

**AUTOPSY  
WINDOWS**

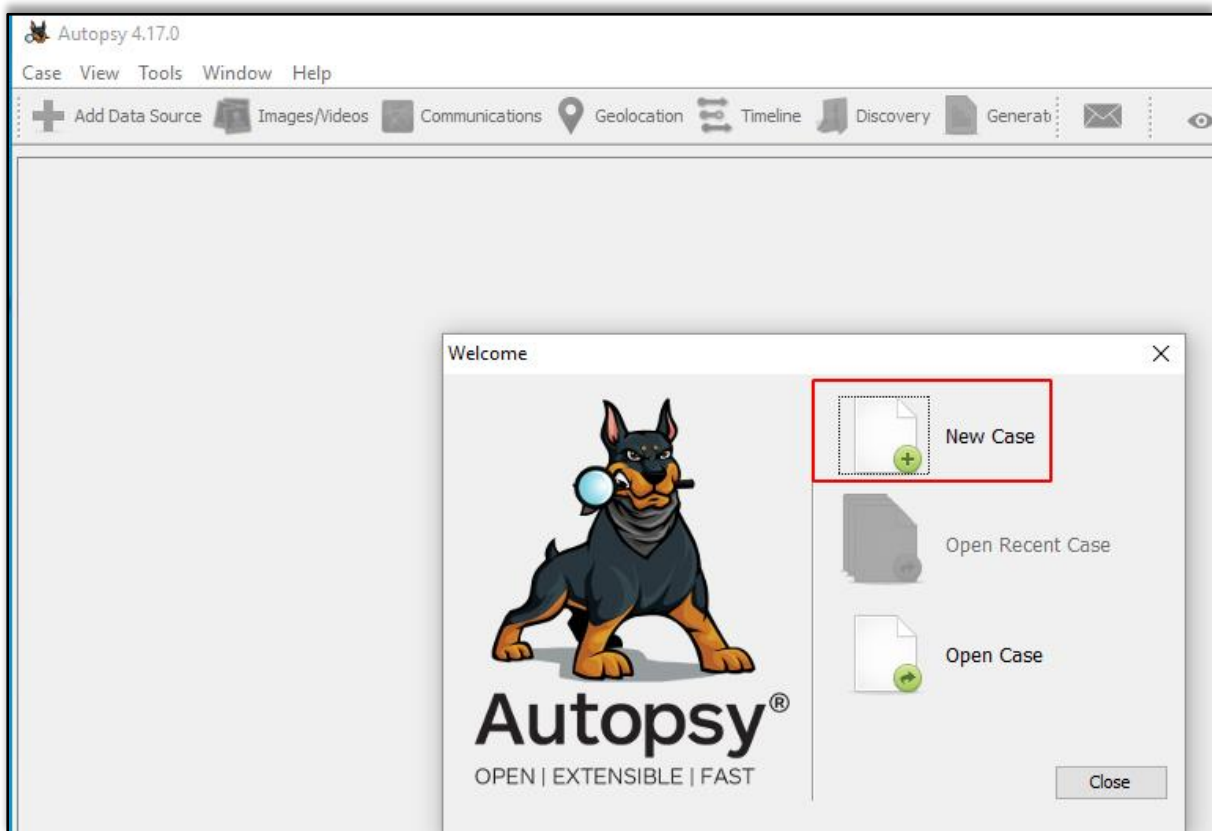
## Autopsy for Windows



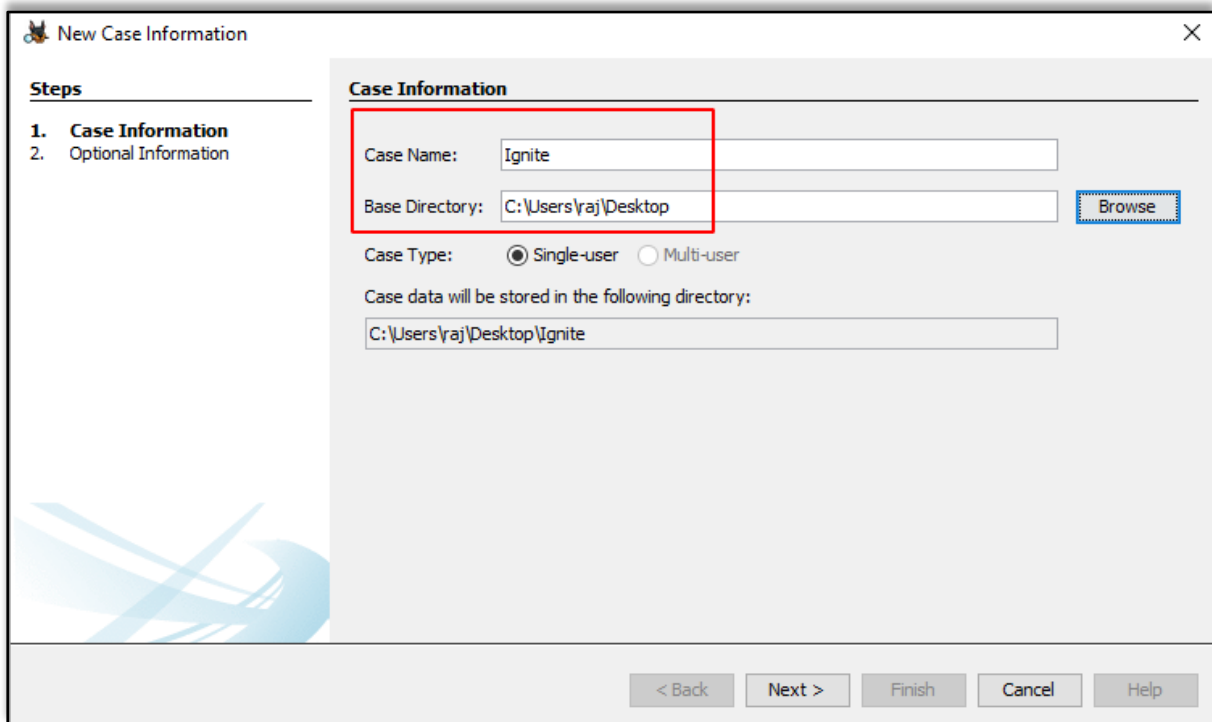
You can download the Autopsy Tool for Windows from [here](#).

## 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.



The screenshot shows the 'New Case Information' dialog box with the 'Case Information' step selected. The 'Case Name' field is filled with 'Ignite' and the 'Base Directory' field is filled with 'C:\Users\raj\Desktop'. A red box highlights these two fields. A 'Browse' button is visible next to the 'Base Directory' field. The 'Case Type' is set to 'Single-user'. The 'Case data will be stored in the following directory:' field is filled with 'C:\Users\raj\Desktop\ignite'. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The bottom of the dialog has buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**New Case Information**

**Steps**

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

**Case Information**

Case Name: Ignite

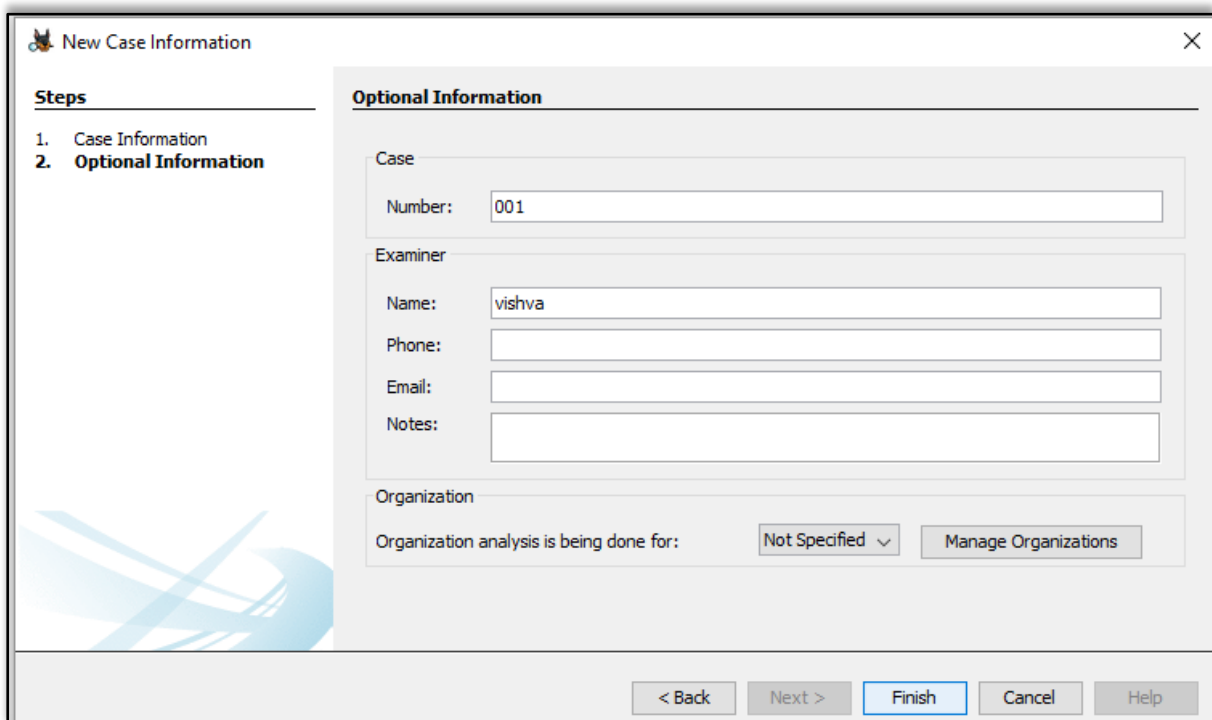
Base Directory: C:\Users\raj\Desktop **Browse**

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.



The screenshot shows the 'New Case Information' dialog box with the 'Optional Information' step selected. The 'Case Number' is '001', the 'Examiner Name' is 'vishva', and the 'Organization analysis is being done for' is 'Not Specified'. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The bottom of the dialog has buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**New Case Information**

**Steps**

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

**Optional Information**

Case

Number: 001

Examiner

Name: vishva

Phone:

Email:

Notes:

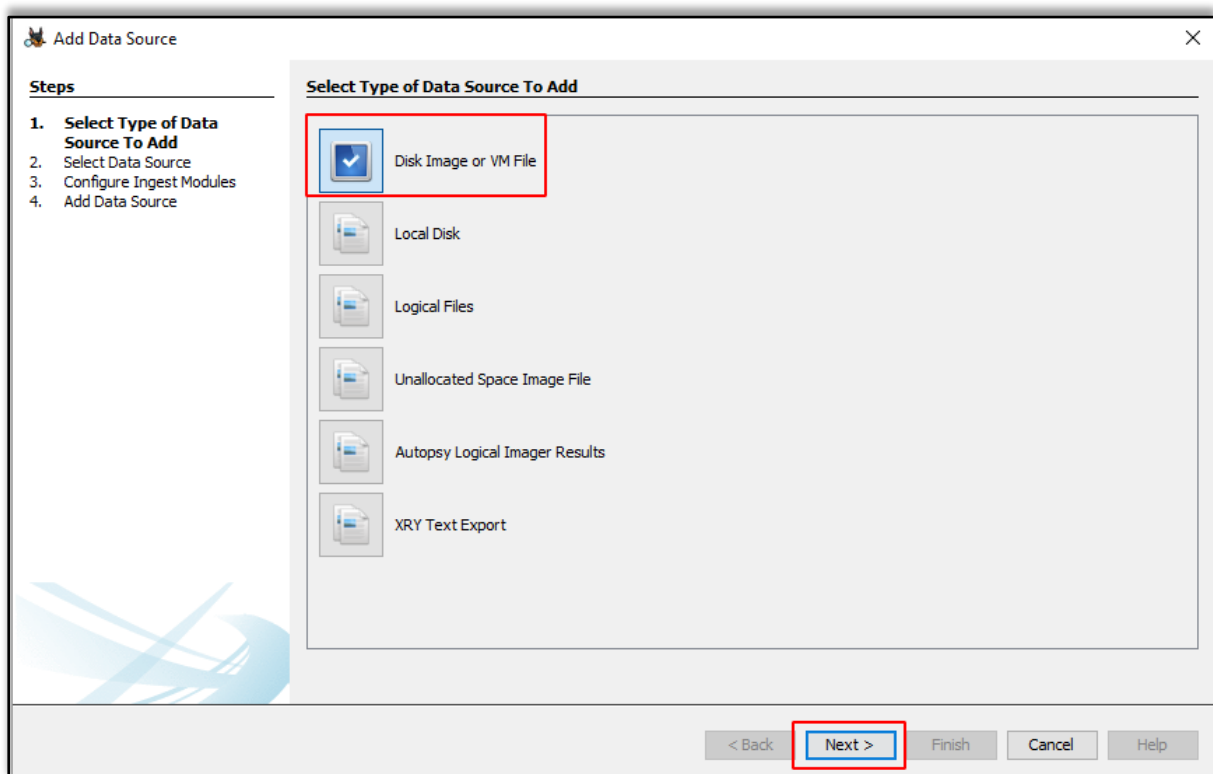
Organization

Organization analysis is being done for: Not Specified **Manage Organizations**

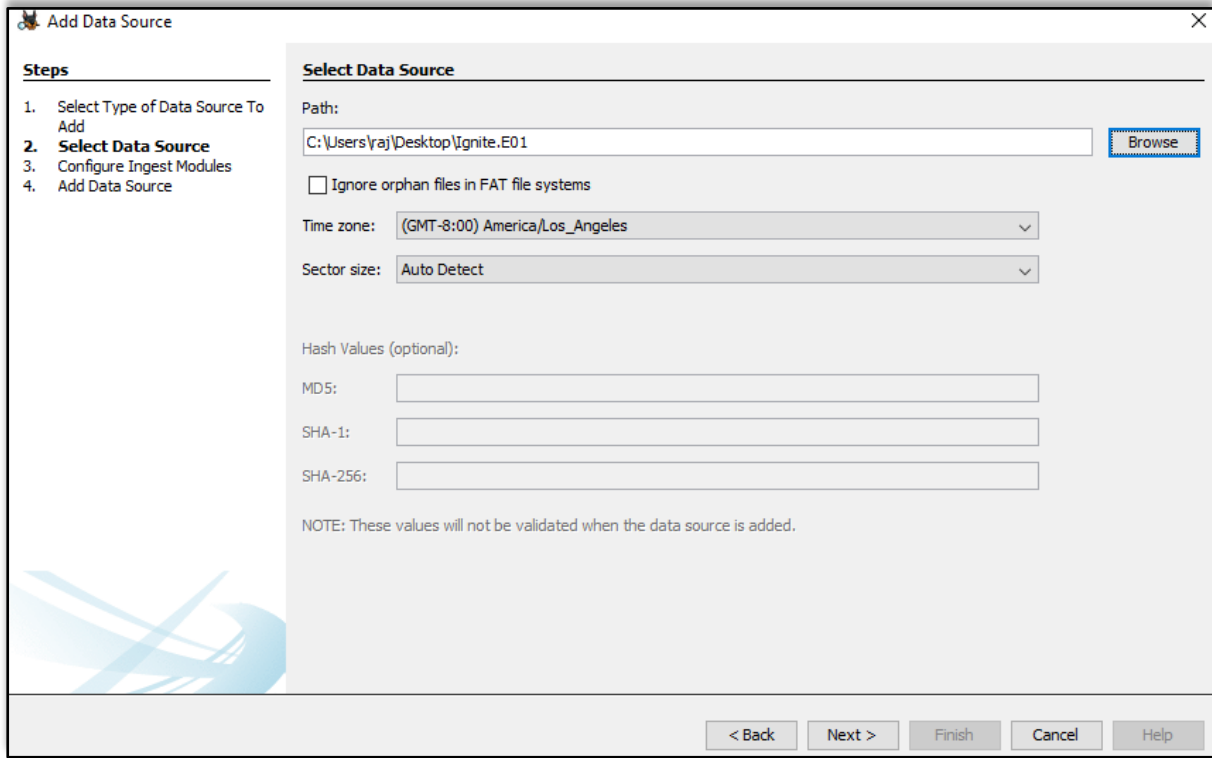
< Back Next > **Finish** Cancel Help

**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.

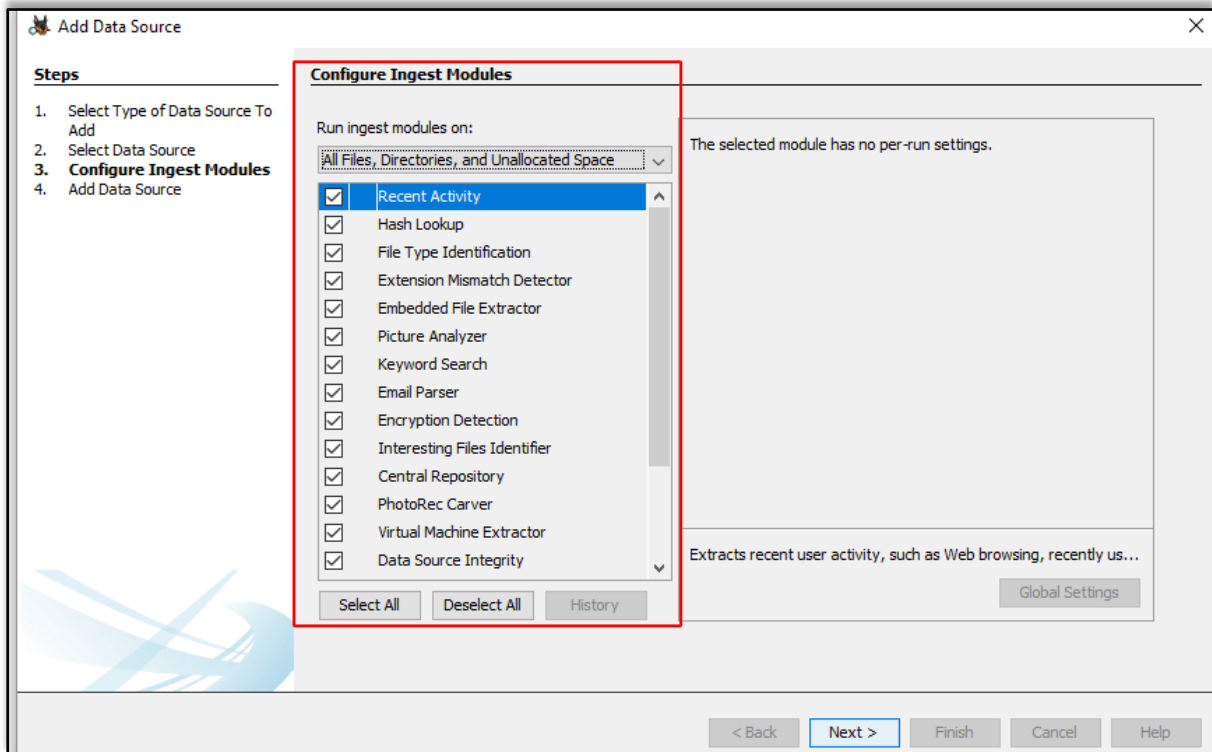


Now let us add the data source. Here we have a previously created image file, so we will add the location of that file.



The screenshot shows the 'Add Data Source' dialog box with the 'Select Data Source' step active. The 'Path' field contains 'C:\Users\raj\Desktop\Ignite.E01' and a 'Browse' button is visible. Below the path field, there is an unchecked checkbox for 'Ignore orphan files in FAT file systems'. The 'Time zone' is set to '(GMT-8:00) America/Los\_Angeles' and 'Sector size' is set to 'Auto Detect'. There are three input fields for 'Hash Values (optional)': MD5, SHA-1, and SHA-256. A note at the bottom states: 'NOTE: These values will not be validated when the data source is added.' The 'Steps' list on the left shows: 1. Select Type of Data Source To Add, 2. **Select Data Source**, 3. Configure Ingest Modules, 4. Add Data Source. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

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



The screenshot shows the 'Add Data Source' dialog box with the 'Configure Ingest Modules' step active. The 'Run ingest modules on:' dropdown is set to 'All Files, Directories, and Unallocated Space'. A list of ingest modules is shown with checkboxes: 'Recent Activity' (checked and highlighted), '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', and 'Data Source Integrity'. Below the list are 'Select All', 'Deselect All', and 'History' buttons. The right pane shows 'The selected module has no per-run settings.' and a description for 'Recent Activity': 'Extracts recent user activity, such as Web browsing, recently us...'. A 'Global Settings' button is also present. The 'Steps' list on the left shows: 1. Select Type of Data Source To Add, 2. Select Data Source, 3. **Configure Ingest Modules**, 4. Add Data Source. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

The contents of the Ingest module are listed below:

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

The screenshot shows the Ignite - Autopsy 4.17.0 interface. The left sidebar shows the 'Data Sources' section expanded. The main window displays a table with columns for Name, Type, and Size (Bytes). The table contains one entry: Ignite.E01, Image, 64420392960. Below the table, there is a hex dump view showing the raw data of the image file.

Name	Type	Size (Bytes)
Ignite.E01	Image	64420392960

Hex dump view:

```

Page: 1 of 3931909      Page: 1      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 7E  .....Y.d...dv
0x00000050: 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  .....3.....l.h.
0x00000060: 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.....f.>.N
0x00000070: 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu..A..U..r...
0x00000080: 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  U.u.....u.....

```

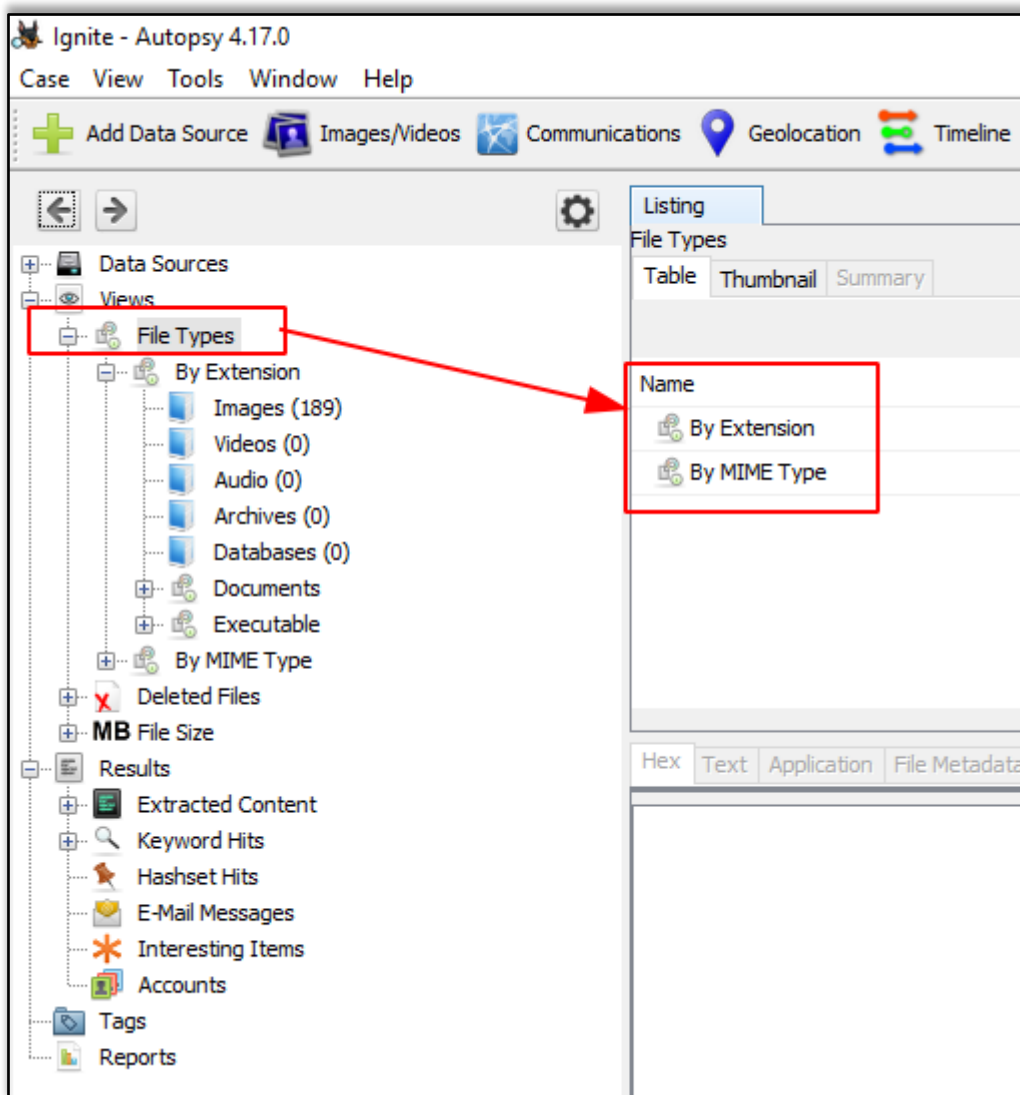
## Views

### File Type

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

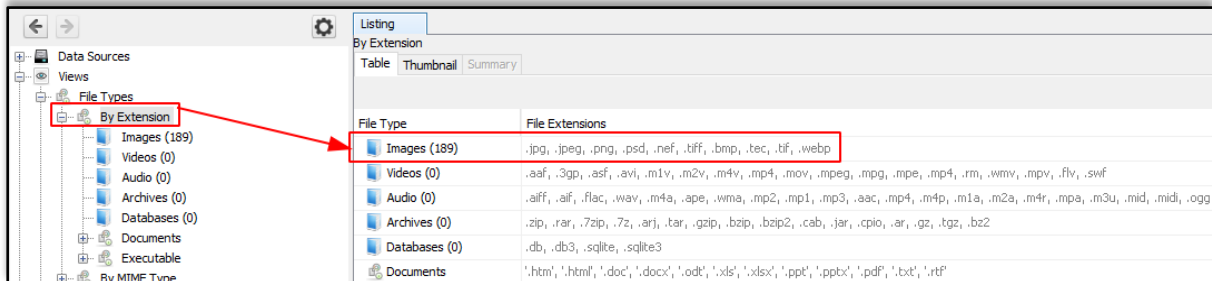
It provides information on file extensions that are commonly used by the OS whereas MIME types are used by the browser to decide what data to represent. It also displays deleted files.

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

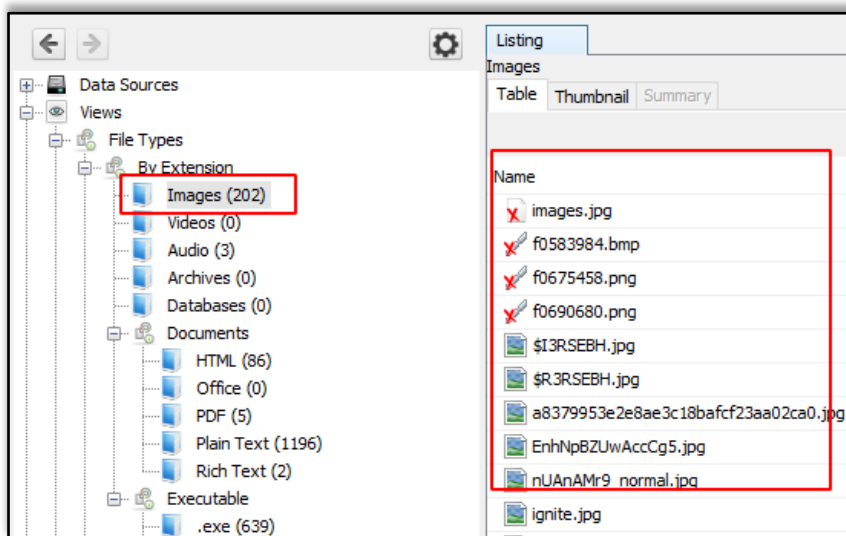


## By Extension

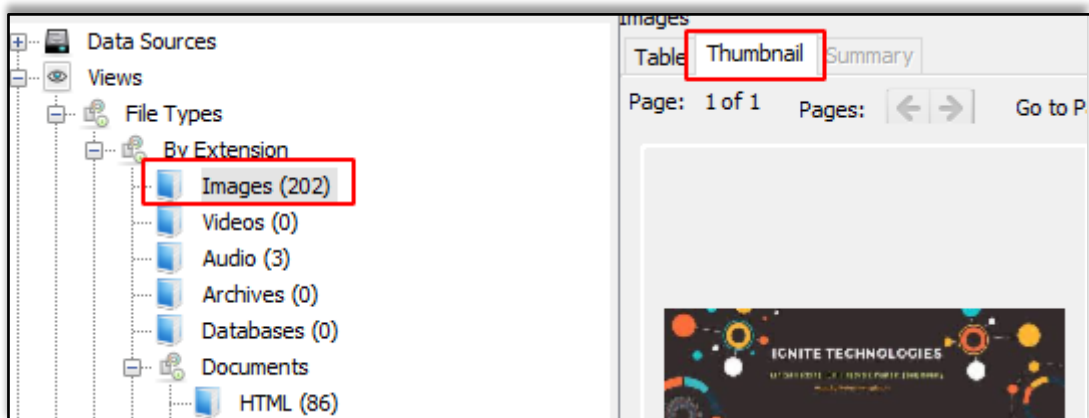
In the category Filetypes by extension and you can see that this has been sub-divided into file types like images, video, audio, archives, databases, etc.



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

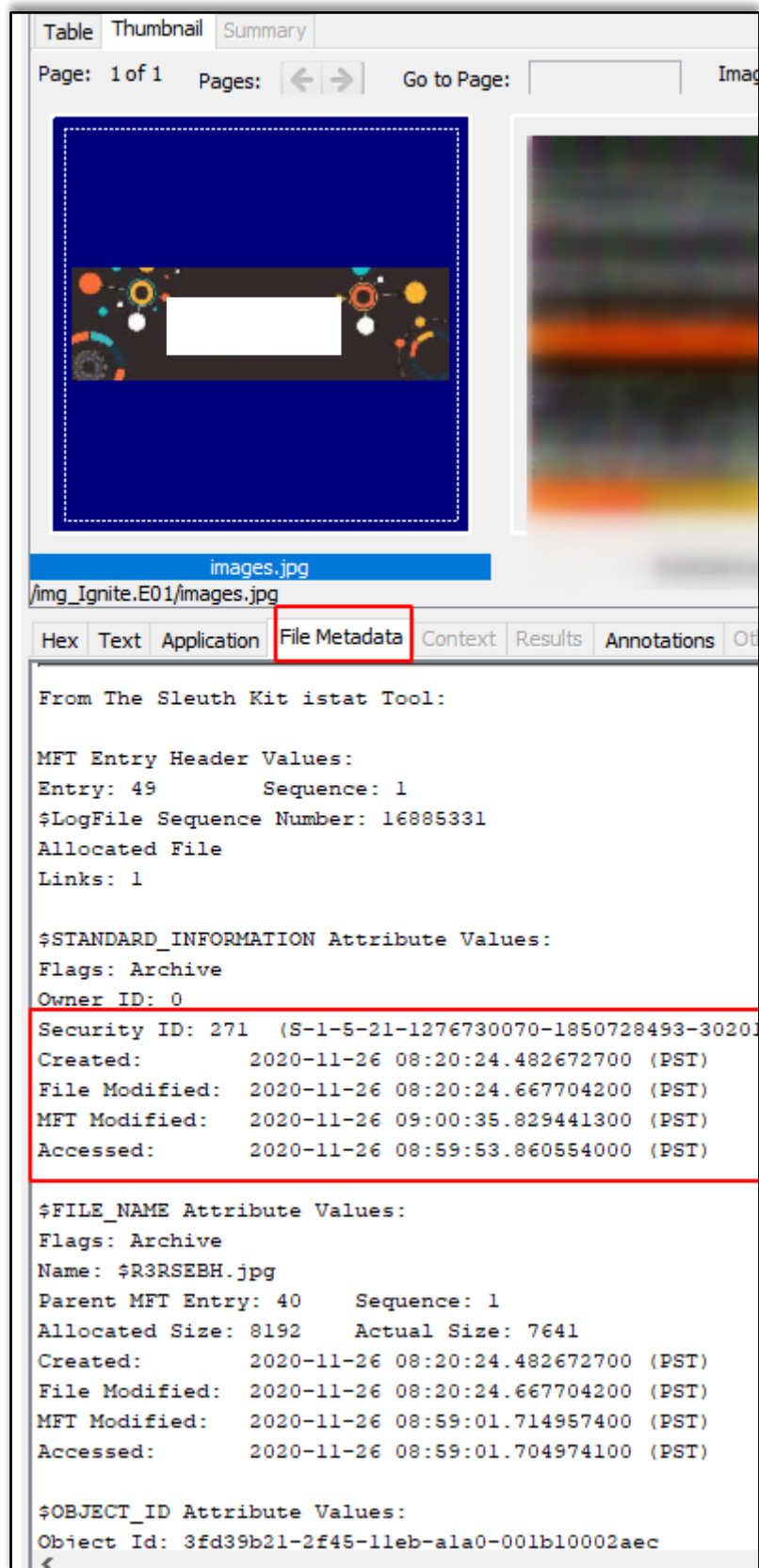


We can also view the thumbnail of the images.





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



The screenshot displays a file viewer interface. At the top, there are tabs for 'Table', 'Thumbnail', and 'Summary'. Below the tabs, it shows 'Page: 1 of 1' and navigation controls. The main area contains a large thumbnail of an image with a blue background and a central graphic, and a smaller, blurred thumbnail to its right. Below the thumbnails, the filename 'images.jpg' is shown, along with the path '/img\_Ignite.E01/images.jpg'. A red box highlights the 'File Metadata' tab. The metadata content is as follows:

```

From The Sleuth Kit istat Tool:

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

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 271 (S-1-5-21-1276730070-1850728493-30201
Created:          2020-11-26 08:20:24.482672700 (PST)
File Modified:   2020-11-26 08:20:24.667704200 (PST)
MFT Modified:    2020-11-26 09:00:35.829441300 (PST)
Accessed:        2020-11-26 08:59:53.860554000 (PST)

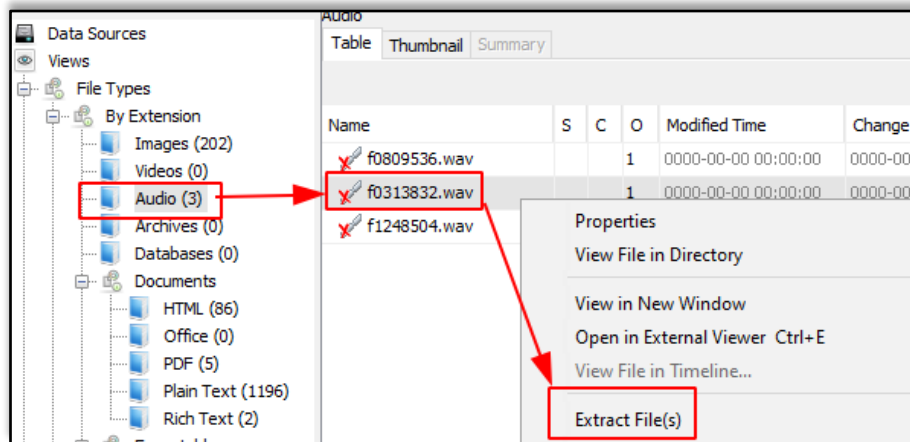
$FILE_NAME Attribute Values:
Flags: Archive
Name: $R3RSEBH.jpg
Parent MFT Entry: 40   Sequence: 1
Allocated Size: 8192   Actual Size: 7641
Created:          2020-11-26 08:20:24.482672700 (PST)
File Modified:   2020-11-26 08:20:24.667704200 (PST)
MFT Modified:    2020-11-26 08:59:01.714957400 (PST)
Accessed: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

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

```

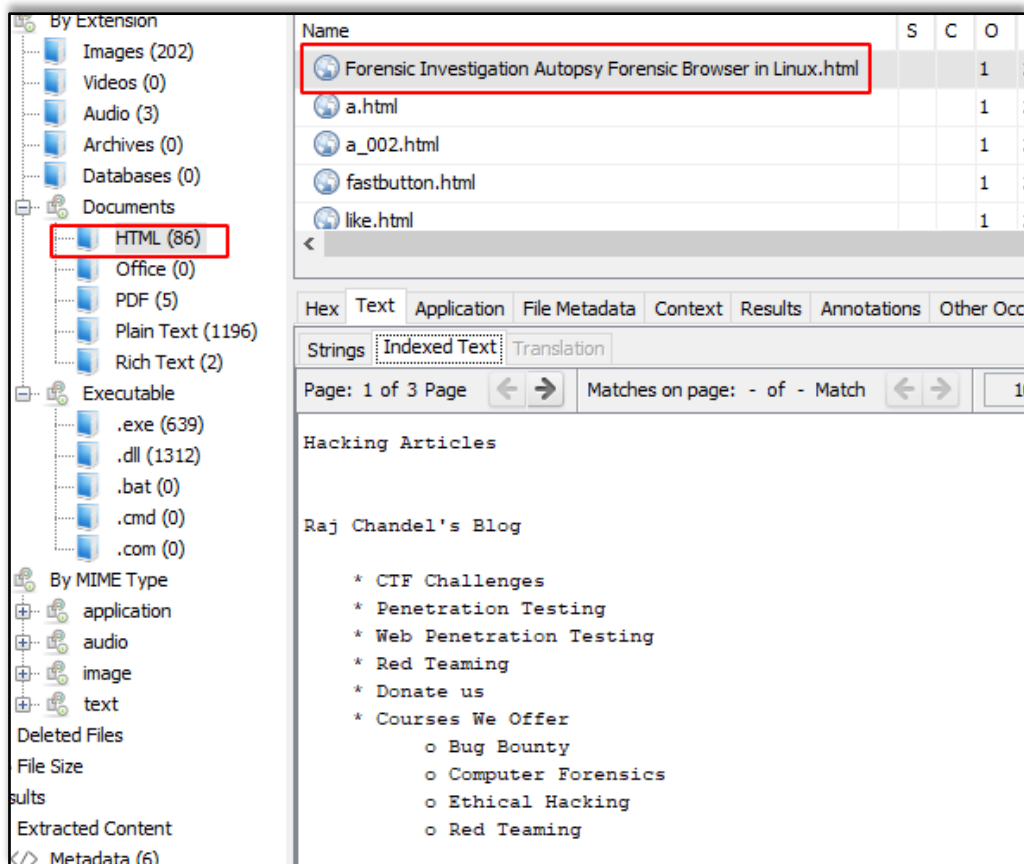


Here we can also view a few audio files that have been recovered. We can extract these files from the system and hear to them using various software.

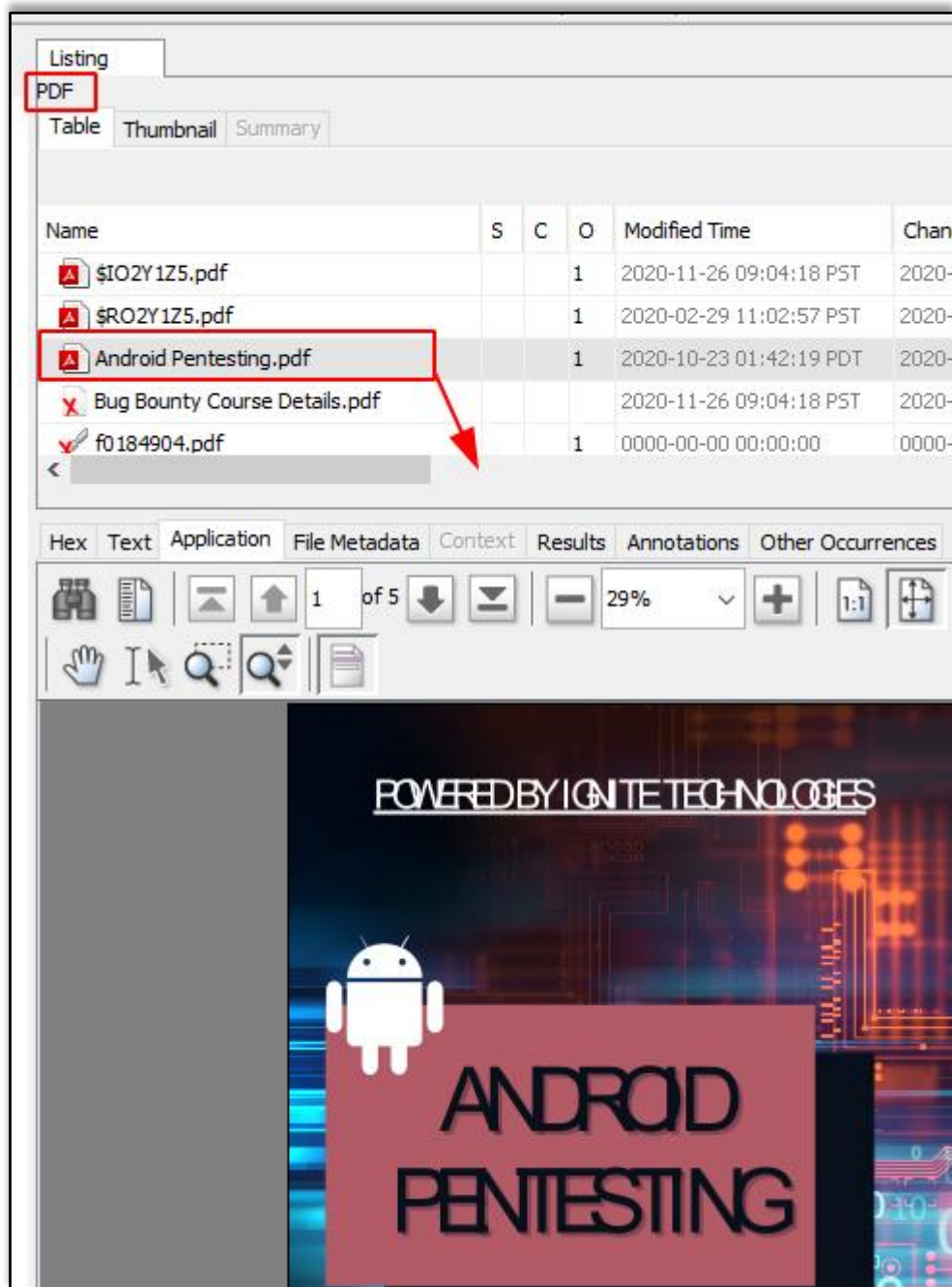


## Documents

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



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



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

The screenshot shows a file explorer interface with a left sidebar containing various file types and a main pane displaying a list of files. A red box highlights the 'Plain Text (1196)' category in the sidebar, and a red arrow points to the selected file '\$RK1MRRO.txt' in the main pane. The main pane also shows a detailed view of the selected file, including its name, size, and modified time, as well as a preview of the file's content.

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

Hex Text Application File Metadata Context Results An

Strings Indexed Text Translation

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

```

NOTICE: The imaging operation was cancelled!

Created By AccessData® FTK® Imager 4.3.1.1

Case Information:
Acquired using: ADI4.3.1.1
Case Number: 001
Evidence Number: AU001
Unique description: Hacking Articles
Examiner: Vishva
Notes:

-----

Information for E:\Ignite:

Physical Evidentiary Item (Source) Information
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 125,821,080
[Physical Drive Information]
Removable drive: False
Source data size: 61436 MB
Sector count: 125821080
  
```

## Executables

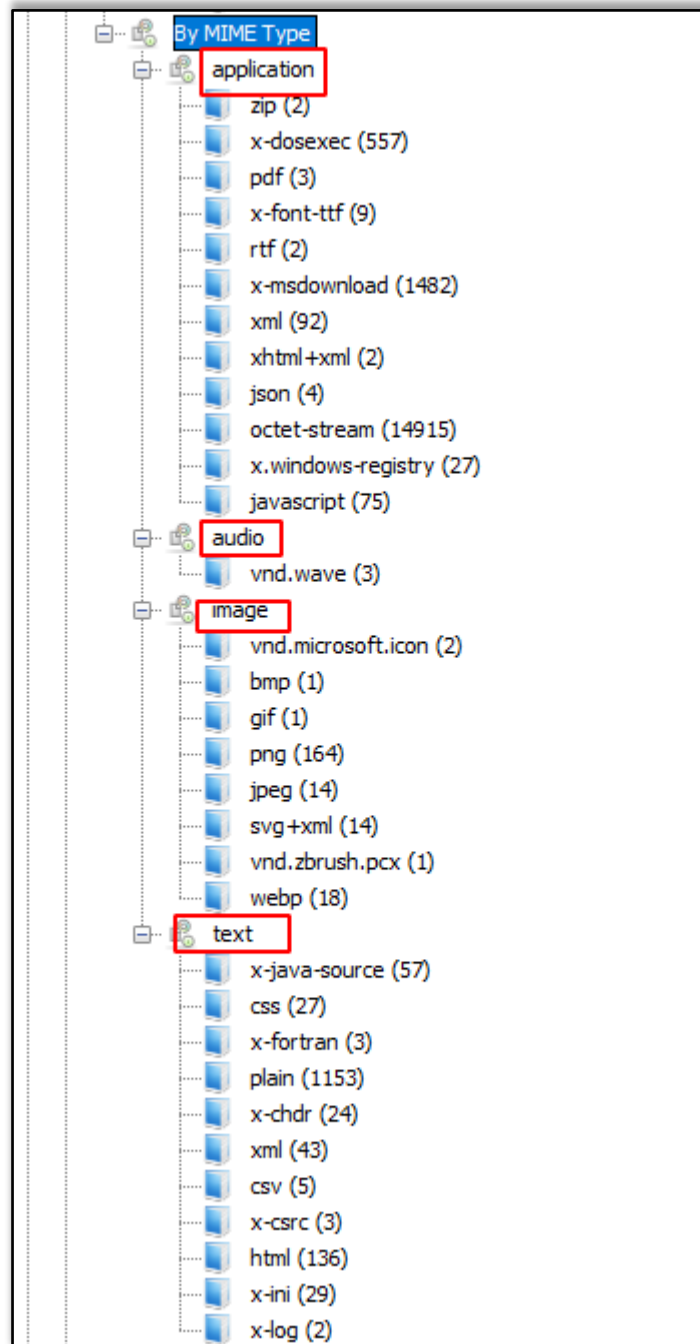
These file types are then sub-divided into .exe, .dll, .bat, .cmd and .com.

The screenshot shows a file explorer interface with a sidebar on the left and a main pane on the right. The sidebar is organized into 'Data Sources', 'Views', and 'File Types'. Under 'File Types', there is a 'By Extension' section with various categories like Images, Videos, Audio, Archives, Databases, and Documents. A red box highlights the 'Executable' category in the sidebar, and a red arrow points from it to a table in the main pane. The table, titled 'Executable', has two columns: 'File Type' and 'File Extensions'. It lists five file types: .exe (639), .dll (1312), .bat (0), .cmd (0), and .com (0). Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', and 'Con'.

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

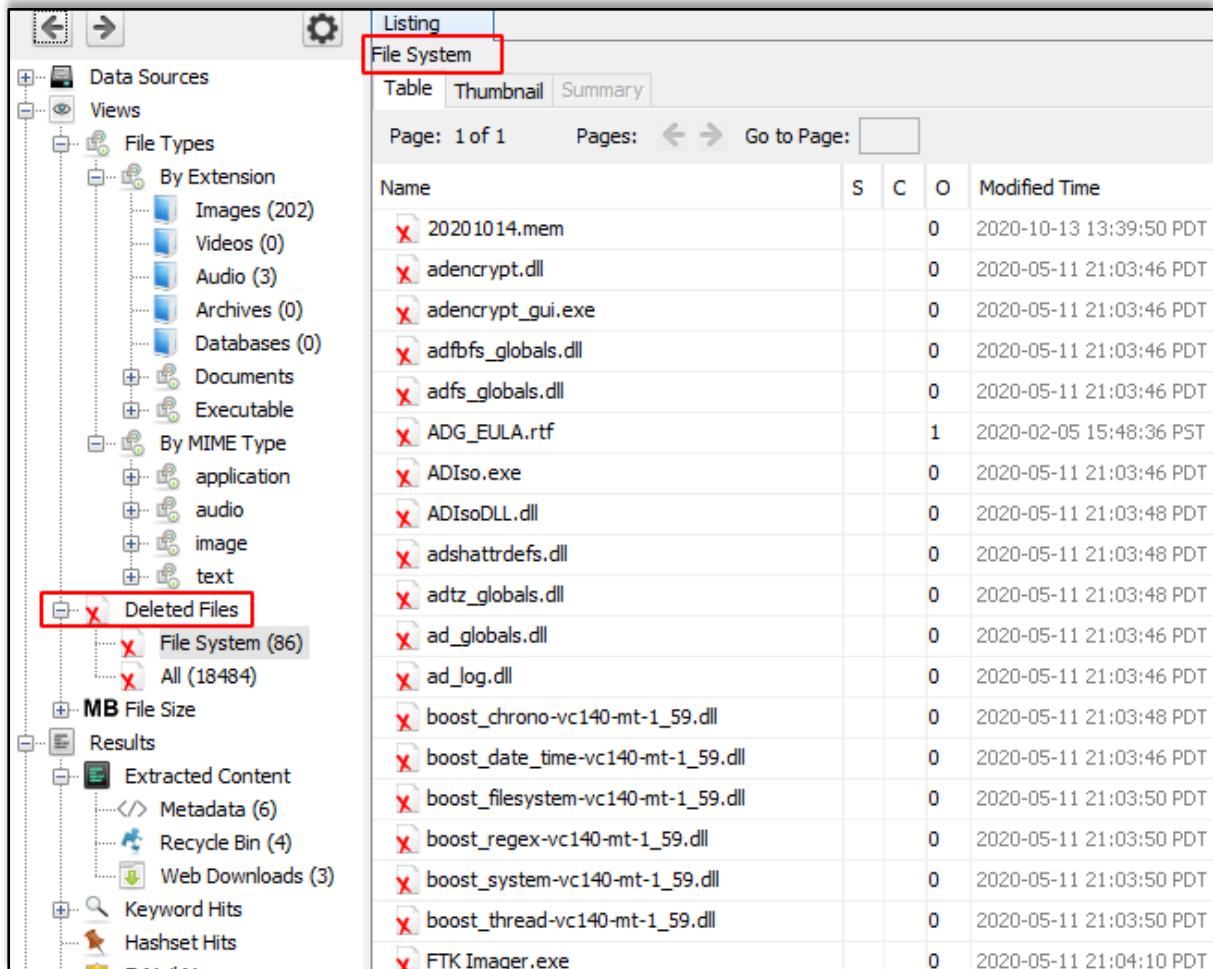
## By Mime Type

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.



## Deleted Files

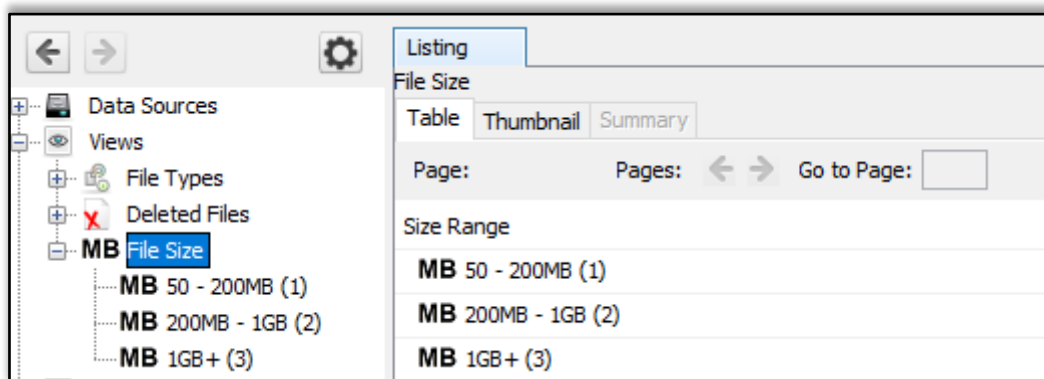
It displays information about the deleted file which can be then recovered.



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
<b>MB 50 - 200MB (1)</b>
<b>MB 200MB - 1GB (2)</b>
<b>MB 1GB+ (3)</b>

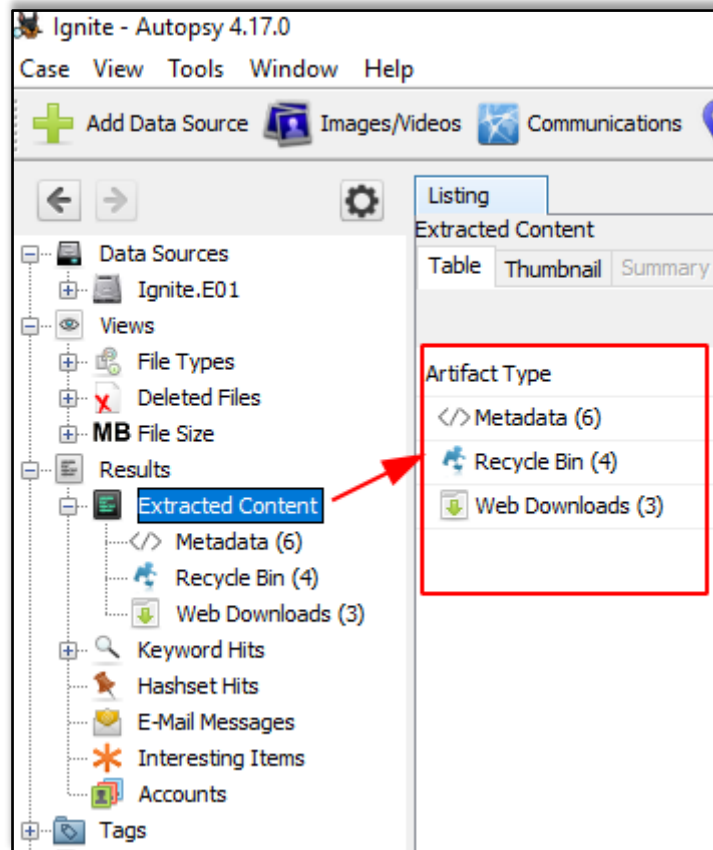


## Results

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.



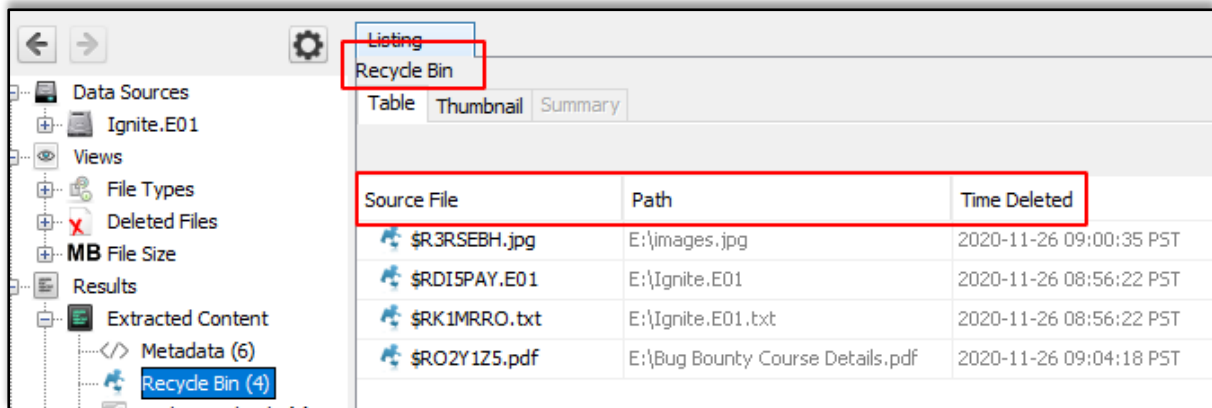
### Metadata

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

## Recycle Bin

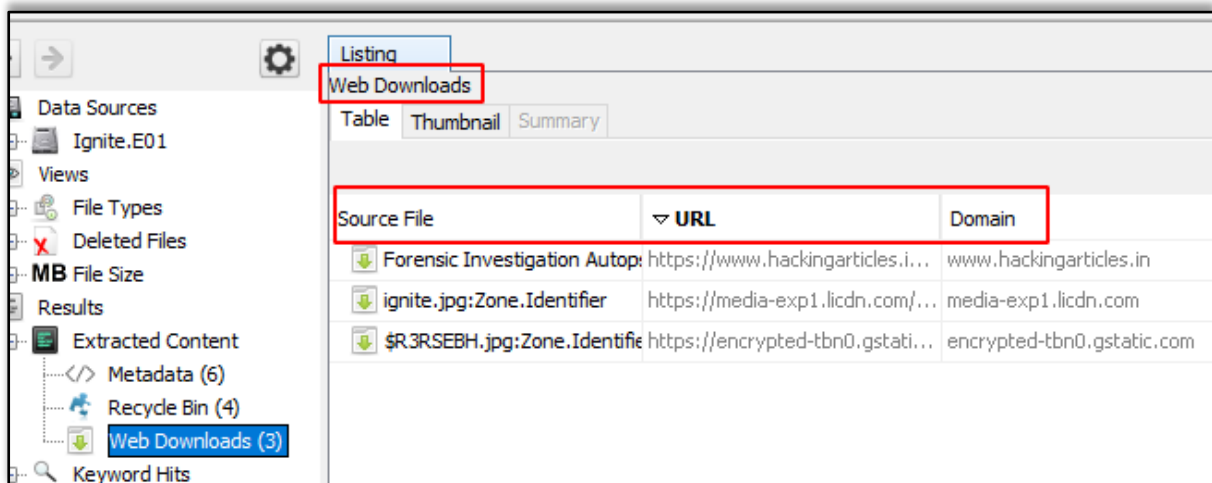
The files that were put in the recycle bin are found in this category.



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

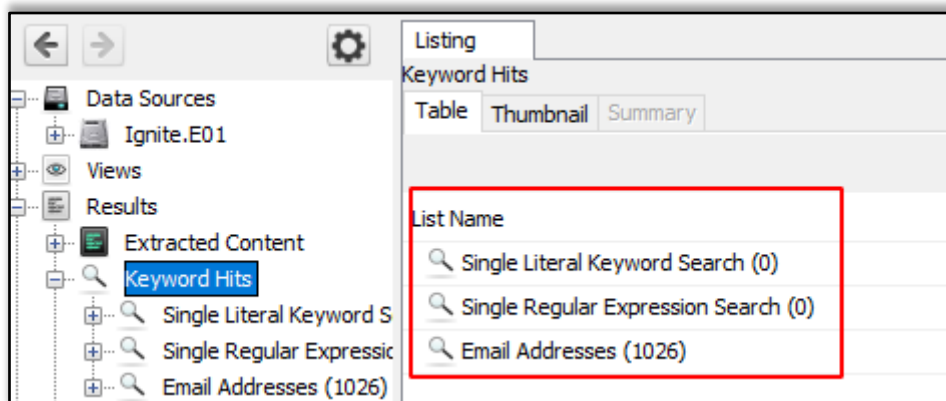
Here you can see the files that were downloaded from the internet.



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.

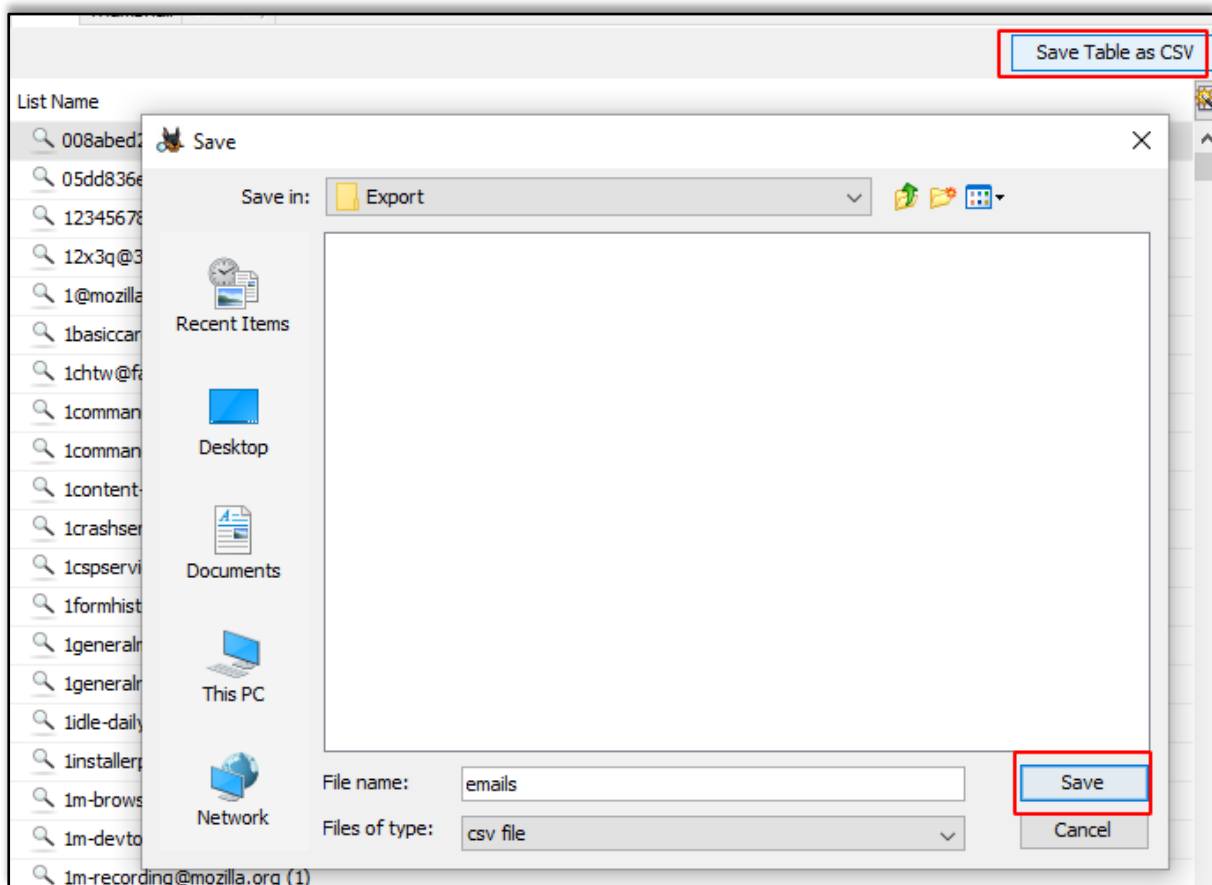


List Name	Count
Single Literal Keyword Search	(0)
Single Regular Expression Search	(0)
Email Addresses	(1026)

You can view the available email addresses.

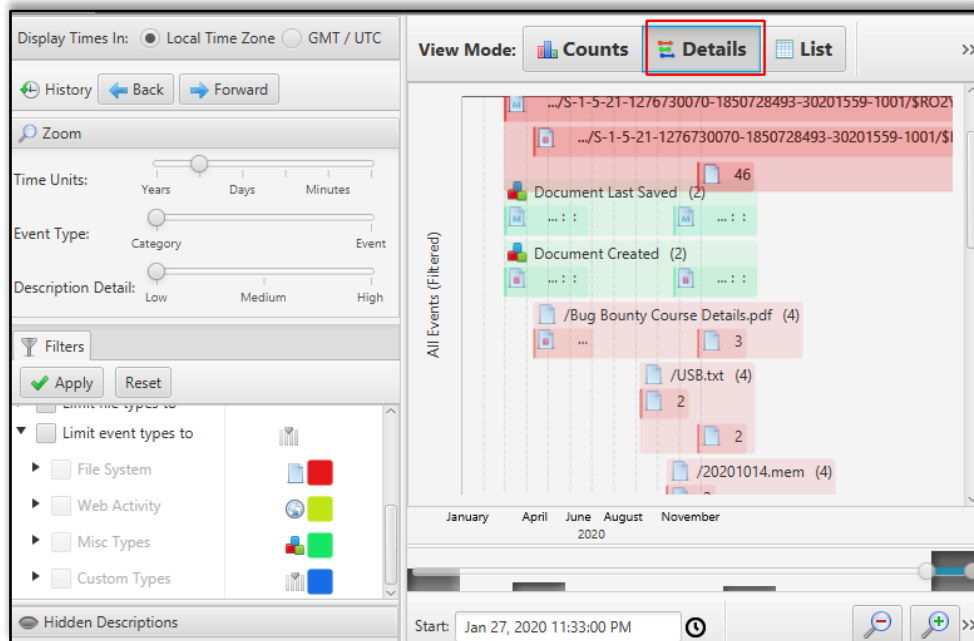
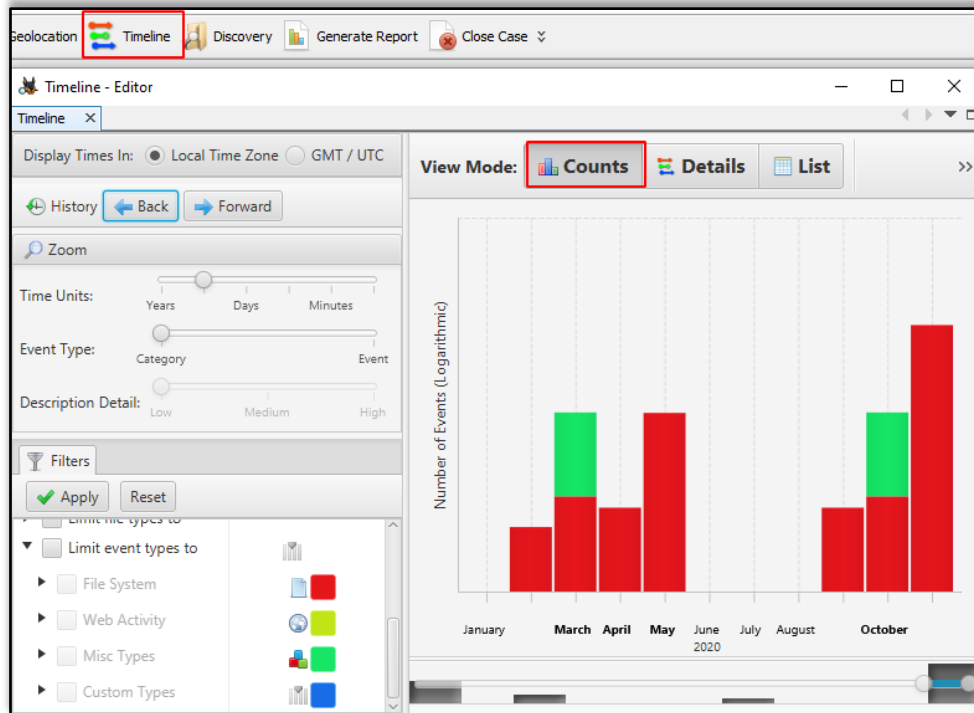
WS	List Name
sults	
Extracted Content	
Keyword Hits	
Single Literal Keyword Search (0)	addons@mozilla.org (1)
Single Regular Expression Search (0)	admin@vietbacsecurity.com (1)
Single Regular Expression Search (0)	admin@youtubeplayer.com (1)
Single Regular Expression Search (0)	admin@youtubespeedup.com (1)
Single Regular Expression Search (0)	adobe@flash.com (1)
Hashset Hits	adservices@accessdata.com (2)
E-Mail Messages	adsremoval@adsremoval.net (1)
Interesting Items	advance@windowsdient.com (1)
Accounts	af-za@dictionaries.addons.mozilla.org (1)
gs	
ports	

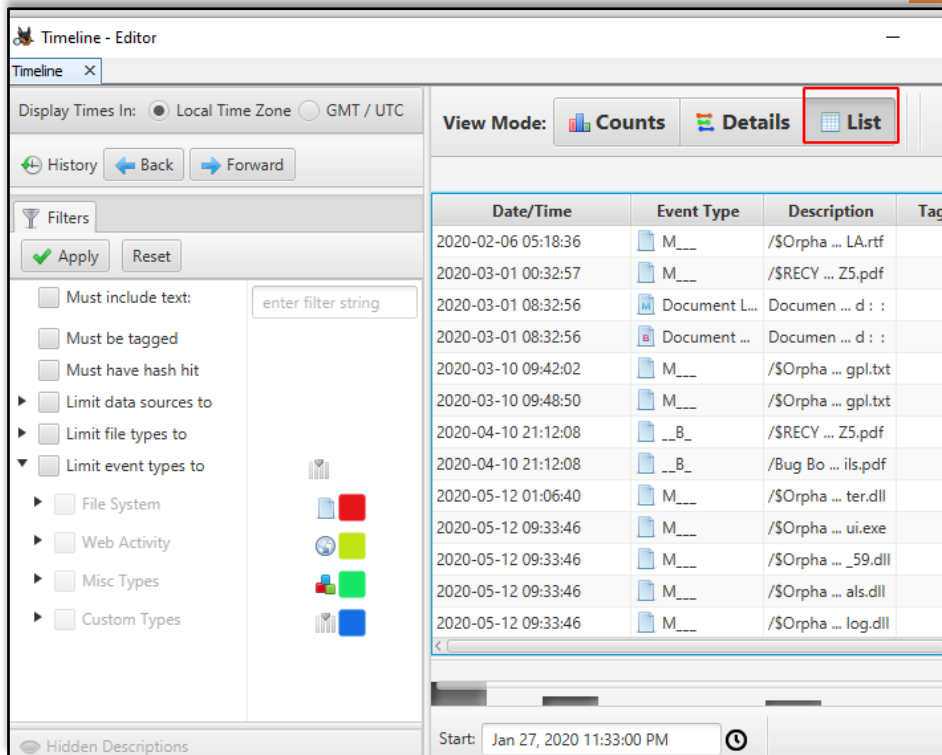
You can choose to export into a CSV format.



# Timeline

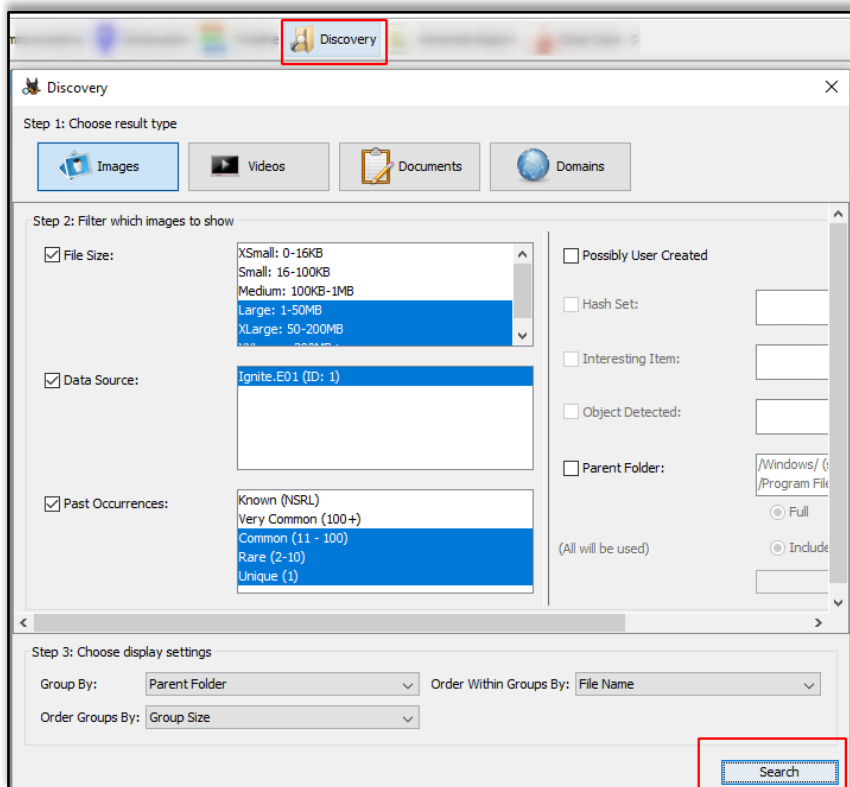
By using this feature, you can get information on the usage of the system in a statistical, detailed, or list form.



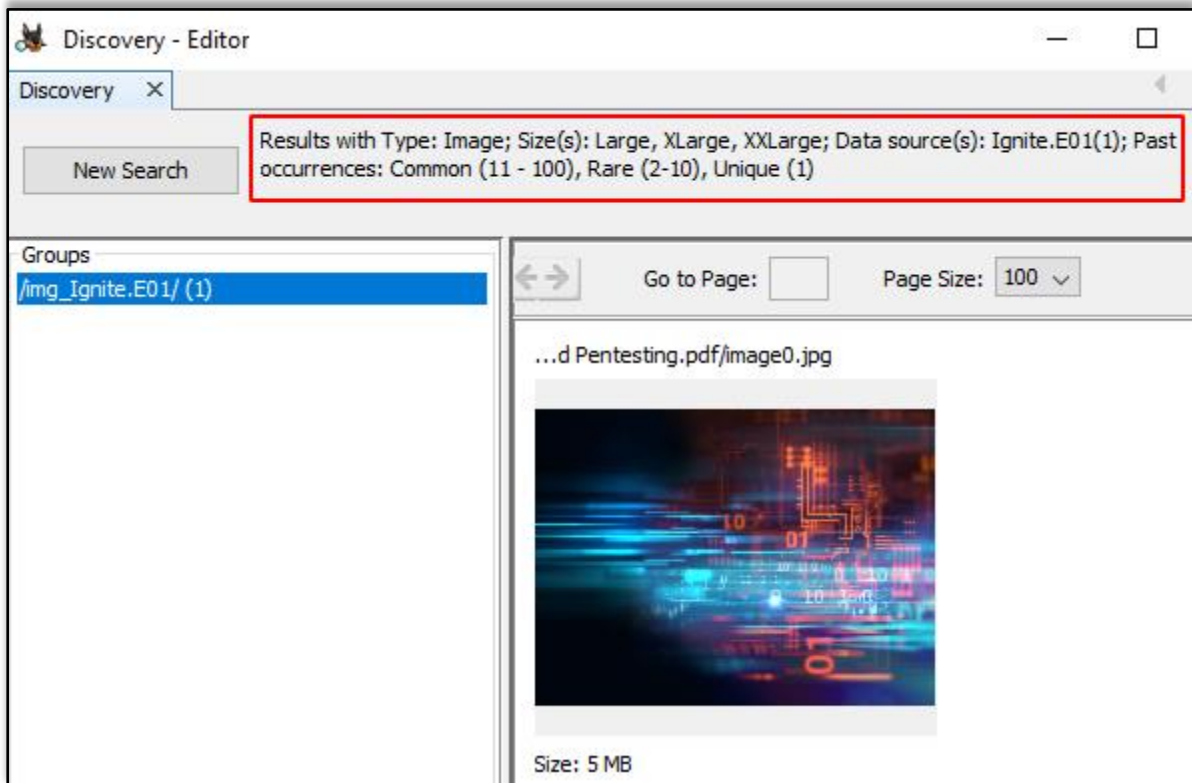


## Discovery

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

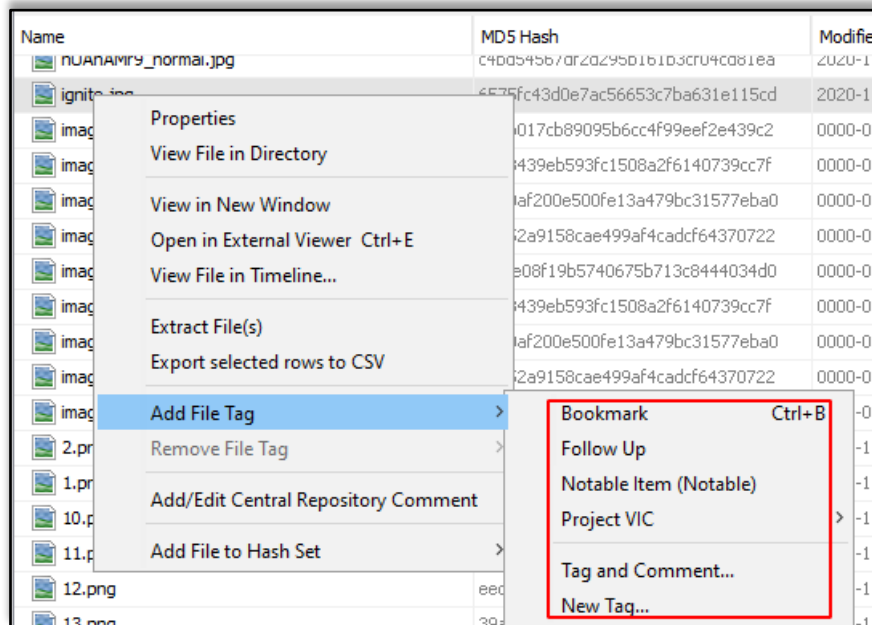
This option is to find images and videos through various options and multiple categories

The screenshot shows the Ignite - Autopsy 4.17.0 interface. The 'Image/Video Gallery - Editor' window is open, displaying a file tree on the left and a gallery of images on the right. The 'Images/Videos' tab is selected in the top navigation bar. The file tree shows a folder named 'img\_Ignite.E01 (2)' containing several sub-folders and files. The 'Mozilla Firefox' folder is highlighted. The gallery on the right shows two images: one with a large 'HA' logo and another with the text 'PASSWORD DUMPING'.

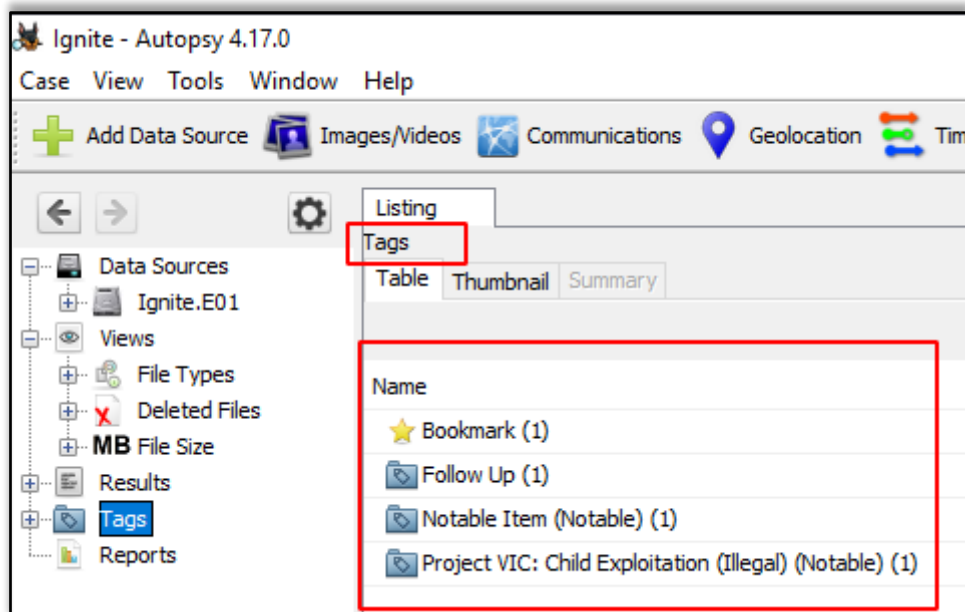
Category	# Files
Child Exploitation (Illegal)	0
Child Exploitation (Non-Ille...	0
CGI/Animation (Child Exploi...	0
Exemplar/Comparison (Inter...	0
Non-pertinent	0

## Add File Tag

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



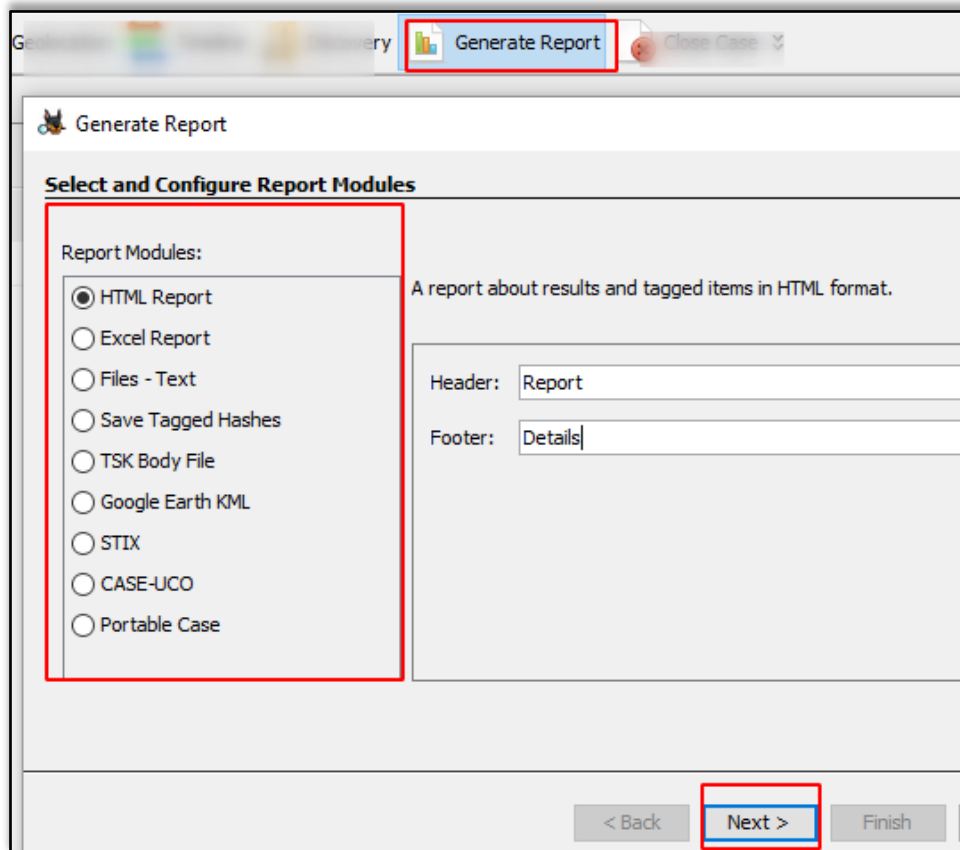
Now when you see the tags options, you will see that files were tagged according to various categories.



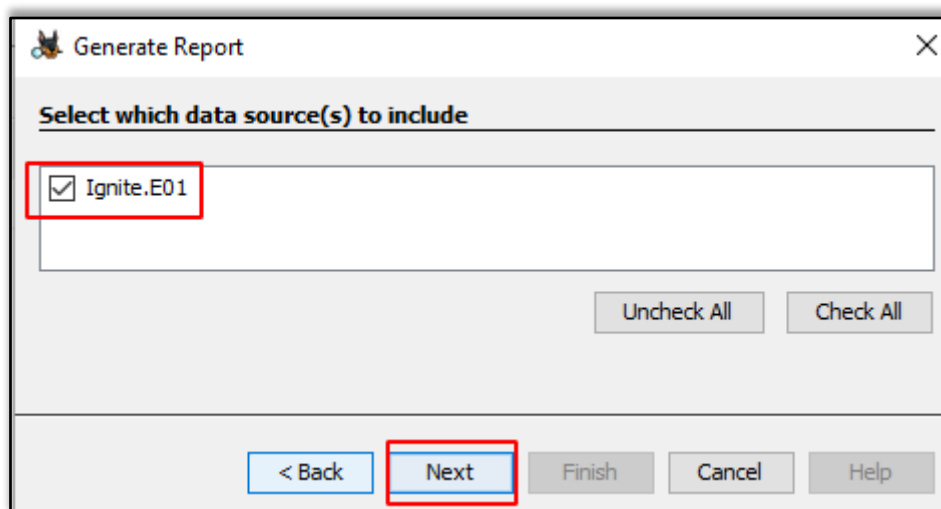


## Generate Report


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




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/>