Forensic Investigation: Autopsy Forensic Browser in Linux

August 13, 2020 By Raj Chandel

Introduction

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 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

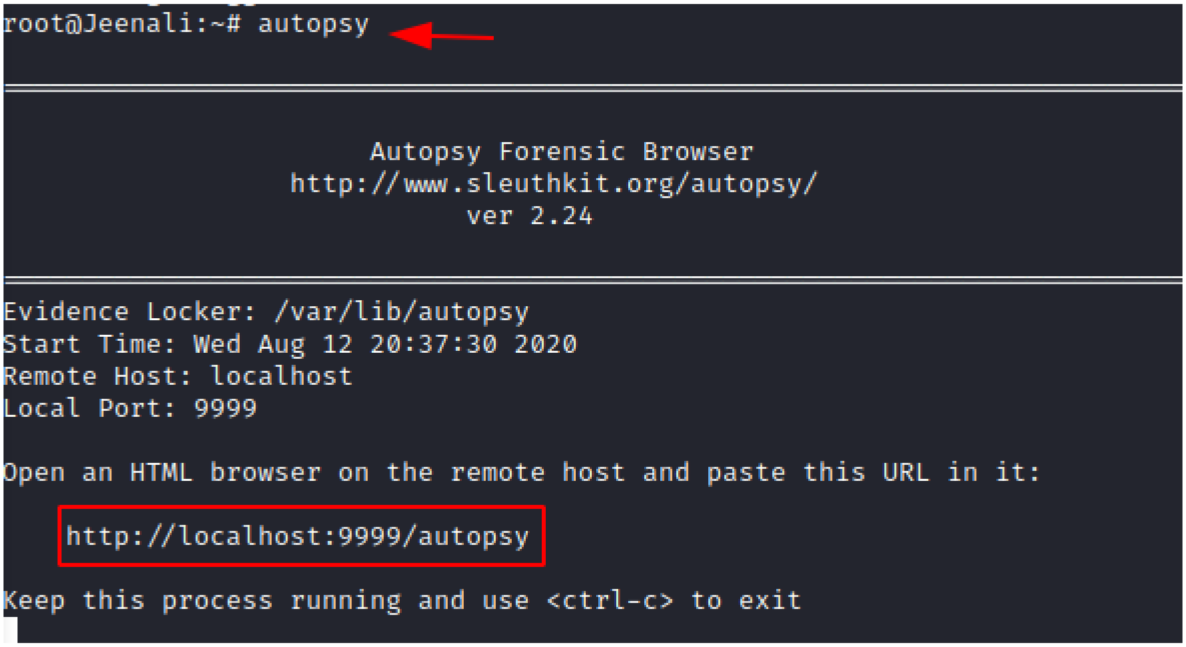
- Investigator can analyse Windows and UNIX storage disks and file systems like NTFS, FAT, UFS1/2, Ext2/3 using Autopsy.
- Autopsy is used by law enforcement, military, and corporate examiners to conduct investigations on a victim's or a criminal's PC.
- One can also use it to recover photos from one's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

Table of Contents:

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.

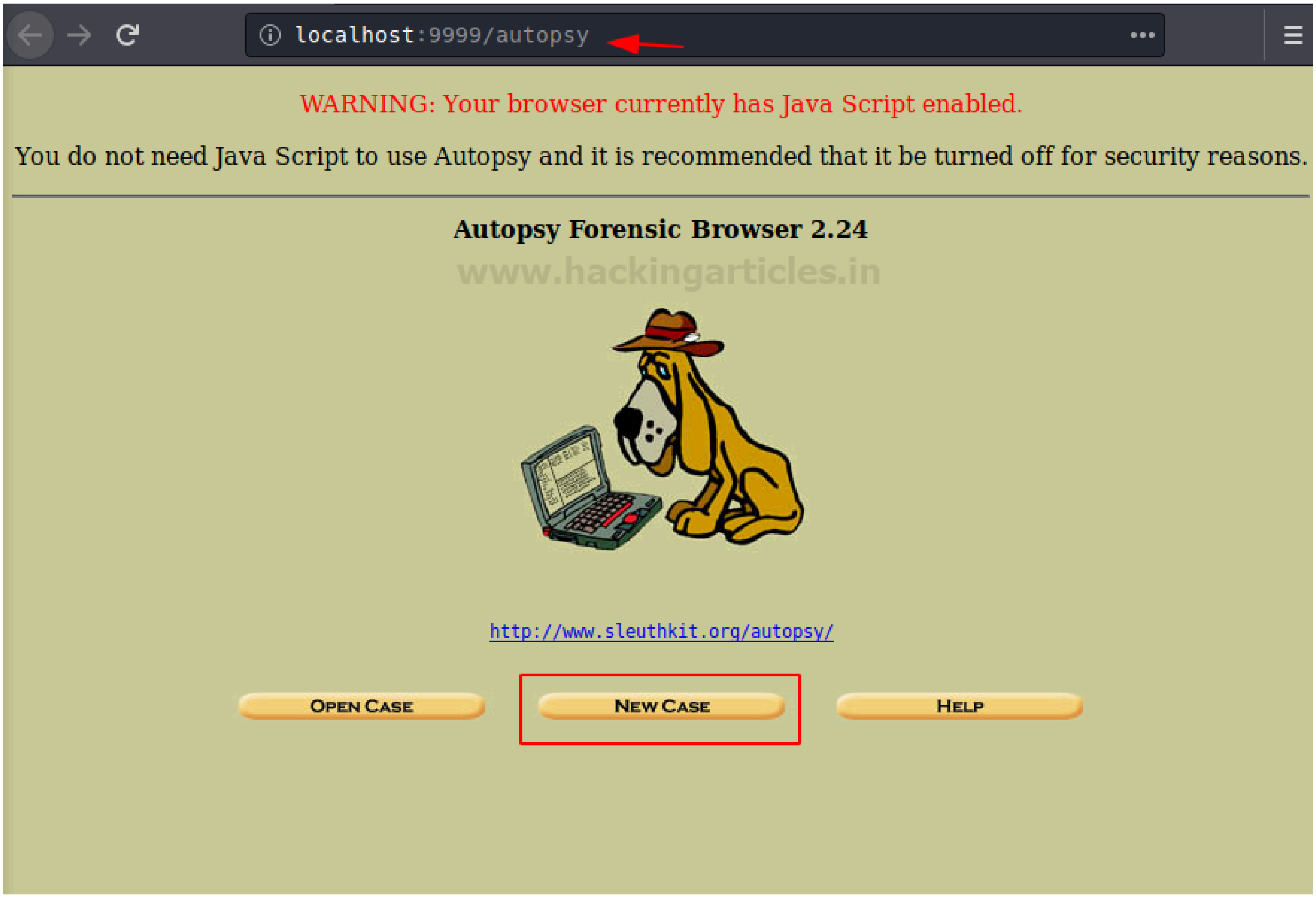


```
root@Jeenali:~# autopsy

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

                       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.

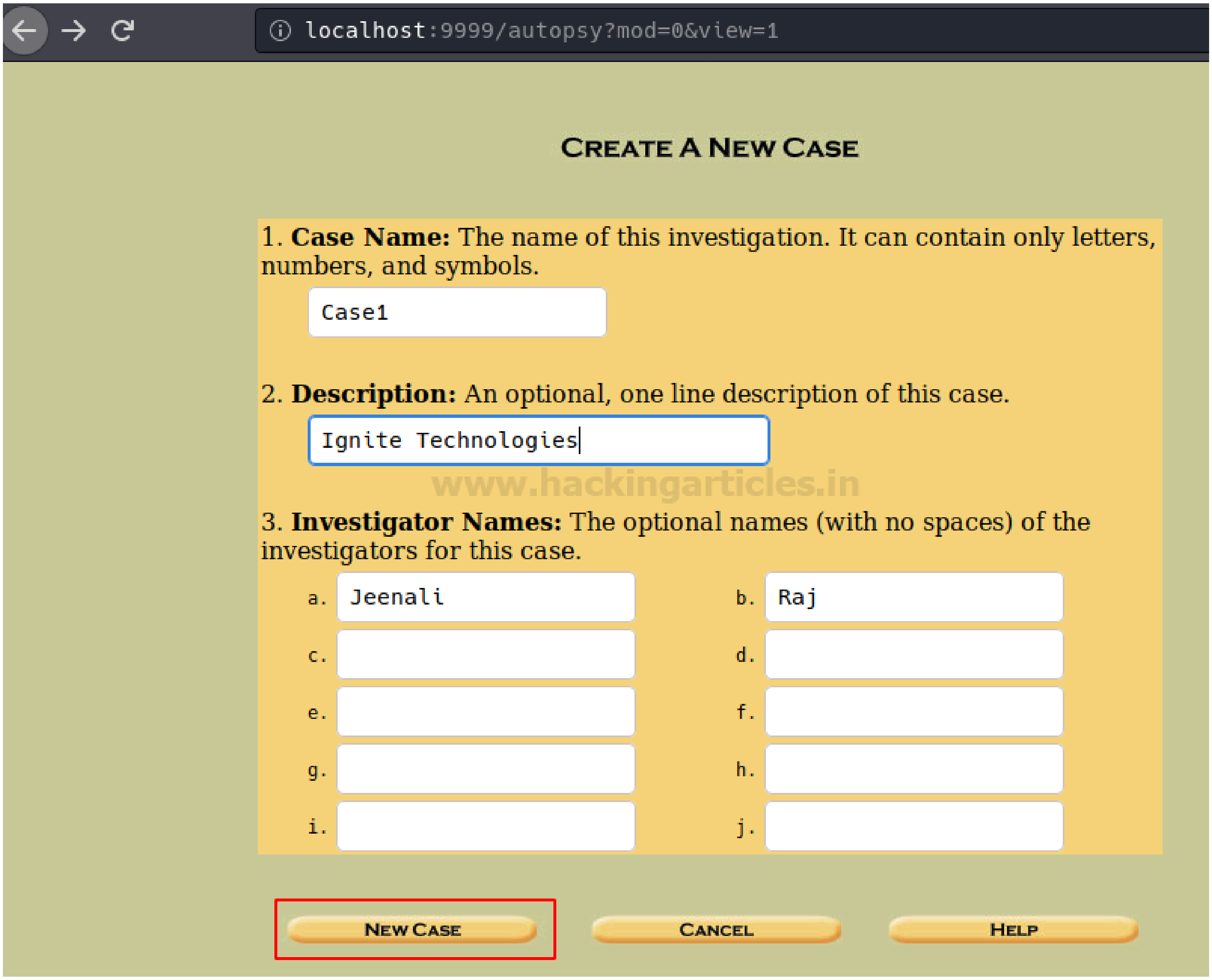


WARNING: Your browser currently has Java Script enabled.

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

Autopsy Forensic Browser 2.24

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’



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.

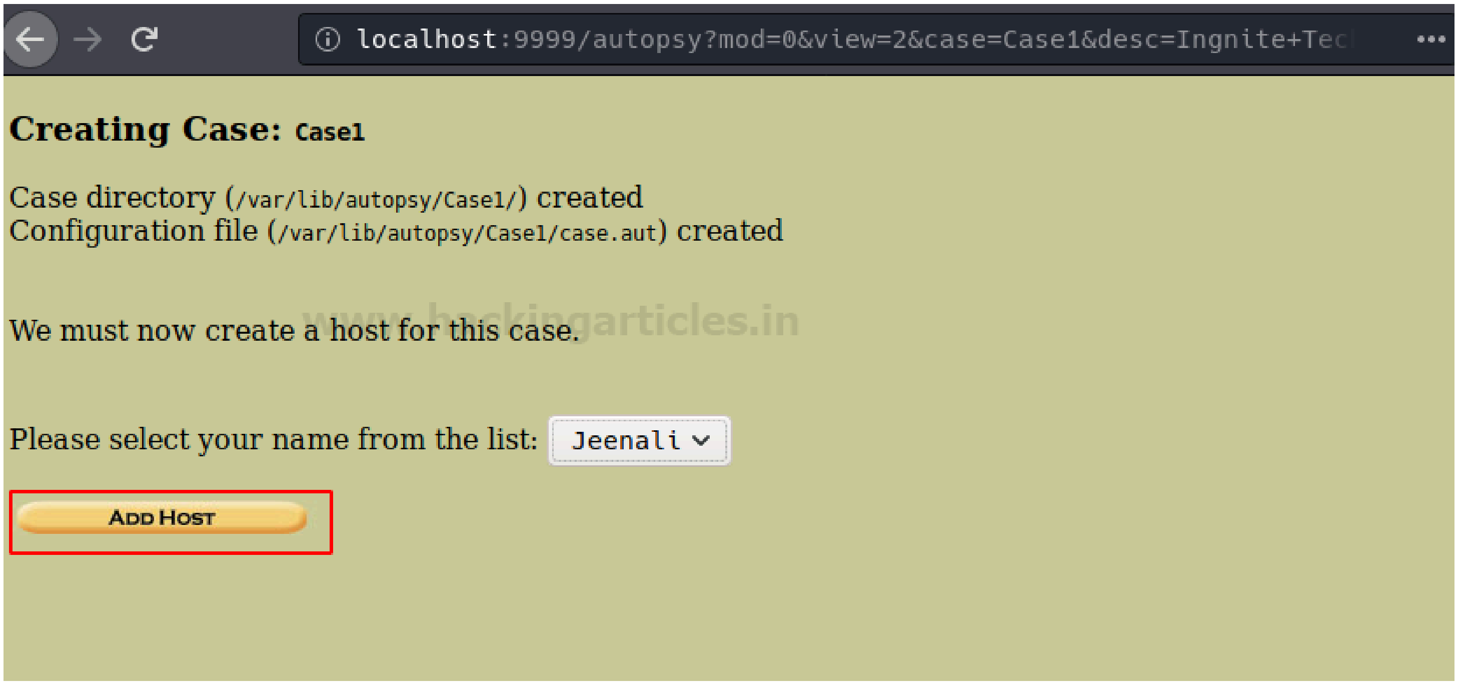
g.

h.

i.

j.

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&view=2&case=Case1&desc=Ingnite+Tec

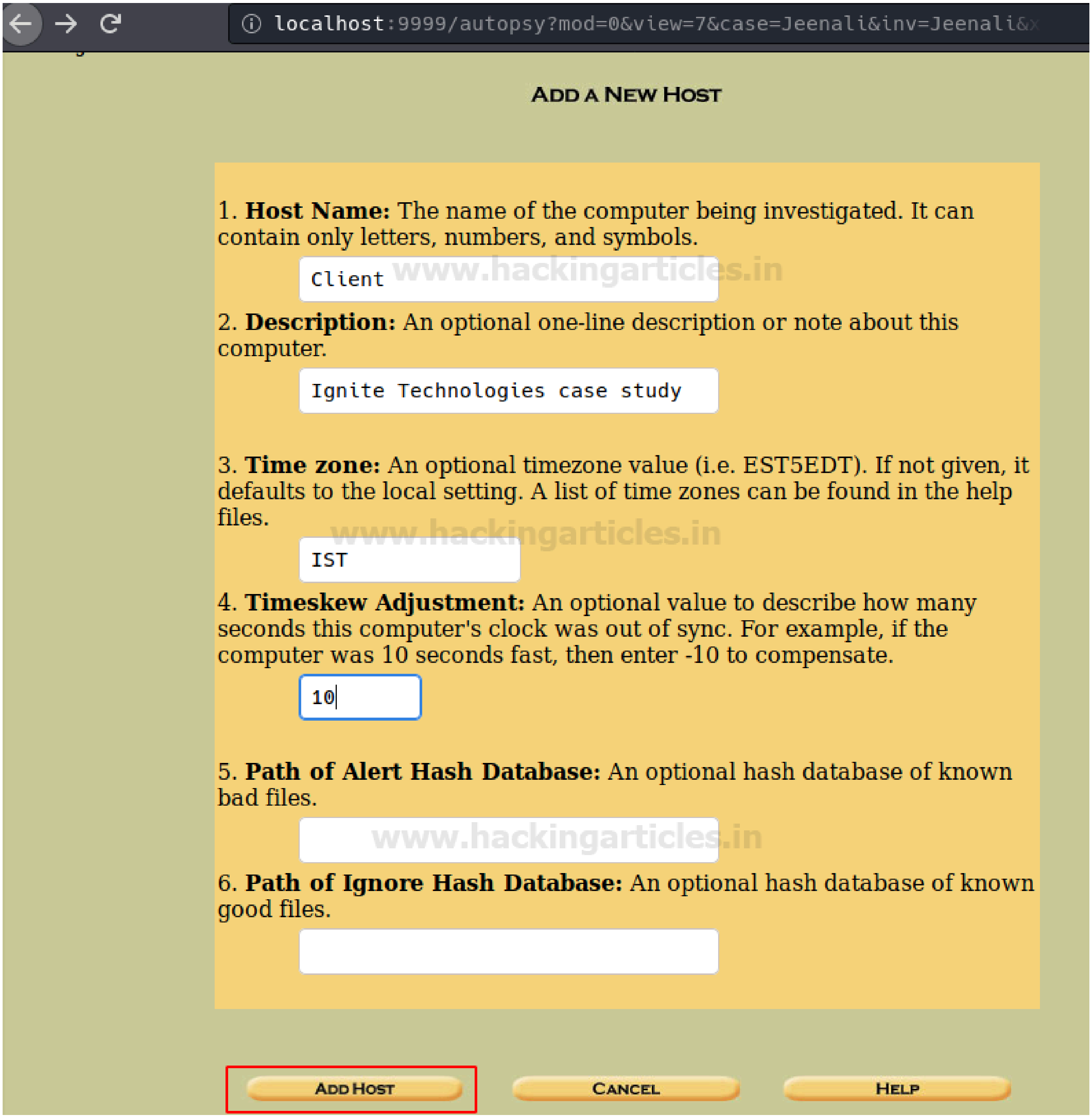
Creating Case: Case1

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 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

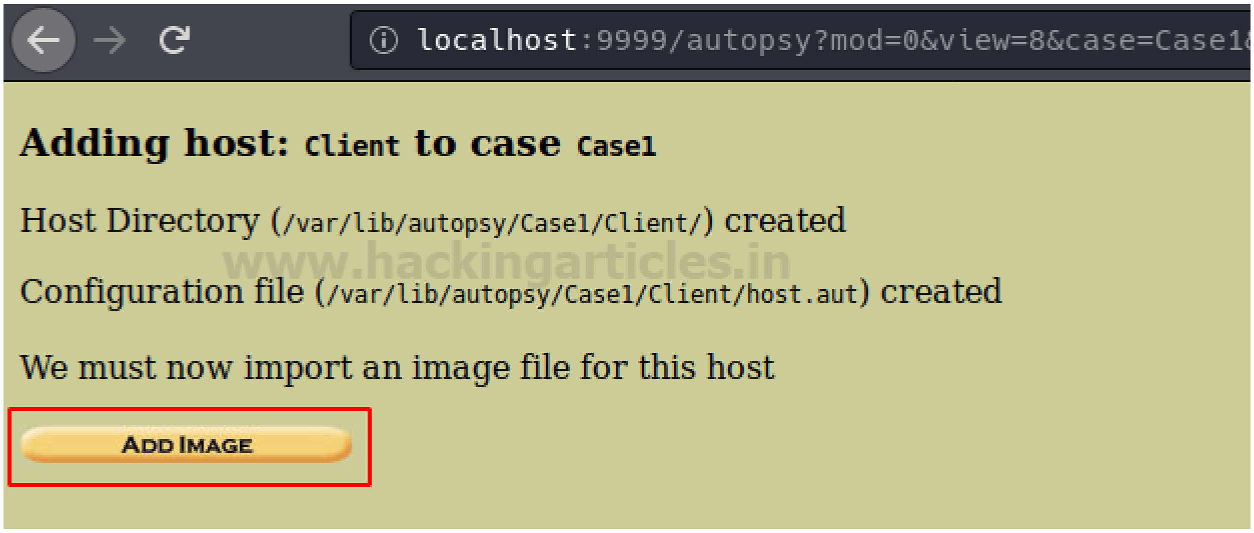
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

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.

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&case=Case1

Adding host: Client to case Case1

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

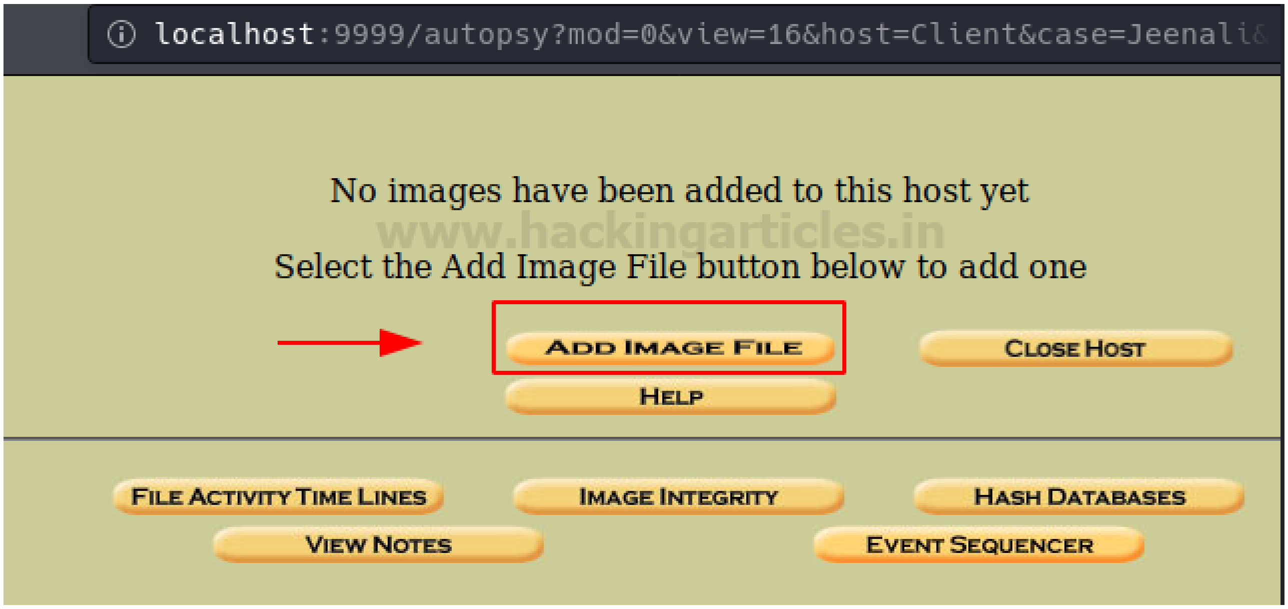
Configuration file (/var/lib/autopsy/Case1/Client/host.aut) created

We must now import an image file for this host

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

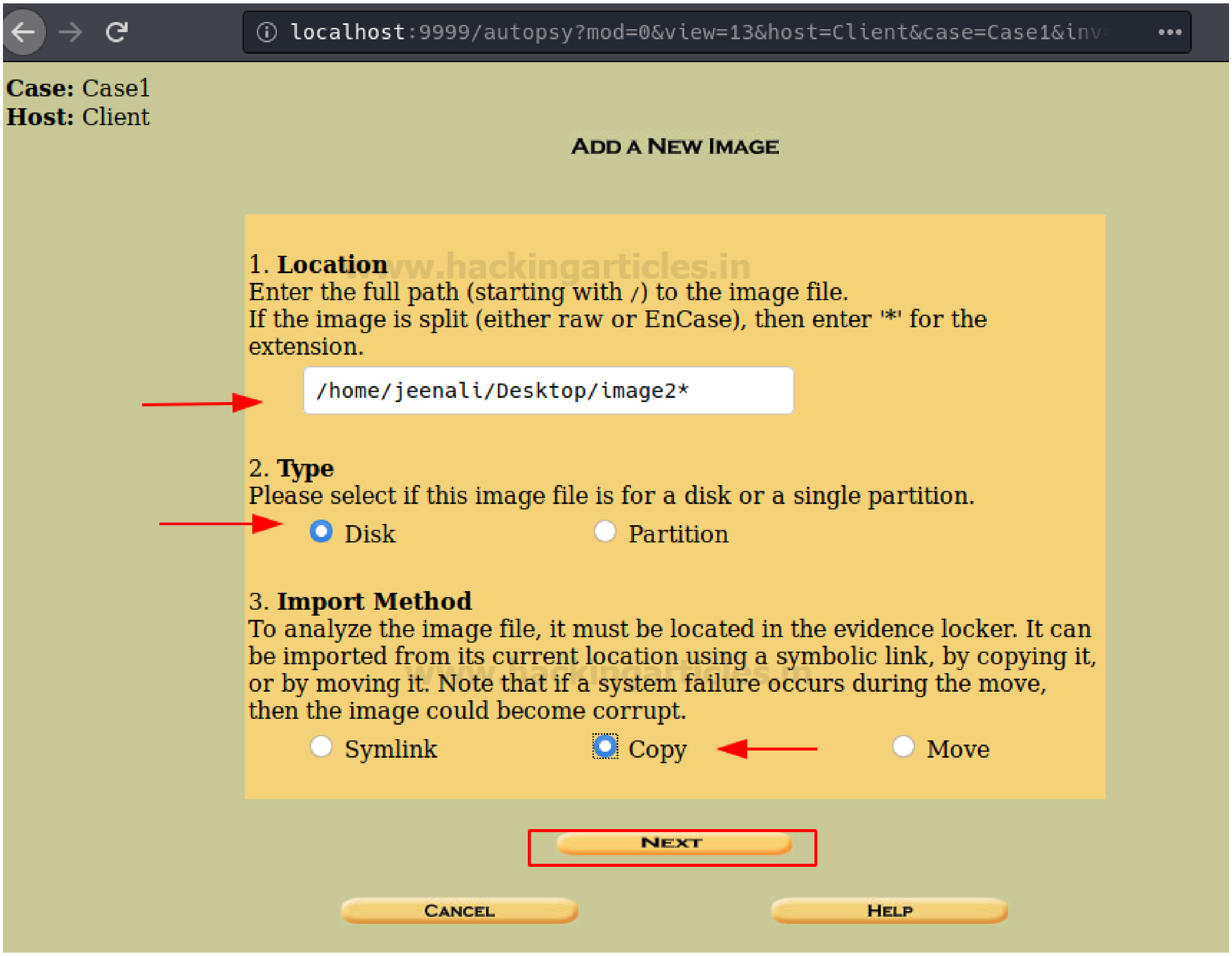


localhost:9999/autopsy?mod=0&view=16&host=Client&case=Jeenali

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*

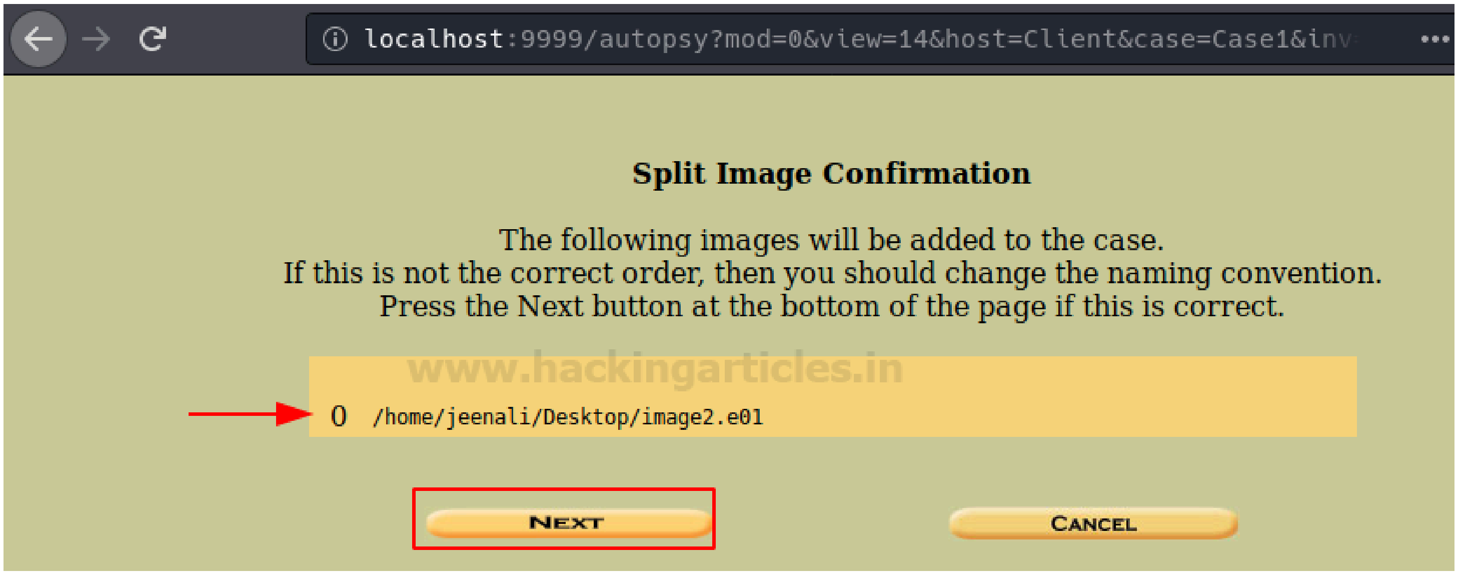
2. **Type**
Please select if this image file is for a disk or a single partition.

● 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

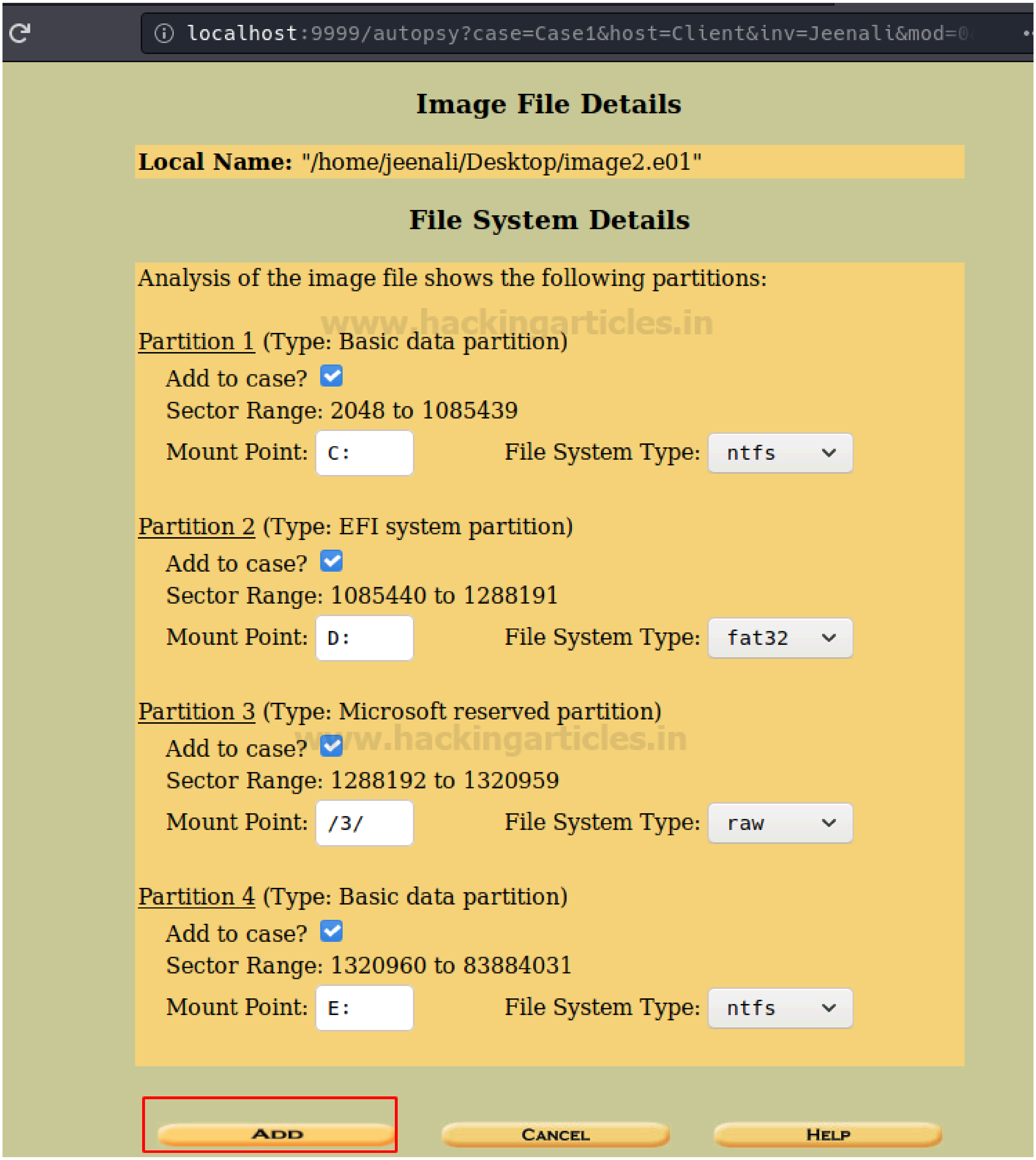
Split Image Confirmation

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

NEXT
CANCEL
www.hackingarticles.in

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:

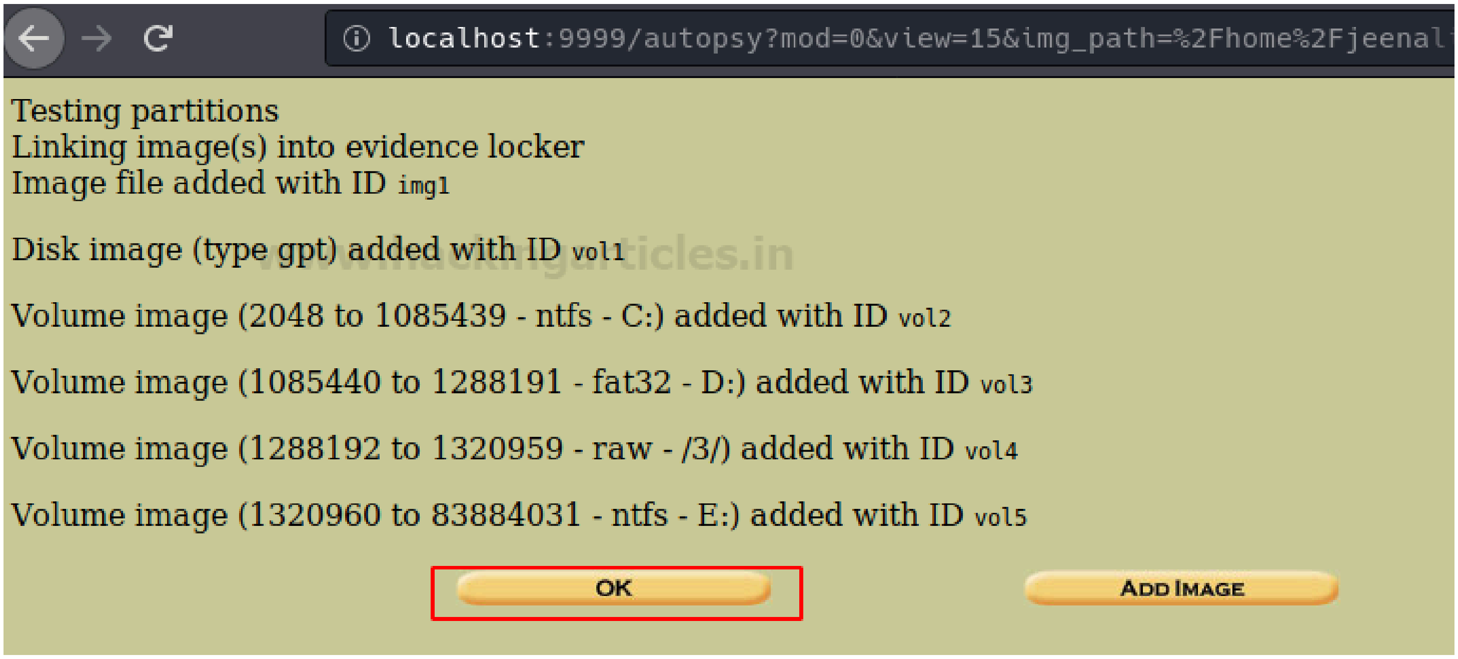
Partition 1 (Type: Basic data partition)
Add to case? ☑
Sector Range: 2048 to 1085439
Mount Point: C: File System Type: ntfs

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

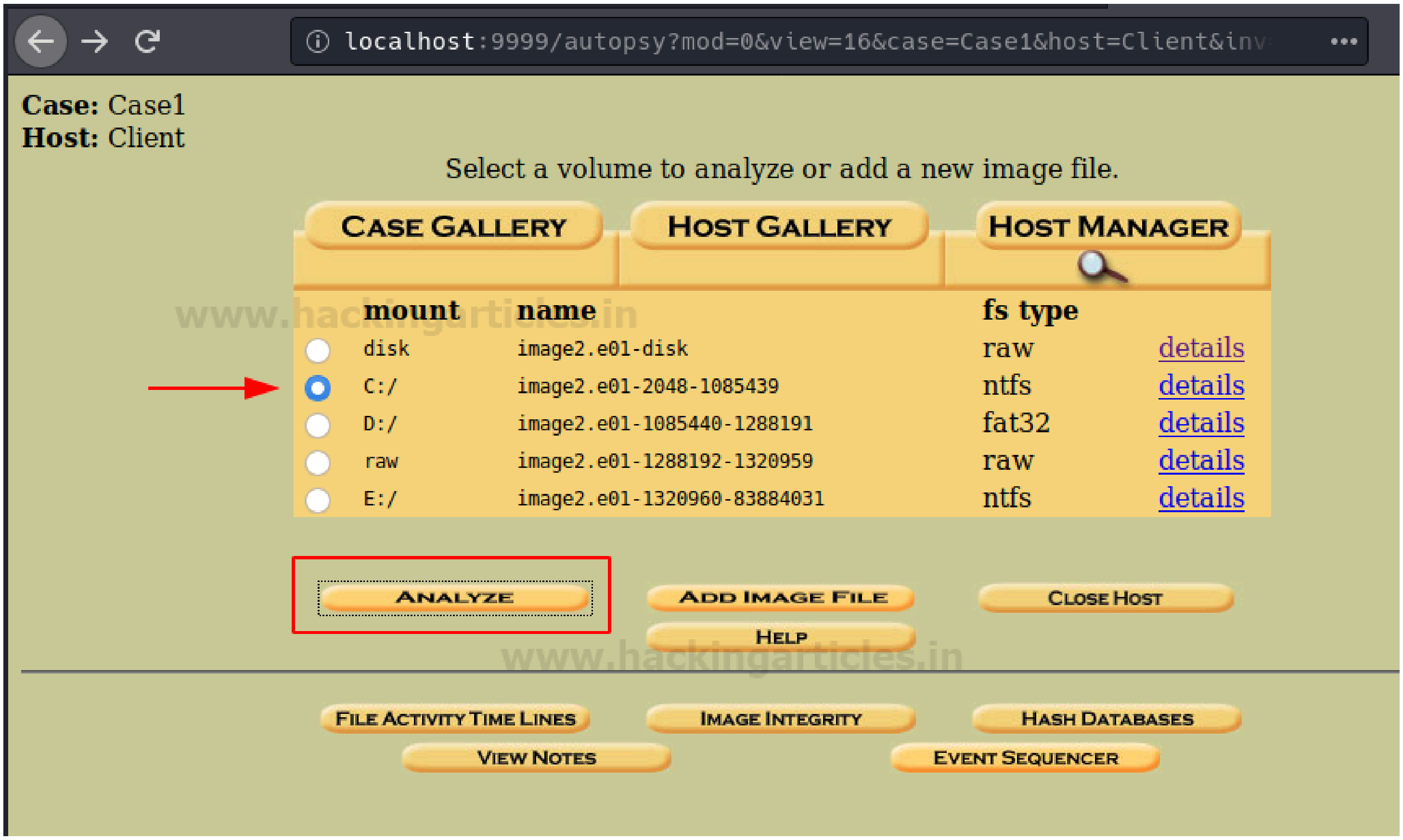
Volume image (2048 to 1085439 - ntfs - C:) added with ID vol2

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

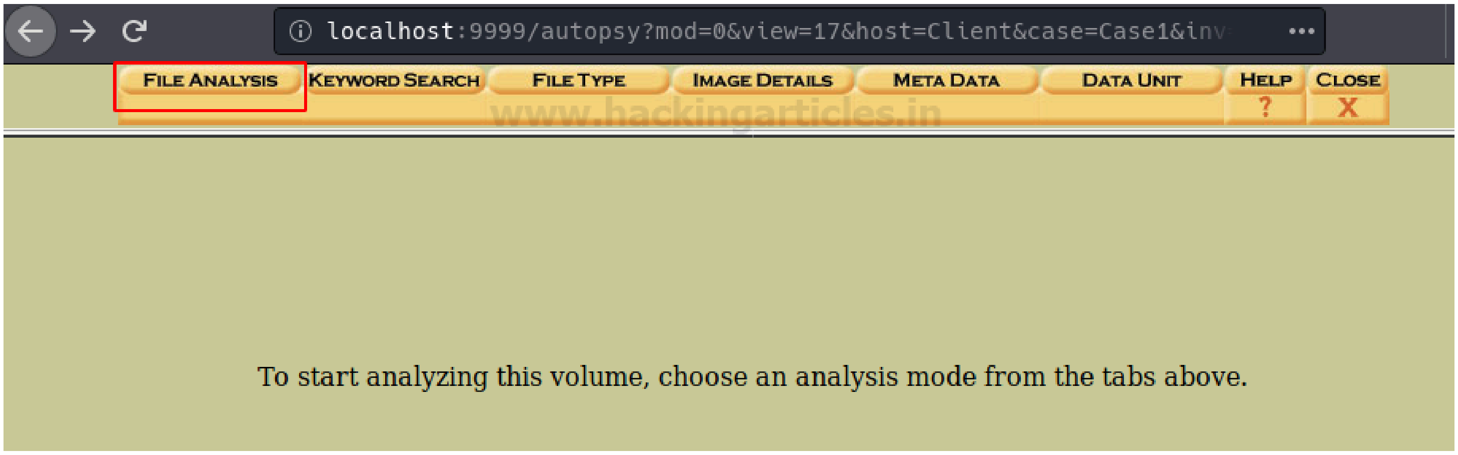
Case: Case1
Host: Client

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

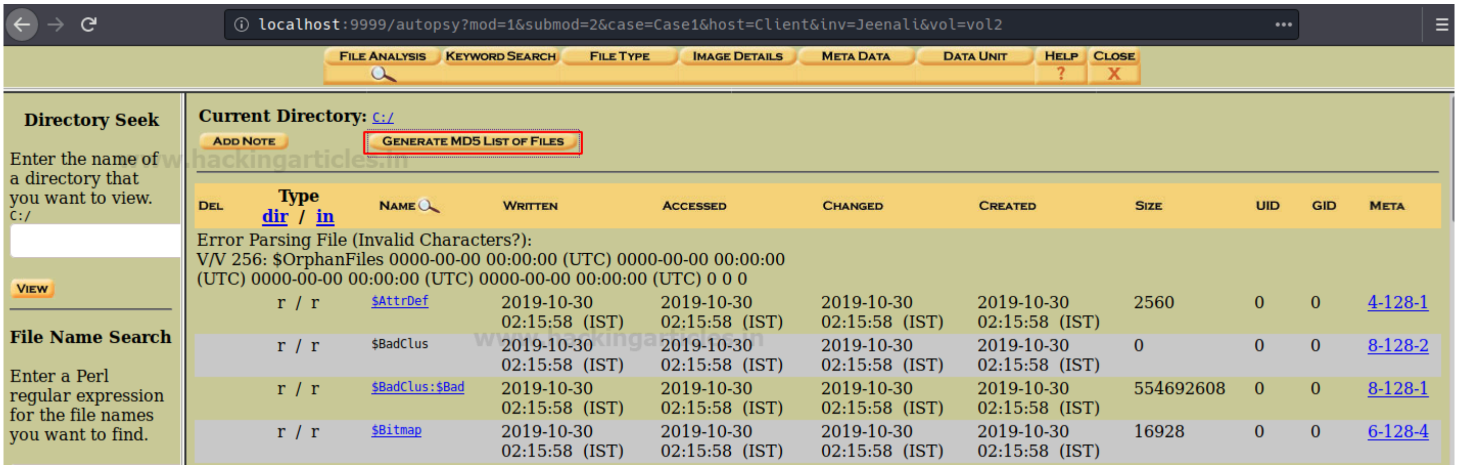
File Analysis-File Browser Mode and Metadata Analysis

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'.



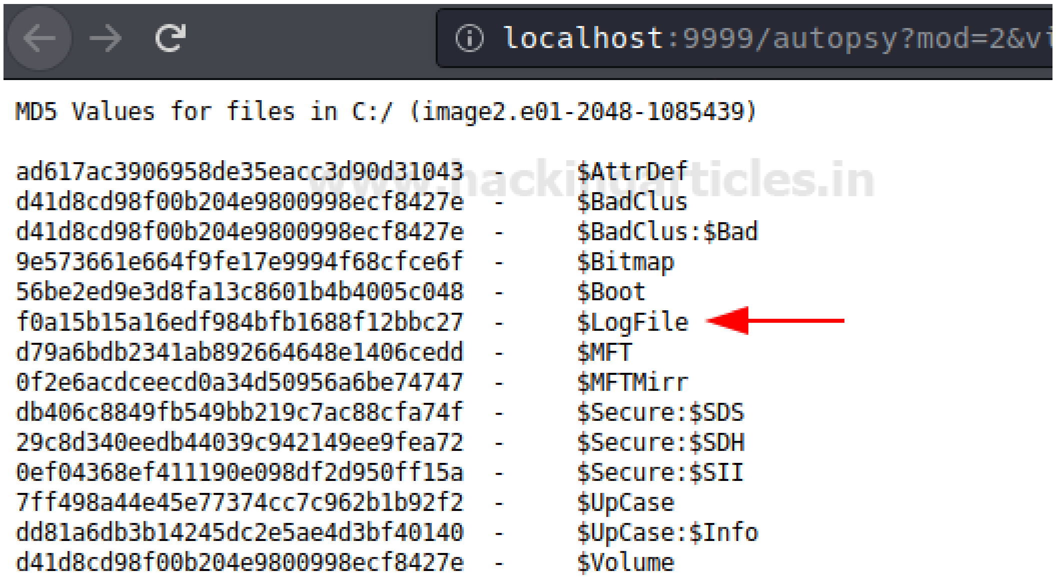
To start analyzing this volume, choose an analysis mode from the tabs above.

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 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'.


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
X
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

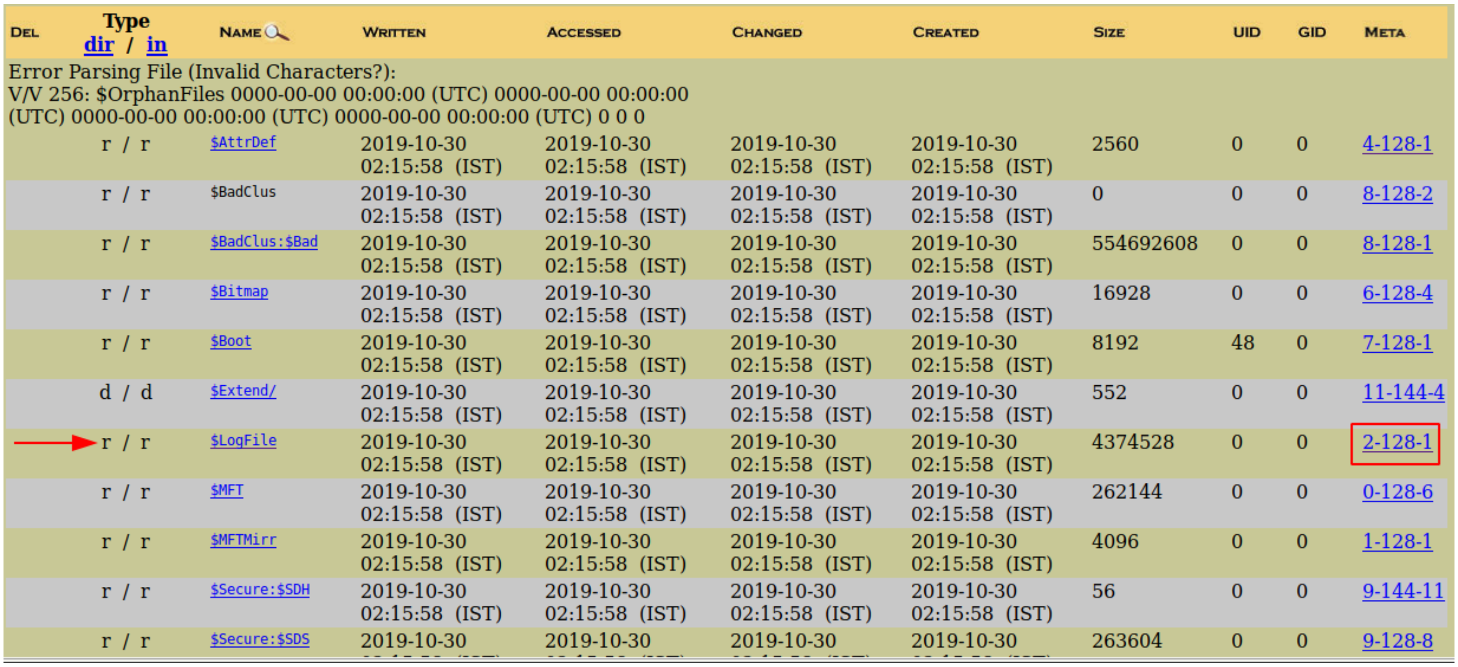
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
Error Parsing File (Invalid Characters?): V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	r / r	$AttrDef	2019-10-30 02:15:58 (IST)	2019-10-30 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
```

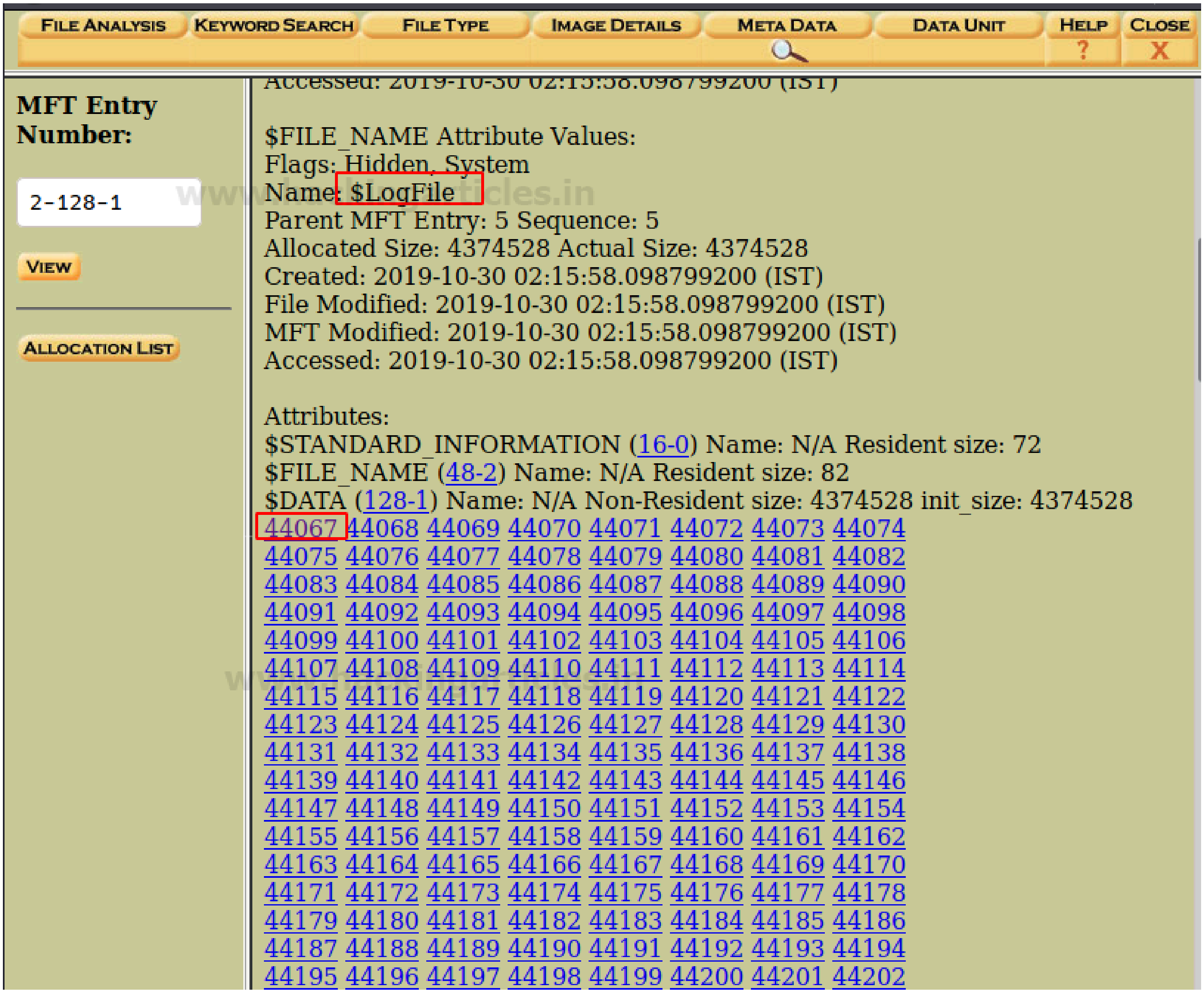
The file browsing mode consists of details of the directories that are shown below. The details include the time and date of the last time the directories were Written, Accessed, Changed and the time it was created with its size and also about its metadata. All the details are displayed in this, so in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



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

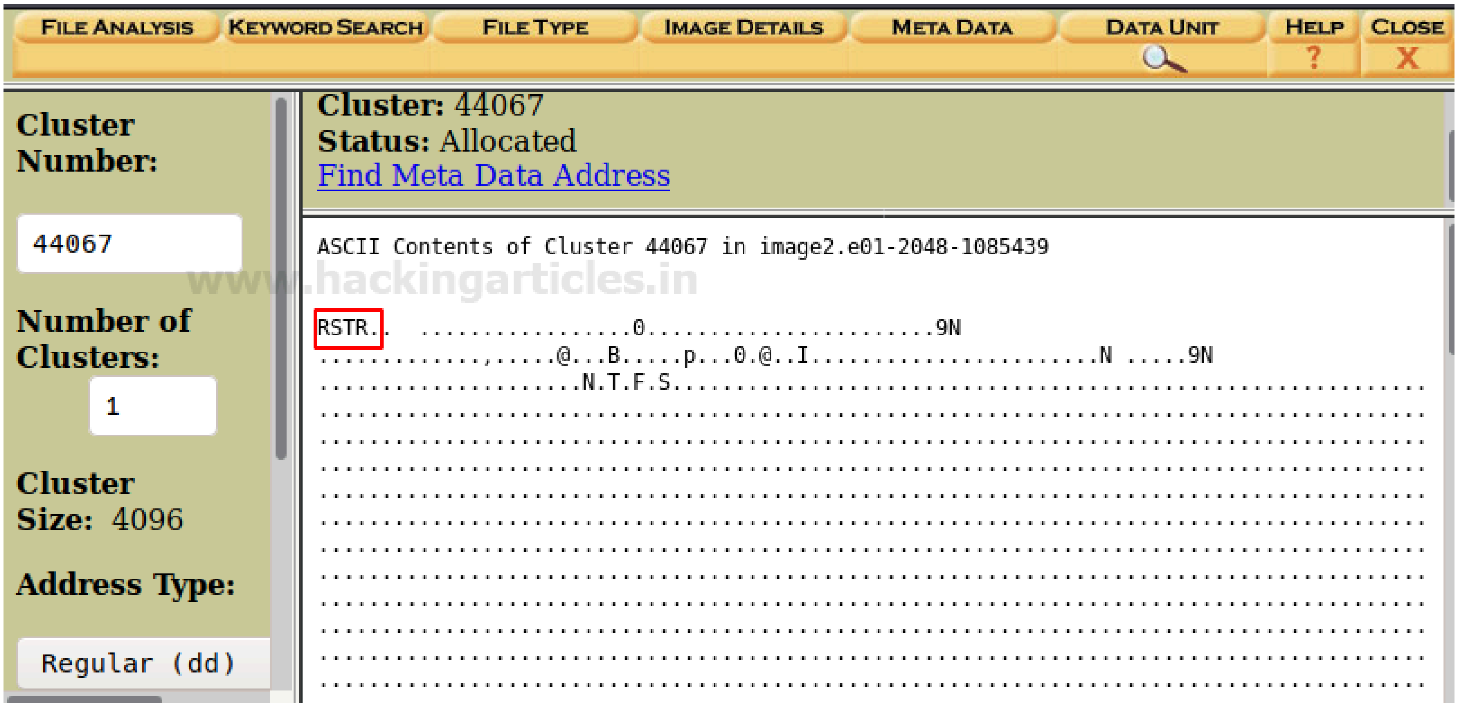
Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	r / r	$AttrDef	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2560	0	0	4-128-1
	r / r	$BadClus	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	2019-10-30 02:15:58 (IST)	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.



```
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

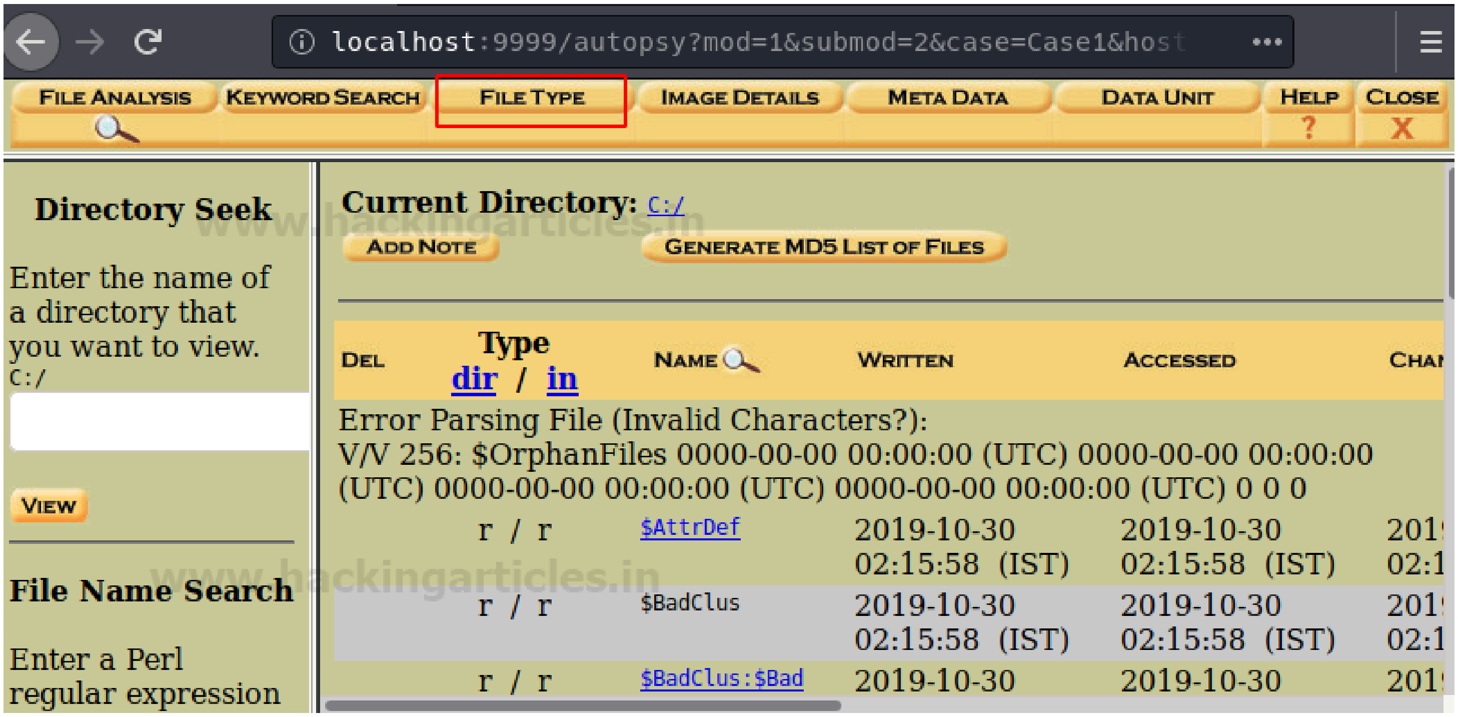
Cluster Size: 4096

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

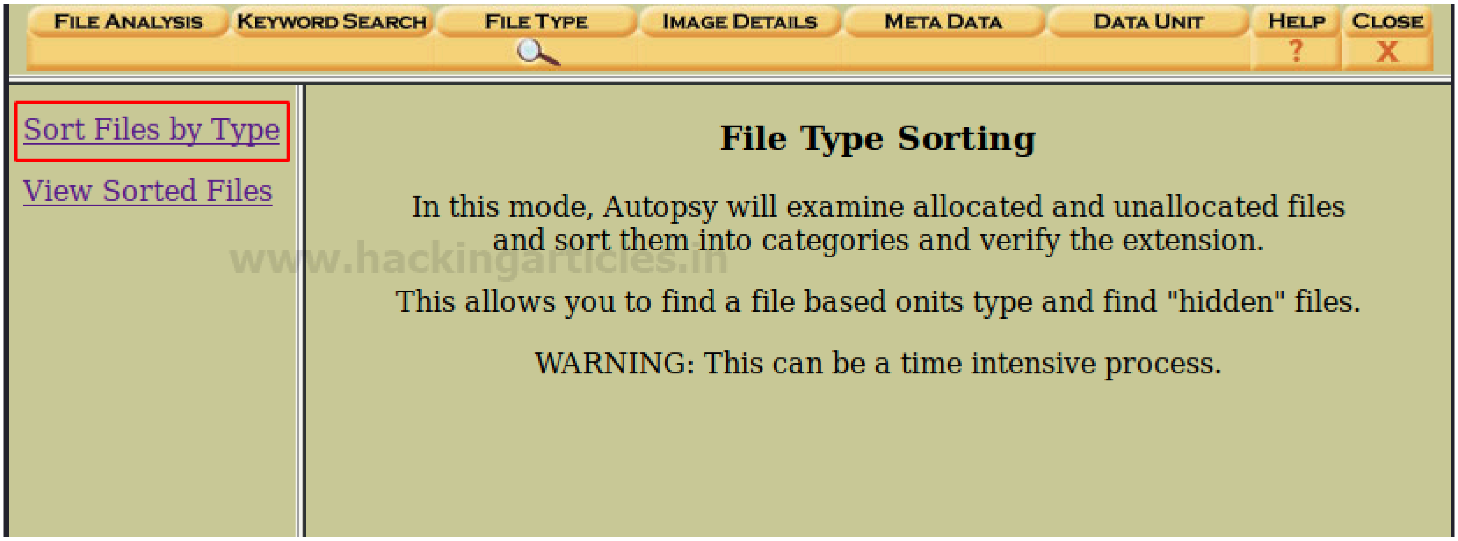
Enter a Perl regular expression

Current Directory: C:/

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHAI
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’.



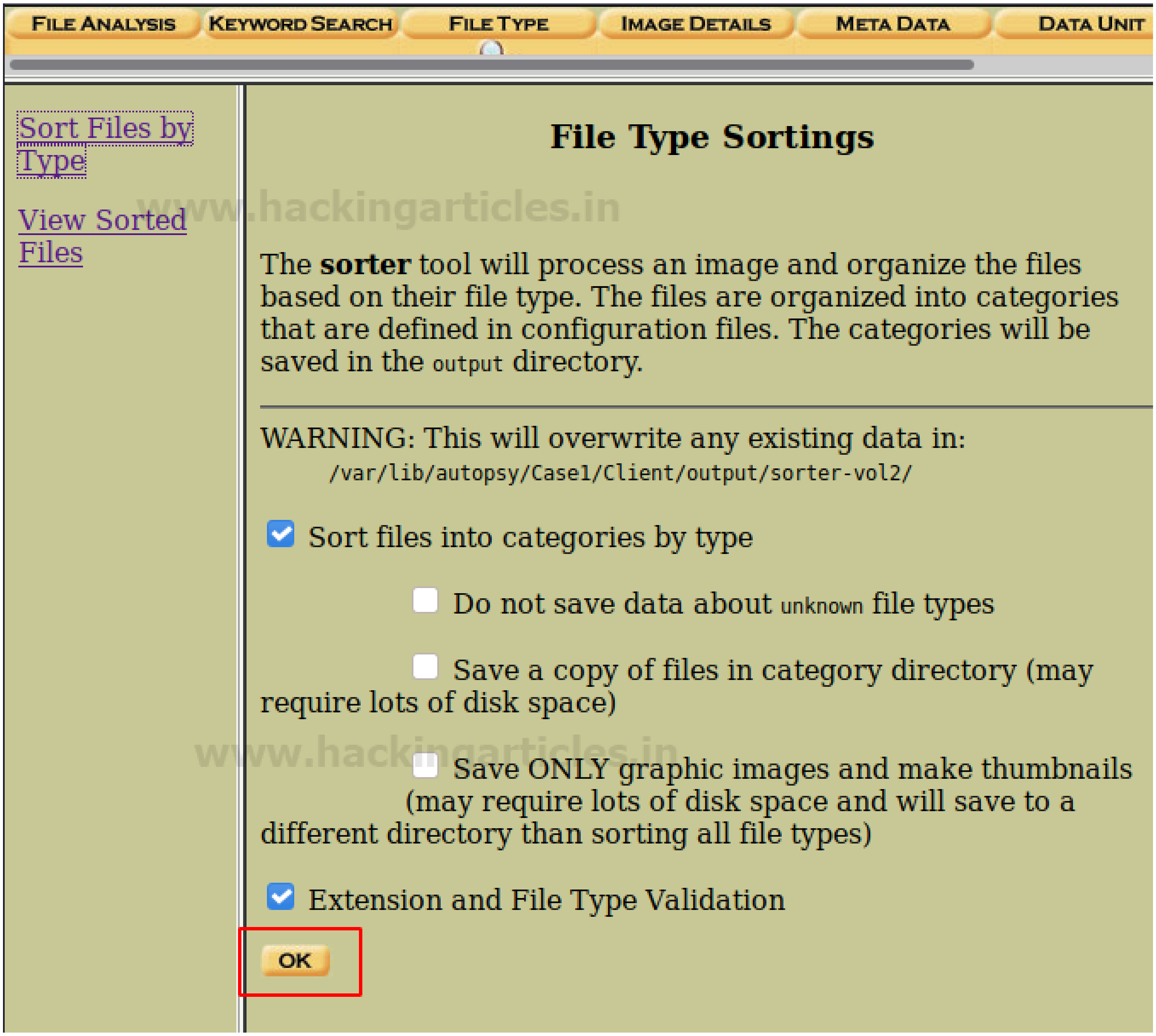
File Type Sorting

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

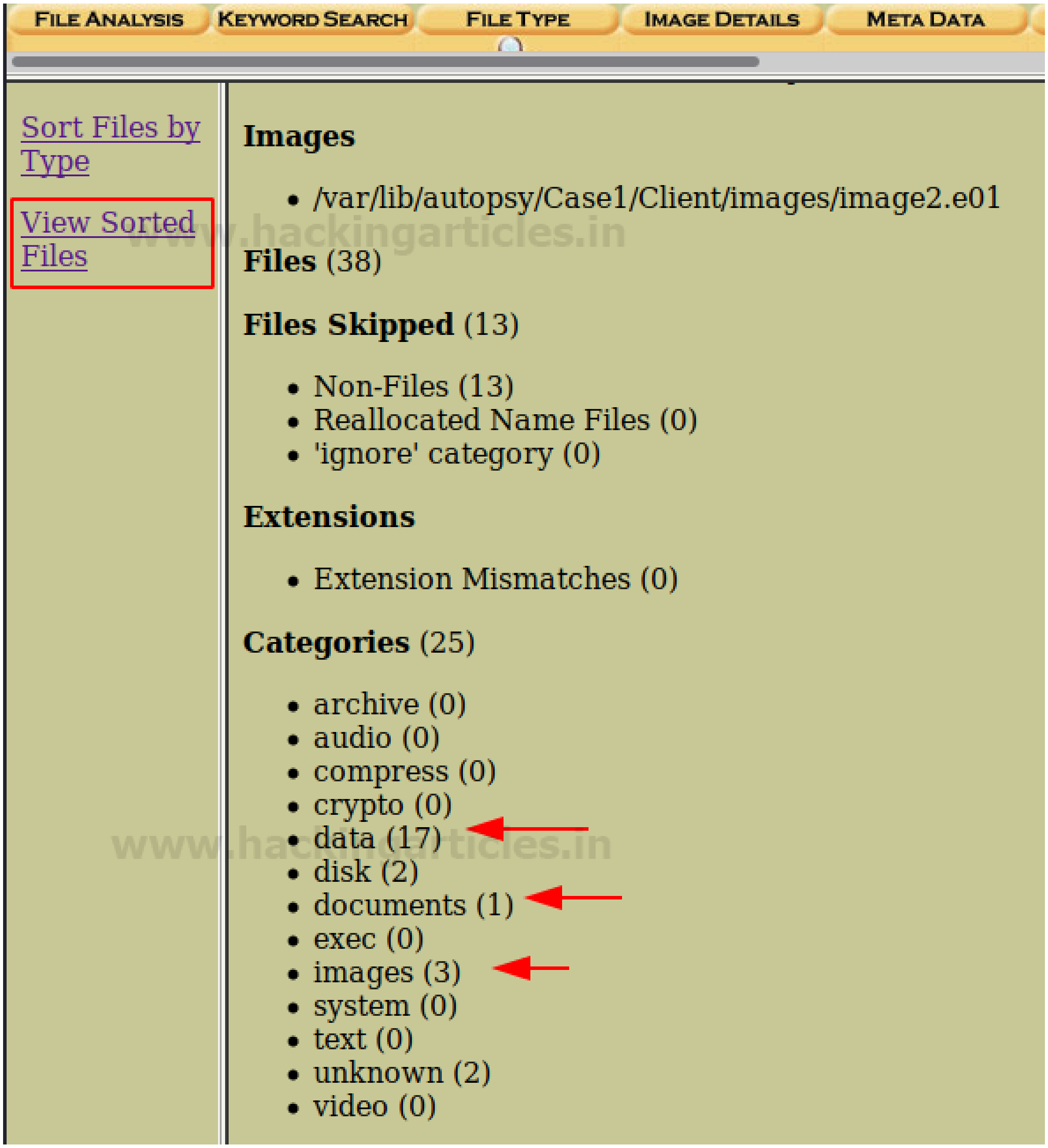
☐ Do not save data about `unknown` file types

☐ 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)

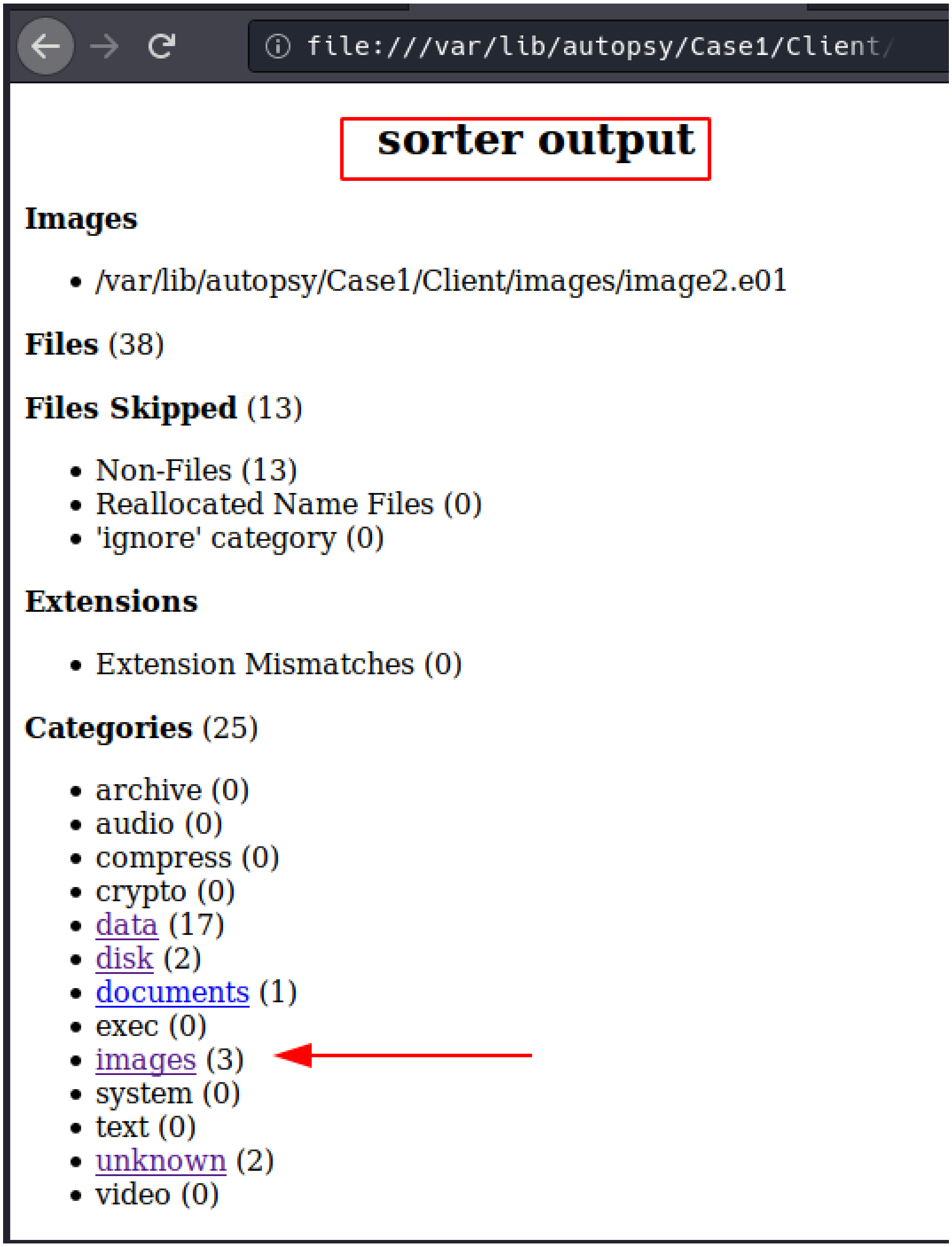
Extensions

- 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.



file:///var/lib/autopsy/Case1/Client/

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)

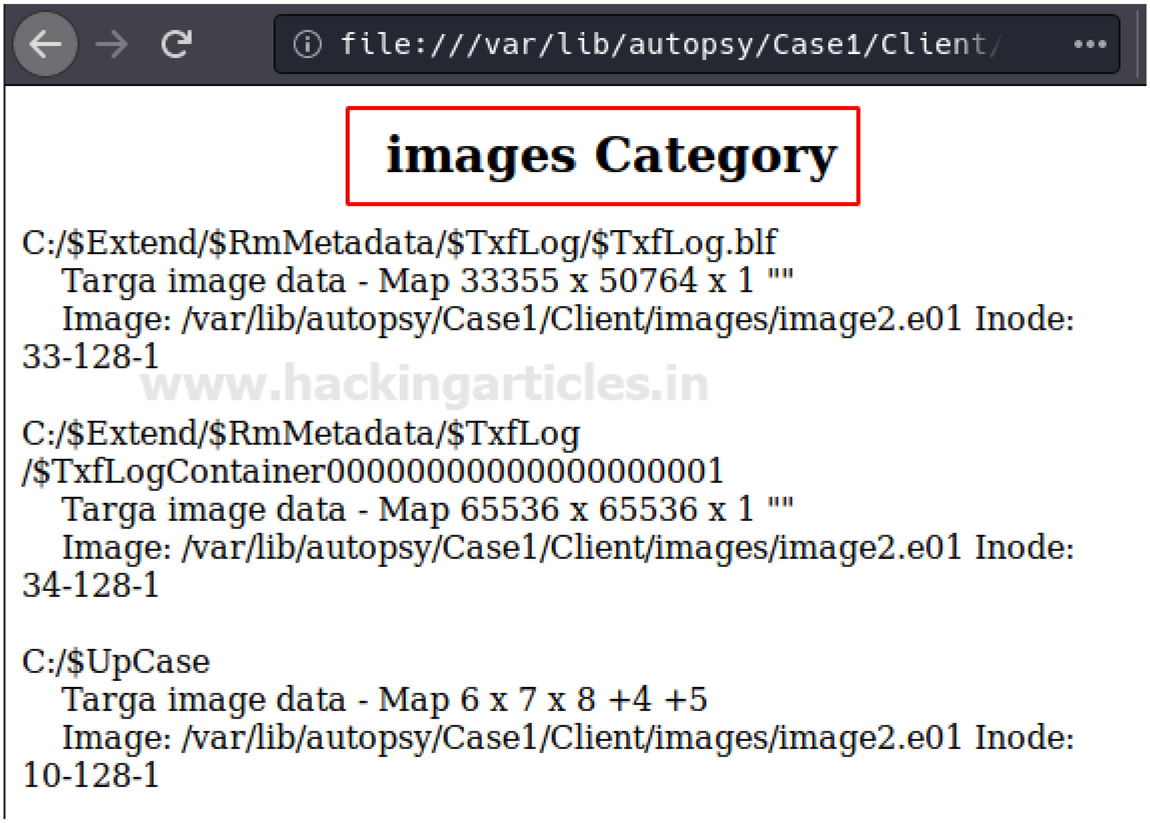
Extensions

- 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

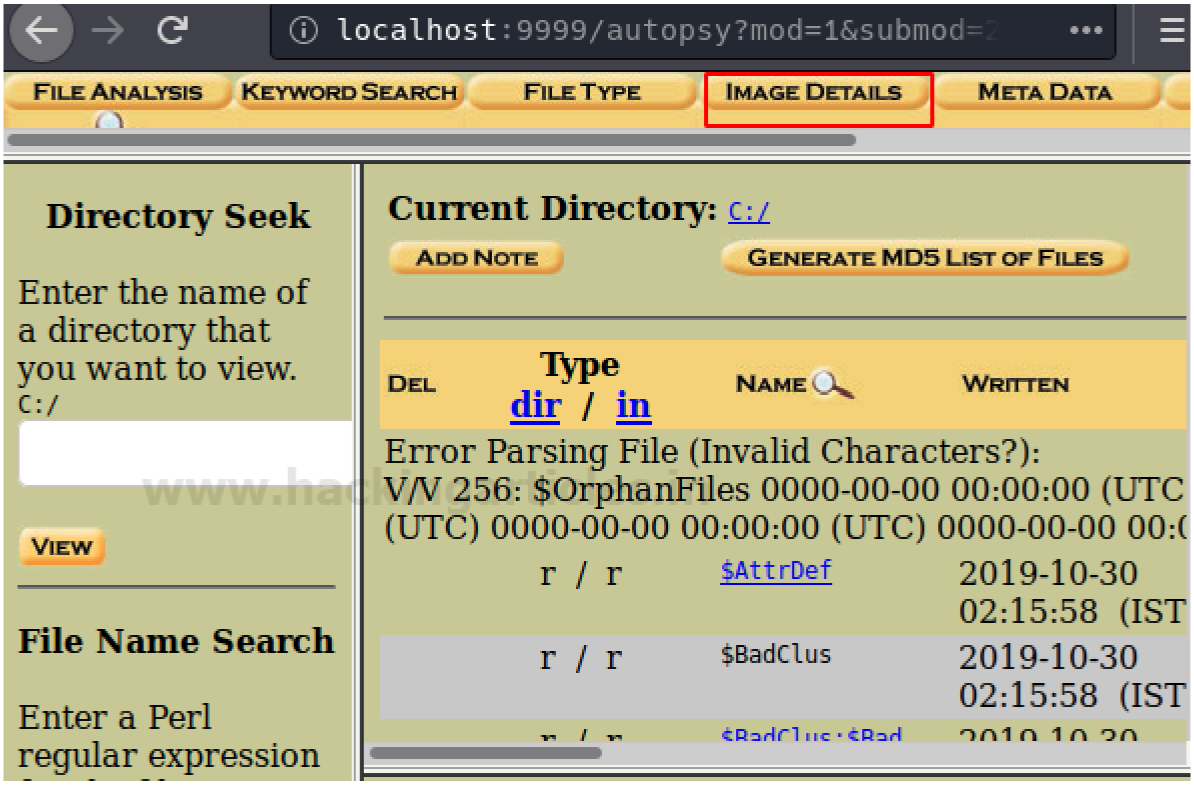
C:/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
    Targa image data - Map 33355 x 50764 x 1 ""
    Image: /var/lib/autopsy/Case1/Client/images/image2.e01 Inode: 33-128-1

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



Directory Seek

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

File Name Search

Enter a Perl regular expression

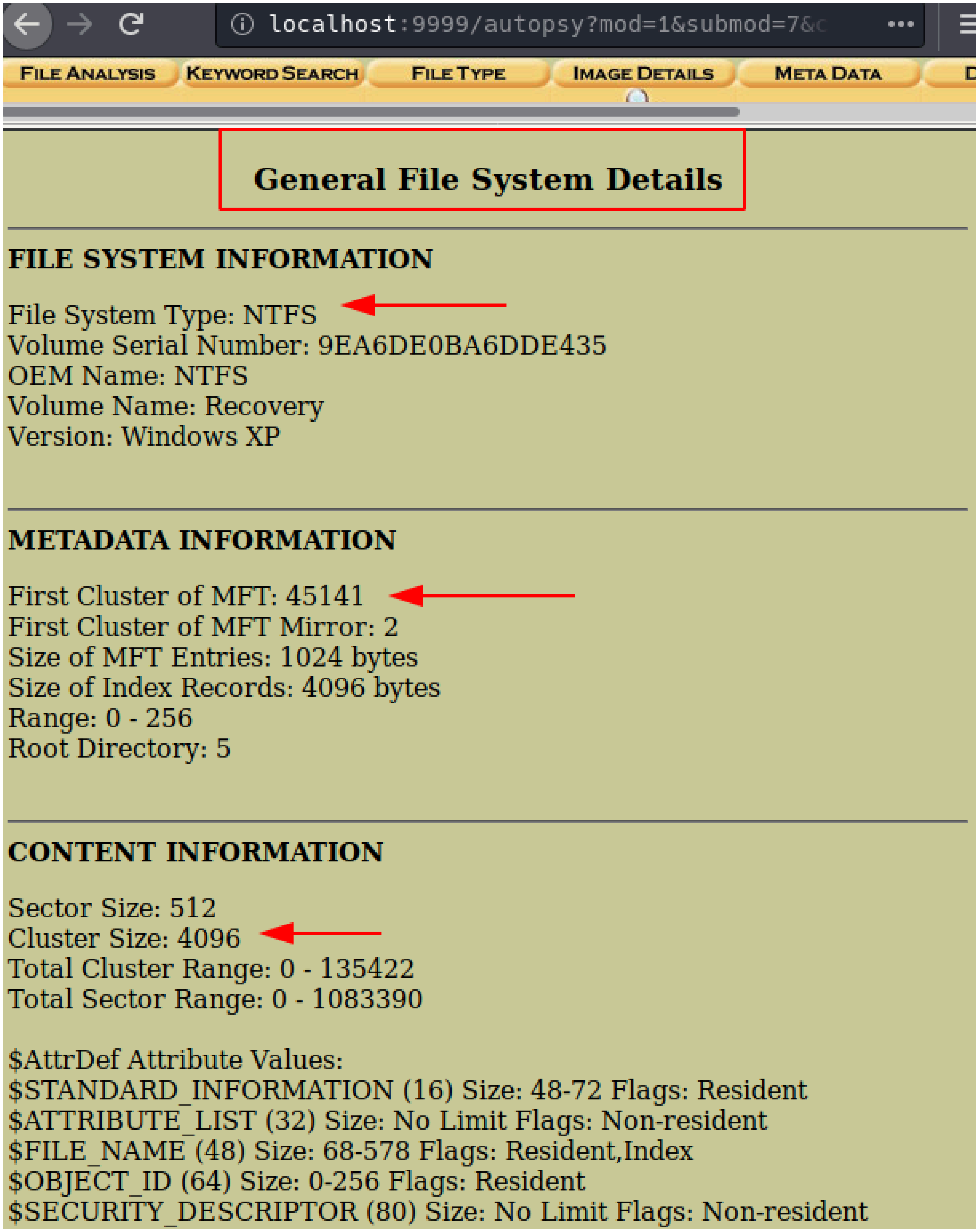
Current Directory: C:/

DEL	Type dir / in	NAME	WRITTEN

Error Parsing File (Invalid Characters?):
V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:0

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

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



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

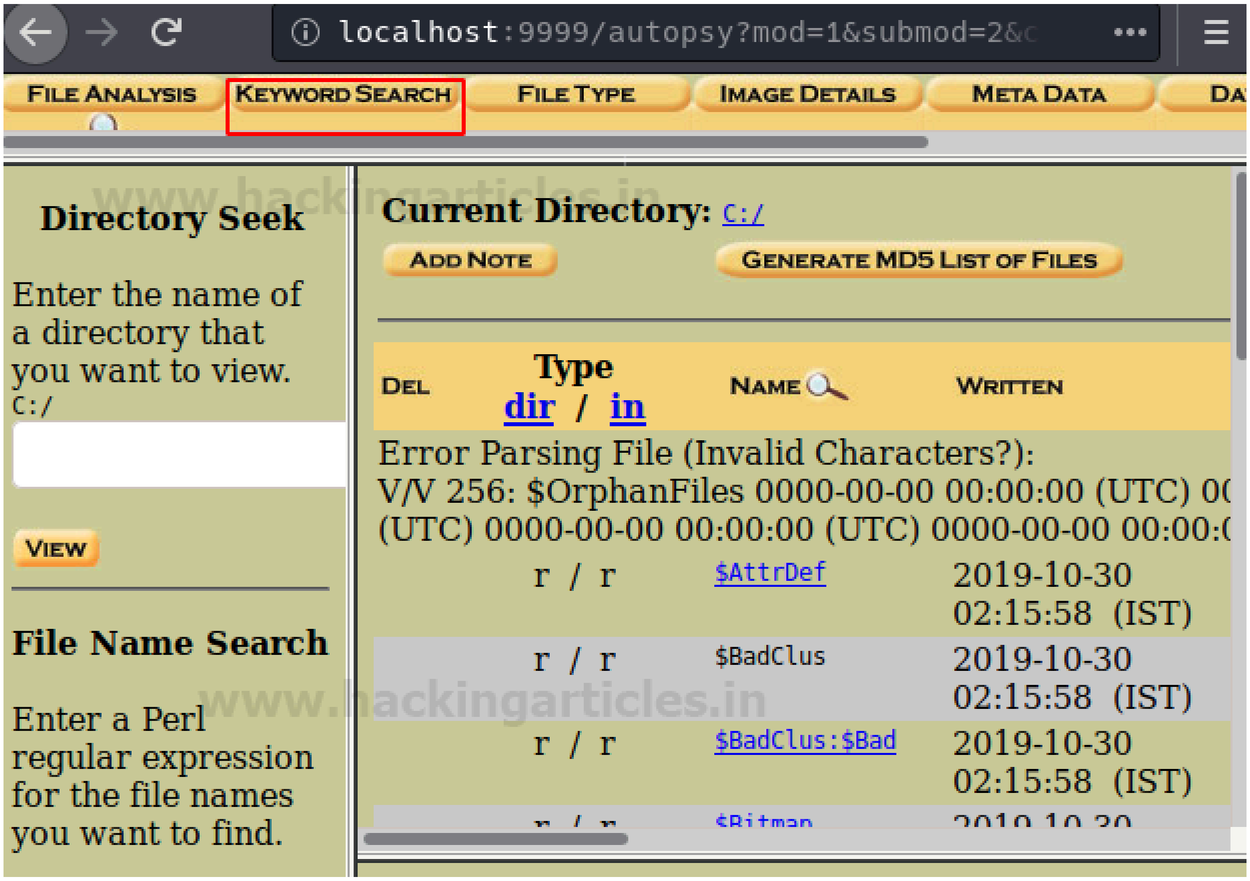
CONTENT INFORMATION

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:/

File Name Search

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

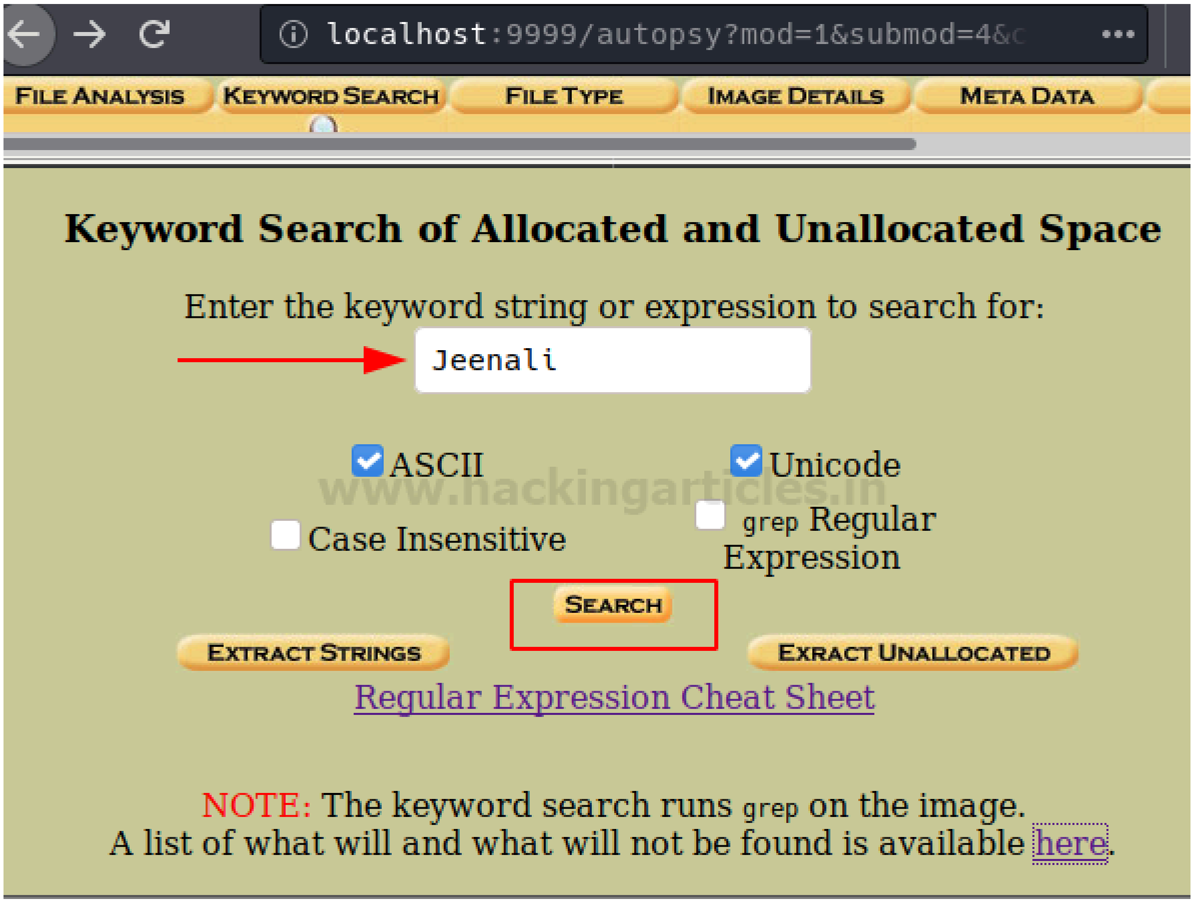
Current Directory: C:/

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

DEL	Type dir / in	NAME	WRITTEN
	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.



Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

Jeenali

☑ ASCII ☑ Unicode

□ Case Insensitive □ grep Regular Expression

Regular Expression Cheat Sheet

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 the Autopsy in Kali Linux. This collection of tools creates quite a powerful forensic analysis platform.