Digital Evidence Handling Using Autopsy

Nisarg Trivedi[1], Dhruv Patel[2]

[1]Institute of Forensic Science, Gujarat Forensic Sciences University, India

[2]Institute of Forensic Science, Gujarat Forensic Sciences University, India

Abstract: *The Autopsy Forensics Browser is a graphical interface to The Sleuth Kit (TASK). Autopsy is a free and open Source Windows-based digital forensics platform for diagnose an event. It is capable of analysing disk images, local drives and directories in order to determine possible causes of an event in a read-only environment. It was designed to be an extensible platform so that it can be an end-to-end digital forensics solution that incorporates plug-in modules from both open and closed source projects. This paper represents the process of installation of Autopsy 3.1.1, ingestion of data, analysing of data and features of the current version of software.*

Keywords: *Digital Investigation, Meta data, Open Source, Report Generation, Timeline Analysis*

I.INTRODUCTION

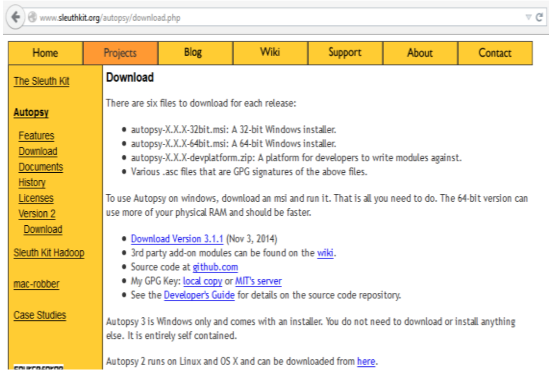
Autopsy is open source digital forensic software which supports NTFS, FAT, Ext2/3/4, HFS/HFS+ and UFS file system types, enabling you to investigate from the input (Image files, local disks or logical files). [1] Autopsy is a user interface that makes it simpler to bring it to use many of the open source programs and plugins used in the Sleuth Kit collection. [2]

Autopsy uses wizards to help the investigator know what the next step is. It uses navigation techniques to help them find their results, and tries to automate as much as possible to reduce errors.[3]Autopsy provides an intuitive workflow for users in the Law Enforcement , Military, Intelligence Agencies , Cyber security and Incident Response communities.[4]

This paper is for users with above average computer skills who have a basic understanding of digital forensics concepts. This paper reflects the installation process of Autopsy 3.1.1 (Released 3rdNovember, 2014[5]). It includes how to use the Autopsy Forensic Browser and process of analysing data as well as timeline analysis and report generation. It also focuses on the features and advantages of current version.

II. DOWNLOAD AND INSTALLATION

Autopsy can be downloaded from the official website [5][6].



Download

There are six files to download for each release:

- autopsy-X.X.X-32bit.msi: A 32-bit Windows installer.
- autopsy-X.X.X-64bit.msi: A 64-bit Windows installer.
- autopsy-X.X.X-devplatform.zip: A platform for developers to write modules against.
- Various .asc files that are GPG signatures of the above files.

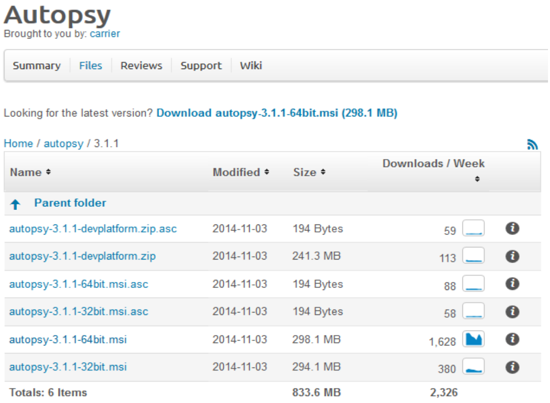
To use Autopsy on windows, download an msi and run it. That is all you need to do. The 64-bit version can use more of your physical RAM and should be faster.

- Download Version 3.1.1 (Nov 3, 2014)
- 3rd party add-on modules can be found on the wiki.
- Source code at github.com
- My GPG Key: local copy or MIT's server
- See the Developer's Guide for details on the source code repository.

Autopsy 3 is Windows only and comes with an installer. You do not need to download or install anything else. It is entirely self contained.

Autopsy 2 runs on Linux and OS X and can be downloaded from here.

Fig.1 Download page for Autopsy 3.1.1



Looking for the latest version? **Download autopsy-3.1.1-64bit.msi (298.1 MB)**

Name	Modified	Size	Downloads / Week
Parent folder			
autopsy-3.1.1-devplatform.zip.asc	2014-11-03	194 Bytes	59
autopsy-3.1.1-devplatform.zip	2014-11-03	241.3 MB	113
autopsy-3.1.1-64bit.msi.asc	2014-11-03	194 Bytes	88
autopsy-3.1.1-32bit.msi.asc	2014-11-03	194 Bytes	58
autopsy-3.1.1-64bit.msi	2014-11-03	298.1 MB	1,628
autopsy-3.1.1-32bit.msi	2014-11-03	294.1 MB	380
Totals: 6 Items		833.6 MB	2,326

Fig.2 Download Latest Version

After downloading the setup file user has to install the software by double clicking on it. Next→Next→Install→Finish. Installation of this software is simple because you have to just click on the next button, give path for destination folder and finish the installation process. Here note that Administrative privileges are needed, so you must be logon as Administrator. After finishing the

Installation process it will create an icon on desktop as shown in figure.

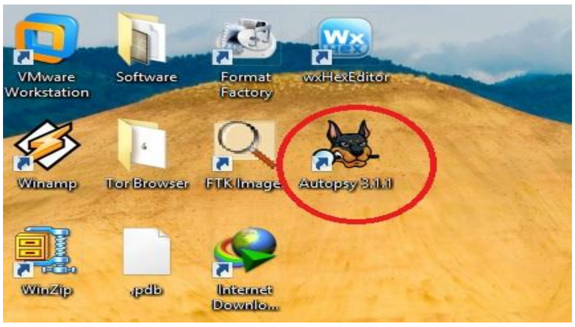


Fig.3 Autopsy 3.1.1 Icon

On double clicking Icon it will open window as shown below which is agraphical interface to the Sleuth Kit. [7][8]

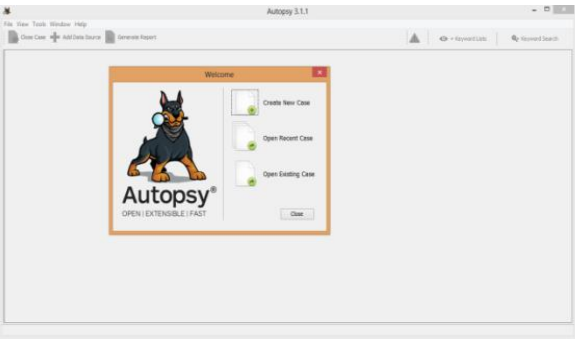
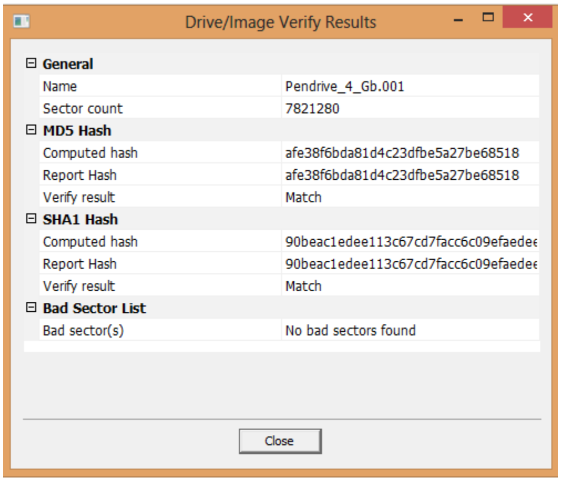


Fig.4 Opening screen of Autopsy

There are mainly three options available. 1. Create New Case, 2.Open Recent Case and 3.Open Existing Case.To start fresh case select first option. If you want to open previous/recent case then choose second option. Any available case in the hard drive or directory folder can be access using third option.

III. IMAGING AND INGESTION PROCESS

In this case we have created an Image of 4 Gb SanDisk Pen driveusing FTK Imager. We can create image by using this software for free.


Drive/Image Verify Results

General	
Name	Pendrive_4_Gb.001
Sector count	7821280
MD5 Hash	
Computed hash	afe38f6bda81d4c23dfbe5a27be68518
Report Hash	afe38f6bda81d4c23dfbe5a27be68518
Verify result	Match
SHA1 Hash	
Computed hash	90beac1edee113c67cd7facc6c09efaedee
Report Hash	90beac1edee113c67cd7facc6c09efaedee
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Fig.5 Image Property of Pen drive

Image shows that there is no bad sector in Pen drive. Here the file is created with ".001" extension and one report is also generated. Now this file will be added to Autopsy for analysis. Note that in Digital Forensic world direct action cannot be taken on original digital evidence. First of all one bit-by-bit forensic copy of the evidence hasbeen generated and necessary work done on it.

Now this Image is ingested in Autopsy and analysed. Step by step solution is given with appropriate screenshots. [9]

Step 1:-

First of all click on create a new case because we have a fresh case to work on.

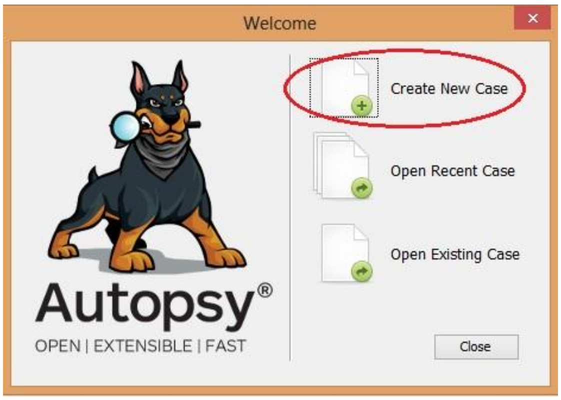
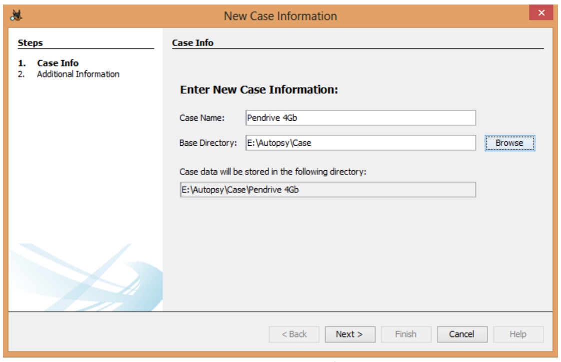


Fig.6 First window in Autopsy

Step 2:-

Enter the name of case and select the base directory of your case where the case data will be store.In below picture we entered case name "Pendrive 4Gb" and select base directory as E:\Autopsy\Case to store the case data Then click on next. One folder will be generated.


New Case Information

Steps
1. Case Info
2. Additional Information

Case Info

Enter New Case Information:

Case Name: Pendrive 4Gb

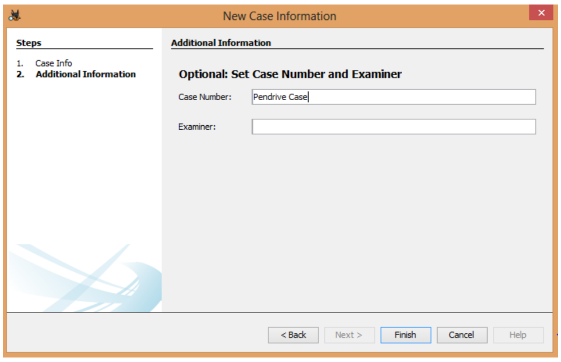
Base Directory: E:\Autopsy\Case

Case data will be stored in the following directory:
E:\Autopsy\Case\Pendrive 4Gb

Fig.7 New Case Information

Step 3:-

Enter Case number and Examiner name. Type the name of the person conducting the investigation and responsible for analysis.


New Case Information

Steps
1. Case Info
2. Additional Information

Additional Information

Optional: Set Case Number and Examiner

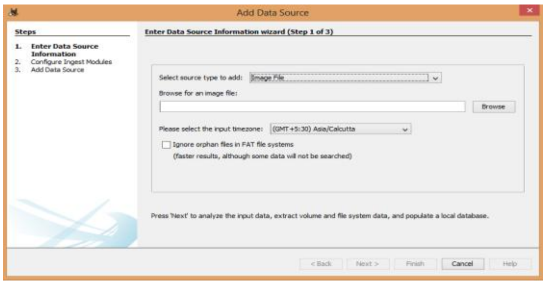
Case Number: Pendrive Case

Examiner:

Fig.8Additional Information

Step 4:-

After then it will open the “Enter Data Source Information” wizard.Select source type to add. You can add image file,local disk,and logical file. In our case we will add image file in autopsy. Now click on browse button to select your source file. Note that you can also change time stamp as per your case requirement.


Add Data Source

Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add: Image File

Browse for an image file:

Please select the input timezone: (GMT+5:30) Asia/Calcutta

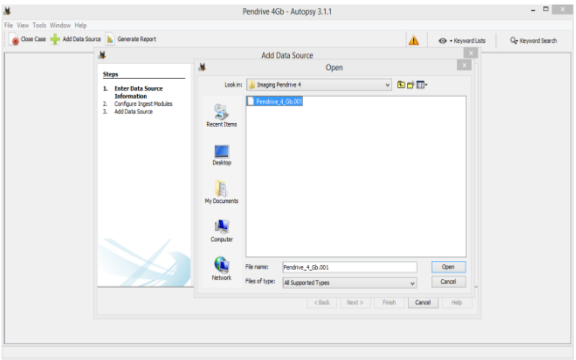
☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

Fig.9 Add Data Source Information

Step 5:-

After click on browse button select the location of the image file/case file. Select the image file and click on Open. Then click next to configure Ingest Module.


Pendrive 4Gb - Autopsy 3.1.1

Add Data Source

Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

Open

Look in: Imaging Pendrive 4

Pendrive_4_Gb.001

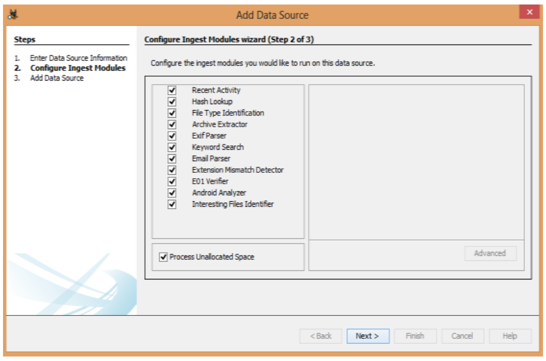
File name: Pendrive_4_Gb.001

Files of type: All Supported Types

Fig.10Import Case Data File

Step 6:-

In this wizard you can configure recent activity, hash lookup, file type identification, Exif parser and other modules as per case requirement. Here we select all the boxes. If you checked the last box then it will process Unallocated Space too.


Add Data Source

Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

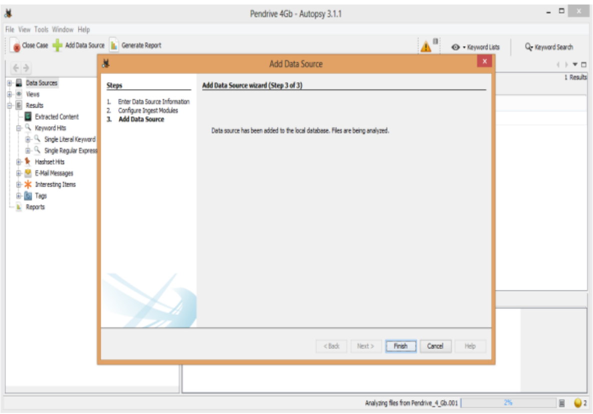
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Archive Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier

☑ Process Unallocated Space

Fig.11 Configure Ingest Modules

Step 7:-

After Click on next button it will open the Add data source wizard. This is the last wizard window. As you can see analysing process is already started in the background. Then click on finish button.



Steps

1. Enter Data Source Information
2. Configure Ingest Modules
3. **Add Data Source**

Add Data Source wizard (Step 3 of 3)

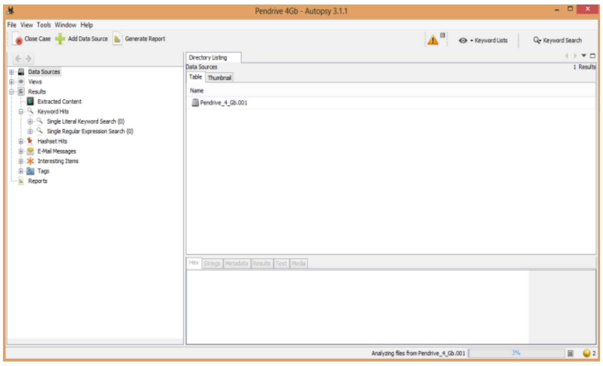
Data source has been added to the local database. Files are being analyzed.

Analyzing files from Pendrive_4_Gb.001 2%

Fig.12Add Data Source Wizard

Step 8:-

Here, main screen is separated in three windows. They are Data Explorer, Content Viewerand Result Viewer. Analysing of the file process is still running at the bottom right corner of the window.

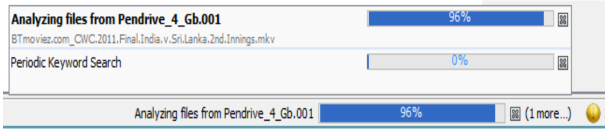


Analyzing files from Pendrive_4_Gb.001

Fig.13Load Data Source File

IV. Analysis

Analysing your file may take time. It depends on the size of the input evidence. Large file takes long time for analysing. You can monitor analysis process. There are mainly two kind of analysis. i) Dead Analysis and ii) Live Analysis. [15][17][22]



Analyzing files from Pendrive_4_Gb.001 96%

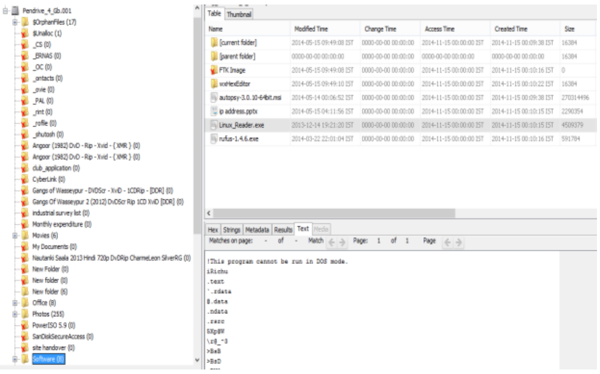
BTmoviez.com_CWC.2011.Final.India.v.Sri.Lanka.2nd.Innings.mkv

Periodic Keyword Search 0%

Analyzing files from Pendrive_4_Gb.001 96% (1 more...)

Fig.14Analysing Data Source File

After analysisprocess completes, all the data available in left panel/Data Explorer viewer. List of folder is shown. In upper right corner/Result viewer files from the selected folder is listed. If we select particular file from result viewer then it will show properties like Hex, Strings, Result, Textand Metadata in Content viewer.



Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2014-05-15 09:49:08 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:09:38 IST	16384
[parent folder]	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384
FTK Image	2014-05-15 09:49:08 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:10:16 IST	0
wxHexEditor	2014-05-15 09:49:10 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:10:22 IST	16384
autopsy-3.0.10-64bit.msi	2014-05-14 00:06:52 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:09:38 IST	270314496
ip address.pptx	2014-05-15 04:11:56 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:10:15 IST	2290354
Linux_Reader.exe	2013-12-14 19:21:20 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:10:15 IST	4509379
rufus-1.4.6.exe	2014-03-22 22:01:04 IST	0000-00-00 00:00:00	2014-11-15 00:00:00 IST	2014-11-15 00:10:16 IST	591784

Matches on page: - of - Match Page: 1 of 1 Page

```
!This program cannot be run in DOS mode.
iRichu
.text
`.rdata
@.data
.ndata
.rsrc
6Xp@W
\r@_~3
>BsB
>BsD
```

Fig.15 Extracted Data from Source File

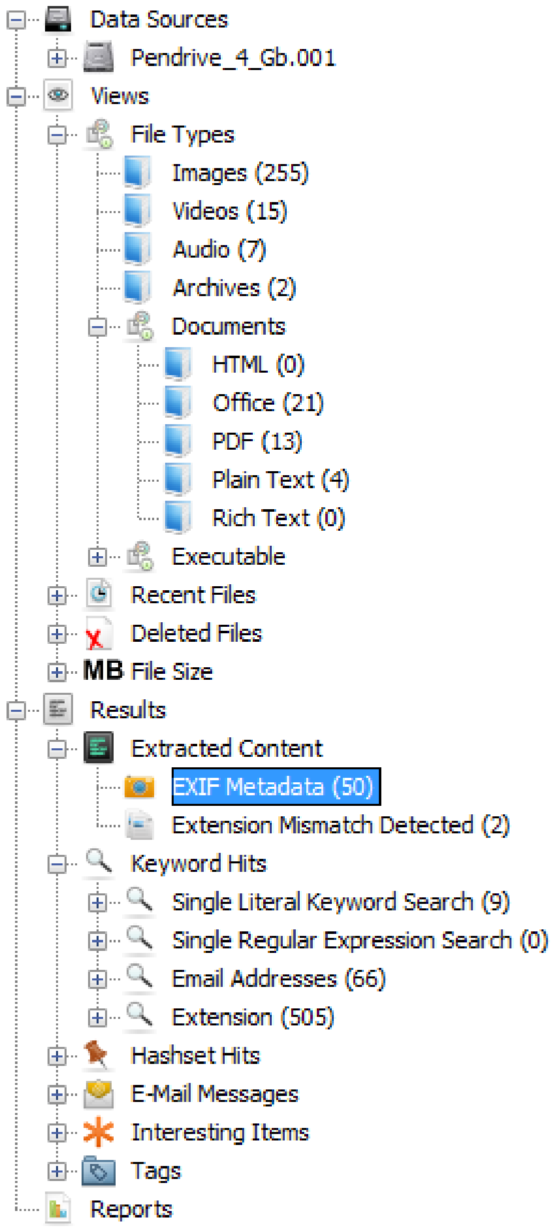


Fig.16 Single Place for All Results

This window is located at the left corner/Data Explorer viewer. [3] Main part of this window is Data Sources, Views, Results and Reports. “Data Sources” part includes details of image. Image includes listing of files and folders located on that drive of image. “Views” will classify the files with File Types, Recent Files, Deleted Files and File Size.[10][11] Next is “Results” which includes Extracted contain (it contains EXIF Metadata), Keywords Hits (modifiable), Hashes Hits, E-mail Messages, Interesting Items and Tags.And last one is “Reports”. In reports results and tagged itemsare written in table format.

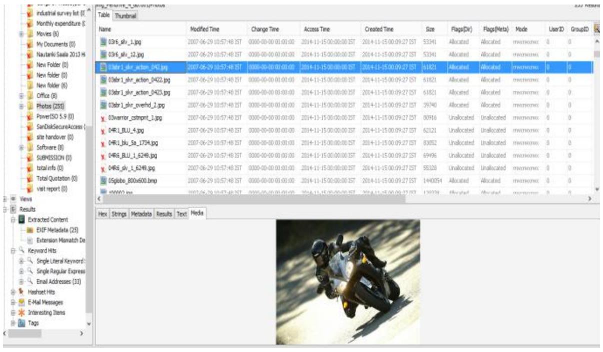


Fig.17Display All folders (Deleted also)

Click on photos folder and the content of data see in right side in table viewIn table view you can see modify time, change time, access time, created time, size , flag(dr), flag(meta) , user ID, group Id of all file.

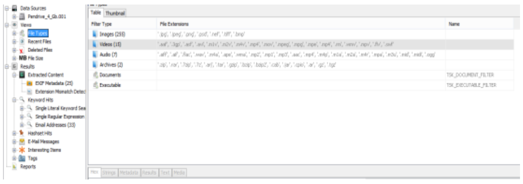


Fig.18Display All File Types

In data explorer region you can see all file type classification like images, video, audio, archives file in right panel as below picture

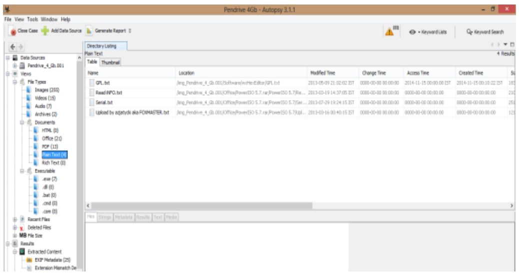


Fig.19Display Document folder

Data explorer region shows all document file like as (Html, office, pdf, plain text, rich text) in autopsy.

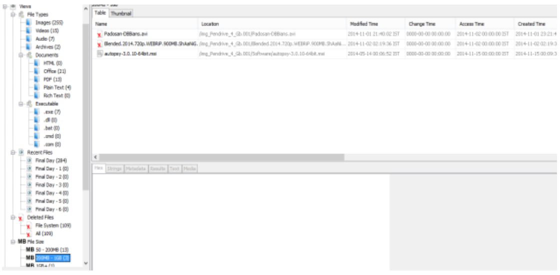


Fig.20Display Filesize

In Data Explorer viewer you can see executable file, recent file, deleted file and MB file size.

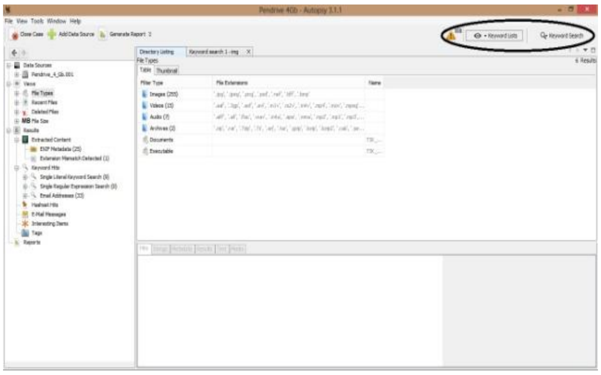


Fig.21Keyword Search Option

In autopsy you can search your own keywords. You can create your own keywords list.

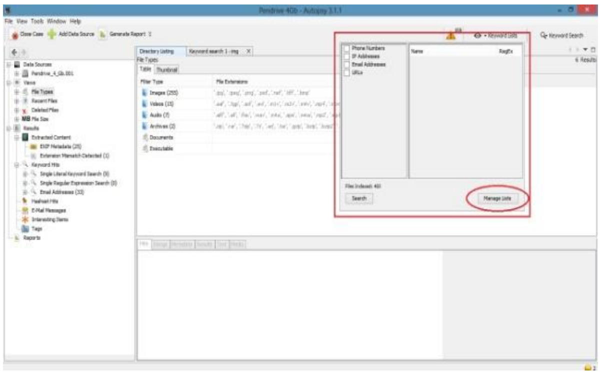


Fig.22Manage Keyword List

After click on keyword List open the popup window and click on Manage.

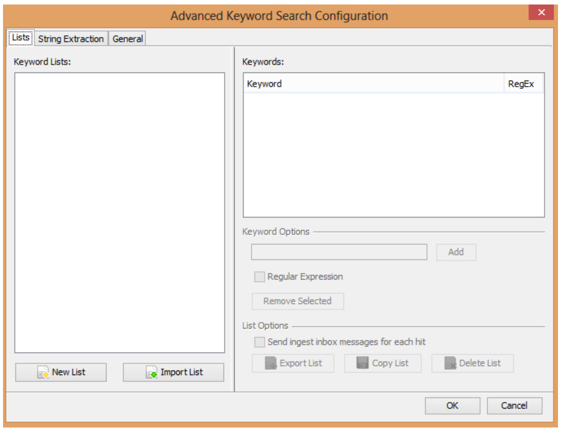


Fig.23 Configure Search Keyword

Open the advance keyword search configuration menu. Click on new list to create new keyword list. You can add multiple keywords in same list.Regular Expression can also be included.

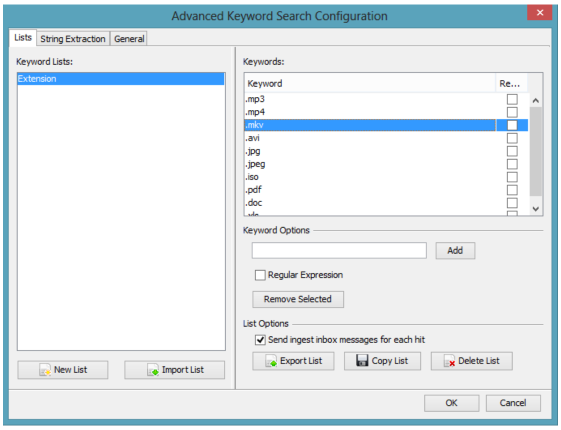


Fig.24 Add File Extension in keyword

In keyword option here we enter the file extension as per our requirement. Click add button to insert the keyword. In keywords select the check box and click on remove button to remove the keyword.Click on ok button after enter the keywords.

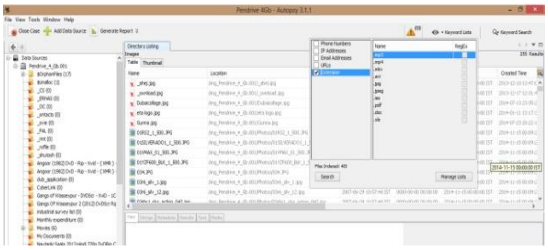
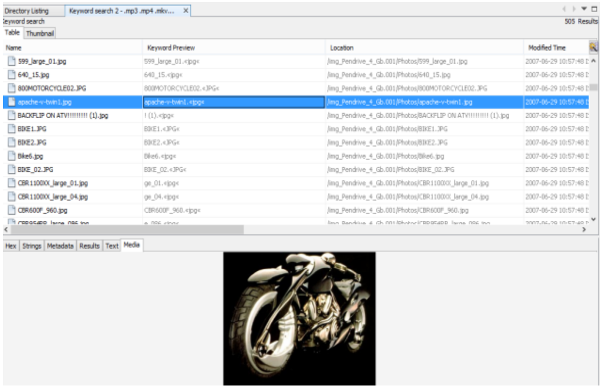


Fig.25 Search keyword

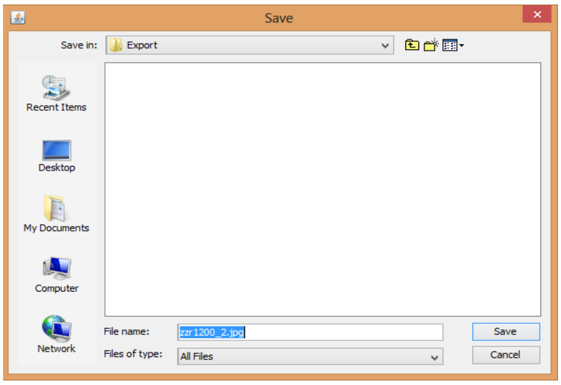
Select the checkbox from list then click on search button. If you add new keywords to the list, you need to restart ingest to perform the search.You can run ingest again by right clicking on case name from data sources.



Name	Keyword Preview	Location	Modified Time
599_large_01.jpg	599_large_01.«jpg«	/img_Pendrive_4_Gb.001/Photos/599_large_01.jpg	2007-06-29 10:57:48
640_15.jpg	640_15.«jpg«	/img_Pendrive_4_Gb.001/Photos/640_15.jpg	2007-06-29 10:57:48
800MOTORCYCLE02.JPG	800MOTORCYCLE02.«JPG«	/img_Pendrive_4_Gb.001/Photos/800MOTORCYCLE02.JPG	2007-06-29 10:57:48
apache-v-twin1.jpg	apache-v-twin1.«jpg«	/img_Pendrive_4_Gb.001/Photos/apache-v-twin1.jpg	2007-06-29 10:57:48
BACKFLIP ON ATV!!!!!!!!!! (1).jpg	! (1).«jpg«	/img_Pendrive_4_Gb.001/Photos/BACKFLIP ON ATV!!!!!!!!!! (1).jpg	2007-06-29 10:57:48
BIKE1.JPG	BIKE1.«JPG«	/img_Pendrive_4_Gb.001/Photos/BIKE1.JPG	2007-06-29 10:57:48
BIKE2.JPG	BIKE2.«JPG«	/img_Pendrive_4_Gb.001/Photos/BIKE2.JPG	2007-06-29 10:57:48
Bike6.jpg	Bike6.«jpg«	/img_Pendrive_4_Gb.001/Photos/Bike6.jpg	2007-06-29 10:57:48
BIKE_02.JPG	BIKE_02.«JPG«	/img_Pendrive_4_Gb.001/Photos/BIKE_02.JPG	2007-06-29 10:57:48
CBR1100XX_large_01.jpg	ge_01.«jpg«	/img_Pendrive_4_Gb.001/Photos/CBR1100XX_large_01.jpg	2007-06-29 10:57:48
CBR1100XX_large_04.jpg	ge_04.«jpg«	/img_Pendrive_4_Gb.001/Photos/CBR1100XX_large_04.jpg	2007-06-29 10:57:48
CBR600F_960.jpg	CBR600F_960.«jpg«	/img_Pendrive_4_Gb.001/Photos/CBR600F_960.jpg	2007-06-29 10:57:48

Fig.26 Analyse data using keyword

Export:-



File name: zzr1200_2.jpg

Files of type: All Files

Fig.27 Path for Exported File

Individual files can be exported into separate folder. By default Export folder will be created by Autopsy Software and your data will exported in that by default.

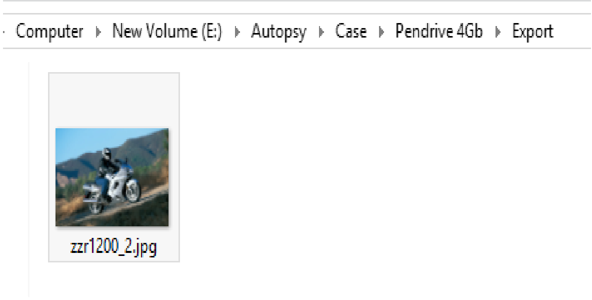
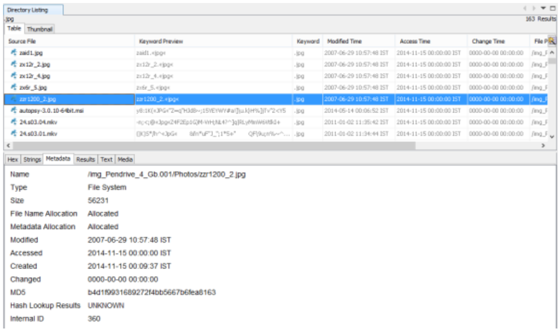

Computer ▸ New Volume (E:) ▸ Autopsy ▸ Case ▸ Pendrive 4Gb ▸ Export

Fig.28 File Exported in Folder

You can change file name. This way we can extract any file from image at any location.

Metadata:-



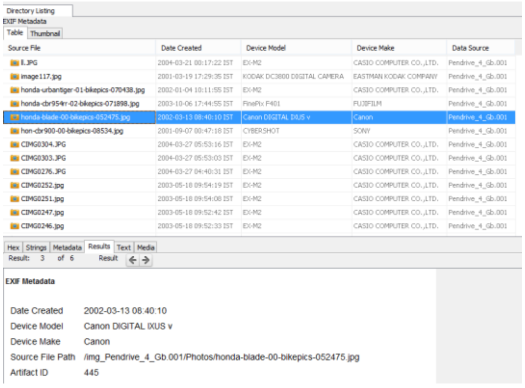
.jpg 163 Results

Source File	Keyword Preview	Keyword	Modified Time	Access Time	Change Time	File P
zaid1.jpg	zaid1.«jpg«	.jpg	2007-06-29 10:57:48 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
zx12r_2.jpg	zx12r_2.«jpg«	.jpg	2007-06-29 10:57:48 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
zx12r_4.jpg	zx12r_4.«jpg«	.jpg	2007-06-29 10:57:48 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
zx6r_5.jpg	zx6r_5.«jpg«	.jpg	2007-06-29 10:57:48 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
zzr1200_2.jpg	zzr1200_2.«jpg«	.jpg	2007-06-29 10:57:48 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
autopsy-3.0.10-64bit.msi	y8:1K(«JPG«"Z=q"H3dB~;15YEYWY#a{]}u.k|H%]}Tv"2<Y5	.jpg	2014-05-14 00:06:52 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
24.s03.04.mkv	-n;<;@«Jpg«Z4F2Ep1G)M-WH;NL4?^]q|RLyMmW6Wtkl2+	.jpg	2011-01-02 11:35:42 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F
24.s03.01.mkv	()K)S*/h^«JpG« 8/m*uF"J_";1*S+" QF(9u;n%~^...	.jpg	2011-01-02 11:34:44 IST	2014-11-15 00:00:00 IST	0000-00-00 00:00:00	/img_F

Name	/img_Pendrive_4_Gb.001/Photos/zzr1200_2.jpg
Type	File System
Size	56231
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2007-06-29 10:57:48 IST
Accessed	2014-11-15 00:00:00 IST
Created	2014-11-15 00:09:37 IST
Changed	0000-00-00 00:00:00
MD5	b4d1f9931689272f4bb5667b6fea8163
Hash Lookup Results	UNKNOWN
Internal ID	360

Fig.29 Metadata of Individual file

Analysis of Metadata can be done. It indicates File name, type, size. Created, modified and accessed date is shown as per the IST. It also indicates that whether the file name and Meta data allocated or not. MD5 hash value is also calculated. In deleted file, name and metadata is Unallocated. But still we are able to fetch timestamp (Created,Modified,and Accessed) of that file and MD5 value.



EXIF Metadata

Source File	Date Created	Device Model	Device Make	Data Source
ll.JPG	2004-03-21 00:17:22 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
image117.jpg	2001-03-19 17:29:35 IST	KODAK DC3800 DIGITAL CAMERA	EASTMAN KODAK COMPANY	Pendrive_4_Gb.001
honda-urbantiger-01-bikepics-070438.jpg	2002-01-04 10:11:55 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
honda-cbr954rr-02-bikepics-071898.jpg	2003-10-06 17:44:55 IST	FinePix F401	FUJIFILM	Pendrive_4_Gb.001
honda-blade-00-bikepics-052475.jpg	2002-03-13 08:40:10 IST	Canon DIGITAL IXUS v	Canon	Pendrive_4_Gb.001
hon-cbr900-00-bikepics-08534.jpg	2001-09-07 00:47:18 IST	CYBERSHOT	SONY	Pendrive_4_Gb.001
CIMG0304.JPG	2004-03-27 05:53:16 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0303.JPG	2004-03-27 05:53:03 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0276.JPG	2004-03-27 04:40:31 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0252.jpg	2003-05-18 09:54:19 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0251.jpg	2003-05-18 09:54:08 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0247.jpg	2003-05-18 09:52:42 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001
CIMG0246.jpg	2003-05-18 09:52:33 IST	EX-M2	CASIO COMPUTER CO.,LTD.	Pendrive_4_Gb.001

Result: 3 of 6 Result

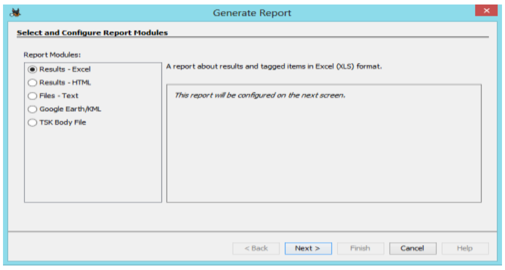
EXIF Metadata

Date Created	2002-03-13 08:40:10
Device Model	Canon DIGITAL IXUS v
Device Make	Canon
Source File Path	/img_Pendrive_4_Gb.001/Photos/honda-blade-00-bikepics-052475.jpg
Artifact ID	445

Fig.30Exif data of ".jpg" file

Exif Metadata property of the file is shown by Autopsy. Here, Exif property of ".jpg" is shown. [12] It shows the Device Model number and Device Make. This kind of Information is forensically important fromthe caseperspective for analyst.

Report:-



Select and Configure Report Modules

Report Modules:

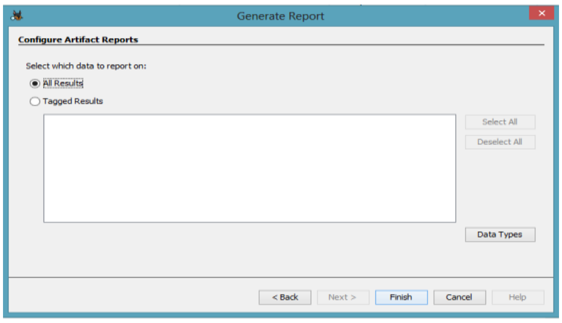
● Results - Excel
○ Results - HTML
○ Files - Text
○ Google Earth/KML
○ TSK Body File

A report about results and tagged items in Excel (XLS) format.

This report will be configured on the next screen.

Fig.31 Different format of Reports

After analysis of case you can create your overall investigation report. This report can begenerated in Excel, Html, Text or other format as your requirement. Select the format of report in left panel and click on next button.



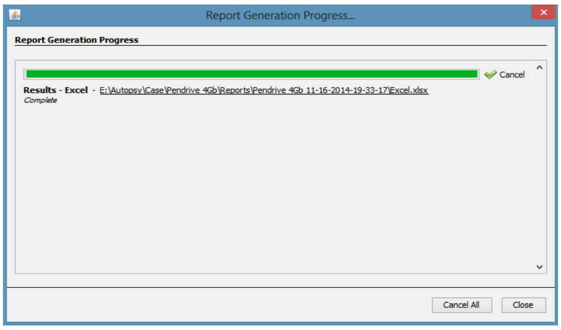
Configure Artifact Reports

Select which data to report on:

● All Results
○ Tagged Results

Fig.32 Configure Artifact report

In report generation you can generate all data result or tagged data result. Autopsy prefers reports generated in CSV format which can be accessed using Microsoft Excel.

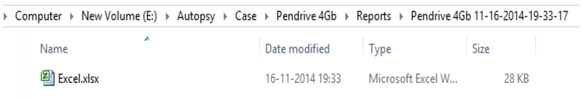


Report Generation Progress

Results - Excel - E:\Autopsy\Case\Pendrive 4Gb\Reports\Pendrive 4Gb 11-16-2014-19-33-17\Excel.xlsx
Complete

Fig.33 Report Generation Progress

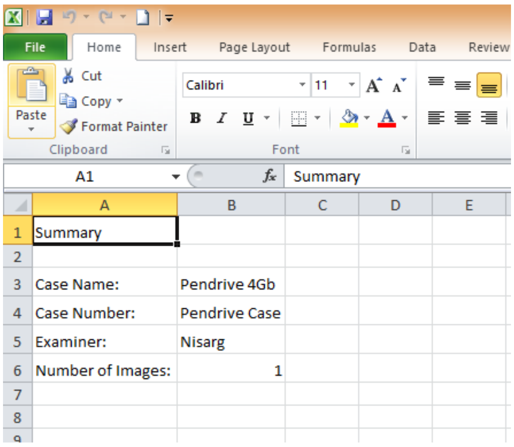
After click on finish button report generation process will start. In report generation process displays the path of report where the report is saved.


Computer ▸ New Volume (E:) ▸ Autopsy ▸ Case ▸ Pendrive 4Gb ▸ Reports ▸ Pendrive 4Gb 11-16-2014-19-33-17

Name	Date modified	Type	Size
Excel.xlsx	16-11-2014 19:33	Microsoft Excel W...	28 KB

Fig.34 Location of Generated Report

After completing the report generation click on result path to open the folder of case report. Here we generated report in CSV format.



A1 *fx* Summary

	A	B	C	D	E
1	Summary				
2					
3	Case Name:	Pendrive 4Gb			
4	Case Number:	Pendrive Case			
5	Examiner:	Nisarg			
6	Number of Images:	1			
7					
8					

Fig.35 Inside of Report

In report display the case name, case number, examiner of case. There is also one raw name “Number of Images”. When we add multiple images in case, numbers will be changed.

Timeline Analysis:-

There is one separated window opened by Autopsy for Timeline analysis. There are two “Visualization Mode”, i) Counts ii) Details

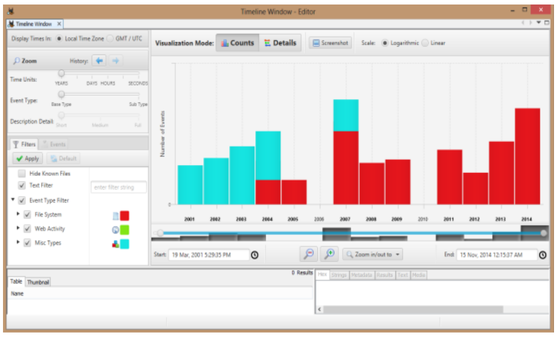


Fig.36 Counts Mode

Numbers of events are shown year by year. You can zoom in/out event. You can minimize the event to days, hours and seconds. There are two types of scale, i) Linear ii) Algorithmic

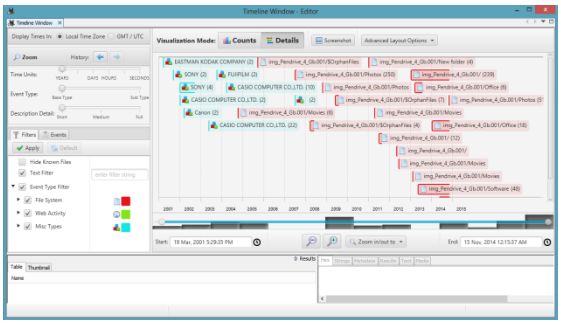


Fig.37 Details View

Number of File system events is shown in this window. Date and Time stamp is also given. We can also use advance layout option to filter data.

V. FEATURES AND ADVANTAGE

Autopsy 3 has been developed with the goal of providing an intuitive layout and simple workflow [11].

One of the main advantages of Autopsy is the implementation of the ingest method, which makes the analysis results available to the user as they are obtained, without waiting for the whole procedure to be completed first [12][11].

File system analysis and recovery which has support for NTFS, FAT, Ext2/3/4, UFS, HFS+.[11][16][18]

Web artifacts like cookie, history, downloads, bookmarksfrom web browsers like Firefox, IE, Chrome and Safari can be obtained. [12]

Some features were added to make sure Autopsy was easy to use for non-technical users also. Some of them are History, Previous Settings and Wizards.[2][3]

Logs are created at the user-level in Autopsy. [14]

Timeline Analysis,Keyword Search,Web Artifacts,Registry Analysis, LNK File Analysis, Analysis, EXIF, File Type Sorting, Thumbnail viewer, Hash Set Filtering, Tags, Unicode Strings Extraction, Unicode Strings Extraction etc.[19]

Autopsy can process disk images or directories to help you generate an event timeline. It assists you in putting the pieces together and determining what might have caused an incident to happen in the first place. Co-relation between events can be identified. [12]

Latest version includes time line feature, Added support for Python modules, Updated HTML report, new logo, etc. [20]

Some previous bugs are also fixed. Now it can extract ZIP files inside of RAR files properly. [20]

Multiple parallel pipelines for ingest, File extension mismatch detection via signatures, Android phone dump ingest module (which includes parses contacts, call logs, messages), PST email file parsing.[13] [21]

Autopsy has an extensible reporting infrastructure that allows additional types of reports for investigations to be created. By default, an HTML, XLS, and Body file report are available. [19][23]

You can extract the individual contents of the unallocated space using the same steps as extracting individual files, or you can extract the space to a single file to a separated folder.

Last but not the least it's free and easy to install, with Simple UI and Fast Result. [23][24]

VI. CONCLUSION

Digital devices can provide many different types of information that are not obvious to the casual user. The Autopsy Forensic Browser is open source software that will let you perform Security tasks. It's free for both personal and commercial use, thus the perfect choice for those that want an alternative for Security programs. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of the data.

Current version of Autopsy works better with good system configuration. Ingestion of large size of file can take long time. Timeline and Report functionality gives better understanding about the case.

REFERENCES

[1] http://www.softpedia.com/get/Others/Miscellaneous/Autopsy.shtml

[2] http://en.wikipedia.org/wiki/Autopsy_%28software%29

[3] http://www.sleuthkit.org/autopsy/intuitive.php

[4] http://www.basistech.com/basis-technology-enhances-digital-media-investigations-with-autopsy-3-1/

[5] http://www.sleuthkit.org/autopsy/download.php

[6] http://sourceforge.net/projects/autopsy/files/autopsy/3.1.1/

[7] http://wiki.sleuthkit.org/index.php?title=Main_Page

[8] http://wiki.sleuthkit.org/index.php?title=The_Sleuth_Kit

[9] http://digital-forensics.sans.org/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/

[10] Incident Response and Computer Forensics, Second Edition

[11] http://articles.forensicfocus.com/2013/08/29/autopsy-3-windows-based-easy-to-use-and-free/

[12] http://www.softpedia.com/get/Others/Miscellaneous/Autopsy.shtml

[13] http://www.basistech.com/medium-dive-medex/

[14] http://wiki.sleuthkit.org/index.php?title=Autopsy_3_Logging_and_Error_Checking

[15] http://www.sleuthkit.org/autopsy/v2/

[16] Digital Evidence & Computer Crime - Forensic Science, Computers, & the Internet, 2nd Edition

[17] File System Forensic Analysis by Brian Carrier

[18] Incident Response Computer Forensics Toolkit by Douglas Schweitzer

[19] http://www.sleuthkit.org/autopsy/features.php

[20] http://www.sleuthkit.org/autopsy/history.php

[21] http://www.basistech.com/digital-forensics/autopsy/

[22] The Official CHFI Exam 312-49 Study Guide

[23] https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Autopsy-3-Extensible-Open-Source-Forensics-Brian-Carrier.pdf

[24] http://juliakeffer.files.wordpress.com/2013/06/autopsy_user_guide.pdf

[25] http://www.basistech.com/digital-forensics/

[26] http://wiki.sleuthkit.org/index.php?title=Autopsy_Developer%27s_Guide

[27] www.atstake.com/research/tools/autopsy/

[28] http://wiki.sleuthkit.org/index.php?title=Autopsy:_Setting_Up_a_Case

[29] http://cyberforensics.et.byu.edu/wiki/Install_Sleuthkit

[30] http://the-autopsy-forensic-browser.soft112.com/