

Table of Contents

Abstract	3
Autopsy for Kali Linux	5
Purpose of Autopsy	5
Creating a New Case	6
Add Image File	9
File Analysis	12
File Type	16
Image Details	19
Keyword Search	21
Autopsy for Windows	23
Creating a New Case	23
Views	28
File Type	28
By Extension	29
By Mime Type	36
Deleted Files	37
MB size Files	37
Results	38
Extracted Content	38
Keyword Hits	39
Timeline	41
Discovery	42
Images/Videos	44
Add File Tag	45
Generate Report	46
References	47
About Us	48

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

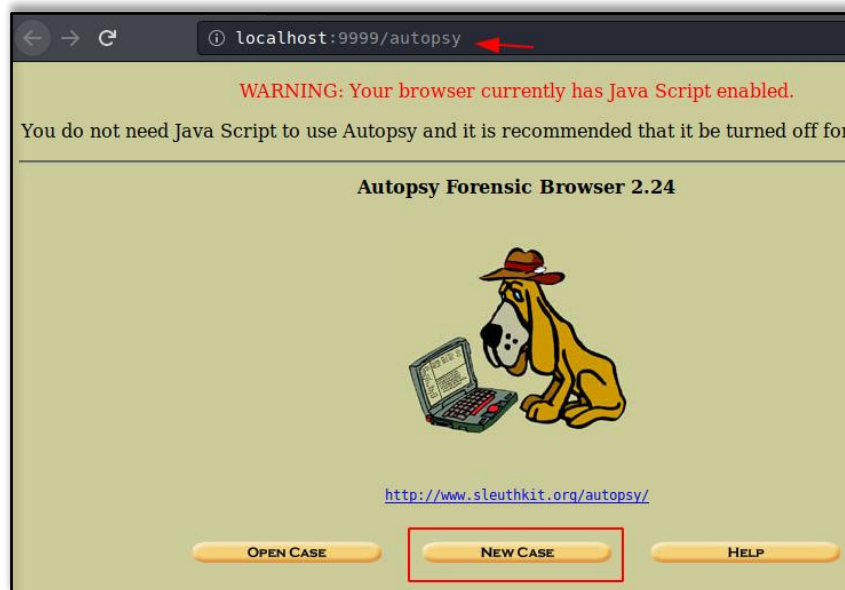
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy

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.



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
c.		d.	
e.		f.	
g.		h.	
i.		j.	

NEW CASE CANCEL HELP

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

ADD HOST

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

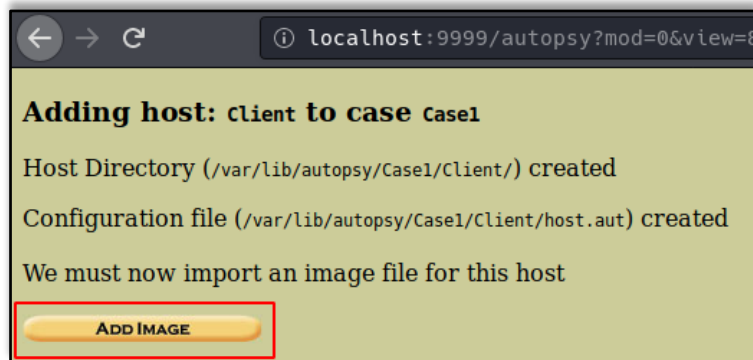
localhost:9999/autopsy?mod=0&view=7&case=Jeenali&inv=Jeenali&

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- 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.
- 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.
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known good files.

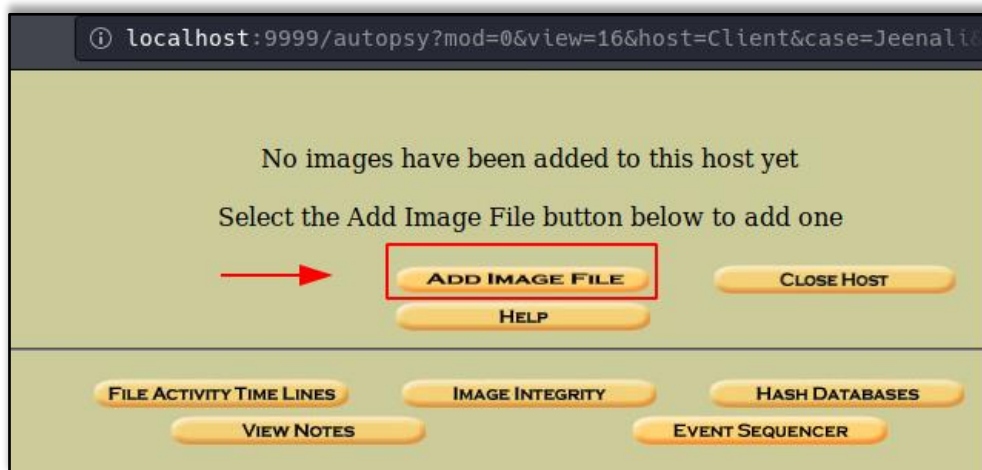
Add Image File

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



It is a golden rule of Digital forensics, that one should never work on the original evidence and hence an image of the original evidence should be created. An image can be created in various methods and tools as well as in various formats.

Once the image is acquired, the **'Add Image File'** option will allow you to import the image file to analyse.



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

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.

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.

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.

The screenshot shows a web browser window with the URL `localhost:9999/autopsy?case=Case1&host=Client&inv=Jeenali&mod=0`. The page title is "Image File Details". Below the title, the "Local Name" is displayed as `"/home/jeenali/Desktop/image2.e01"`. The "File System Details" section contains the following information:

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:

At the bottom of the form, there are three buttons: "ADD" (highlighted with a red box), "CANCEL", and "HELP".

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

The screenshot shows the Autopsy interface with the following text:

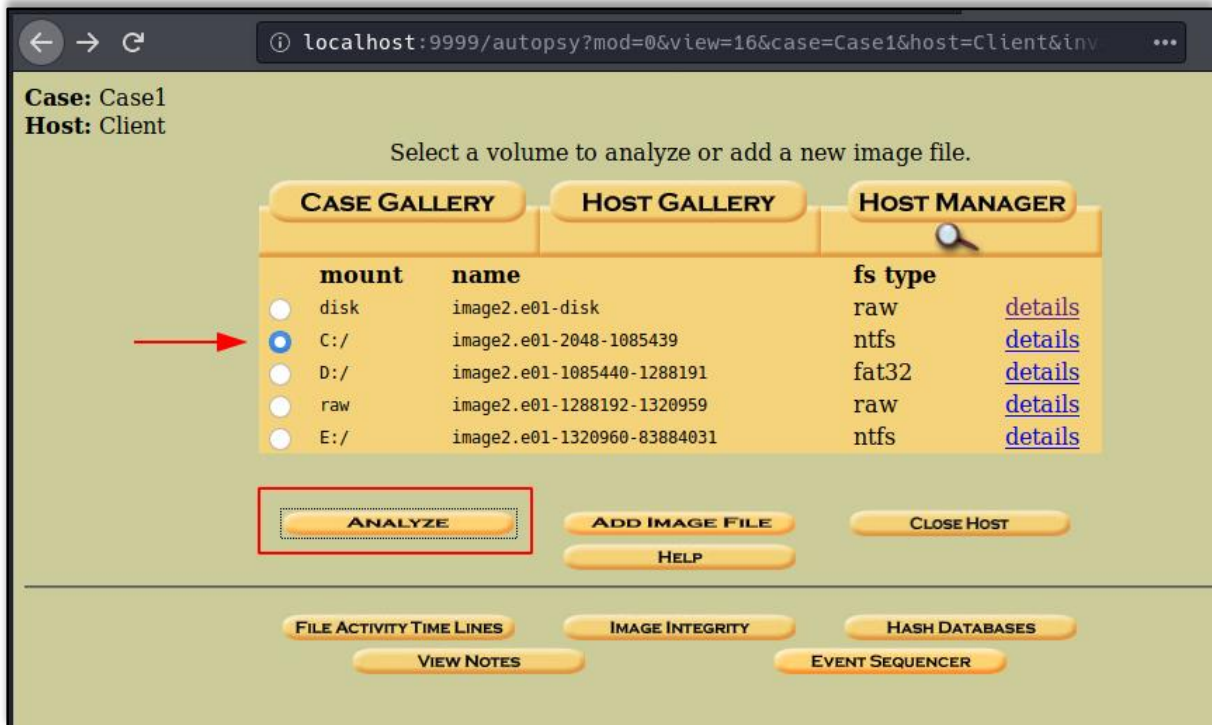
```

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
  
```

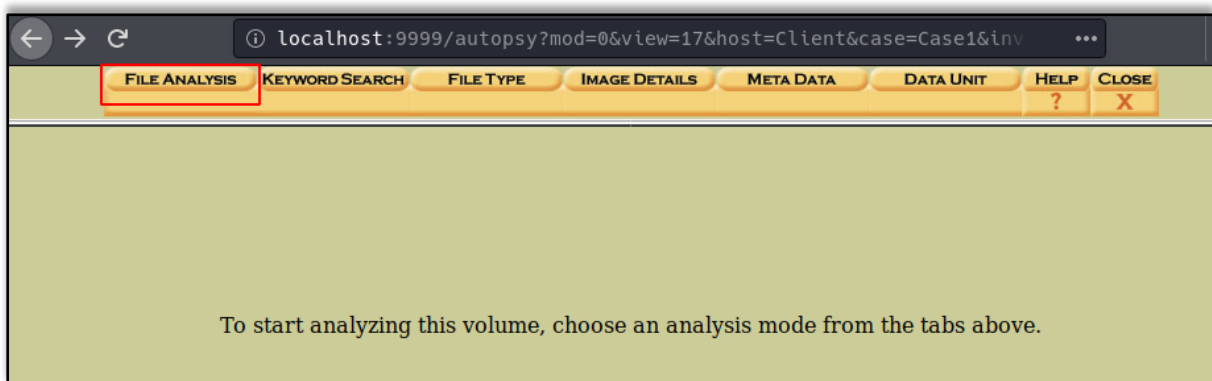
At the bottom, there are two buttons: "OK" (highlighted with a red box) and "ADD IMAGE".

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

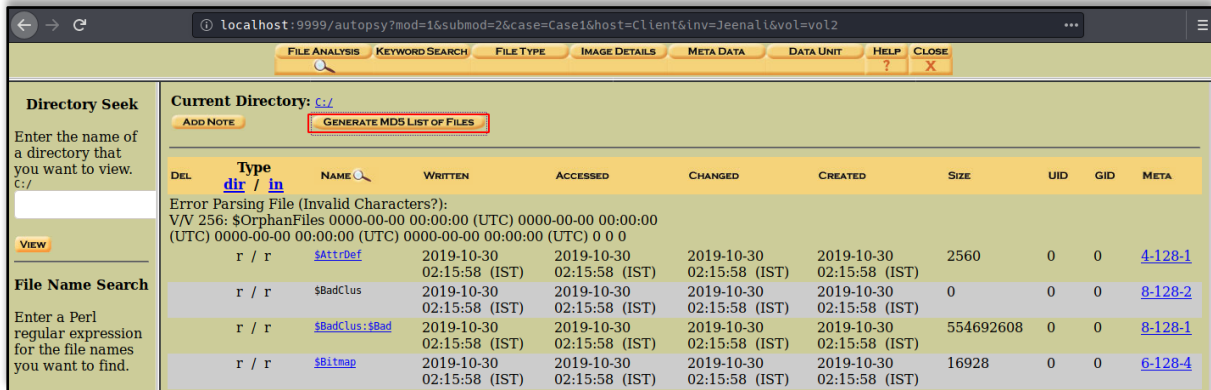


File Analysis

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

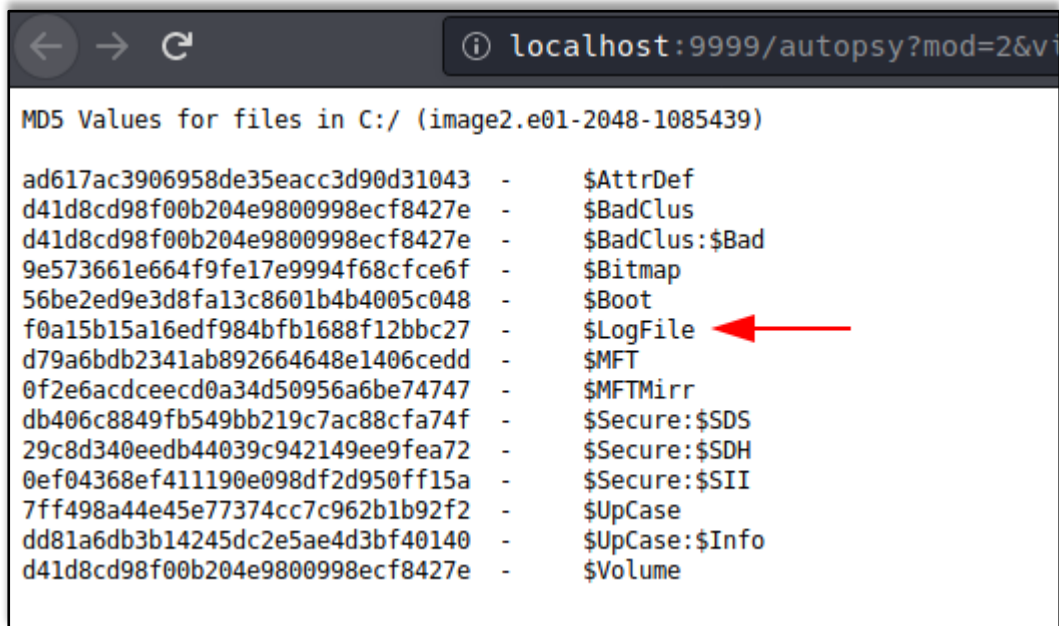


Now files will appear, which will give you the list of files and directories that are inside in this volume. From here you can analyze the content of the required image file and conduct the type of investigation you prefer. You can first generate a MD5 hash list of all the files present in this volume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



DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	dir / in	\$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
	dir / in	\$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
	dir / in	\$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
	dir / in	\$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
0f2e6acdcecd0a34d50956a6be74747 - $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	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	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) 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.

FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE

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

MFT Entry Number: 2-128-1

VIEW

ALLOCATION LIST

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

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

RSTR.0.....9N
@...B....p...0.@...I.....N9N
N.T.F.S.....

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

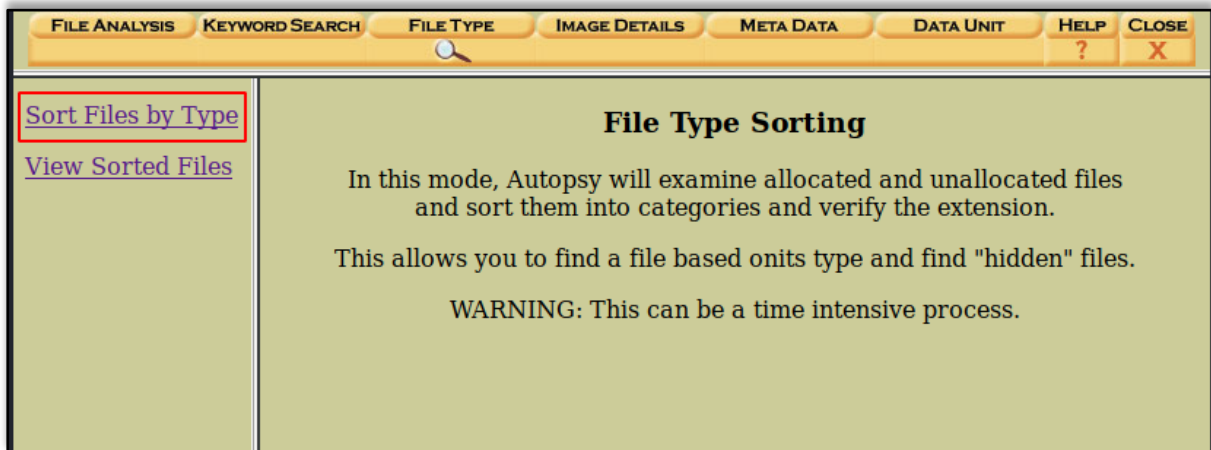
Current Directory: C:/

ADD NOTE GENERATE MD5 LIST OF FILES

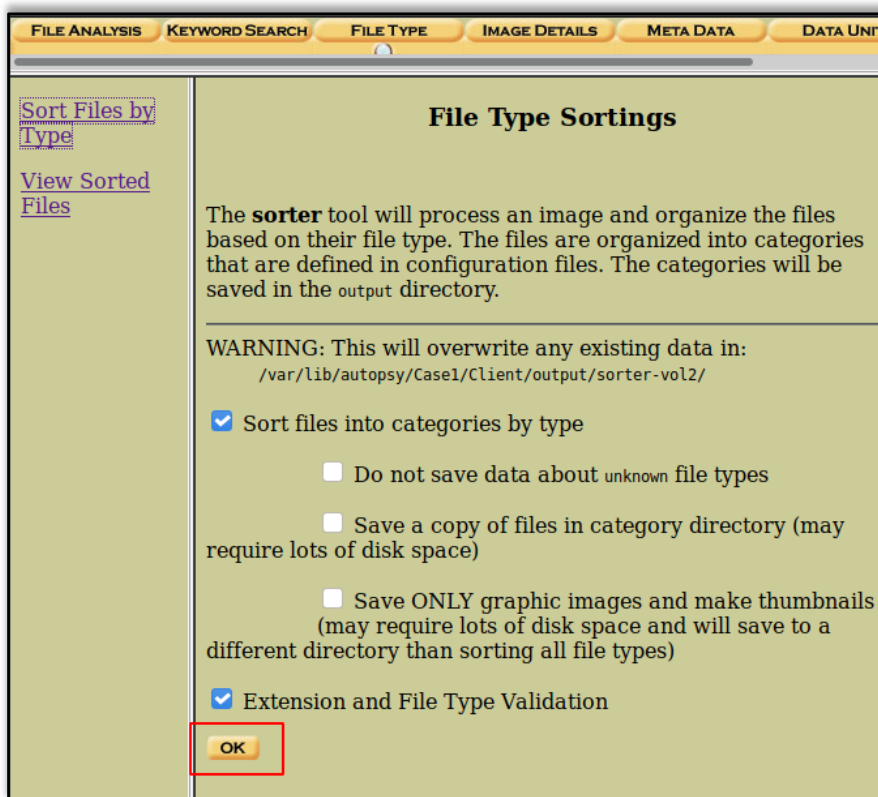
DEL	Type	NAME	WRITTEN	ACCESSED	CHAR
	dir / in				
	Error Parsing File (Invalid Characters?):				
	V/V 256: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0				
	r / r	\$AttrDef	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)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

File Type

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



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



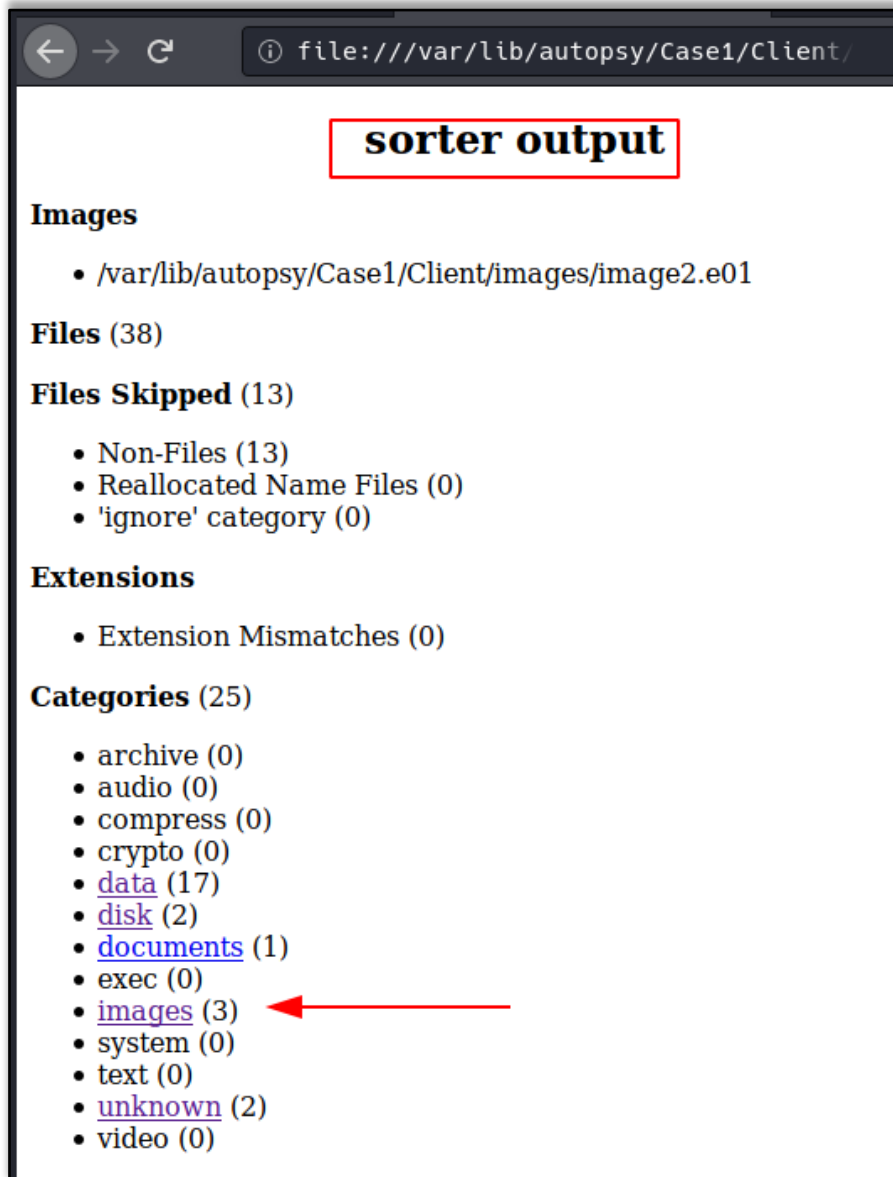
The categories of the file types will be displayed. Now to view the sorted files, click on 'View sorted files' and you will be displayed the list of sorted files.

The screenshot shows a web-based file analysis tool interface. At the top, there are five tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, and META DATA. The 'FILE TYPE' tab is currently selected. On the left side, there are two links: 'Sort Files by Type' and 'View Sorted Files', with the latter highlighted by a red box. The main content area displays the following information:

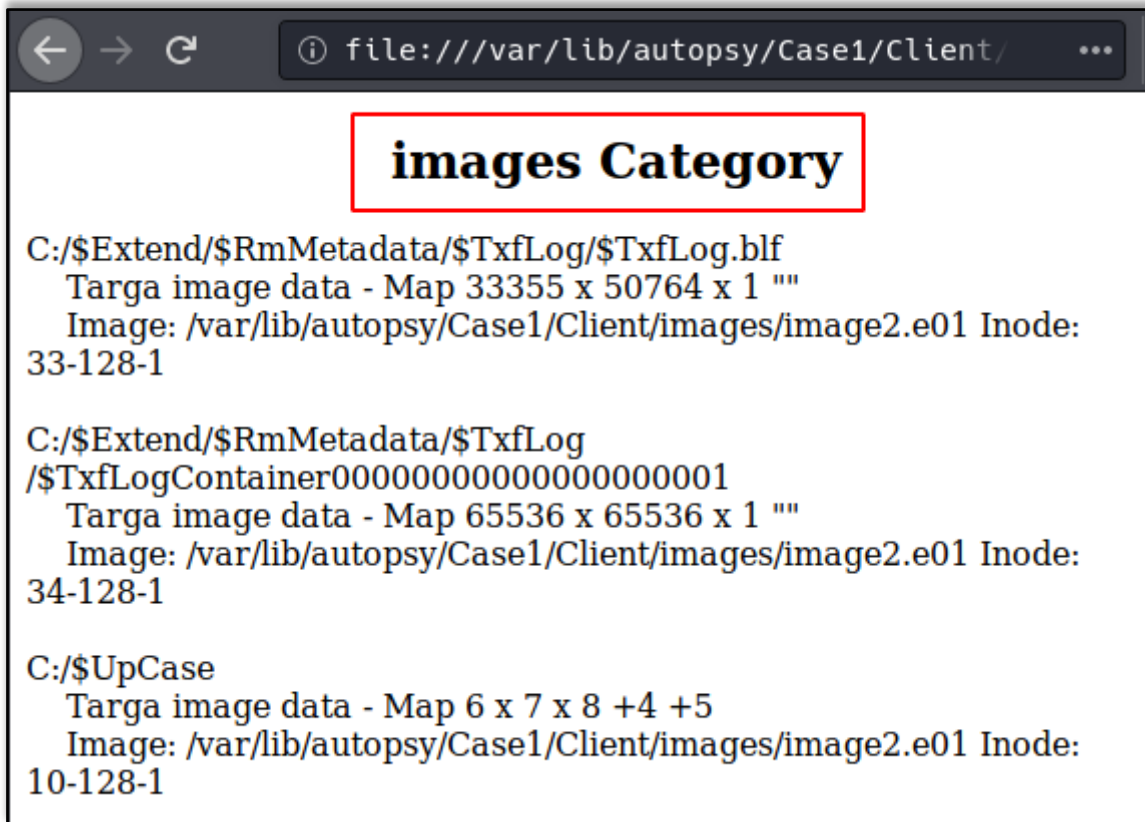
- Images**
 - /var/lib/autopsy/Case1/Client/images/image2.e01
- Files (38)**
- Files Skipped (13)**
 - Non-Files (13)
 - Reallocated Name Files (0)
 - 'ignore' category (0)
- Extensions**
 - Extension Mismatches (0)
- Categories (25)**
 - archive (0)
 - audio (0)
 - compress (0)
 - crypto (0)
 - data (17) ←
 - disk (2)
 - documents (1) ←
 - exec (0)
 - images (3) ←
 - system (0)
 - text (0)
 - unknown (2)
 - video (0)

Red arrows point to the 'data (17)', 'documents (1)', and 'images (3)' categories in the list.

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.



```

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

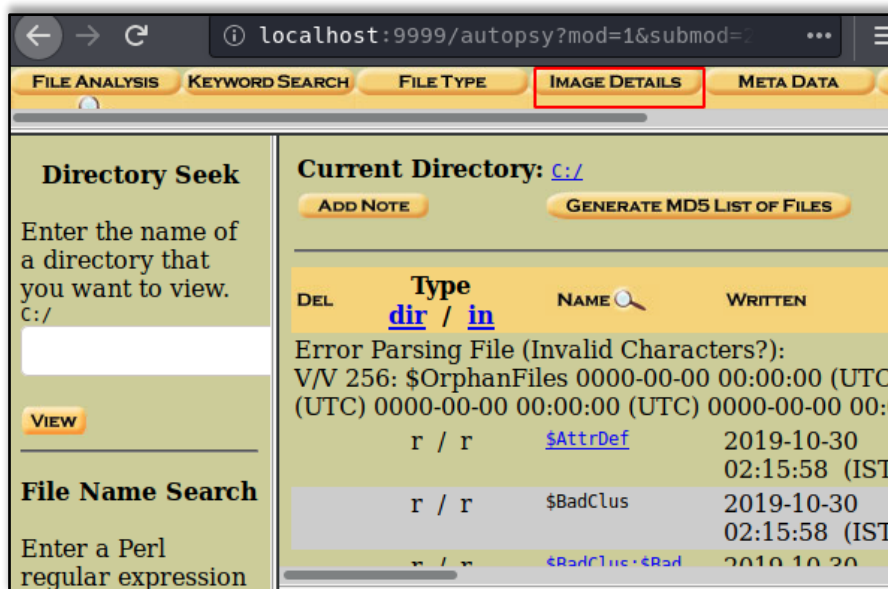
C:/$Extend/$RmMetadata/$TxfLog
/$TxfLogContainer000000000000000000000001
  Targa image data - Map 65536 x 65536 x 1 ""
  Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode:
  34-128-1

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

```

Image Details

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



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

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

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

File Name Search
Enter a Perl regular expression

Current Directory: C:/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type	NAME	WRITTEN
	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)
	r / r	\$AttrDef	2019-10-30 02:15:58 (IST)
	r / r	\$BadClus	2019-10-30 02:15:58 (IST)
	r / r	\$BadClus · \$Bad	2019-10-30

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

← → ↻ localhost:9999/autopsy?mod=1&submod=7&c ...

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA

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

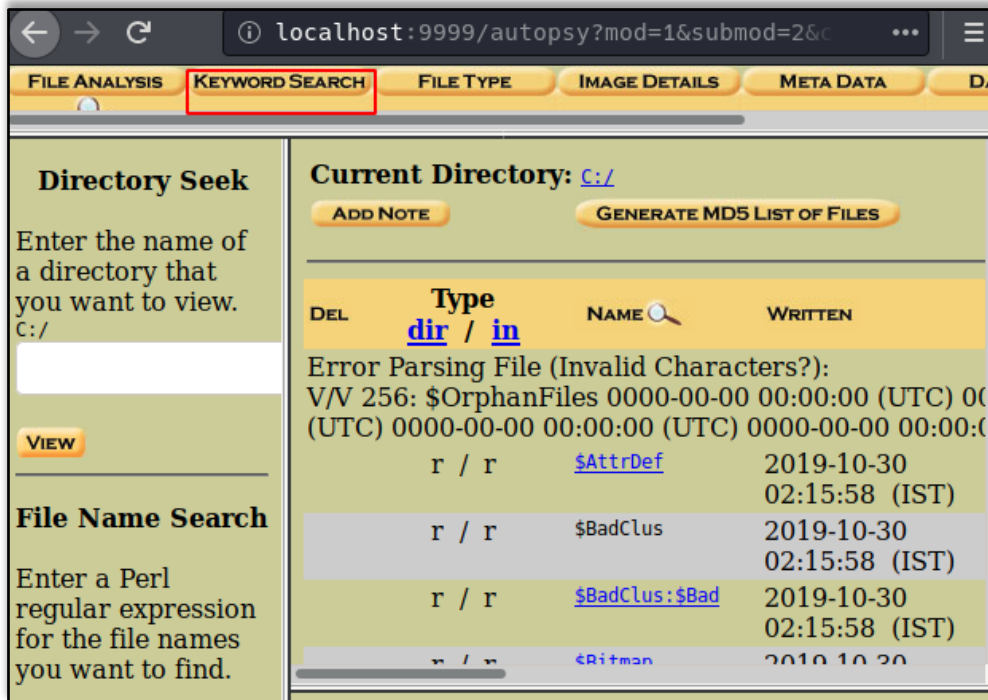
CONTENT INFORMATION

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.



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

