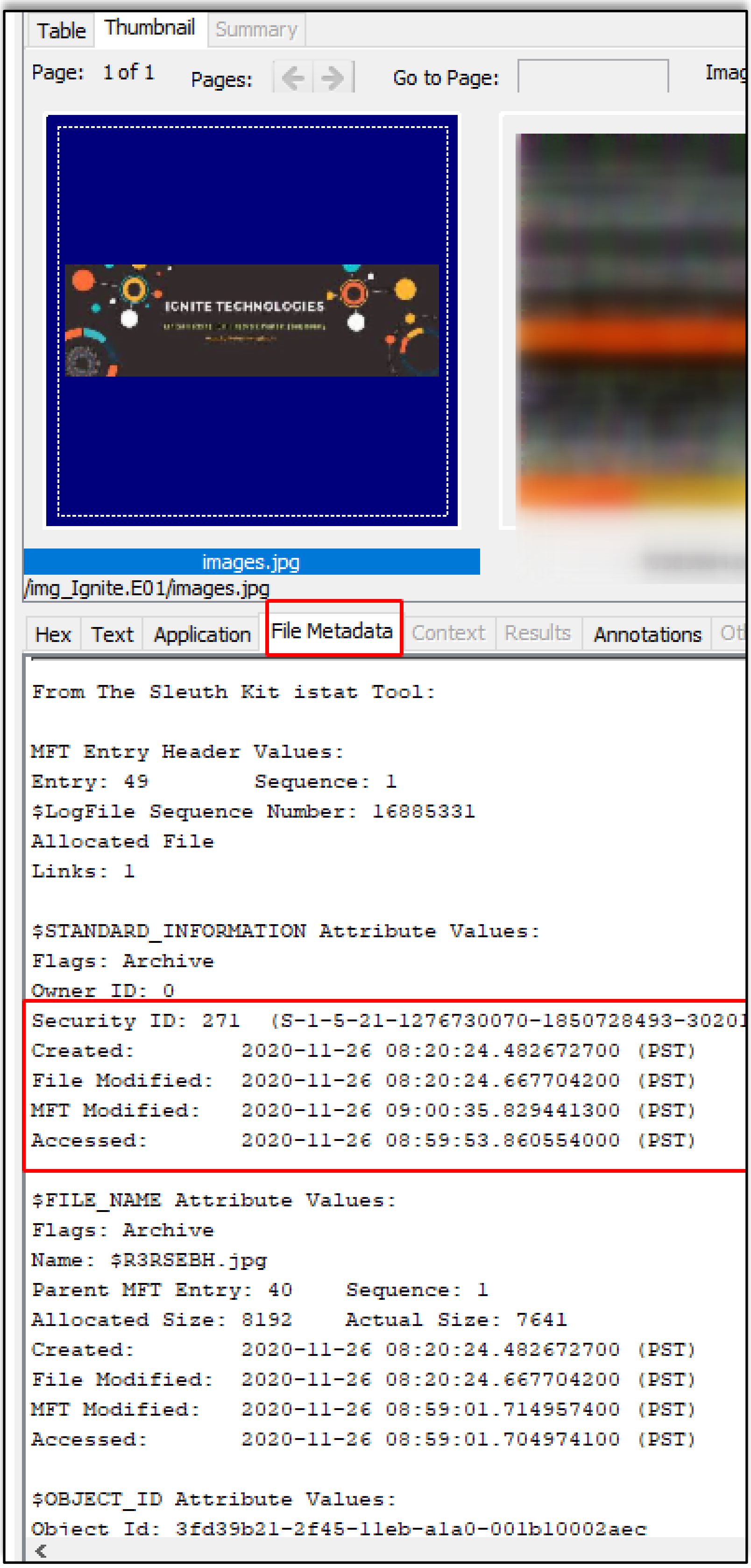


Name
images.jpg
f0583984.bmp
f0675458.png
f0690680.png
$I3RSEBH.jpg
$R3RSEBH.jpg
a8379953e2e8ae3c18bafcf23aa02ca0.jpg
EnhNpBZUwAccCg5.jpg
nUAnAMr9_normal.jpg
ignite.jpg

We can also view the thumbnail of the images.

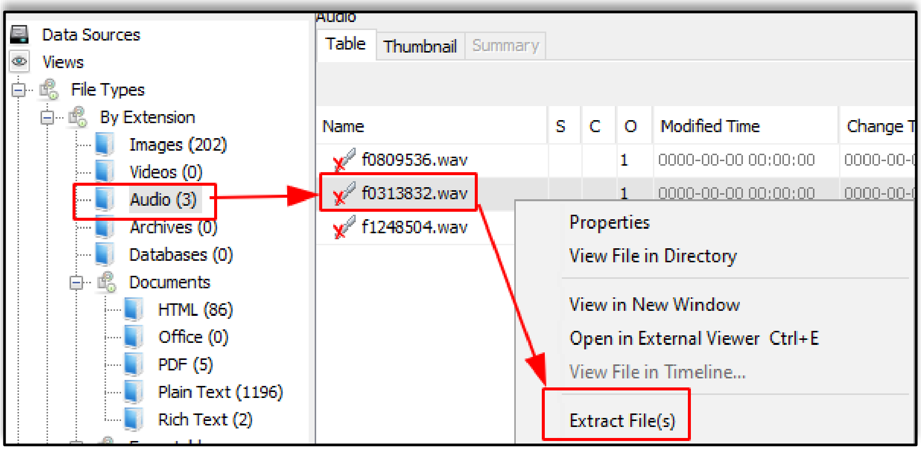


On viewing the thumbnail, you can view the file metadata and details about the image.



```
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-1-5-21-1276730070-1850728493-3020
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-a1a0-001b10002aec
```

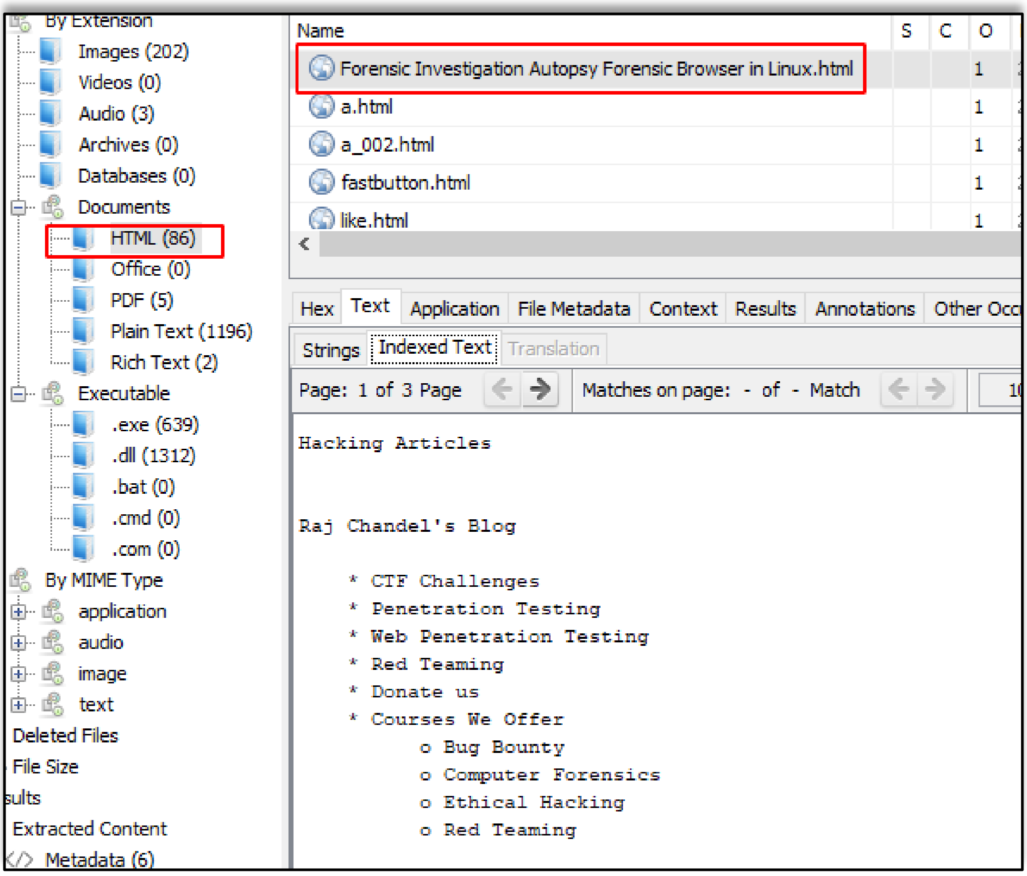
Here we can also view a few audio files that have been recovered. We can extract these files from the system and hear to them using various software.



Name	S	C	O	Modified Time	Change T
f0809536.wav			1	0000-00-00 00:00:00	0000-00-(
f0313832.wav			1	0000-00-00 00:00:00	0000-00-(
f1248504.wav					

Documents

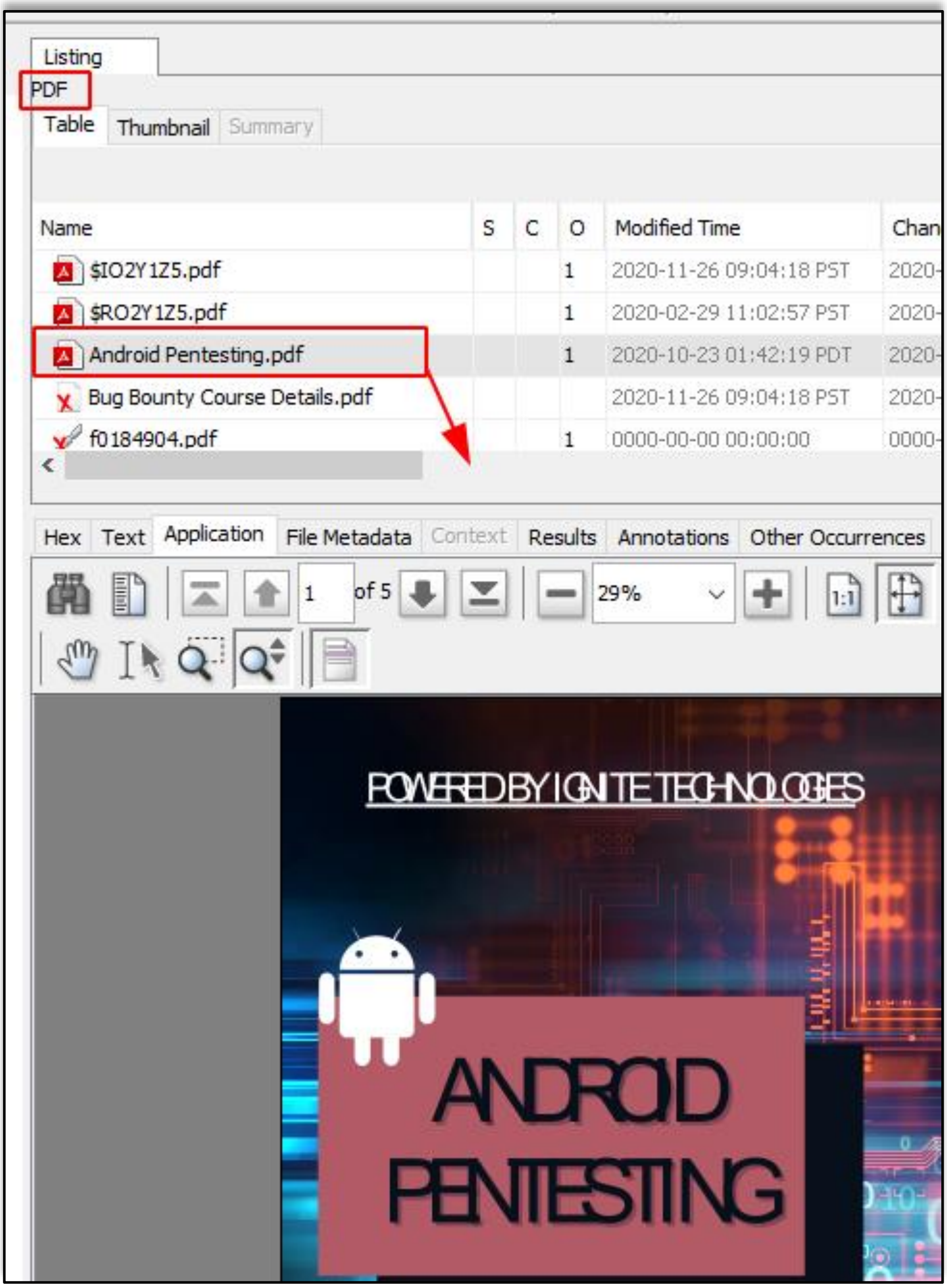
The documents are categorized into 5 types: HTML, office, PDF, Plain Text, Rich Text.
On exploring the documents option, you can see all the HTML documents present, you can click on the important ones to view them.



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

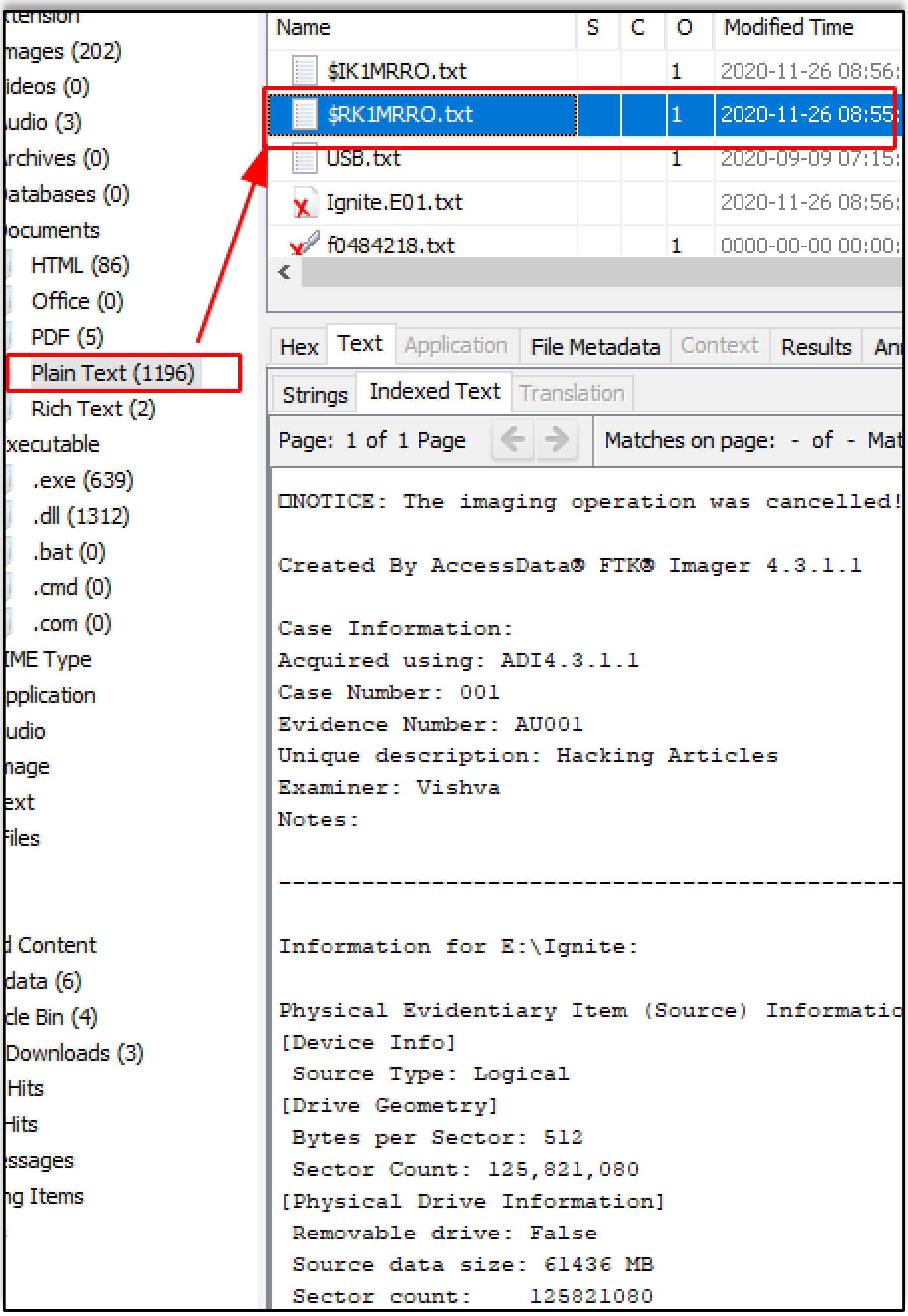
```
Hacking Articles


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
```

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



Name	S	C	O	Modified Time	Chan
$IO2Y1Z5.pdf			1	2020-11-26 09:04:18 PST	2020-
$RO2Y1Z5.pdf			1	2020-02-29 11:02:57 PST	2020-
Android Pentesting.pdf			1	2020-10-23 01:42:19 PDT	2020-
Bug Bounty Course Details.pdf				2020-11-26 09:04:18 PST	2020-
f0184904.pdf			1	0000-00-00 00:00:00	0000-

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

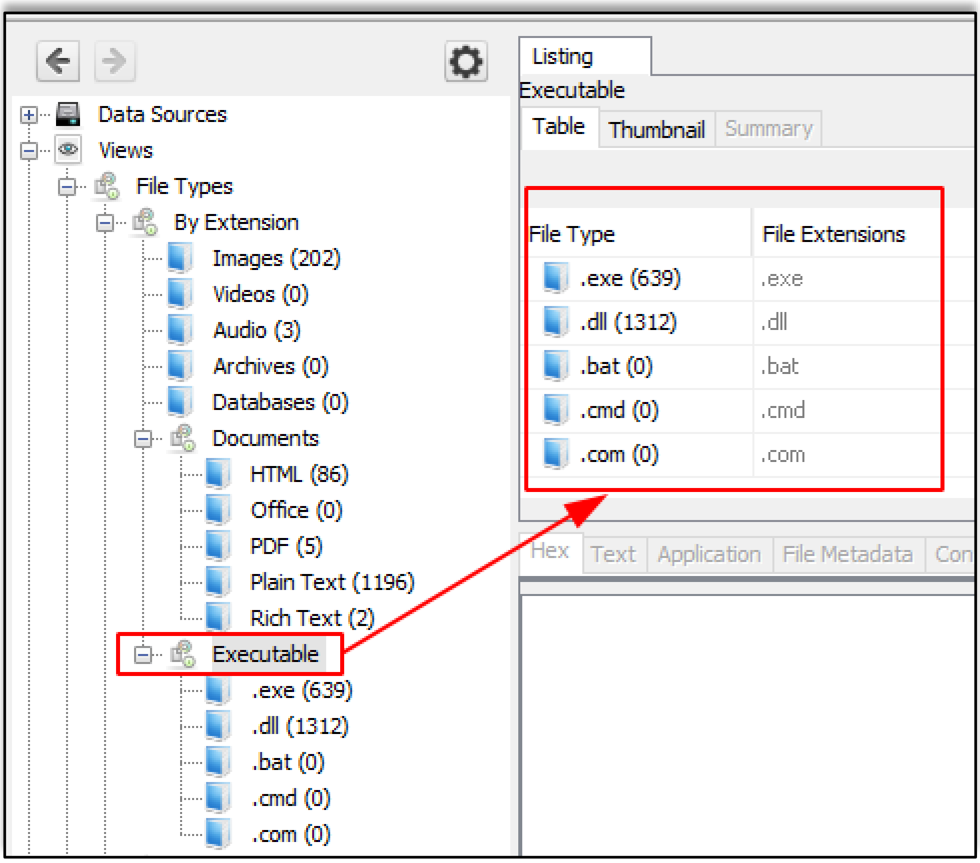


Name	S	C	O	Modified Time
$IK1MRRO.txt			1	2020-11-26 08:56:
$RK1MRRO.txt			1	2020-11-26 08:55:
USB.txt			1	2020-09-09 07:15:
Ignite.E01.txt				2020-11-26 08:56:
f0484218.txt			1	0000-00-00 00:00:

```
□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) Informatio
[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

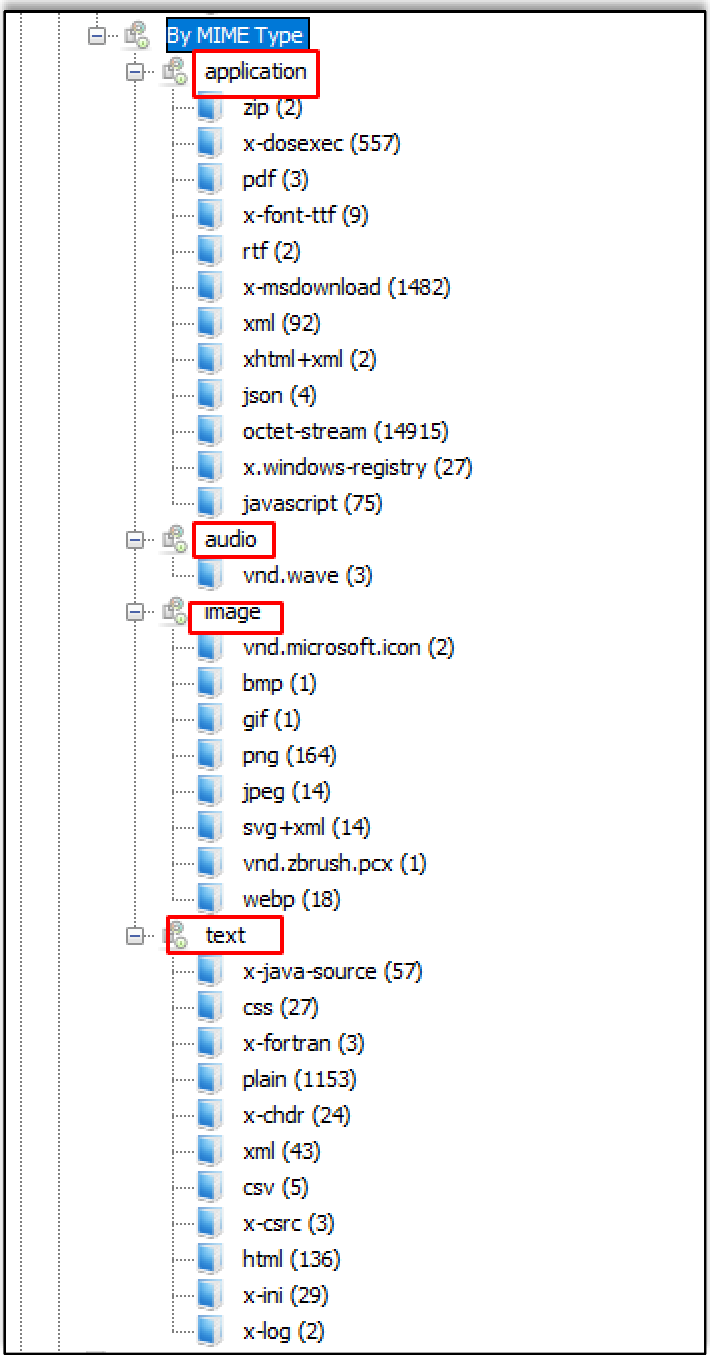
These file types are then sub-divided into .exe, .dll, .bat, .cmd and .com.



File Type	File Extensions
.exe (639)	.exe
.dll (1312)	.dll
.bat (0)	.bat
.cmd (0)	.cmd
.com (0)	.com

By Mime Type

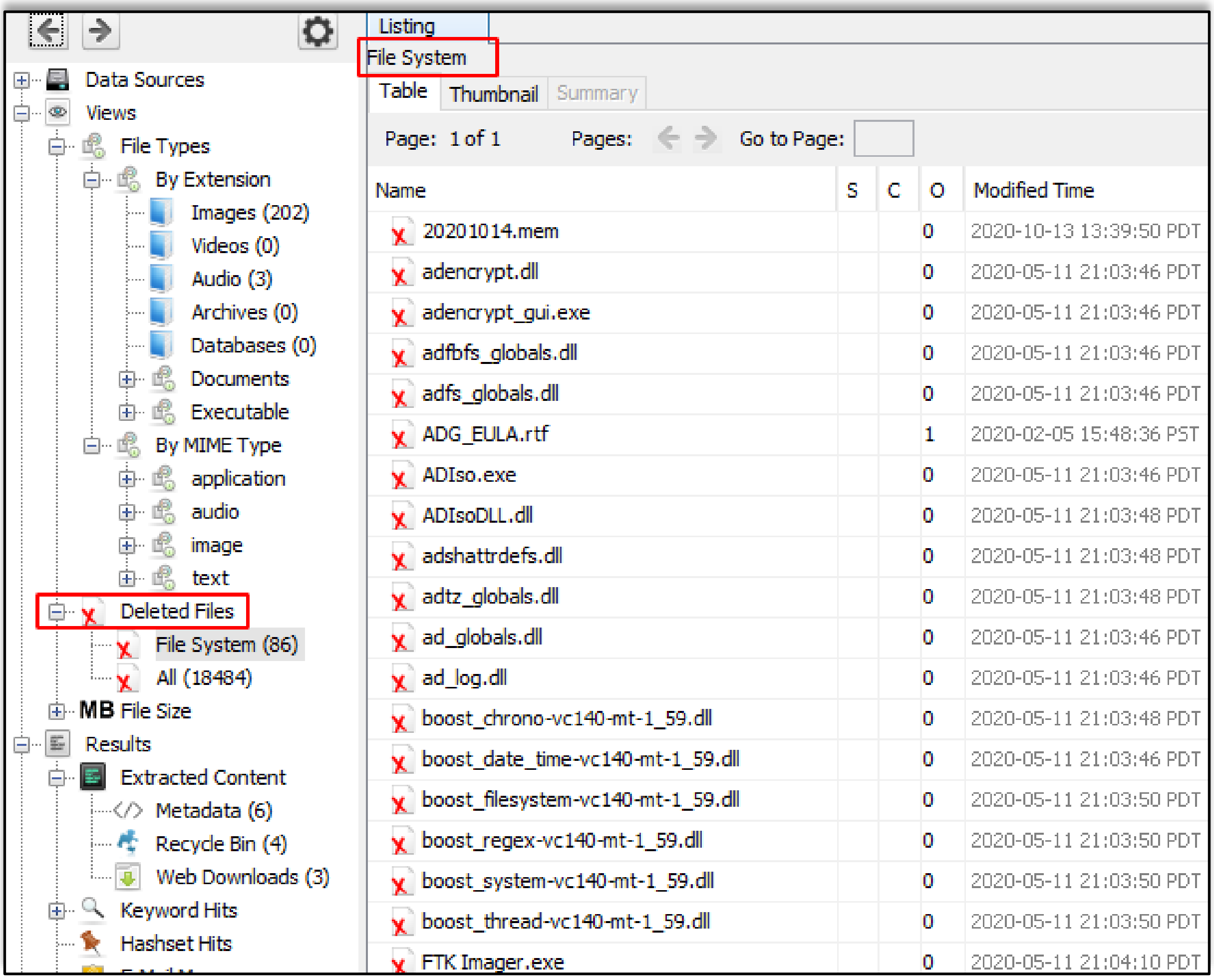
In this type of category, there are four sub-categories like application, audio, image, and text. They are divided further into more sections and file types.



By MIME Type
- application
  - zip (2)
  - x-dosexec (557)
  - pdf (3)
  - x-font-ttf (9)
  - rtf (2)
  - x-msdownload (1482)
  - xml (92)
  - xhtml+xml (2)
  - json (4)
  - octet-stream (14915)
  - x.windows-registry (27)
  - javascript (75)
- audio
  - vnd.wave (3)
- image
  - vnd.microsoft.icon (2)
  - bmp (1)
  - gif (1)
  - png (164)
  - jpeg (14)
  - svg+xml (14)
  - vnd.zbrush.pcx (1)
  - webp (18)
- text
  - x-java-source (57)
  - css (27)
  - x-fortran (3)
  - plain (1153)
  - x-chdr (24)
  - xml (43)
  - csv (5)
  - x-csrc (3)
  - html (136)
  - x-ini (29)
  - x-log (2)

Deleted Files

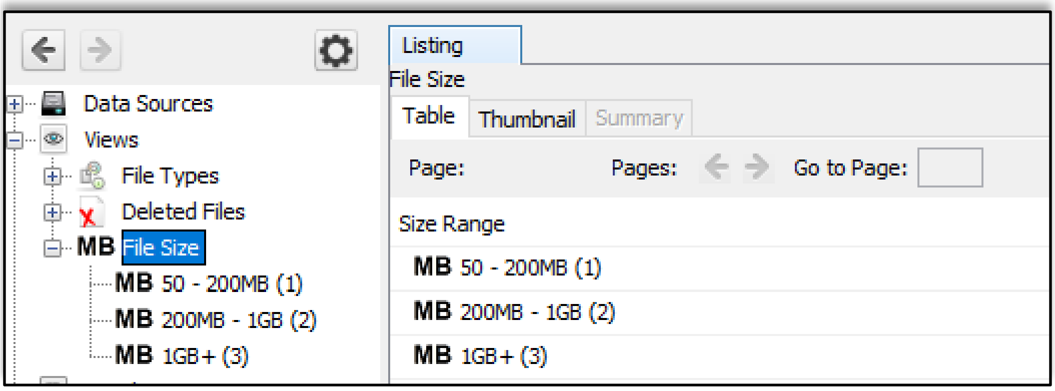
It displays information about the deleted file which can be then recovered.



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
adfbfs_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.



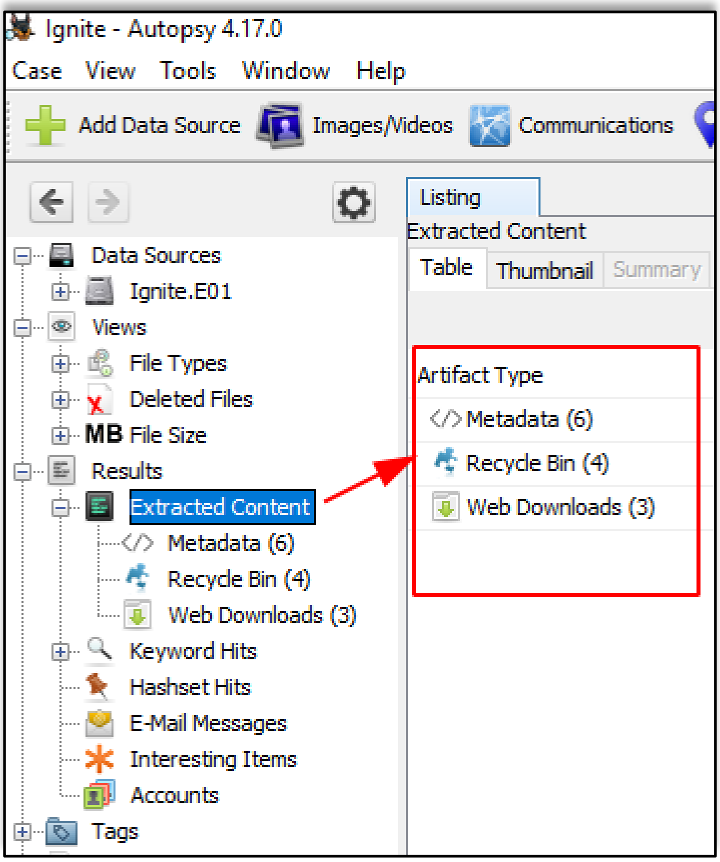
Size Range
MB 50 - 200MB (1)
MB 200MB - 1GB (2)
MB 1GB+ (3)

Results

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

Extracted Content

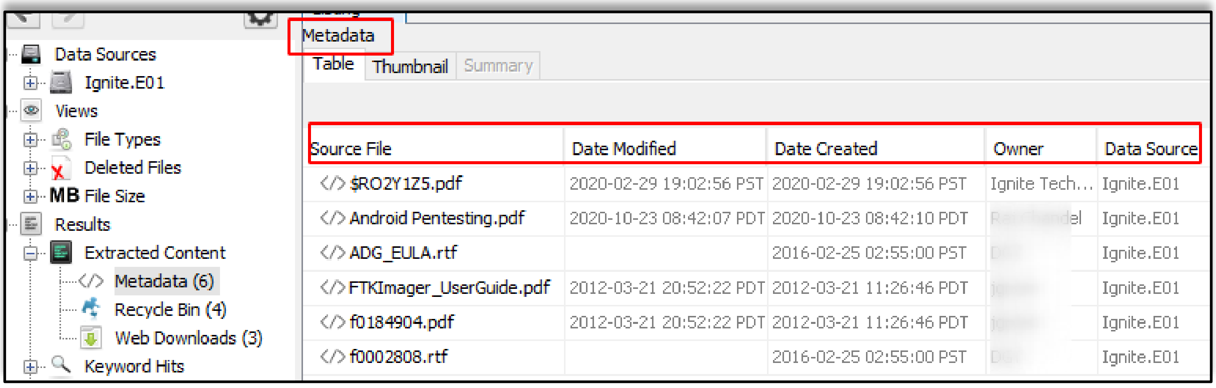
All the content that was extracted, is segregated further in detail. Here we have found metadata, Recycle Bin, and web downloads. Let us further view each one of them.



Artifact Type
Metadata (6)
Recycle Bin (4)
Web Downloads (3)

Metadata

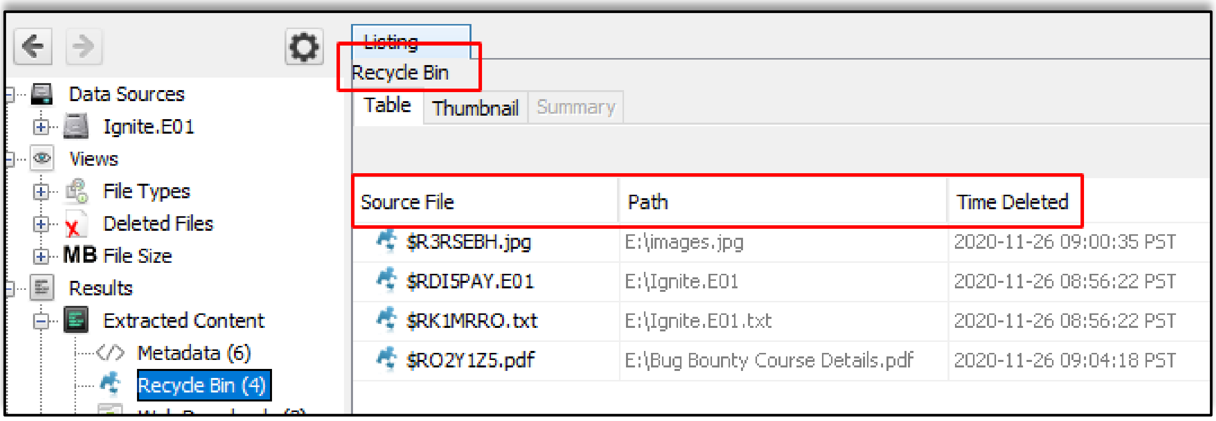
Here we can view all the information about the files like the date it was created, to was modified, file's owner, etc.



Source File	Date Modified	Date Created	Owner	Data Source
$RO2Y1Z5.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	[redacted]	Ignite.E01
ADG_EULA.rtf		2016-02-25 02:55:00 PST	[redacted]	Ignite.E01
FTKImager_UserGuide.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	[redacted]	Ignite.E01
f0184904.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	[redacted]	Ignite.E01
f0002808.rtf		2016-02-25 02:55:00 PST	[redacted]	Ignite.E01

Recycle Bin

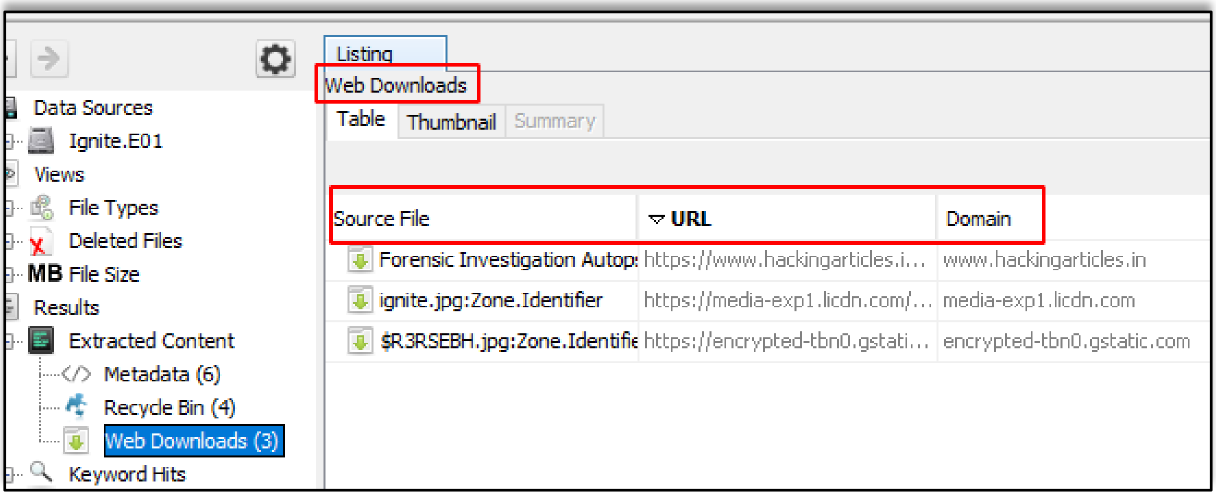
The files that were put in the recycle bin are found in this category.



Source File	Path	Time Deleted
$R3RSEBH.jpg	E:\images.jpg	2020-11-26 09:00:35 PST
$RDI5PAY.E01	E:\Ignite.E01	2020-11-26 08:56:22 PST
$RK1MRRO.txt	E:\Ignite.E01.txt	2020-11-26 08:56:22 PST
$RO2Y1Z5.pdf	E:\Bug Bounty Course Details.pdf	2020-11-26 09:04:18 PST

Web Downloads

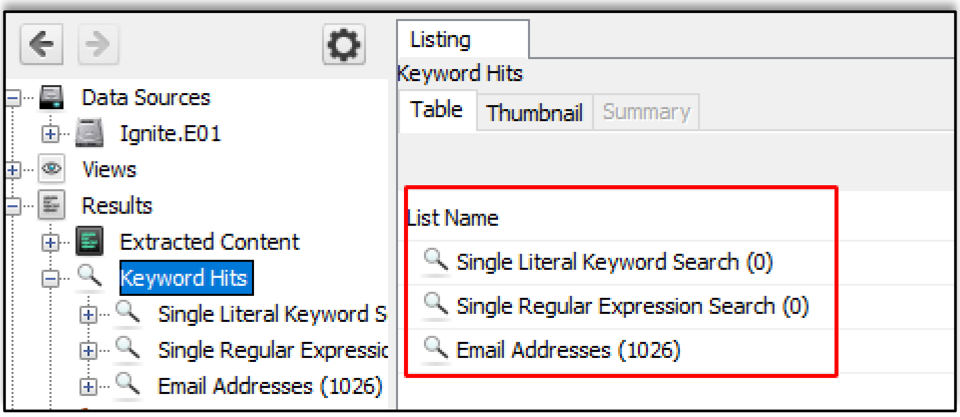
Here you can see the files that were downloaded from the internet.



Source File	URL	Domain
Forensic Investigation Autop:	https://www.hackingarticles.i...	www.hackingarticles.in
ignite.jpg:Zone.Identifier	https://media-exp1.licdn.com/...	media-exp1.licdn.com
$R3RSEBH.jpg:Zone.Identifie	https://encrypted-tbn0.gstati...	encrypted-tbn0.gstatic.com

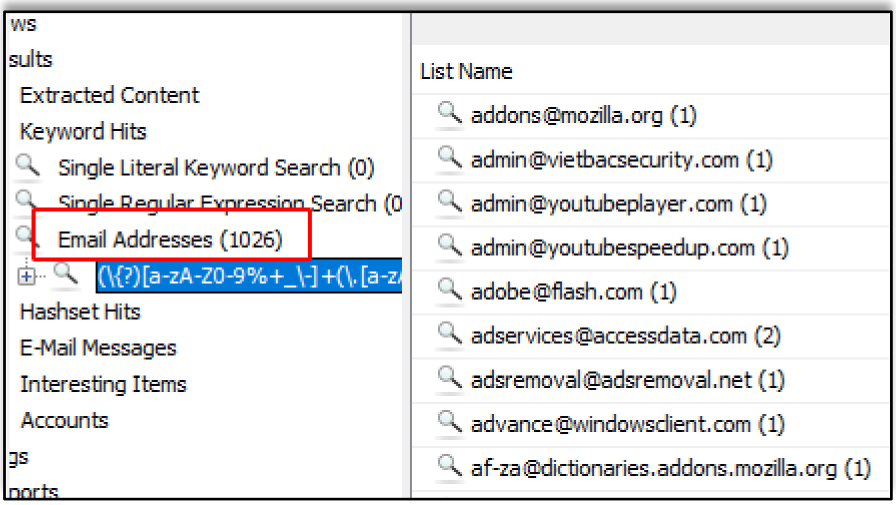
Keyword Hits

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.

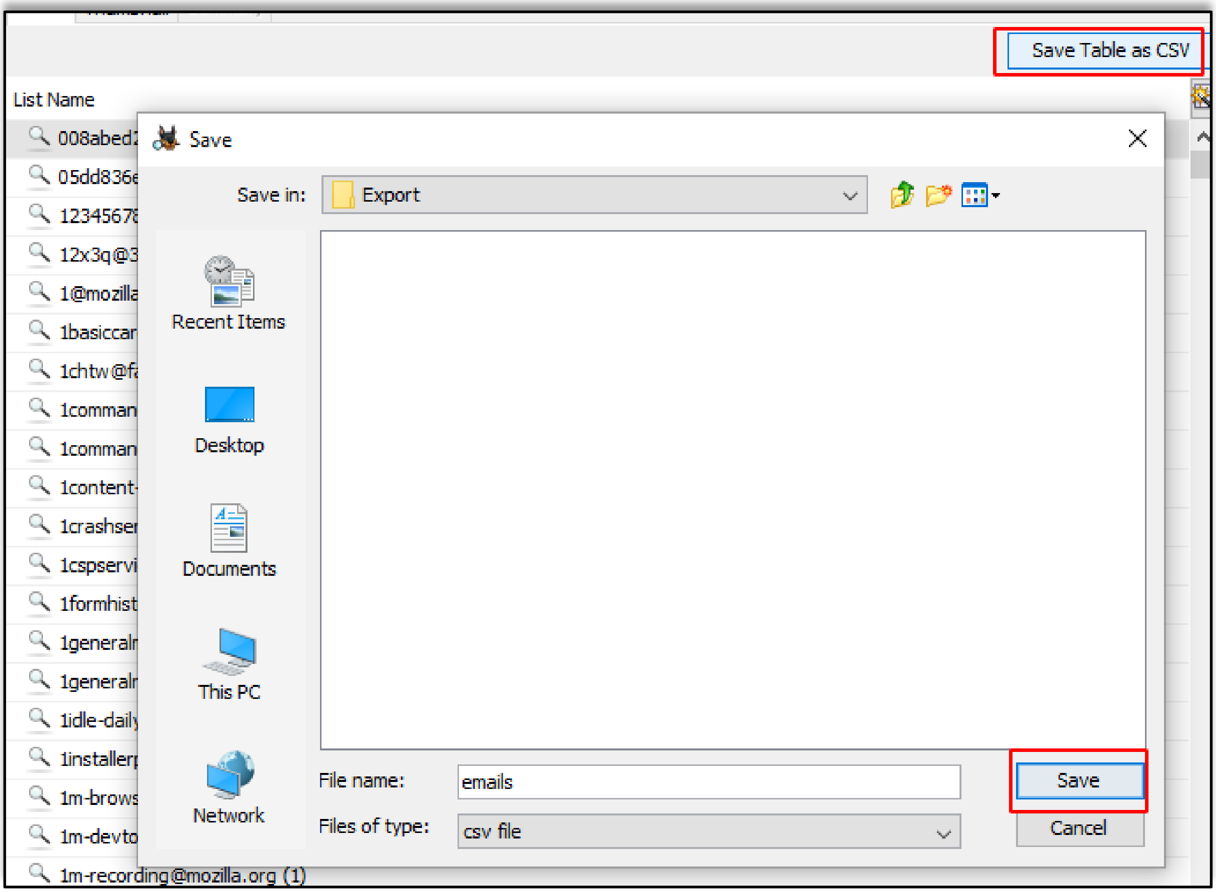


List Name
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (1026)

You can view the available email addresses.

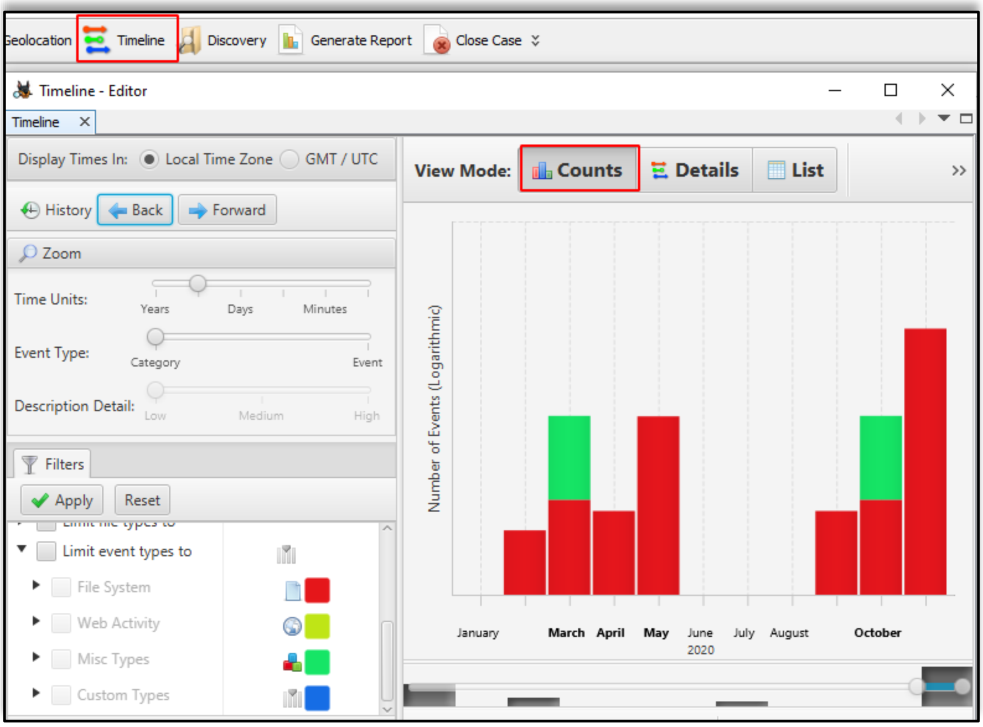

ws
sults
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0
Email Addresses (1026)
(\{?)[a-zA-Z0-9%+_\-]+(\.[a-z
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
gs
ports
List Name
addons@mozilla.org (1)
admin@vietbacsecurity.com (1)
admin@youtubeplayer.com (1)
admin@youtubespeedup.com (1)
adobe@flash.com (1)
adservices@accessdata.com (2)
adsremoval@adsremoval.net (1)
advance@windowsclient.com (1)
af-za@dictionaries.addons.mozilla.org (1)

You can choose to export into a CSV format.

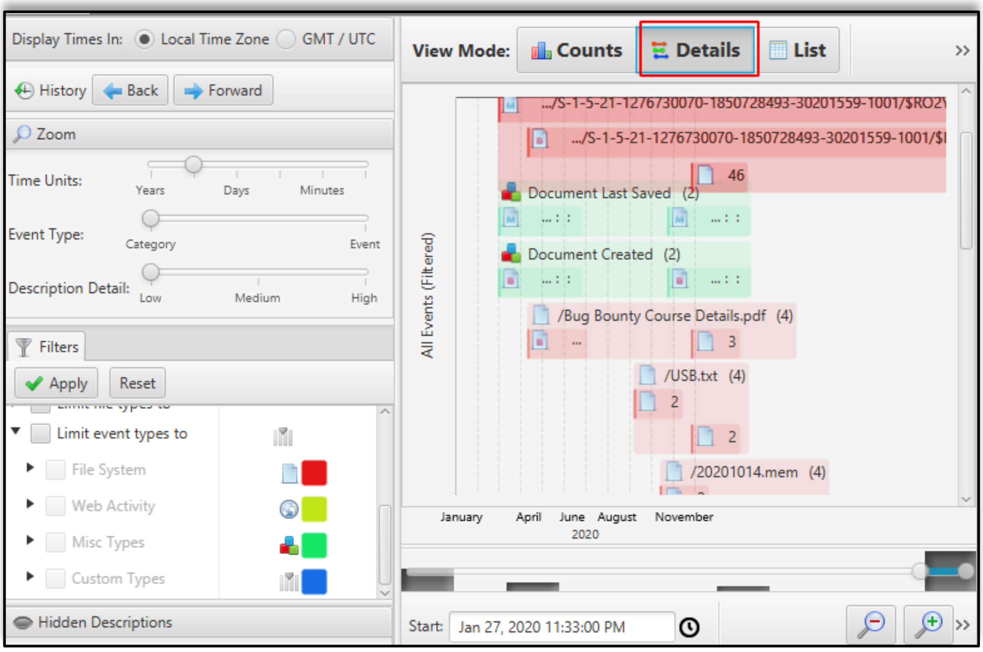


Timeline

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

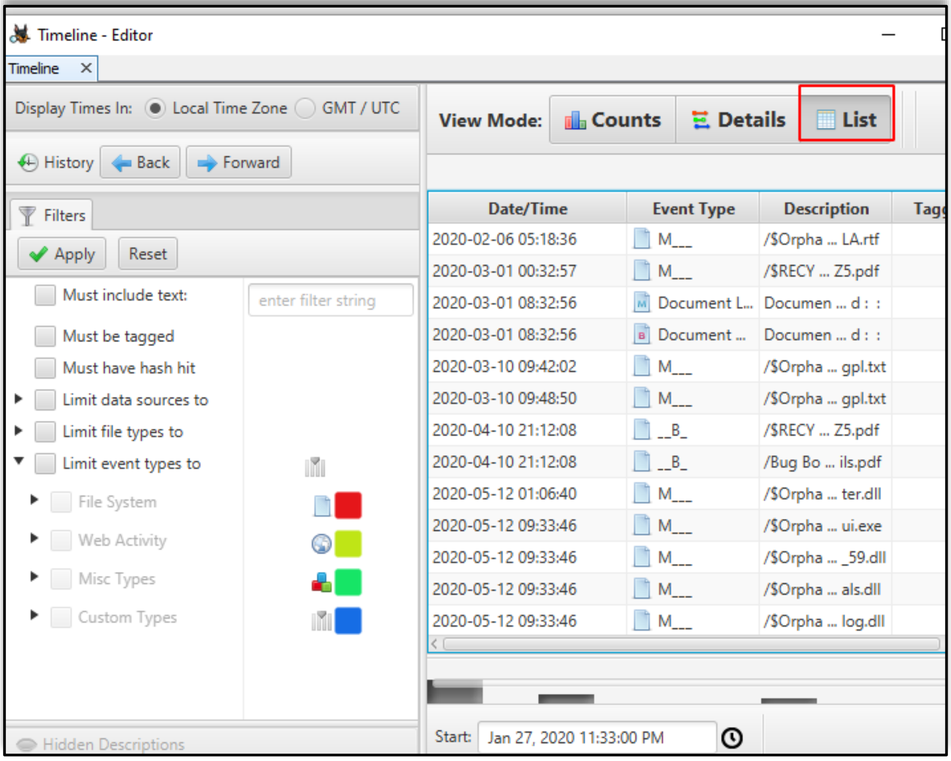


Display Times In: ● Local Time Zone ○ GMT / UTC



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

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



Timeline - Editor

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

View Mode: Counts | Details | List

Filters: Apply | Reset

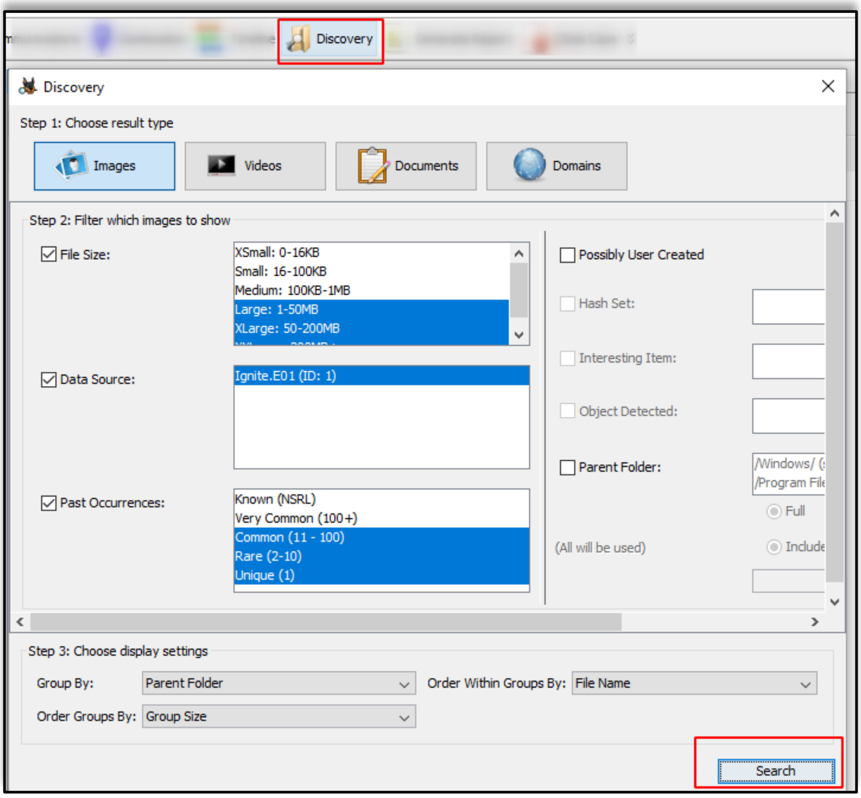
□ Must include text: enter filter string
□ Must be tagged
□ Must have hash hit
□ Limit data sources to
□ Limit file types to
□ Limit event types to
□ File System
□ Web Activity
□ Misc Types
□ Custom Types

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	Document L...	Documen ... d : :	
2020-03-01 08:32:56	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.



Discovery

Step 1: Choose result type

Images | Videos | Documents | Domains

Step 2: Filter which images to show

☑ File Size: XSmall: 0-16KB, Small: 16-100KB, Medium: 100KB-1MB, **Large: 1-50MB**, **XLarge: 50-200MB** (selected)

☑ Data Source: **Ignite.E01 (ID: 1)** (selected)

☑ Past Occurrences: Known (NSRL), Very Common (100+), **Common (11 - 100)**, **Rare (2-10)**, **Unique (1)** (selected)

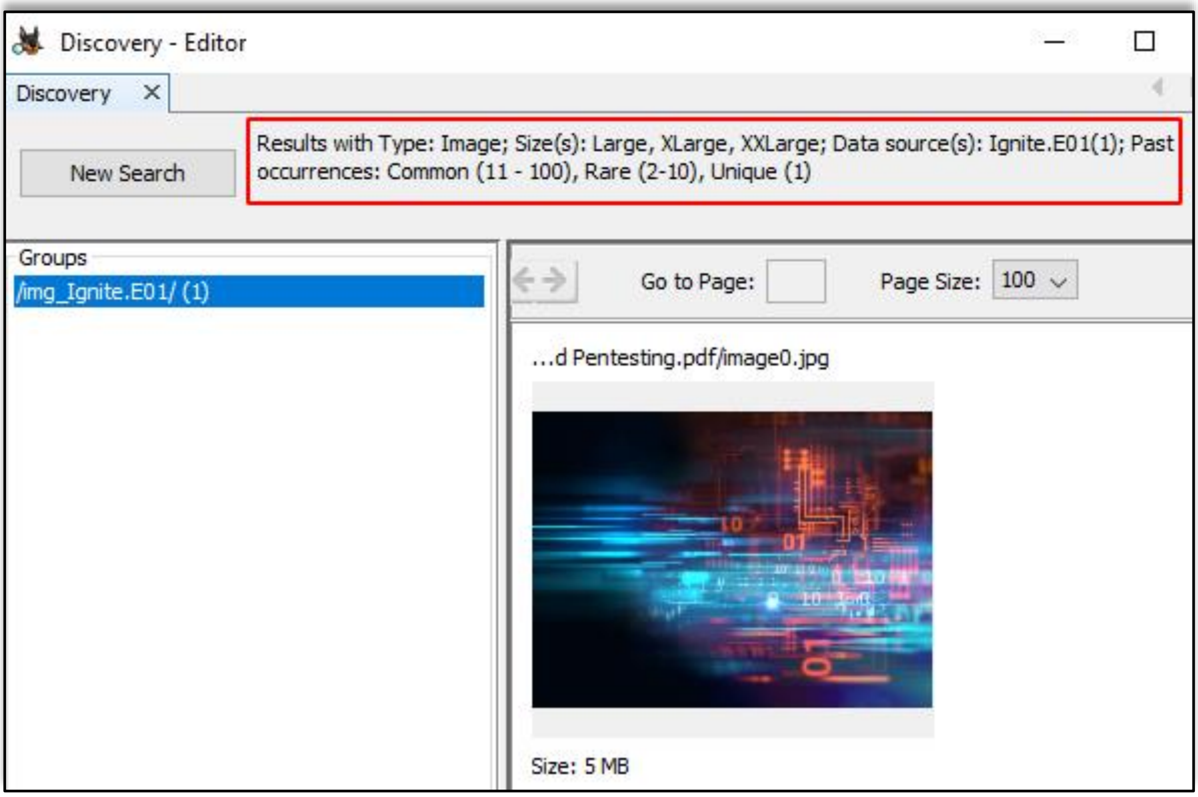
□ Possibly User Created
□ Hash Set:
□ Interesting Item:
□ Object Detected:
□ Parent Folder: /Windows/ /Program File
○ Full ○ Include
(All will be used)

Step 3: Choose display settings

Group By: Parent Folder
Order Within Groups By: File Name
Order Groups By: Group Size

Search

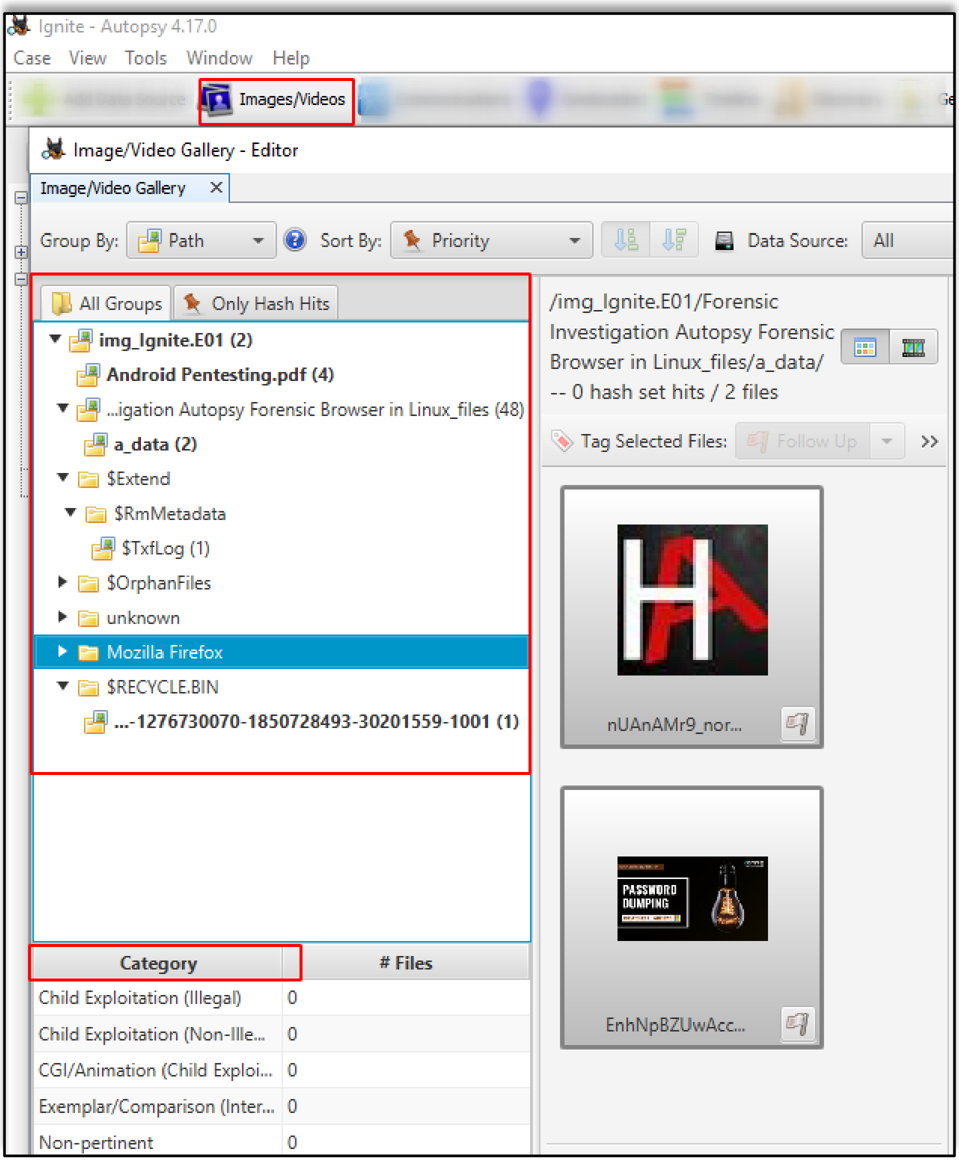
According to the selected options, you can get the desired results.



Results with Type: Image; Size(s): Large, XLarge, XXLarge; Data source(s): Ignite.E01(1); Past occurrences: Common (11 - 100), Rare (2-10), Unique (1)

Images/Videos

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



Group By: Path | Sort By: Priority | Data Source: All

- 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

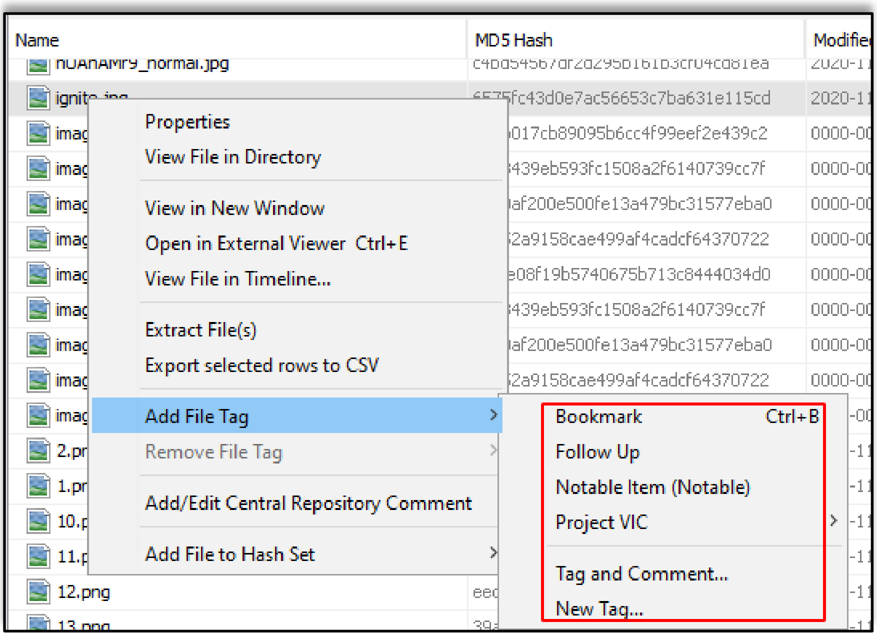
nUAnAMr9_nor...

EnhNpBZUwAcc...

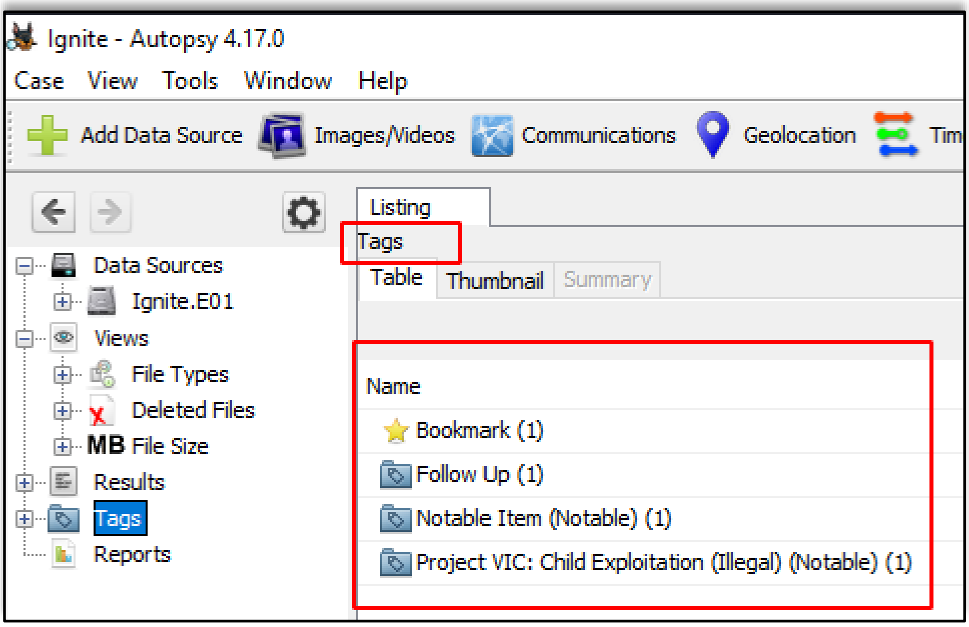
Category	# Files
Child Exploitation (Illegal)	0
Child Exploitation (Non-Ille...	0
CGI/Animation (Child Exploi...	0
Exemplar/Comparison (Inter...	0
Non-pertinent	0

Add File Tag

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

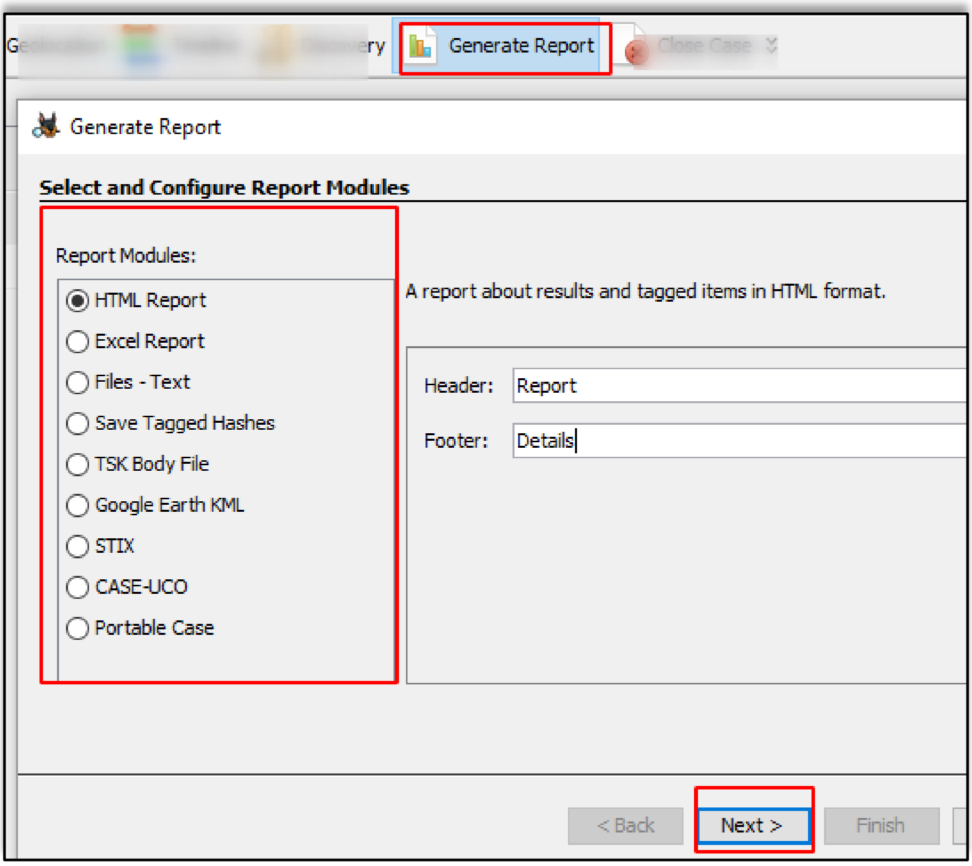


Now when you see the tags options, you will see that files were tagged according to various categories.



Generate Report

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

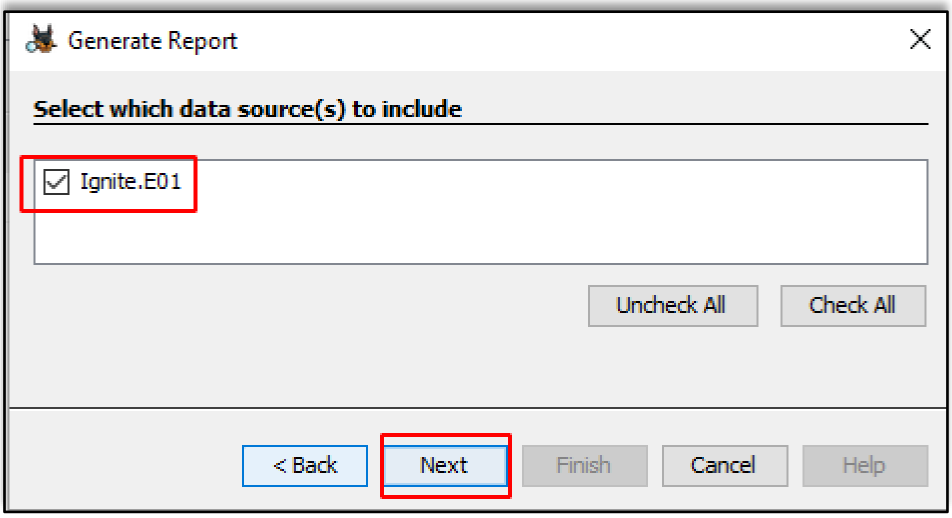


A report about results and tagged items in HTML format.

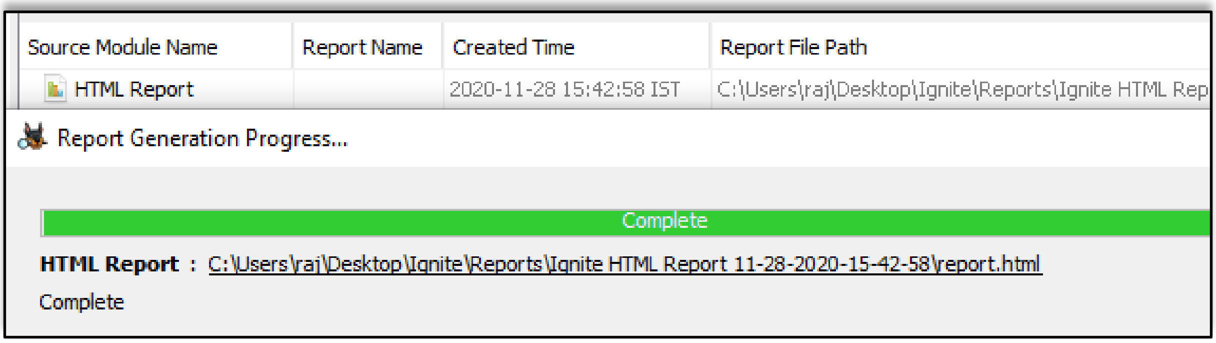
Header: Report

Footer: Details

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

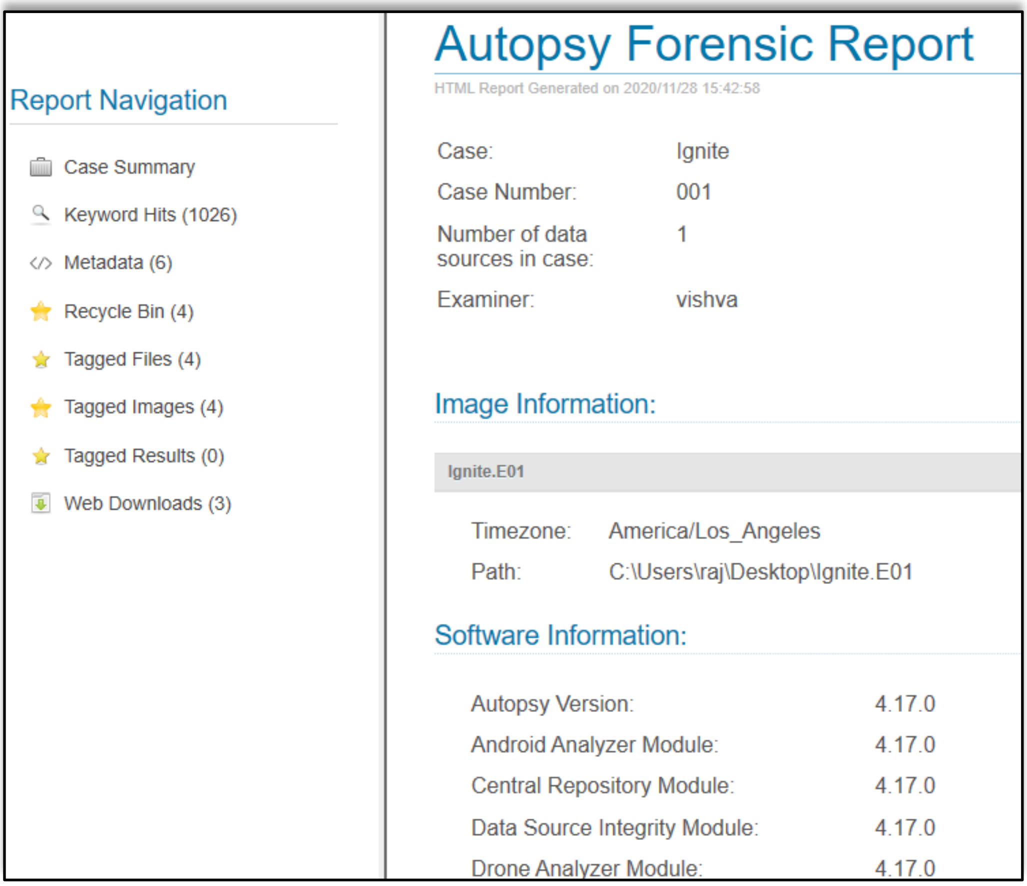
Report Generation Progress...

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

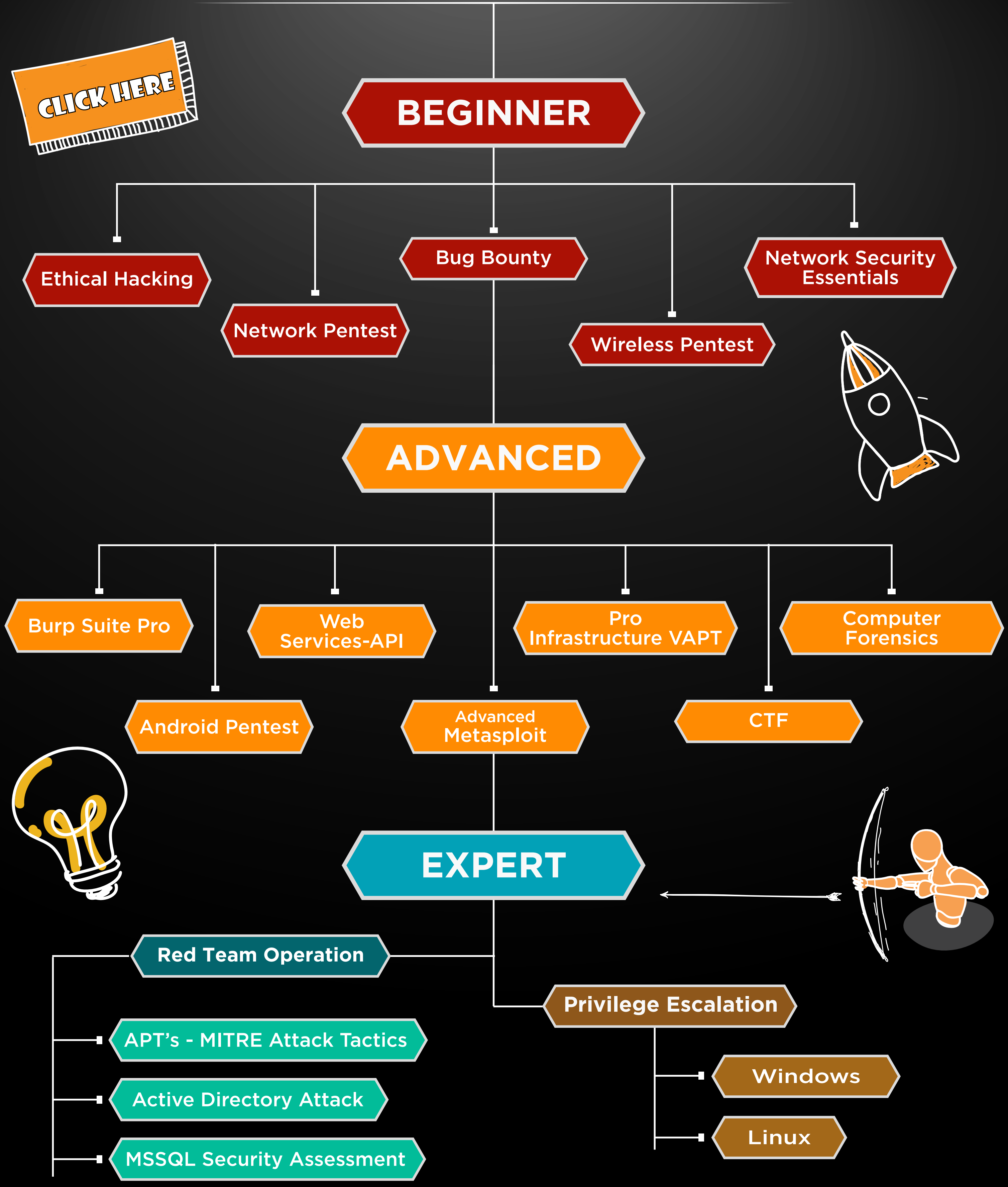
References

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

iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE



BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in