

Comprehensive Guide on Autopsy Tool (Windows)

December 14, 2020 By Raj Chandel

Autopsy is an open-source tool that is used to perform forensic operations on the disk image of the evidence. 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.

Table of Contents

- **Creating a New Case**

- **Data Sources**

- **Views**

1. File Type

2. MIME-type

- **Deleted Files**

- **MB File size**

- **Results**

1. Extracted Content

2. Keyword Hits

- **Timeline**

- **Discovery**

- **Images/Videos**

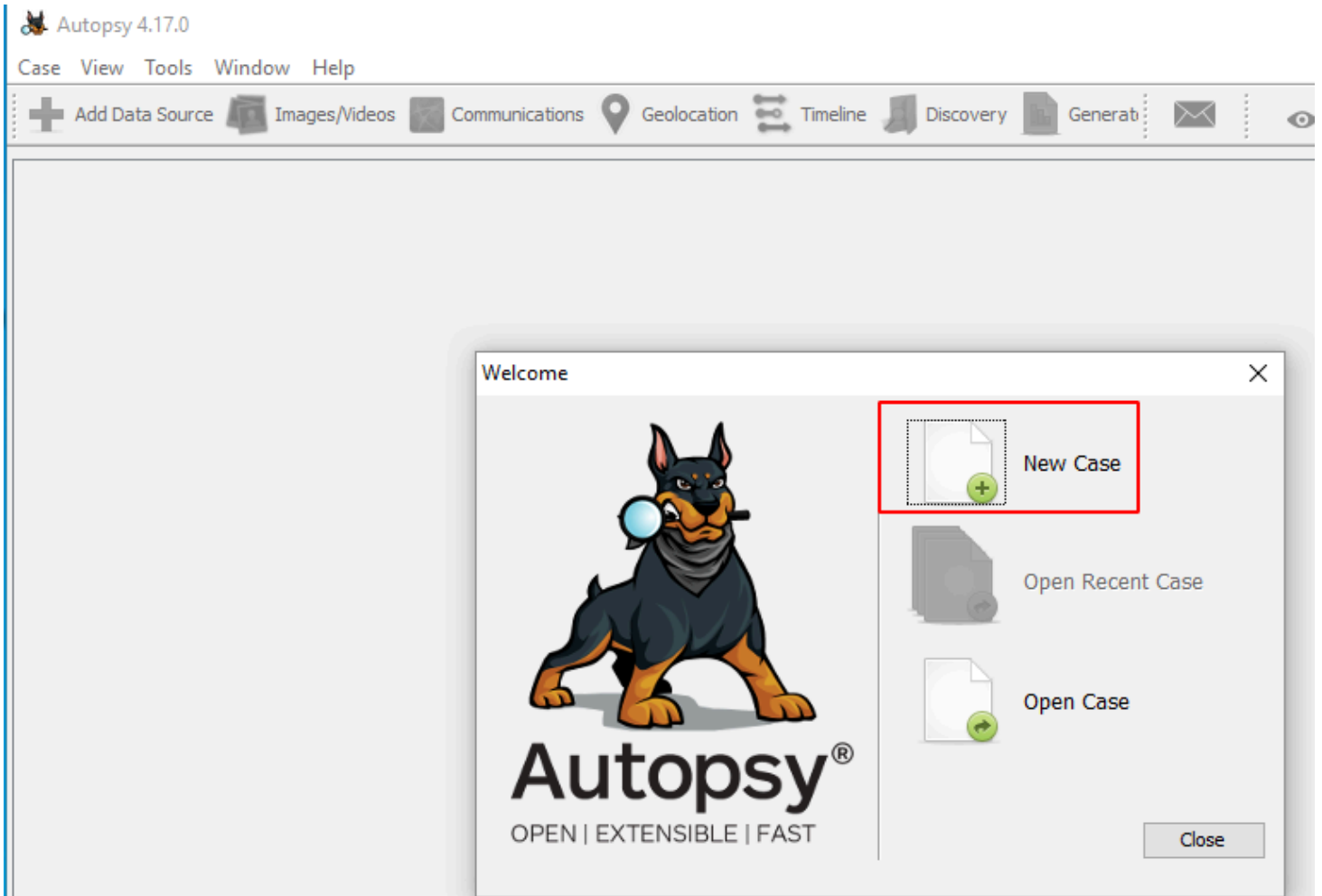
- **Add File Tags**

- **Generate Reports**


So, let us get started! Download the Autopsy Tool 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 Browse

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:
C:\Users\raj\Desktop\Ignite

< Back


Next >

Finish

Cancel

Help

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 Manage Organizations

< Back

Next >

Finish

Cancel

Help

Now let us add the type of data source. There are various types to choose from.

Disk Image or VM file: This includes the image file which can be an exact copy of a hard drive, media card, or even a virtual machine.

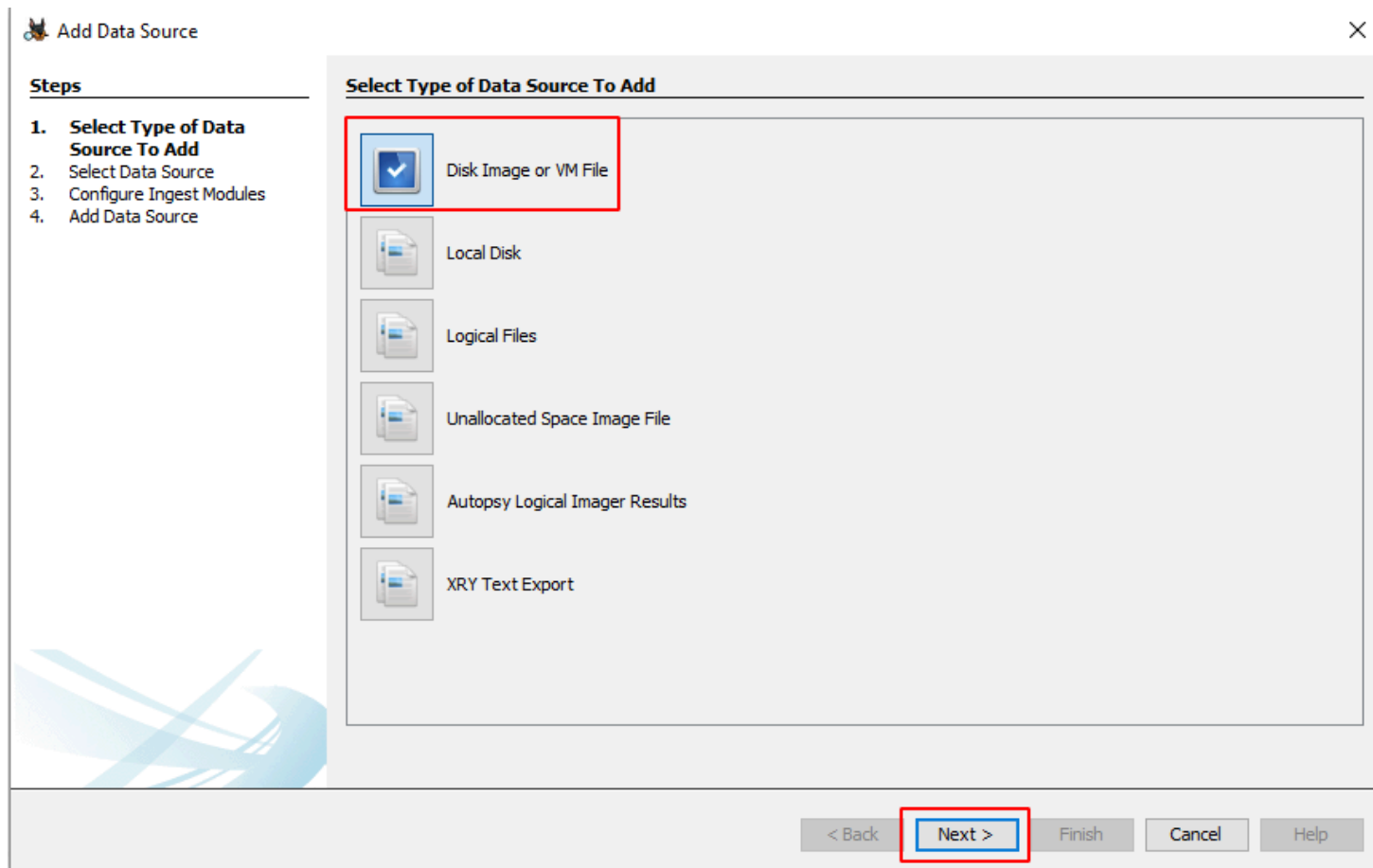
Local Disk: This option includes devices like Hard disk, Pen drives, memory cards, etc.

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

Unallocated Space Image File: They include files that do not contain any file system and run with the help of the ingest module.

Autopsy Logical Imager Results: They include the data source from running the logical imager.

XRY Text Export: This includes the data source from exporting text files from XRY,



Now let us add the data source. Here we have a previously created image file, so we will add the location of that file.

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

Browse

☐ 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.

< Back

Next >

Finish

Cancel

Help

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

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

Select All

Deselect All

History

The selected module has no per-run settings.

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

Global Settings

< Back

Next >

Finish

Cancel

Help

The contents of the Ingest module are listed below:

INGEST MODULE	
Recent Activity	It is used to discover the recent operations that were performed on the disk, like the files that were viewed recently.
Extension Mismatch Detector	It is used to identify files whose extensions were tampered with or had been changed to hide the evidence.
Hash Lookup	It is used to identify a particular file using its hash value.
File Type Identification	This is used to identify files based on their internal file signatures than just the file extensions.
Embedded File Extractor	It is used to extract embedded files like .zip, .rar, etc. and use those files for analysis.
Keyword Search	This is used to search for any particular keyword or a pattern in the image file.
Email Parser	This is used to extract information from email files if the disk holds any email database information.
Encryption Detection	This helps to detect and identifies encrypted password-protected files.
Interesting File Identifier	Using this feature the examiner is notified when results pertaining to the set of rules that are defined to identify a particular type of file.
PhotoRec Carver	This helps the examiner to recover files, photos, etc. from the unallocated space on the image disk.
Virtual Machine Extractor	It helps to extract and analyze if any Virtual machine is found on the disk image.
Data Source Integrity	It helps to calculate the hash value and store them in the database.

Data Source information displays basic metadata. Its detailed analysis is displayed at the bottom. It can be extracted one after the other.

Ignite - Autopsy 4.17.0

Case View Tools Window Help

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

Listing

Data Sources

Table Thumbnail Summary

Name	Type	Size (Bytes)
Ignite.E01	Image	64420392960

Hex Text Application File Metadata Context Results Annotations Other Occurrences

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

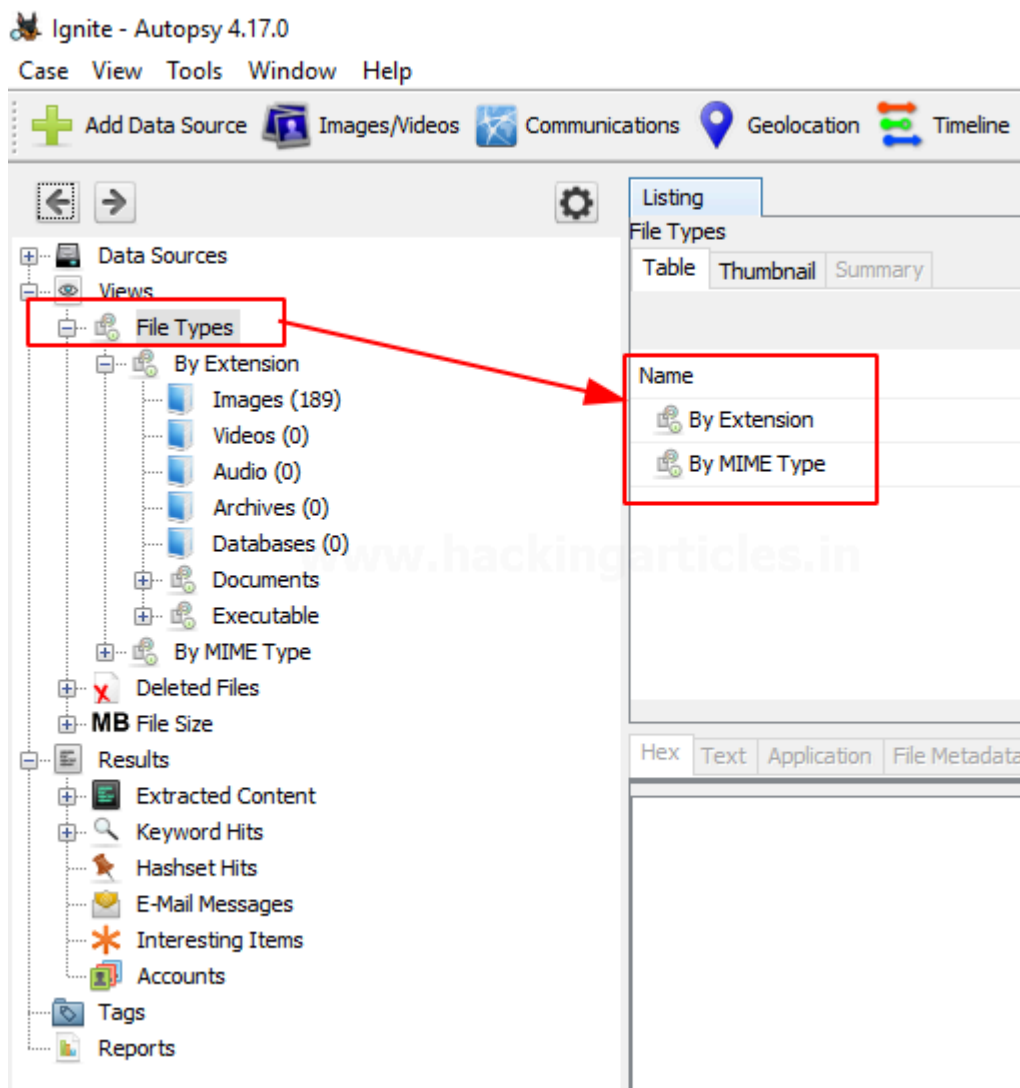
0x00000000:	EB 52 90 4E 54 46 53 20	20 20 20 00 02 08 00 00	.R.NIFS
0x00000010:	00 00 00 00 00 F8 00 00	3F 00 FF 00 00 58 E0 03? X . .
0x00000020:	00 00 00 00 80 00 80 00	FF D7 1B 01 00 00 00 00
0x00000030:	00 00 0C 00 00 00 00 00	02 00 00 00 00 00 00 00
0x00000040:	F6 00 00 00 01 00 00 00	17 59 BE 64 96 BE 64 76Y.d..dv
0x00000050:	00 00 00 00 FA 33 C0 8E	D0 BC 00 7C FB 68 C0 073h..
0x00000060:	1F 1E 68 66 00 CB 88 16	0E 00 66 81 3E 03 00 4E	. .hf.f.>..N
0x00000070:	54 46 53 75 15 B4 41 BB	AA 55 CD 13 72 0C 81 FB	TFSu..A..U..r...
0x00000080:	55 AA 75 06 F7 C1 01 00	75 03 E9 DD 00 1E 83 EC	U.u.....u.....

Views

File Type: It can be classified in the form of File extension or MIME type.

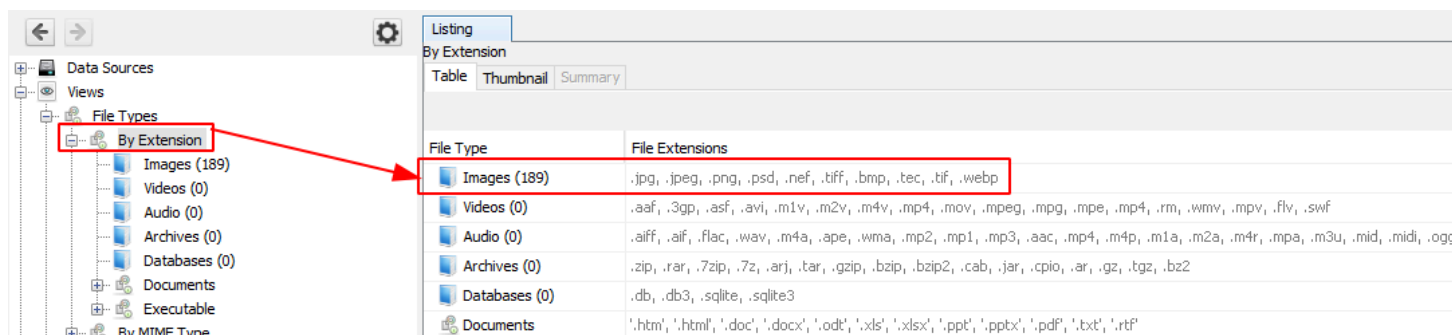
It provides information on file extensions that are commonly used by the OS whereas MIME types are used by the browser to decide what data to represent. It also displays deleted files.

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

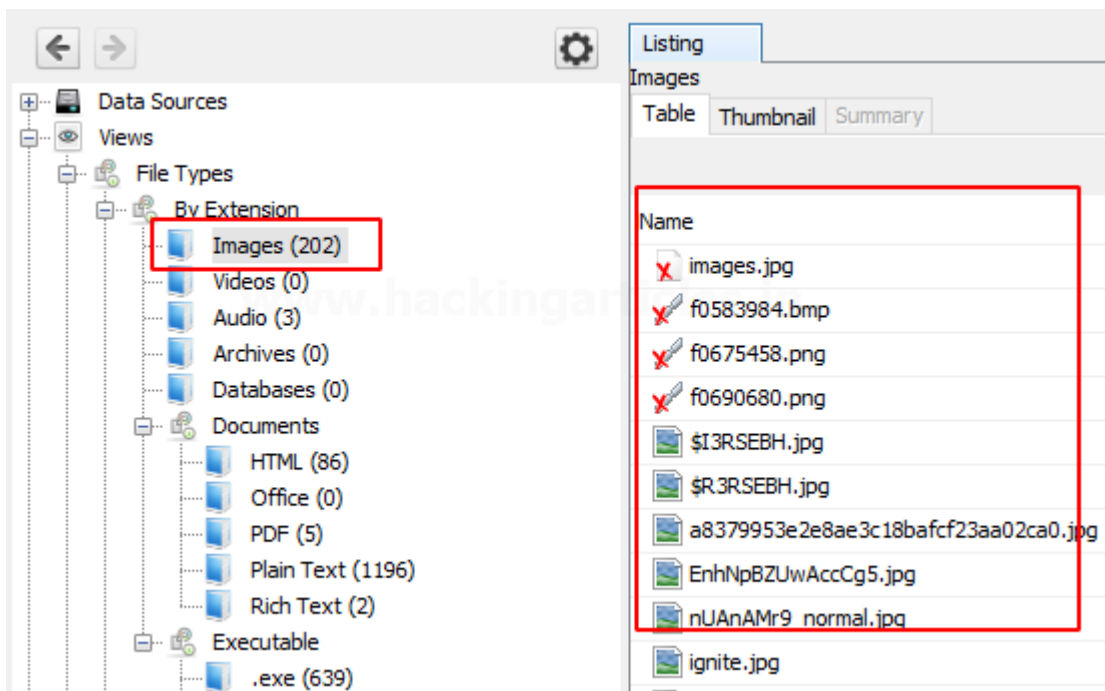


By Extension

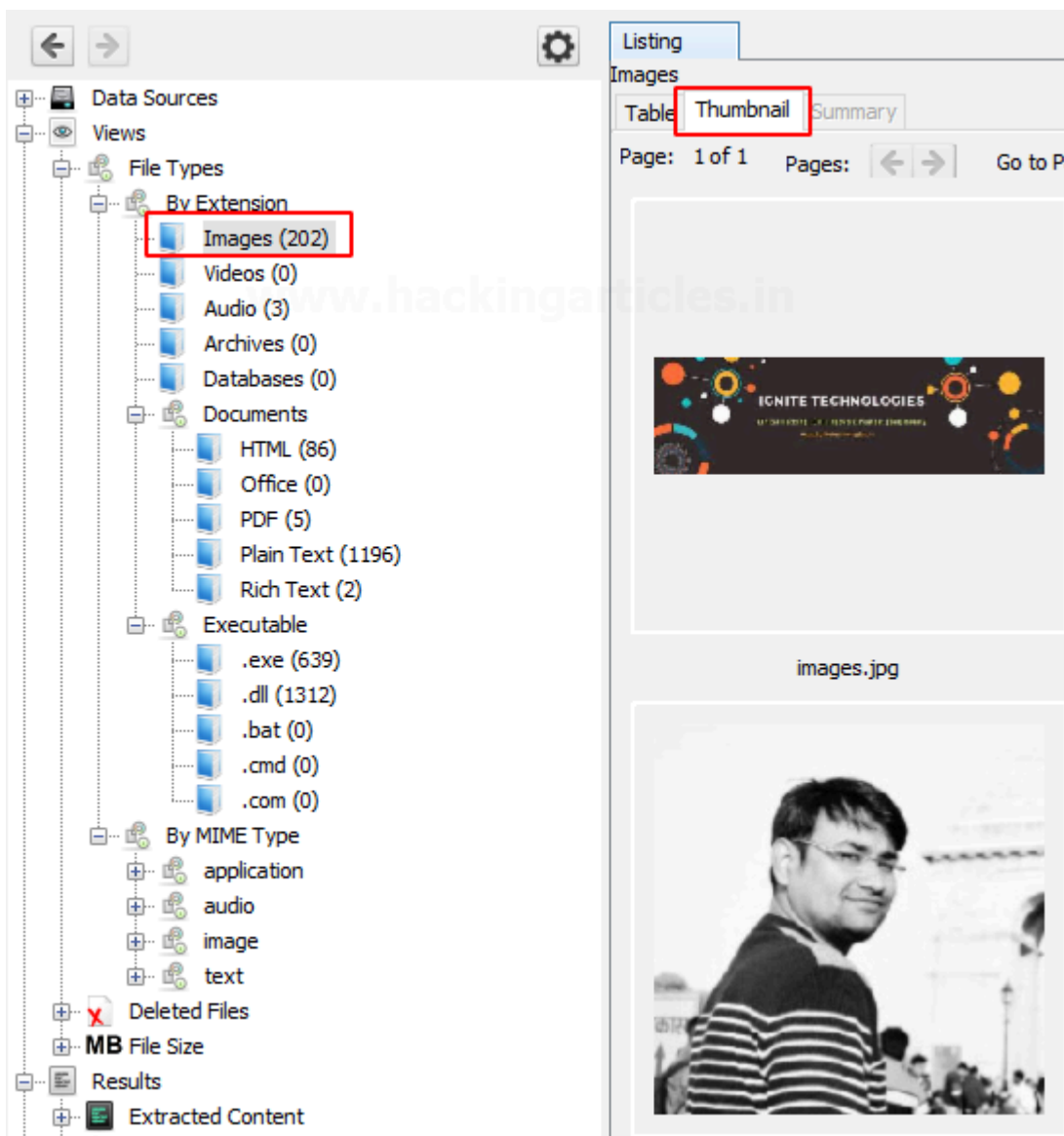
In the category Filetypes by extension and you can see that this has been sub-divided into file types like images, video, audio, archives, databases, etc.



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



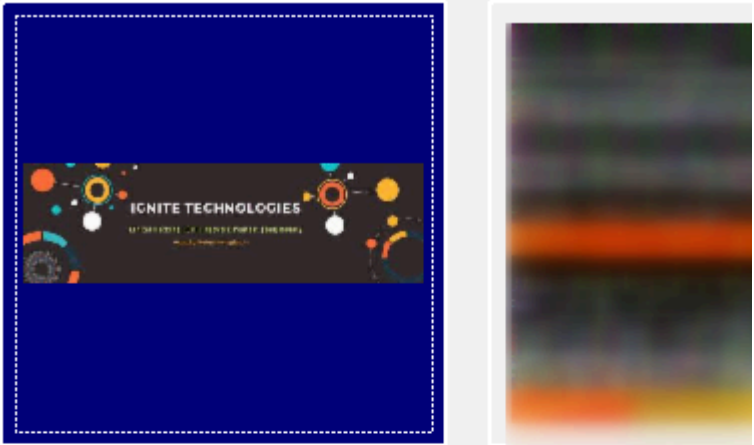
We can also view the thumbnail of the images.



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

Table Thumbnail Summary

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



images.jpg
/img_Ignite.E01/images.jpg

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

From The Sleuth Kit istat Tool:

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

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

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

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

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

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

The screenshot shows a file explorer interface with a tree view on the left and a table of audio files on the right. The tree view is organized into 'Data Sources', 'Views', and 'File Types'. Under 'File Types', there are 'By Extension' and 'By MIME Type' categories. The 'By Extension' category is expanded, showing various file types like Images, Videos, Audio, Archives, Databases, Documents, and Executable. The 'Audio (3)' folder is highlighted with a red box. A red arrow points from this box to the table of audio files. The table has columns for Name, S, C, O, Modified Time, and Change T. The file 'f0313832.wav' is highlighted with a red box. A context menu is open over the table, showing options like 'Properties', 'View File in Directory', 'View in New Window', 'Open in External Viewer Ctrl+E', 'View File in Timeline...', 'Extract File(s)', 'Export selected rows to CSV', 'Add File Tag', 'Remove File Tag', 'Add/Edit Central Repository Comment', and 'Add File to Hash Set (Ingest is running)'. The 'Extract File(s)' option is highlighted with a red box.

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

The screenshot displays a file analysis tool interface. On the left, a sidebar lists various file types and categories, including 'HTML (86)' which is highlighted with a red box. The main panel shows a table of HTML files, with 'Forensic Investigation Autopsy Forensic Browser in Linux.html' highlighted by a red rectangle. Below the table, there are tabs for 'Strings', 'Indexed Text', and 'Translation'. The 'Indexed Text' tab is active, showing a list of strings including 'Hacking Articles', 'Raj Chandel's Blog', and a list of topics like 'CTF Challenges', 'Penetration Testing', etc.

File Types List:

- Images (202)
- Videos (0)
- Audio (3)
- Archives (0)
- Databases (0)
- Documents
- HTML (86)**
- Office (0)
- PDF (5)
- Plain Text (1196)
- Rich Text (2)
- Executable
 - .exe (639)
 - .dll (1312)
 - .bat (0)
 - .cmd (0)
 - .com (0)
- By MIME Type
 - application
 - audio
 - image
 - text
- Deleted Files
- File Size
- Results
 - Extracted Content
 - Metadata (6)
 - Recycle Bin (4)
 - Web Downloads (3)
- Keyword Hits
- Hashset Hits
- E-Mail Messages

HTML File List:

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

Indexed Text Content:

```

Hacking Articles

Raj Chandel's Blog

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

Forensic Investigation: Autopsy Forensic Browser in Linux






posted inCyber Forensics on August 13, 2020 by Raj Chandel
SHARE
Save
  
```

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

Listing

PDF

Table Thumbnail Summary

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-

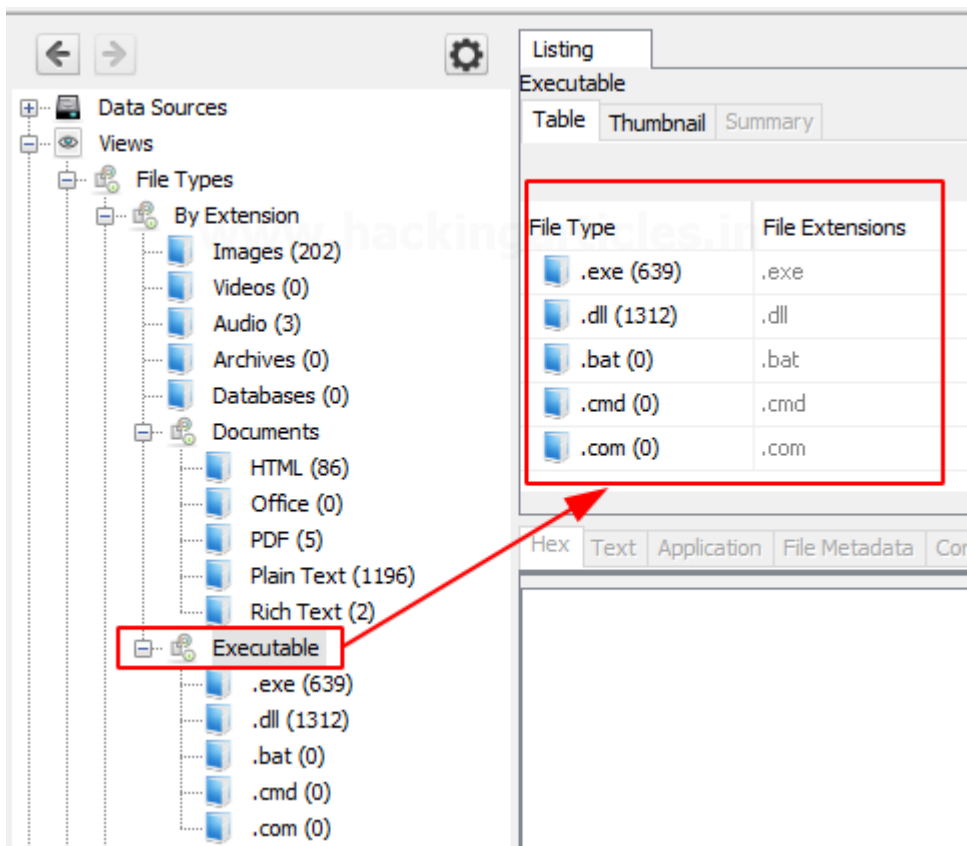
Hex Text Application File Metadata Context Results Annotations Other Occurrences

1 of 5 29%

POWERED BY IGNITE TECHNOLOGIES

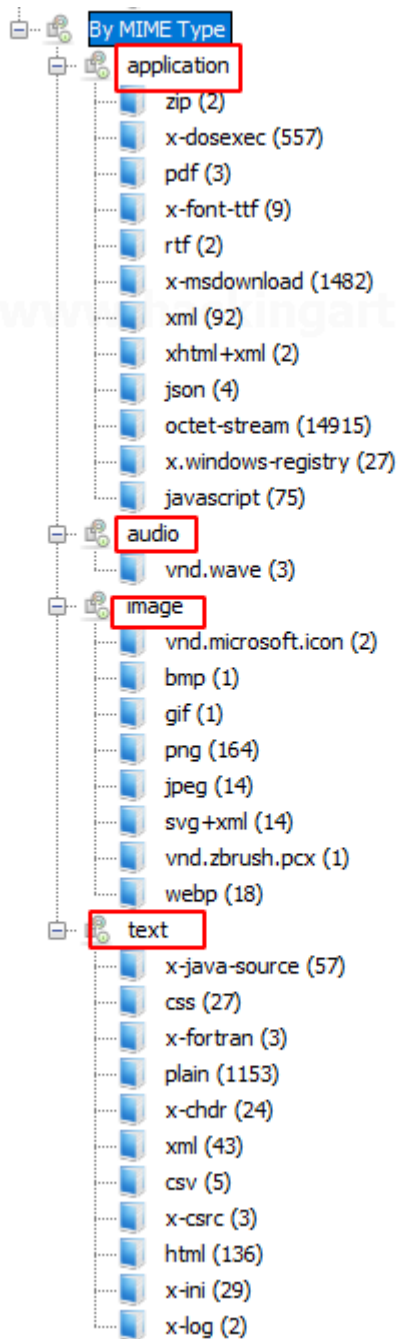
ANDROID PENTESTING

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



By MIME Type

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



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

File System

Table Thumbnail Summary

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

Name	S	C	O	Modified Time
20201014.mem			0	2020-10-13 13:39:50 PDT
adencrypt.dll			0	2020-05-11 21:03:46 PDT
adencrypt_gui.exe			0	2020-05-11 21:03:46 PDT
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.

MB File Size

Table Thumbnail Summary

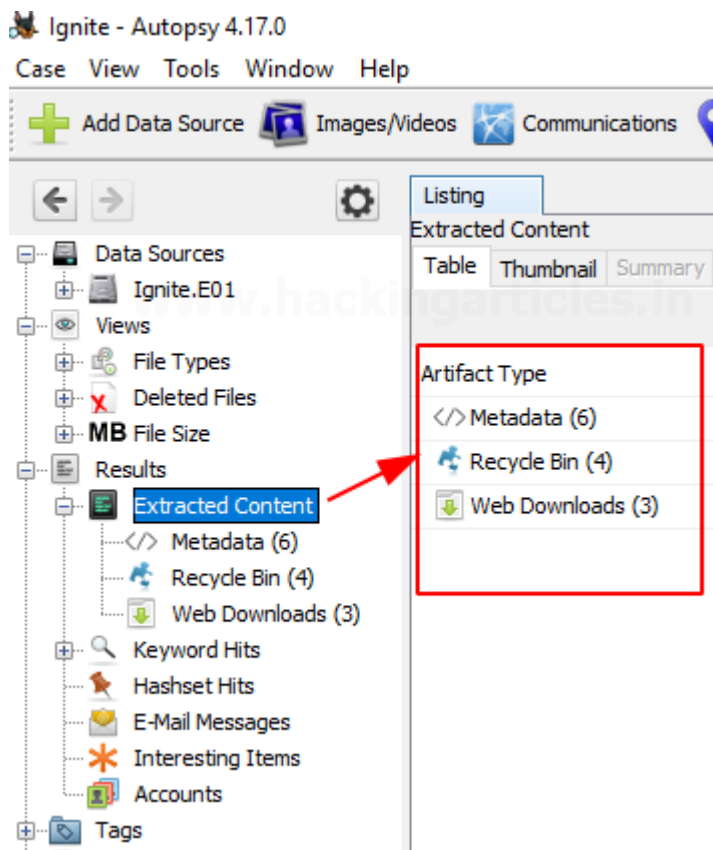
Page: Pages: < > Go to Page:

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.

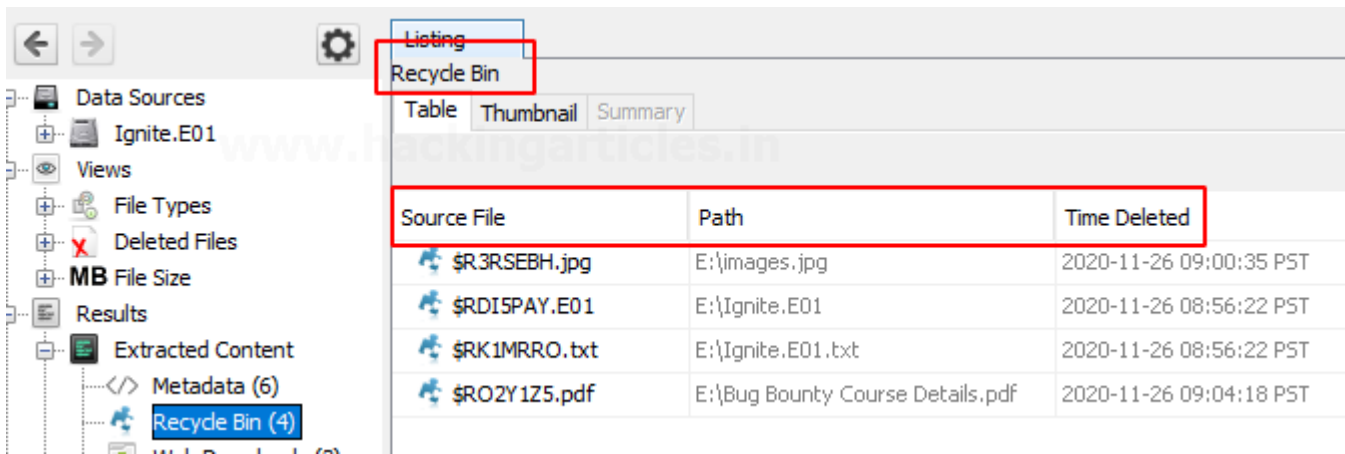
Extracted Content: All the content that was extracted, is segregated further in detail. Here we have found metadata, Recycle Bin, and web downloads. Let us further view each one of them.



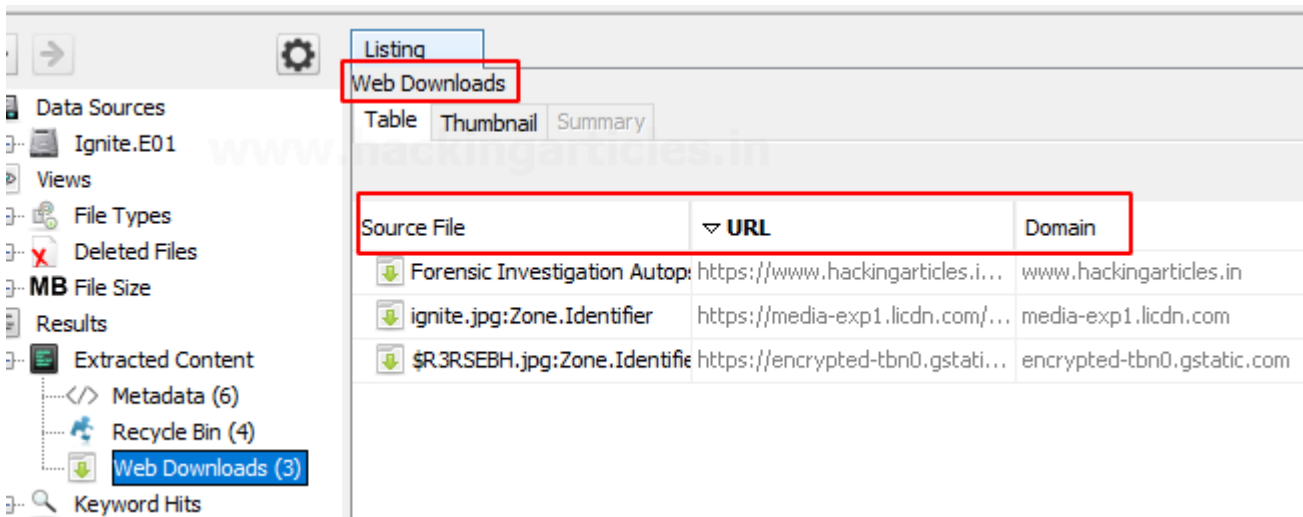
Metadata: Here we can view all the information about the files like the date it was created, to was modified, file's owner, etc.

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	Recycle Bin	Ignite.E01
</> ADG_EULA.rtf		2016-02-25 02:55:00 PST	Recycle Bin	Ignite.E01
</> FTKImager_UserGuide.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	Recycle Bin	Ignite.E01
</> f0184904.pdf	2012-03-21 20:52:22 PDT	2012-03-21 11:26:46 PDT	Recycle Bin	Ignite.E01
</> f0002808.rtf		2016-02-25 02:55:00 PST	Recycle Bin	Ignite.E01

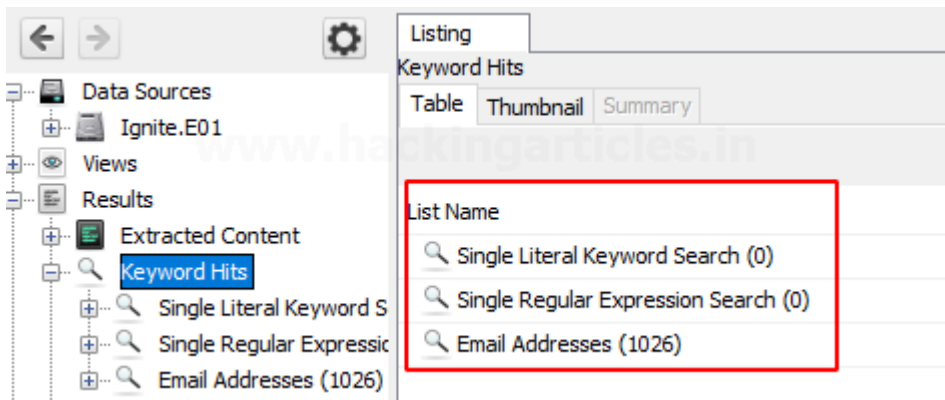
Recycle Bin: The files that were put in the recycle bin are found in this category.



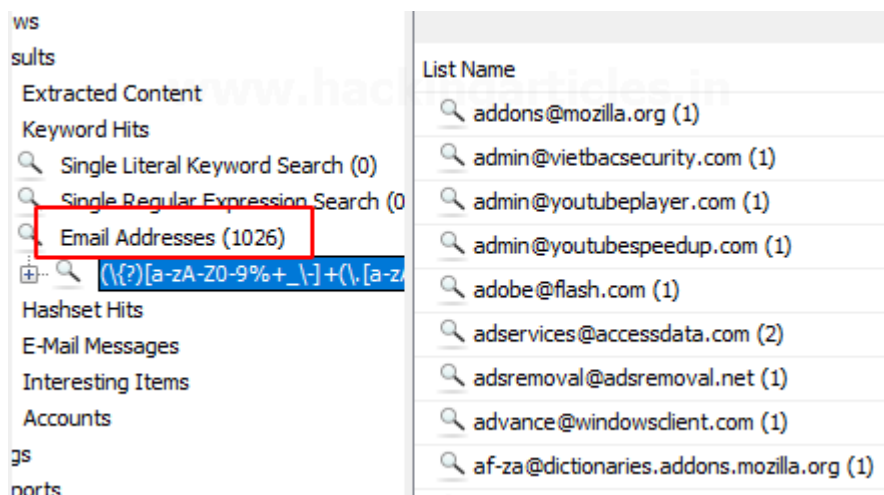
Web Downloads: Here you can see the files that were downloaded from the internet.



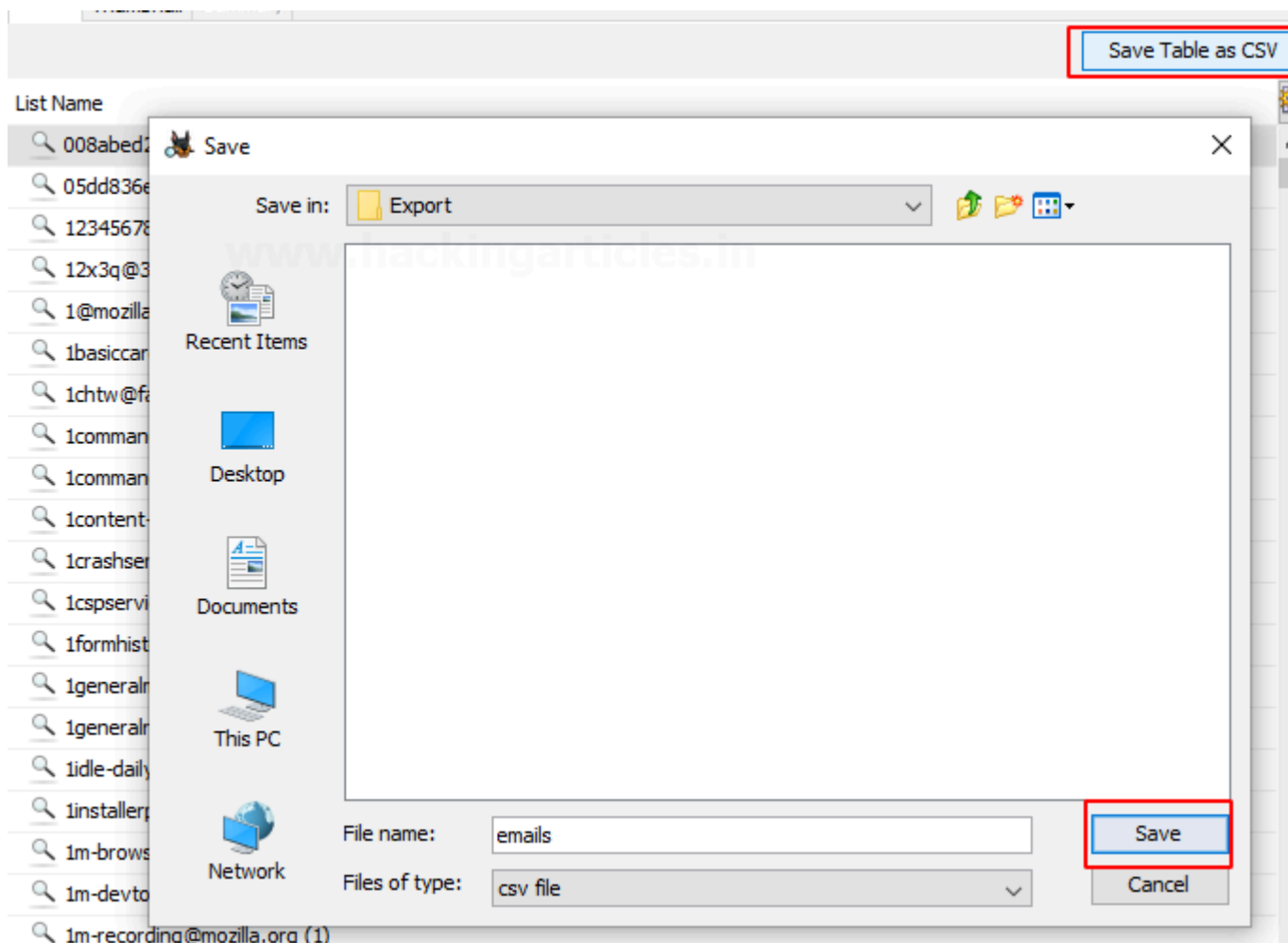
Keyword Hits: In this, any specific keywords can be looked up for in the disk image. The search can be conducted concerning the Exact match, Substring matches, Emails, Literal words, Regular expressions, etc.



You can view the available email addresses.

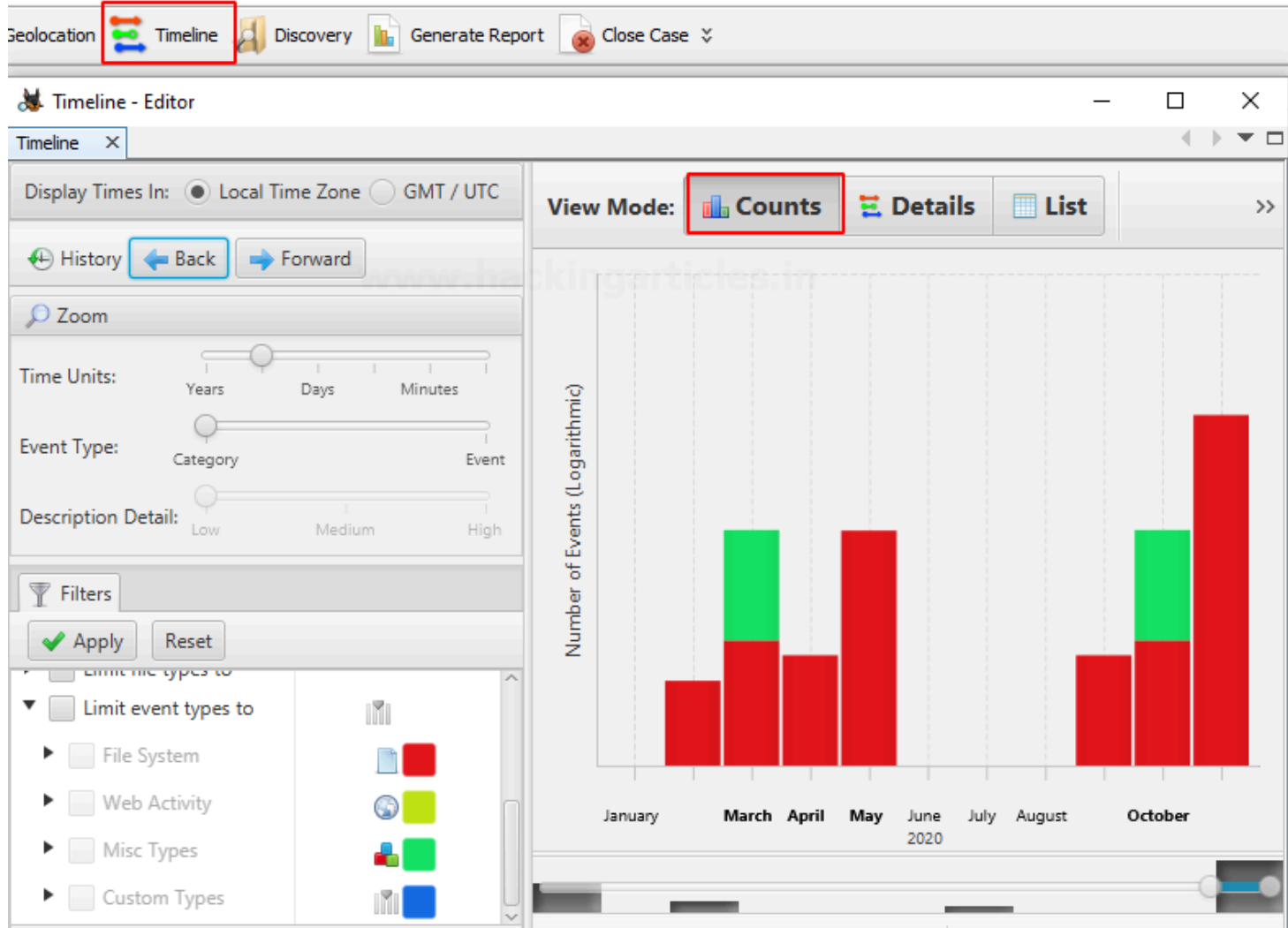


You can choose to export into a CSV format.



Timeline

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



Display Times In: ☒ Local Time Zone ☐ GMT / UTC

History ← Back → Forward

Zoom

Time Units:

Years Days Minutes

Event Type:

Category Event

Description Detail:

Low Medium High

Filters

Apply Reset

Limit event types to

☐ File System

☐ Web Activity

☐ Misc Types

☐ Custom Types

Hidden Descriptions

View Mode:

Counts Details List

All Events (Filtered)

.../S-1-5-21-1276730070-1850728493-30201559-1001/\$RO21

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

Document Last Saved (2) 46

... : :

Document Created (2)

... : :

/Bug Bounty Course Details.pdf (4)

... 3

/USB.txt (4)

2

2

/20201014.mem (4)

January April June August November

2020

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

Timeline - Editor

Timeline

Display Times In: ☒ Local Time Zone ☐ GMT / UTC

History Back Forward

Filters

Apply Reset

☐ Must include text: enter filter string
☐ Must be tagged
☐ Must have hash hit
☐ Limit data sources to
☐ Limit file types to
☒ Limit event types to

☐ File System
☐ Web Activity
☐ Misc Types
☐ Custom Types

View Mode: ☒ Counts ☐ Details ☒ List

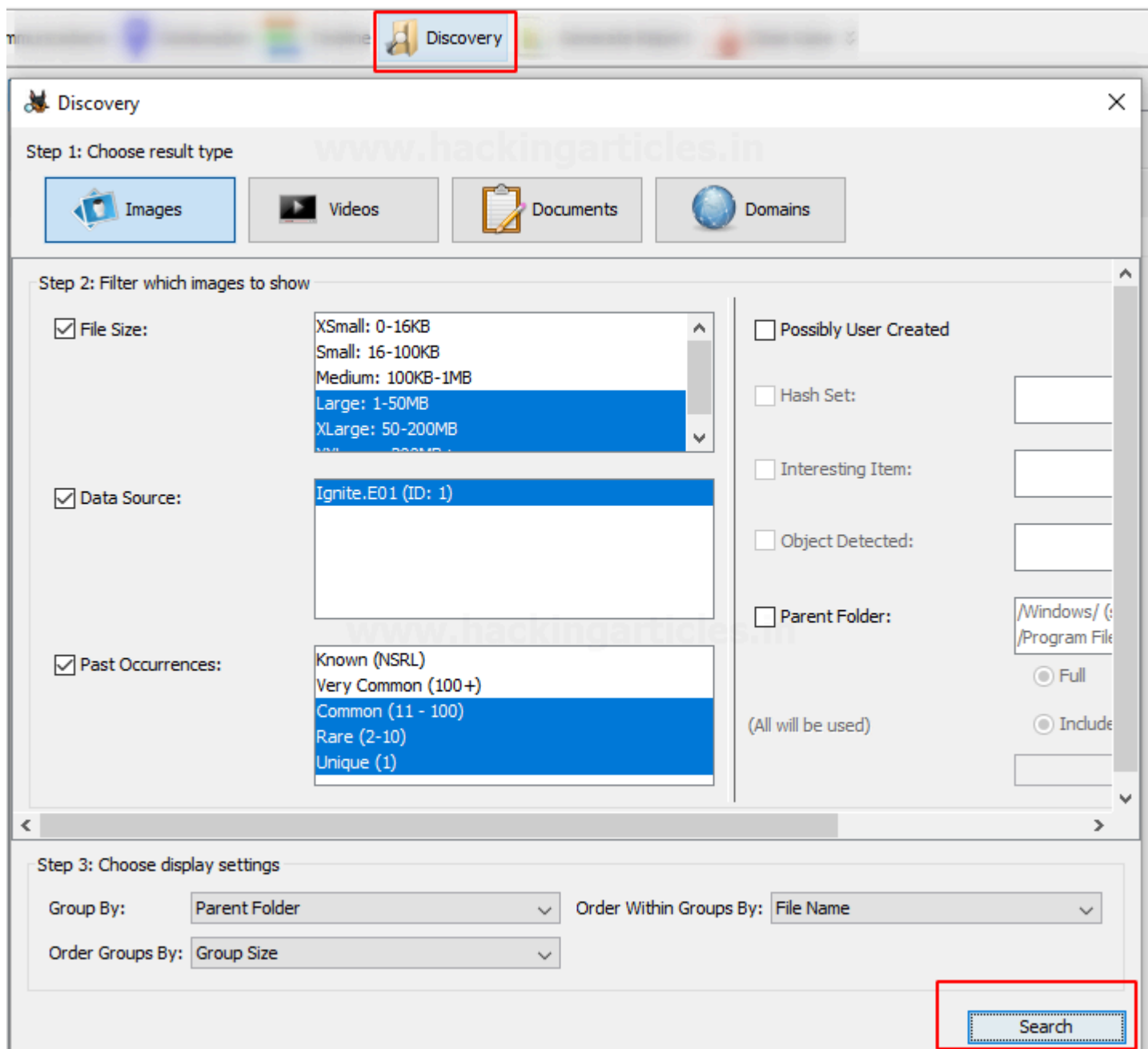
Date/Time	Event Type	Description	Tags
2020-02-06 05:18:36	M__	/\$Orpha ... LA.rtf	
2020-03-01 00:32:57	M__	/\$RECY ... Z5.pdf	
2020-03-01 08:32:56	Document L...	Documen ... d :	
2020-03-01 08:32:56	Document ...	Documen ... d :	
2020-03-10 09:42:02	M__	/\$Orpha ... gpl.txt	
2020-03-10 09:48:50	M__	/\$Orpha ... 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	

☒ Hidden Descriptions

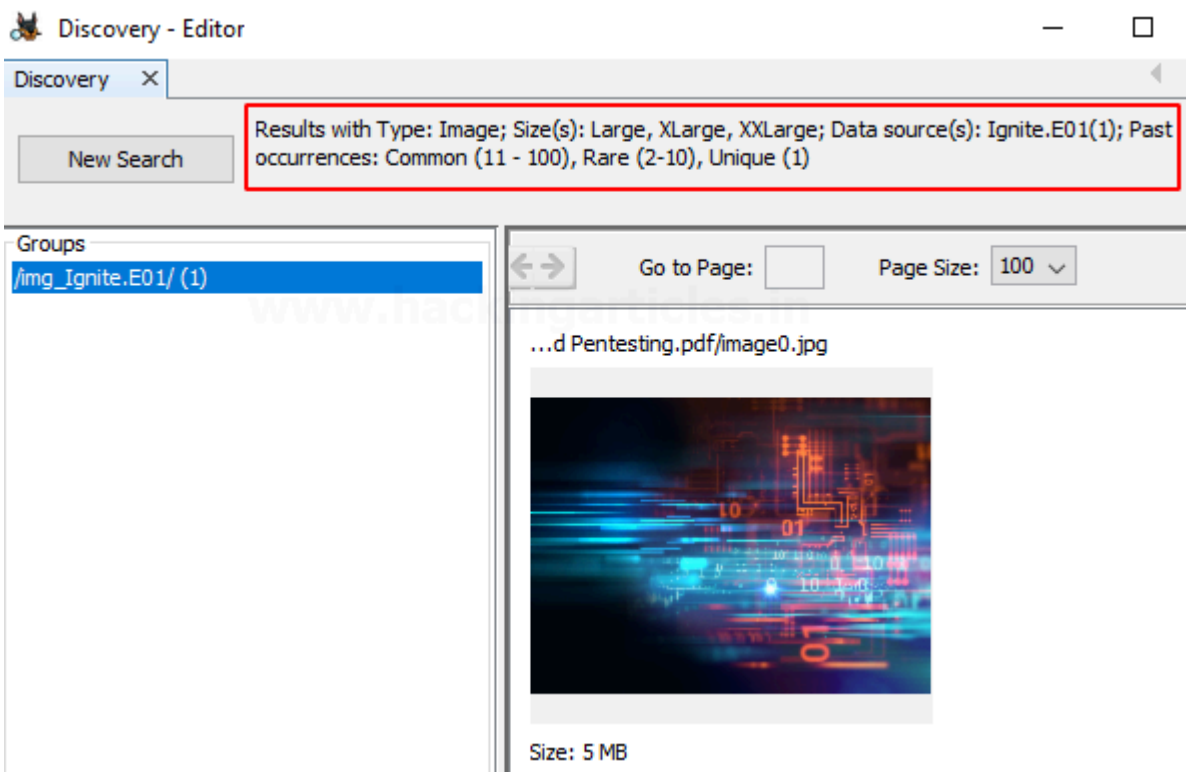
Start: Jan 27, 2020 11:33:00 PM

Discovery

This option allows finding media using different filters that are present on the disk image.

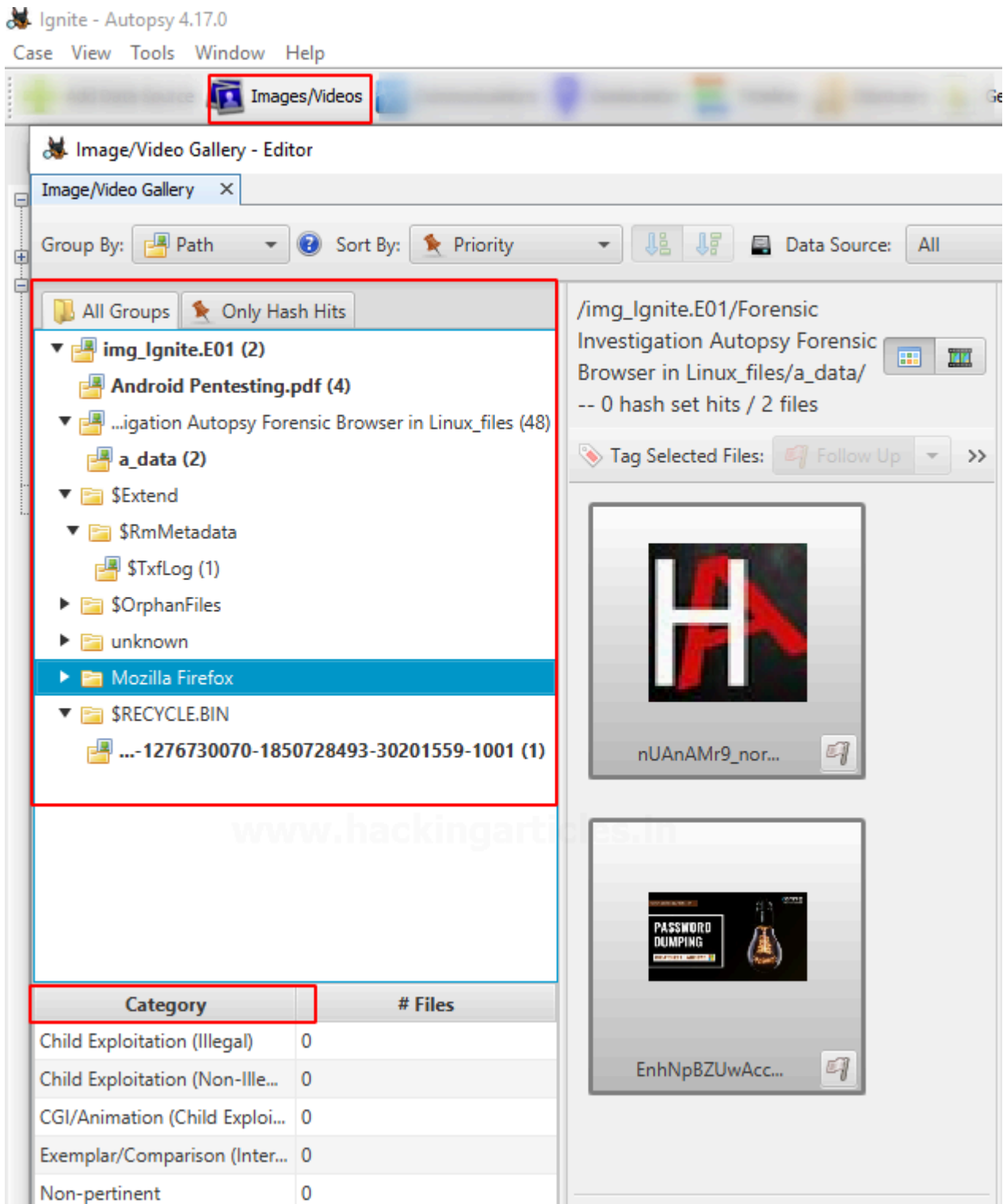


According to the selected options, you can get the desired results.



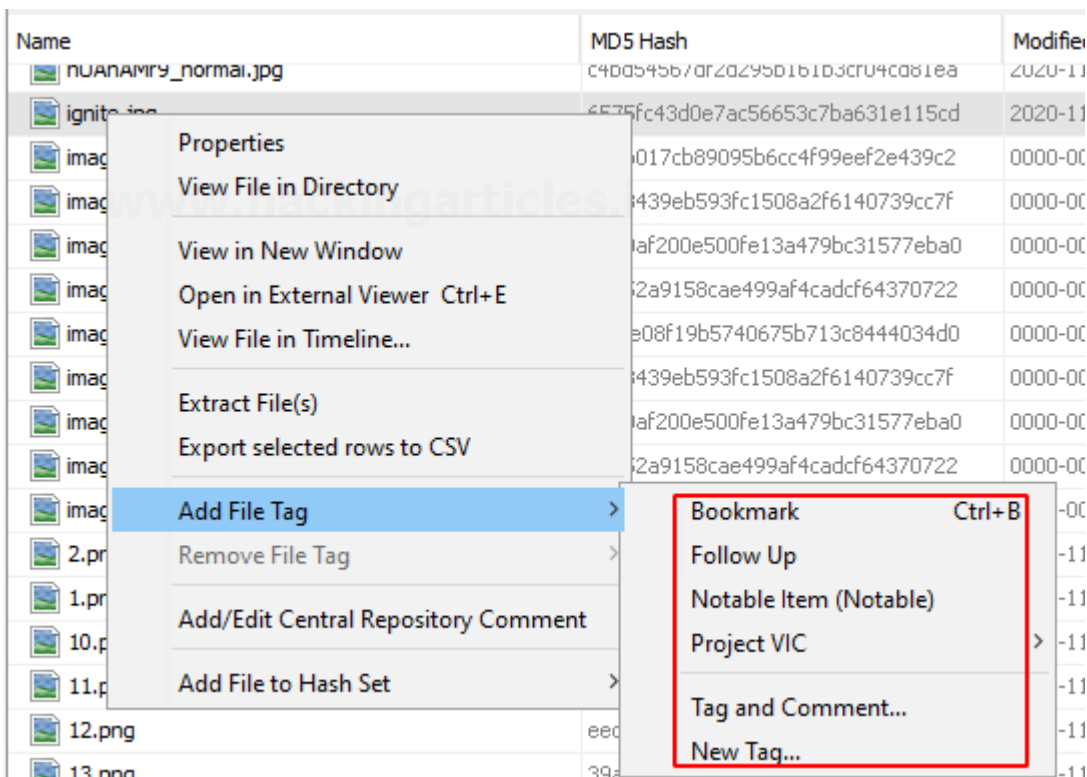
Images/Videos

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

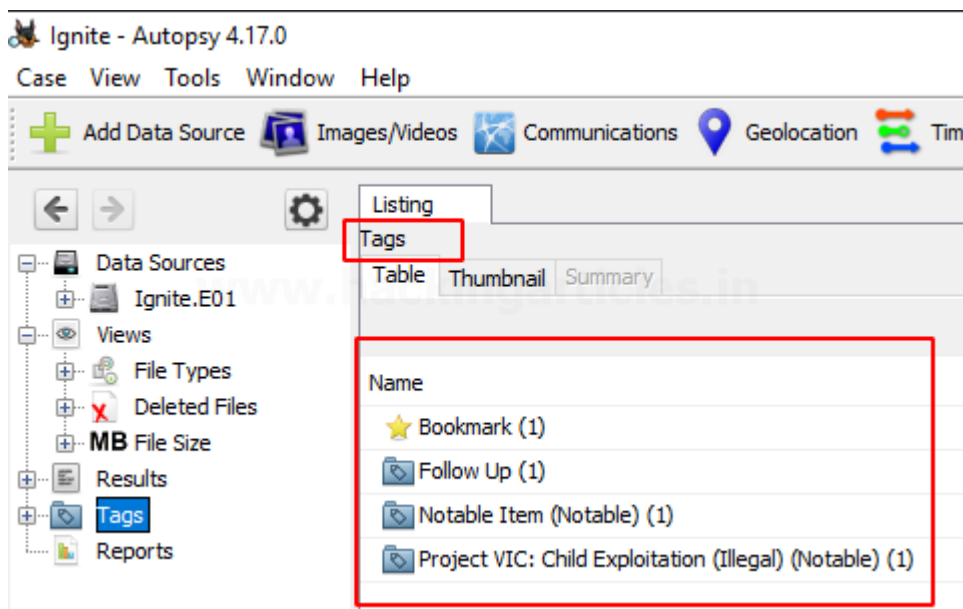


Add File Tag

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



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



Generate Report

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

Generate Report

Select and Configure Report Modules

Report Modules:

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

A report about results and tagged items in HTML format.

Header: Report

Footer: Details

< Back Next > Finish

Check the data source whose report needs to be generated.

Generate Report


Select which data source(s) to include


☒ Ignite.E01

Uncheck All Check All

< Back Next Finish Cancel Help

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