A Comparative Study of Analysis and Extraction of Digital Forensic Evidences from exhibits using Disk Forensic Tools

Kumarshankar Raychaudhuri
LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs
Govt. of India

ABSTRACT

Digital exhibits such as USB drive, external hard disks etc. found at the crime scene contain evidences of essential value. Forensic Imaging of exhibits, which is an indispensable part of digital forensic examination, not only provides all the active files and directories, but also deleted or hidden data from the storage device. Various open-source and proprietary forensic tools are available for acquisition of data from digital exhibits. However, there might be instances of the exhibit being wiped, formatted, overwritten multiple times or data permanently deleted. Therefore, a critical question arises regarding the type and amount of data that might be recoverable. In this research work, the primary objective is to compare and analyse the performance of open-source and proprietary disk forensic tools in recovering data from storage devices. Different samples of USB thumb drives are created and artifacts are acquired using both open-source and proprietary tools. Based on the results, a comparative analysis is done to determine the performance of the tools. The results of this research would be helpful for forensic examiners in using the appropriate forensic tool for enhanced examination of different cases of cyber-crime investigation.

KEYWORDS

Disk Forensic Tools, Digital Evidence, Digital Forensics, Analysis and Extraction, Forensic Imaging, Wiping, Digital Exhibit, Deletion, Formatting.

1 INTRODUCTION

Technological innovations and advancements have increasingly led to the storage of sensitive and confidential data being stored in digital formats [1]. As the storage space increases, more and more data are being stored in digital exhibits such as hard disks or other USB storage devices [2]. Due to ease of portability, such exhibits have gained popularity and their usage have increased. The data stored can range from personal and corporate data to email messages, their attachments, social networking, hidden and encrypted files etc. Such digital exhibits are commonly found artifacts not just in cyber-crime but also in other crime incidents [3]. For detailed and comprehensive investigation of such incidents, it is essential to forensic investigation of such exhibits digitally. Digital Forensics is the science of investigation, which deals with the extraction of digital evidences from computing devices for creating a hypothesis through reconstruction of events, to make it usable in the court of law [17]. According to the principles laid out by the Association of Chief Police Officers (ACPO) [13], “The action taken by Law Enforcement Agencies, persons employed within those agencies or their agents should not change the data in any manner, which may subsequently be relied upon in court.” As a result, instead of working directly on the original exhibit, forensic copy of the seized exhibit is created in order to acquire the data and do further analysis. There are various proprietary and open-source digital forensic tools available for the purpose of analysing and extracting the data from the digital exhibits [4]. Some of the popular tools in this regard include FTK Imager and Analyzer, Encase, Autopsy etc.

It might not always be easy to unearth evidences from digital exhibits. There are instances of data deletion or the exhibit being found in formatted or wiped state during examination. In such circumstances, extraction of important artifacts becomes difficult and to a large extent might depend upon the forensic tool being used for imaging and acquisition. Therefore, with this background, this research work primarily focuses on the analysis and extraction of artifacts (which is of evidential importance) from digital exhibits using different disk forensic tools. The objective is to compare the performance of open-source and proprietary disk imaging tools. This is done by performing imaging and extraction of various data items from different samples of USB thumb drives. A comparative study and analysis of the performance of the tools would be the key to determine the type and amount of data that can be recovered/extracted from each sample using both the tools in case of each of the samples, thus making it easier for forensic experts to select the appropriate disk forensic tool while performing examination of digital exhibits.

The paper is divided into the following sections: Section II highlights the related work, Section III includes the Experimental Design that highlights the testing data, testing samples and the digital forensic tools used for conducting the experiments; Section IV consists of the results obtained from the experiments and related discussions, followed by Section V, which concludes the research work.

2 BACKGROUND

In digital forensics, the goal of the practitioner is to collect and analyze the digital evidence with a view to present it in the court of law or legal proceedings [2]. The process of copying or extraction of the data stored in the digital exhibits, is known as Data Acquisition. The data is acquired through the scientific process known as forensic imaging or bit-stream imaging, which is the technique of performing a bit-by-bit or sector-by-sector copy of any logical or physical drive such as Hard Disks, USB drives, CDs or DVDs etc. in an exact duplicate [14]. The data storage within an exhibit takes place in the form of bits arranged in sectors and clusters, as a result of which capturing each and every bit including deleted and hidden data, is an achievable task. This process is also known as “acquisition of image” of a suspect drive. The probability of recovering data from the disk increases if the image is more exact [14]. Generally, this is the first procedure implemented on reception of seized digital exhibit to the forensic laboratory. The essential data items are analyzed and extracted from the forensic image rather than the original exhibit. This practice prevents tampering of original exhibit and preserved its integrity. During analysis and examination of digital evidences, deleted, formatted or wiped data pose a challenge for the forensic experts.

In any digital exhibit such as hard disks, USB devices etc., the data storage takes place in a binary format (in the form of 0’s and 1’s). In the digital paradigm, every file or folder is a unique combination of 0’s and 1’s. Also, every storage media has their own native file system, which maintains information about the data it stores, in the form of metadata. The file system consists of a file allocation table, which keeps digital evidence about the user-data residing in the disk [15]. When one hits the “delete” button or deletes a file, the data residing in the file is not actually deleted [7,9]. The file allocation table marks the cluster (where the original file was residing) as free for storing of new data. Until the storage of new data in the device, the deleted data is not overwritten (the combination of 0’s and 1’s is not re-arranged) and can be easily recovered using various data recovery tools or while analysis of the forensic image of the storage media [11]. The storage of new data item overwrites the existing combination of binary digits (representing the deleted data), replacing it by a new combination, which makes data recovery difficult.

Formatting, also known as logical formatting is the process of creating a file-system on a disk, which the operating system uses for storing and accessing data [16]. The type of logical formatting always depends on the operating system that is in use. Windows operating system allows for quick format as well as full format. When performing quick formatting on the media, the files are deleted and file-system, volume label and clusters are rebuilt. The journal, which keeps track of the data and their locations on the storage media, is also destroyed. However, if the media is Full Formatted, then the data is erased completely from the media and the entire file-system is rebuilt. Hence, in the case of formatting, the data subject to recovery depends on the type of formatting performed. Therefore, there are higher chances of data recovery in case of Quick Format rather than Full Format. However, there is a possibility of data being carved out of the slack space or unallocated space even from a formatted storage device [9,11].

As compared to deletion or formatting, wiping is more of an irreversible process. The process of wiping erases both the data and the file-system present on the storage media and replaces by either all 0's or all 1's. Therefore, it is always mandatory to format the storage device before it becomes usable for data storage. Hence, it is not possible to recover any data from a disk, which has been wiped multiple times. This is due to the fact that the original bit combination of 0's and 1's (originally stored data) does not exist. This is why wiping removes the data permanently, as compared to deletion and formatting [7,9,11].

3 RELATED WORK

The objective of this research is to compare and measure the performance of both open-source and proprietary tools in recovery of digital evidences from different types of samples of exhibits. A joint study has been conducted by University of Hertfordshire and De Montfort University [3] to determine whether any information is retrievable and data is effectively erased or not in computer hard disks purchased from the second hand market. The study performed on more than 100 hard disks showed that the information is not sanitized effectively and could be recovered easily using digital forensic tools.

In [7], significant work has been done to show how structured analysis and presentation process can be used to enhance examinations of digital evidences. The procedures and techniques proposed in the work ensure correct analysis, contextualization and validation of digital evidences, which are helpful for the forensic examiner in preparing the case evidences.

In [9], a study carried out by Blancco, on used hard disks and SSDs, revealed that more than 35 percent of the used HDDs/SSDs contained residual data, which was not deleted properly. This resulted in the recovery of both individual as well as organizational information from the storage devices.

In [10], the researchers conducted similar study of data recovery from sanitized hard disks, and based on the results, they have recommended that sanitization of disks and drives on computer systems and storage media, which are sold, destroyed or repurposed, should be sanitized properly to ensure that no residual data remains on the disk. Proper tools should be used for deleting or wiping of data from storage devices.

4 EXPERIMENTAL DESIGN

The experiments have been carried out using different samples of USB thumb drives. These samples have been prepared by storing same set of different data items in the thumb drives. The objective has been to make them as similar as possible to a real-life digital exhibit as seized from a crime scene. A brief description of the various tools used for the research work, the data items used for preparing the samples and different types of samples used for experimentation has been included in this section.

4.1 Tools Used

The different digital forensic tools used for conducting the experiments are as follows:

FTK Imager – Forensic Toolkit (FTK) Imager is an imaging tool developed by AccessData, which is used for creating a forensic image of a physical drive, logical drive or contents of file and folder. It can create the image in different formats such as AFF, Raw (dd), SMART or E01 [5].

FTK 7.0 – FTK 7.0 is used for forensic analysis of digital exhibits and evidences. It can index, filter and search the data in an efficient manner. It can find active files and folders, deleted data, encrypted data, emails and related attachments and many more from the available disk or forensic image. It has advanced data carving engine to avoid irrelevant data being carved out [5].

Autopsy – Autopsy is a digital investigation analysis tool developed by The Sleuth Kit. It is an HTML-based tool and can run on both Windows as well as UNIX platform. Both active and deleted files can be analysed and the contents can be viewed in raw or Hex format [6].

File Shredder – File Shredder is a wiping tool that is used for wiping files and folders in a manner such that they cannot be recovered. It has multiple shredding algorithms to wipe the data from the hard disk or any other storage media [12].

4.2 Test Data Set

The exhibit samples have been prepared with the following set of data items:

a) Microsoft Office Documents such as Word Document, PowerPoint Presentations etc.
b) Image files with .jpg, .png and .bmp file types.
c) Multimedia video files of MP4 file type.
d) Encrypted document files (protected with password).
e) Files with Bad Extensions. The extension of the file is changed to create a mismatch between file type and file extension. The extension of a file is changed for the purpose of hiding the particular data item.
f) Files with Alternate Data Streams.
g) Emails and associated files.
h) Web Artifacts (HTML files, Internet Temporary files etc.)
i) Executable files
j) Internet Files consisting of Chrome Browser files. These files can be found at the location C:\Users\User\AppData\Local\Google\Chrome\UserData\Default. The Internet files consists of Cache files, Bookmarks, Cookies and Browser History files.

4.3 Test Samples

The experiment for the research is conducted by preparing four different test samples. A sample is prepared by using a sterile exhibit (USB thumb drive of 4GB capacity wiped multiple times and NTFS-formatted) and then storing the test data in the exhibit [8,10]. The samples are described as follows:

a) **Sample A** – The exhibit contains all the data files and folders in active state.
b) **Sample B** – The exhibit consists of some of the data files and folders while the rest of the data has been deleted permanently. New data items are stored in the storage device.
c) **Sample C** – The exhibit is formatted using the formatting feature available in Windows operating system.
d) **Sample D** – The exhibit is wiped completely using wiping tool.

5 RESULTS AND DISCUSSION

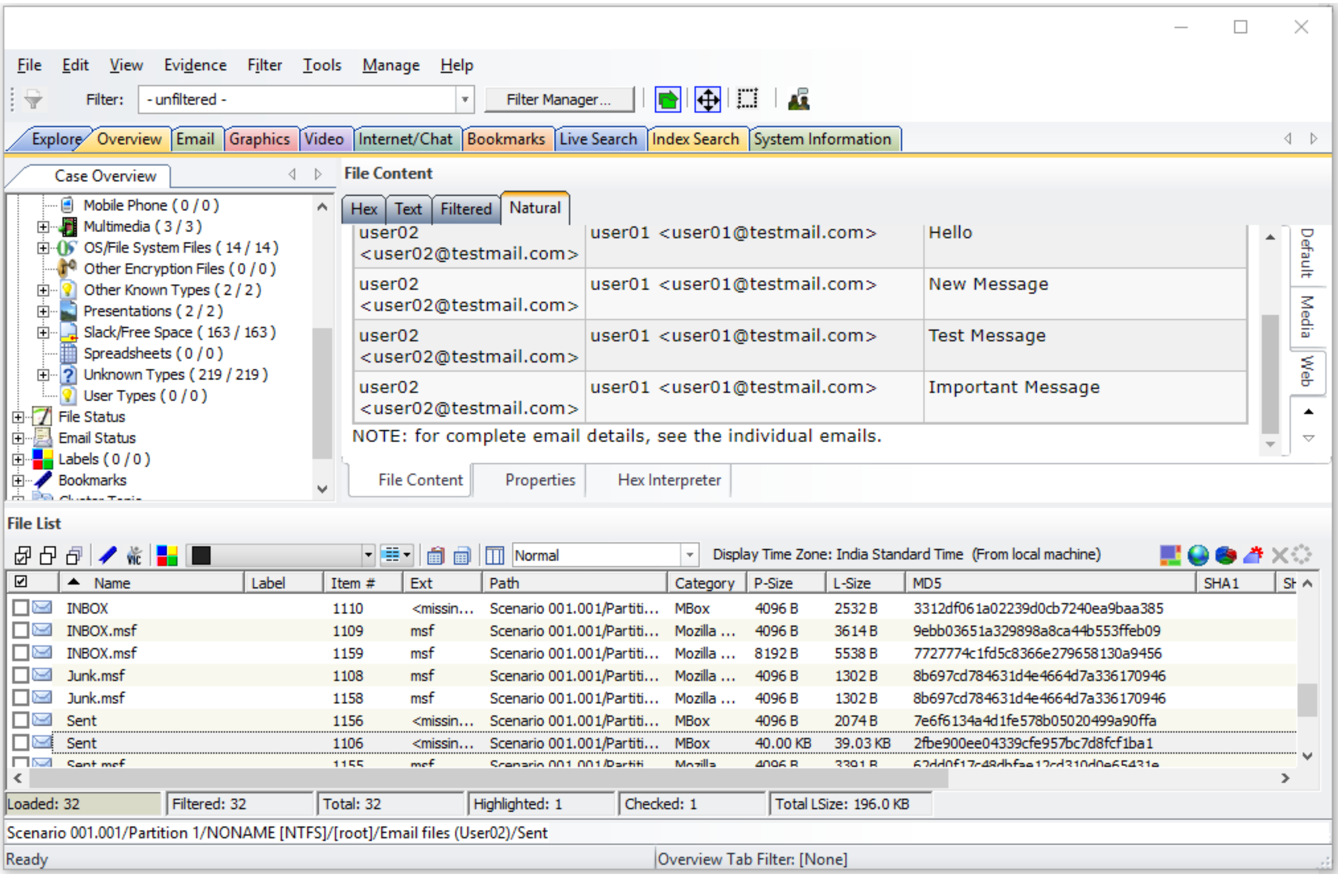
A bit-stream image of the exhibit is created while experimenting each of the samples, using FTK Imager. The analysis and extraction of data from the image of the exhibit is done using both FTK 7.0 (proprietary tool) as well as Autopsy (open-source tool). The results obtained for each sample have been compared and discussed in this section.

5.1 Data Extraction and Forensic Analysis of Sample A

Sample A has been prepared with the data in active state (i.e. without deleting or wiping any data item from the exhibit). The forensic imaging is done and analysed using proprietary tool, snapshot of which is shown in Fig.1

On analysis and extraction, it is found that the proprietary tool is able to recover all the data from the forensic image of the sample (exhibit). Some types of files such as browsing history files, cookies files, Alternate Data Streams (Data files hidden inside other documents) etc. that could not be viewed using the windows explorer, were also recovered in a plain-text readable format. The properties of the data items (metadata) before and after analysis were compared and found to be matching.

The same sample is also analysed using the open-source tool, shown in Fig.2. Open-source tool also reported the same result when compared to that given by proprietary tool. All data items from the sample were fully recovered. The properties of the data items (metadata) before and after analysis were compared and found to be matching.


File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information
Case Overview
Mobile Phone (0 / 0)
Multimedia (3 / 3)
OS/File System Files (14 / 14)
Other Encryption Files (0 / 0)
Other Known Types (2 / 2)
Presentations (2 / 2)
Slack/Free Space (163 / 163)
Spreadsheets (0 / 0)
Unknown Types (219 / 219)
User Types (0 / 0)
File Status
Email Status
Labels (0 / 0)
Bookmarks
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal

user02 <user02@testmail.com>	user01 <user01@testmail.com>	Hello
user02 <user02@testmail.com>	user01 <user01@testmail.com>	New Message
user02 <user02@testmail.com>	user01 <user01@testmail.com>	Test Message
user02 <user02@testmail.com>	user01 <user01@testmail.com>	Important Message

NOTE: for complete email details, see the individual emails.

Display Time Zone: India Standard Time (From local machine)

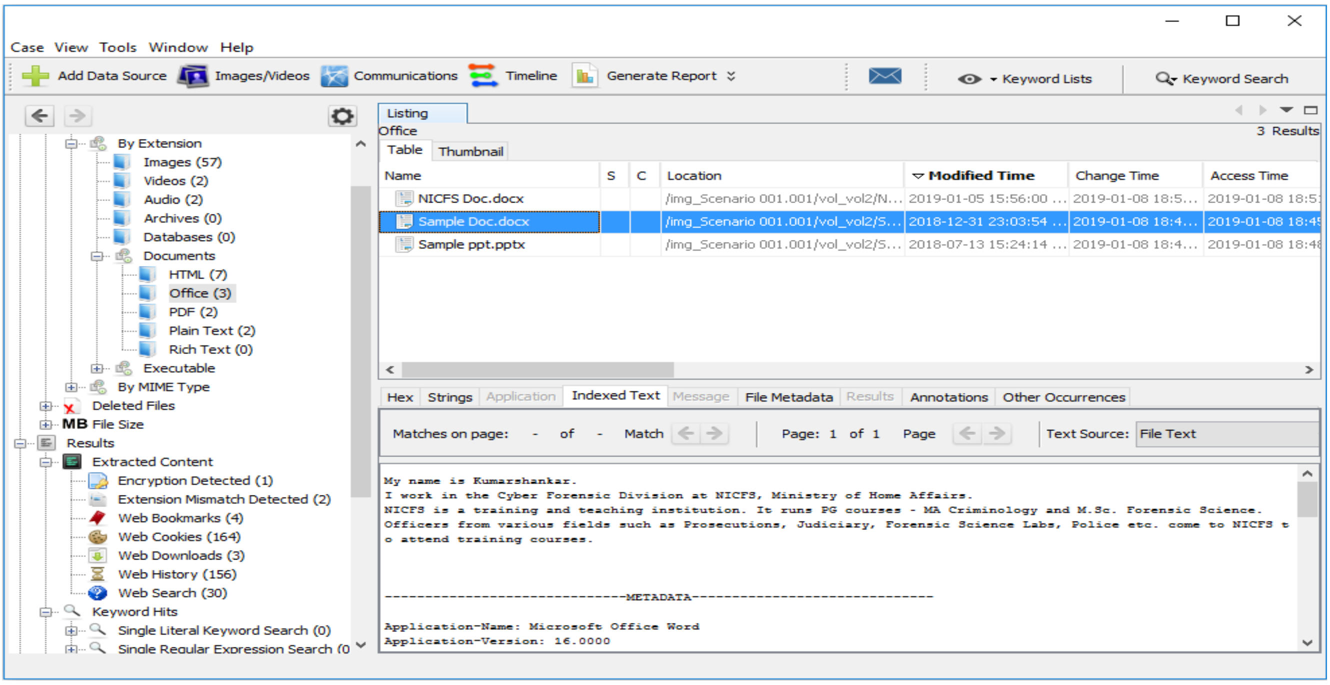
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1
□	INBOX		1110	<missin...	Scenario 001.001/Partiti...	MBox	4096 B	2532 B	3312df061a02239d0cb7240ea9baa385	
□	INBOX.msf		1109	msf	Scenario 001.001/Partiti...	Mozilla ...	4096 B	3614 B	9ebb03651a329898a8ca44b553ffeb09	
□	INBOX.msf		1159	msf	Scenario 001.001/Partiti...	Mozilla ...	8192 B	5538 B	7727774c1fd5c8366e279658130a9456	
□	Junk.msf		1108	msf	Scenario 001.001/Partiti...	Mozilla ...	4096 B	1302 B	8b697cd784631d4e4664d7a336170946	
□	Junk.msf		1158	msf	Scenario 001.001/Partiti...	Mozilla ...	4096 B	1302 B	8b697cd784631d4e4664d7a336170946	
□	Sent		1156	<missin...	Scenario 001.001/Partiti...	MBox	4096 B	2074 B	7e6f6134a4d1fe578b05020499a90ffa	
□	Sent		1106	<missin...	Scenario 001.001/Partiti...	MBox	40.00 KB	39.03 KB	2fbe900ee04339cfe957bc7d8fcf1ba1	

Loaded: 32 | Filtered: 32 | Total: 32 | Highlighted: 1 | Checked: 1 | Total LSize: 196.0 KB

Scenario 001.001/Partition 1/NONAME [NTFS]/[root]/Email files (User02)/Sent

Ready | Overview Tab Filter: [None]

Figure 1: Snapshot of Data Analysis and Extraction of Sample A using FTK Analyzer 7.0



Office 3 Results

Name	S	C	Location	Modified Time	Change Time	Access Time
NICFS Doc.docx			/img_Scenario 001.001/vol_vol2/N...	2019-01-05 15:56:00 ...	2019-01-08 18:5...	2019-01-08 18:5
Sample Doc.docx			/img_Scenario 001.001/vol_vol2/S...	2018-12-31 23:03:54 ...	2019-01-08 18:4...	2019-01-08 18:4
Sample ppt.pptx			/img_Scenario 001.001/vol_vol2/S...	2018-07-13 15:24:14 ...	2019-01-08 18:4...	2019-01-08 18:4

Matches on page: - of - Match | Page: 1 of 1 Page | Text Source: File Text

```
My name is Kumarshankar.
I work in the Cyber Forensic Division at NICFS, Ministry of Home Affairs.
NICFS is a training and teaching institution. It runs PG courses - MA Criminology and M.Sc. Forensic Science.
Officers from various fields such as Prosecutions, Judiciary, Forensic Science Labs, Police etc. come to NICFS t
o attend training courses.



------------------------------METADATA------------------------------

Application-Name: Microsoft Office Word
Application-Version: 16.0000
```

Figure 2: Snapshot of Analysis and Extraction of data from Sample A using Autopsy

5.2 Data Extraction and Forensic Analysis of Sample B

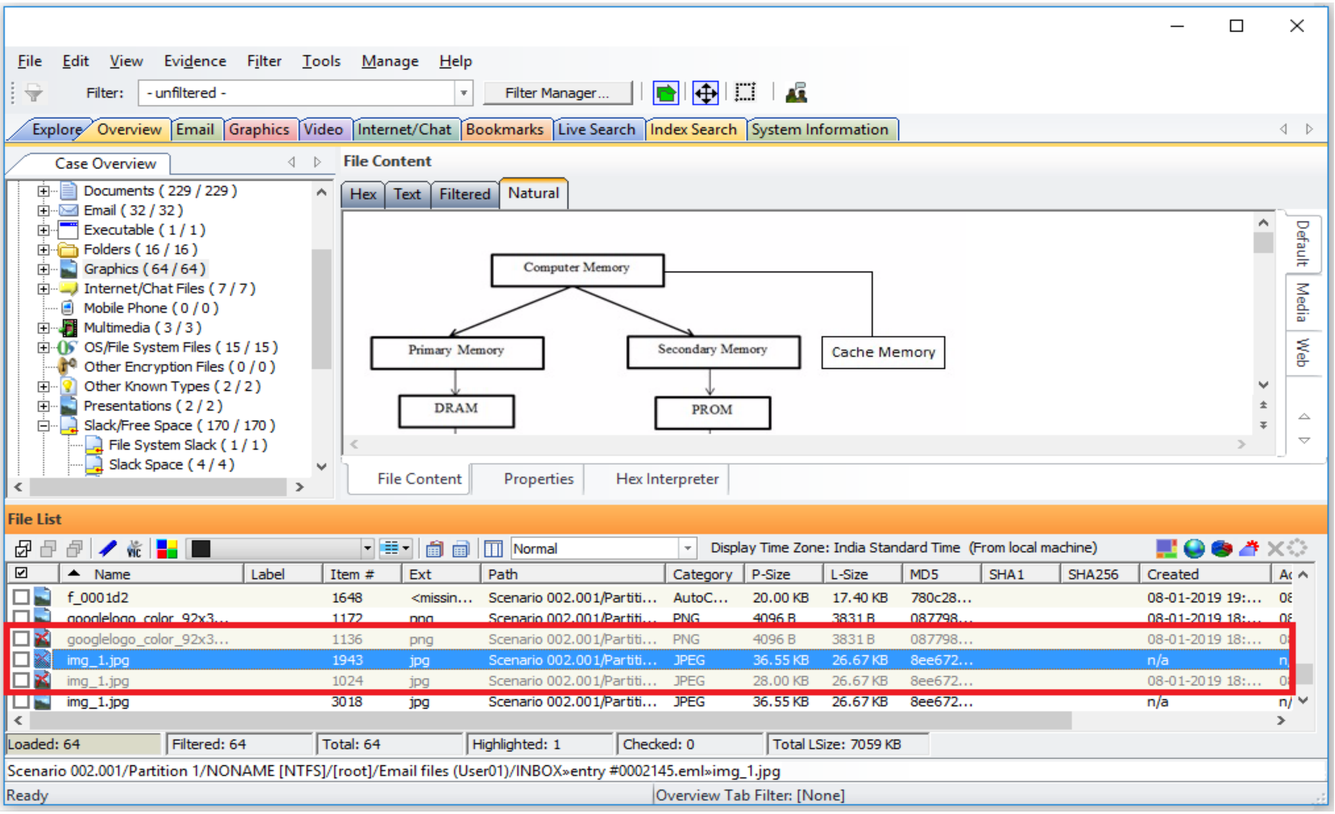
Sample B has been prepared by deleting some of the data items from the exhibit. The data items have been deleted permanently (using the key combination shift + delete), so that they cannot be restored back from the Recycle Bin. After deleting the original data items, new data items were added to the exhibit. Bit-stream image of the exhibit is created and is analyzed using proprietary tool, snapshot of which is shown in Fig.3

On analyzing the extracted data from Sample B (Fig. 3), it was observed that some of the deleted data was recovered and found in readable format [9,11]. Some of the data items were corrupt and could not be opened, while the rest were recovered partially. Data was also found in the slack space. Slack space is a form of internal fragmentation i.e. the leftover space in a storage device. It is created when a data file does not occupy all the space allocated to it [14]. In such circumstances, when the old data is deleted and overwritten with new data, there is a possibility of recovering the traces of older data from the slack space.

Fig.4 shows a snapshot of the analysis of Sample B done using open-source tool. In this case, deleted files were recovered both totally as well as partially along with data found in the slack space. However, a comparative study is performed between the results given by the tools based on the few parameters. The results are shown in Table 1 and graphically represented in Fig. 5.

Table 1: Comparison between performance of proprietary and open-source tool based on result analysis of Sample B

Parameters	Proprietary Tool (FTK 7.0)	Open-Source Tool (Autopsy)
Number of original data items totally recovered	45	45
Number of original data items partially recovered	40	30
Number of data items recovered from Slack Space	170	155
Number of data items found not readable	5	10



Display Time Zone: India Standard Time (From local machine)

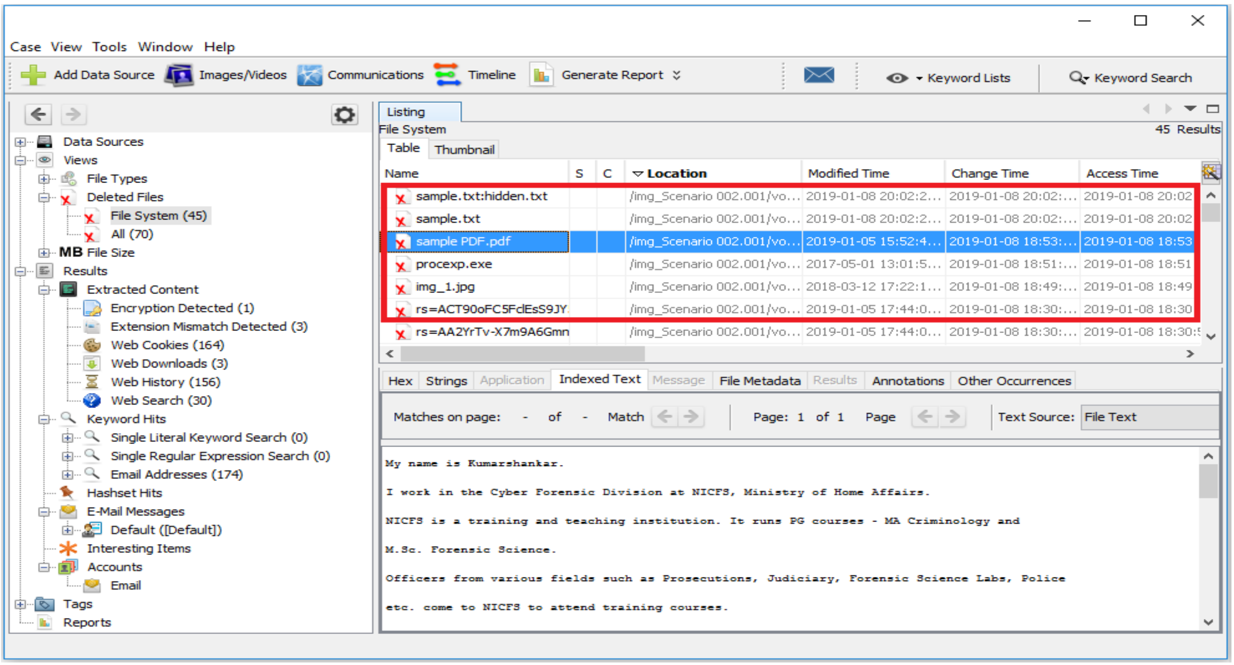
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Ac
☐	f_0001d2		1648	<missin...	Scenario 002.001/Partiti...	AutoC...	20.00 KB	17.40 KB	780c28...			08-01-2019 19:...	08
☐	googlelogo_color_92x3...		1172	png	Scenario 002.001/Partiti...	PNG	4096 B	3831 B	087798...			08-01-2019 18:...	08
☐	googlelogo_color_92x3...		1136	png	Scenario 002.001/Partiti...	PNG	4096 B	3831 B	087798...			08-01-2019 18:...	0
☐	img_1.jpg		1943	jpg	Scenario 002.001/Partiti...	JPEG	36.55 KB	26.67 KB	8ee672...			n/a	n
☐	img_1.jpg		1024	jpg	Scenario 002.001/Partiti...	JPEG	28.00 KB	26.67 KB	8ee672...			08-01-2019 18:...	0
☐	img_1.jpg		3018	jpg	Scenario 002.001/Partiti...	JPEG	36.55 KB	26.67 KB	8ee672...			n/a	n/

Loaded: 64 Filtered: 64 Total: 64 Highlighted: 1 Checked: 0 Total LSize: 7059 KB

Scenario 002.001/Partition 1/NONAME [NTFS]/[root]/Email files (User01)/INBOX»entry #0002145.eml»img_1.jpg

Ready Overview Tab Filter: [None]

Figure 3: Snapshot of Analysis and Extraction of Data from Sample B using FTK Analyzer 7.0



Name	S	C	Location	Modified Time	Change Time	Access Time
sample.txt:hidden.txt			/img_Scenario 002.001/vo...	2019-01-08 20:02:2...	2019-01-08 20:02:...	2019-01-08 20:02
sample.txt			/img_Scenario 002.001/vo...	2019-01-08 20:02:2...	2019-01-08 20:02:...	2019-01-08 20:02
sample PDF.pdf			/img_Scenario 002.001/vo...	2019-01-05 15:52:4...	2019-01-08 18:53:...	2019-01-08 18:53
procexp.exe			/img_Scenario 002.001/vo...	2017-05-01 13:01:5...	2019-01-08 18:51:...	2019-01-08 18:51
img_1.jpg			/img_Scenario 002.001/vo...	2018-03-12 17:22:1...	2019-01-08 18:49:...	2019-01-08 18:49
rs=ACT90oFC5FdEsS9JY			/img_Scenario 002.001/vo...	2019-01-05 17:44:0...	2019-01-08 18:30:...	2019-01-08 18:30
rs=AA2YrTv-X7m9A6Gmn			/img_Scenario 002.001/vo...	2019-01-05 17:44:0...	2019-01-08 18:30:...	2019-01-08 18:30:5

```
My name is Kumarshankar.

I work in the Cyber Forensic Division at NICFS, Ministry of Home Affairs.

NICFS is a training and teaching institution. It runs PG courses - MA Criminology and

M.Sc. Forensic Science.

Officers from various fields such as Prosecutions, Judiciary, Forensic Science Labs, Police

etc. come to NICFS to attend training courses.
```

Figure 4: Snapshot of Analysis and Extraction of data from Sample B using Autopsy

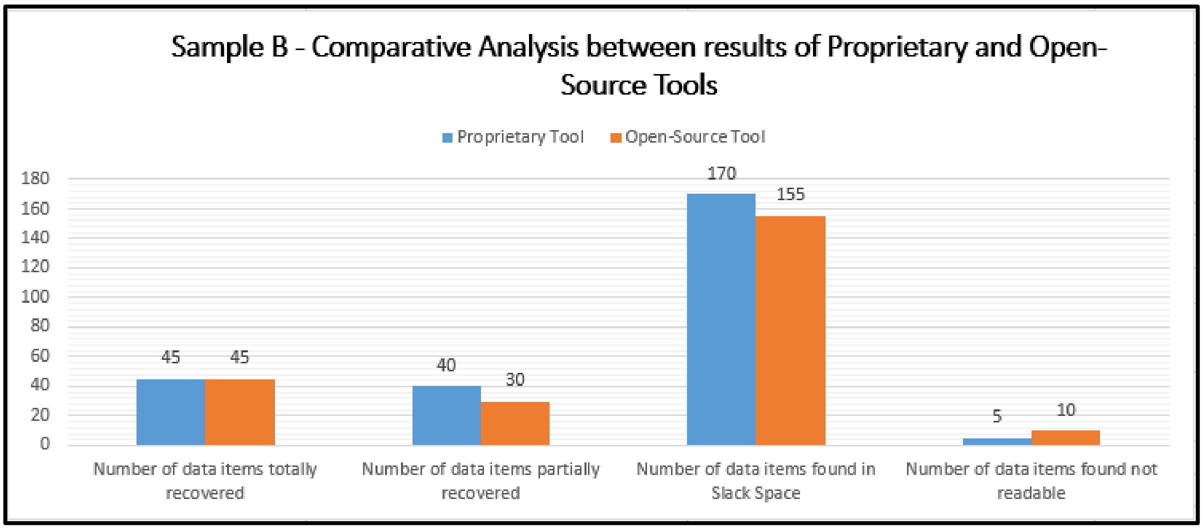
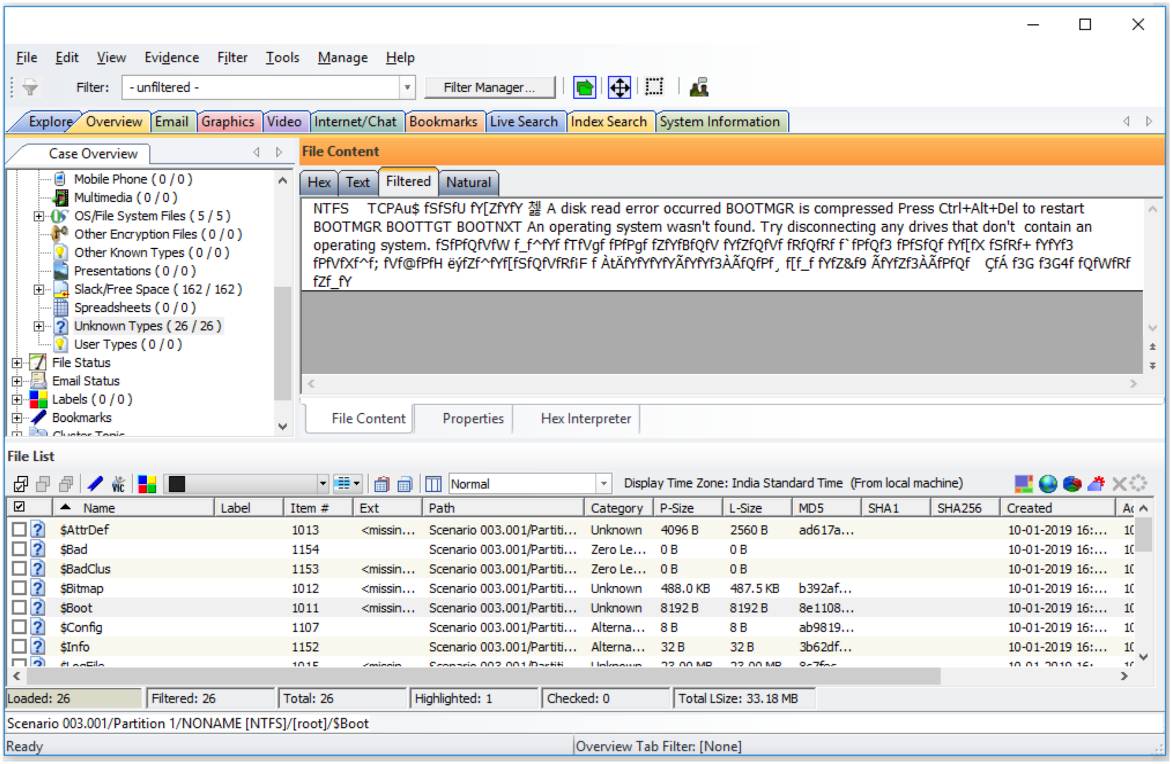


Figure 5: Comparison Graph between results of Proprietary and Open-source tool in analysis of Sample B

From Table 1 and the graph as shown in Fig.5, it can be interpreted that the number of deleted data items totally recovered by the open-source and proprietary tool were equal in number. However, it can also be observed that there is a difference between the number of data items partially recovered and number of data items found in the slack space when the results of both tools are compared. The open-source tool could recover a smaller number of data items (partially recovered and slack space data) than the proprietary tool. Hence, it is inferred that the proprietary tool shows a relatively better performance than the open-source tool while recovering deleted data from an exhibit.

5.3 Data Extraction and Forensic Analysis of Sample C

Sample C has been prepared by formatting the exhibit. A full format of the exhibit is done. After formatting, a forensic image of the exhibit was captured using FTK Imager and the image was analyzed using the proprietary tool. The results of the analysis and extraction of data is shown in Fig.6


File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information
Case Overview
Mobile Phone (0 / 0)
Multimedia (0 / 0)
OS/File System Files (5 / 5)
Other Encryption Files (0 / 0)
Other Known Types (0 / 0)
Presentations (0 / 0)
Slack/Free Space (162 / 162)
Spreadsheets (0 / 0)
Unknown Types (26 / 26)
User Types (0 / 0)
File Status
Email Status
Labels (0 / 0)
Bookmarks
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: India Standard Time (From local machine)

```
NTFS    TCPAu$ fSfSfU fY[ZfYfY 젍 A disk read error occurred BOOTMGR is compressed Press Ctrl+Alt+Del to restart
BOOTMGR BOOTTGT BOOTNXT An operating system wasn't found. Try disconnecting any drives that don't  contain an
operating system. fSfPfQfVfW f_f^fYf fTfVgf fPfPgf fZfYfBfQfV fYfZfQfVf fRfQfRf f`fPfQf3 fPfSfQf fYf[fX fSfRf+ fYfYf3
fPfVfXf^f; fVf@fPfH ëýfZf^fYf[fSfQfVfRfiF f ÀtÄfYfYfYfYÃfYfYf3ÀÃfQfPf¸ f[f_f fYfZ&f9 ÃfYfZf3ÀÃfPfQf   ÇfÁ f3G f3G4f fQfWfRf
fZf_fY
```

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Ac
☐	$AttrDef		1013	<missin...	Scenario 003.001/Partiti...	Unknown	4096 B	2560 B	ad617a...			10-01-2019 16:...	1(
☐	$Bad		1154		Scenario 003.001/Partiti...	Zero Le...	0 B	0 B				10-01-2019 16:...	1(
☐	$BadClus		1153	<missin...	Scenario 003.001/Partiti...	Zero Le...	0 B	0 B				10-01-2019 16:...	1(
☐	$Bitmap		1012	<missin...	Scenario 003.001/Partiti...	Unknown	488.0 KB	487.5 KB	b392af...			10-01-2019 16:...	1(
☐	$Boot		1011	<missin...	Scenario 003.001/Partiti...	Unknown	8192 B	8192 B	8e1108...			10-01-2019 16:...	1(
☐	$Config		1107		Scenario 003.001/Partiti...	Alterna...	8 B	8 B	ab9819...			10-01-2019 16:...	1(
☐	$Info		1152		Scenario 003.001/Partiti...	Alterna...	32 B	32 B	3b62df...			10-01-2019 16:...	1(

Loaded: 26 | Filtered: 26 | Total: 26 | Highlighted: 1 | Checked: 0 | Total LSize: 33.18 MB

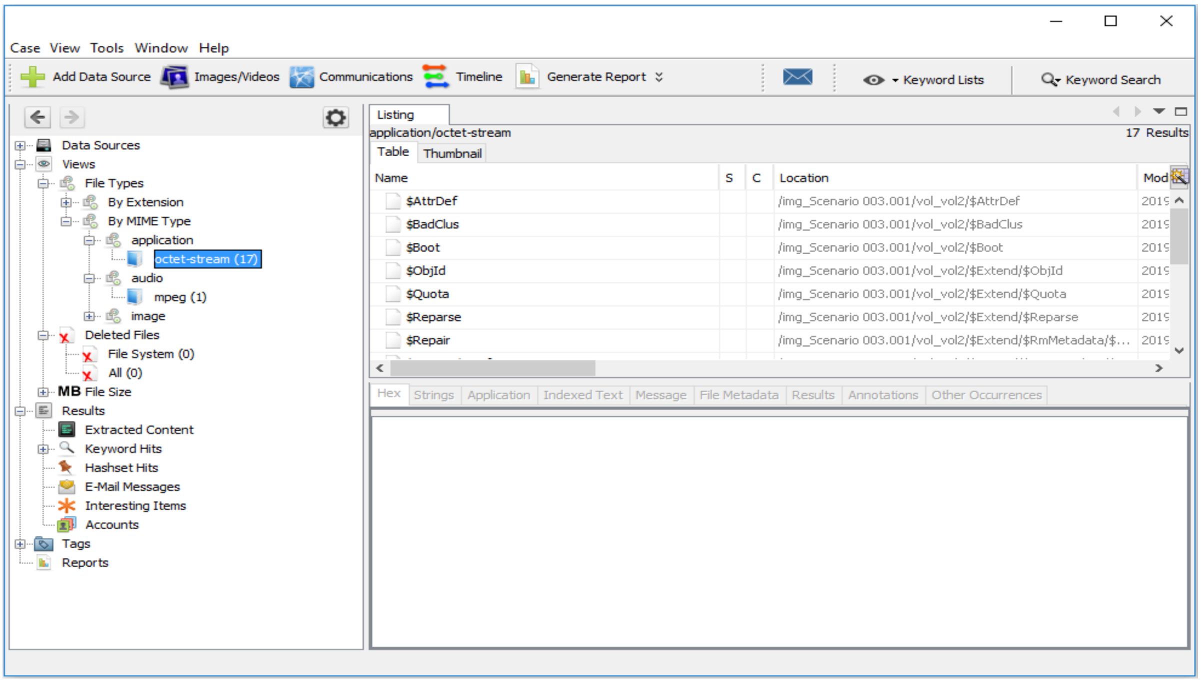
Scenario 003.001/Partition 1/NONAME [NTFS]/[root]/$Boot

Ready | Overview Tab Filter: [None]

Figure 6: Snapshot of Analysis and Extraction of data from Sample C using FTK Analyzer 7.0

The analysis and extraction of data using proprietary tool showed that data files could be recovered only from the slack space and unallocated spaces. Unallocated space, also refers to the unused space in a storage device, which is not used for storing data [14].

The open-source tool could also recover data from the slack space only [11]. However, data could not be recovered from the unallocated spaces, as shown in Fig.7. A comparative study is performed between the results given by both the open-source and proprietary tools based on different parameters, as shown in Table 2. The comparative study has been graphically interpreted and shown in Fig. 8.



application/octet-stream 17 Results

Name	S	C	Location	Mod
$AttrDef			/img_Scenario 003.001/vol_vol2/$AttrDef	2019
$BadClus			/img_Scenario 003.001/vol_vol2/$BadClus	2019
$Boot			/img_Scenario 003.001/vol_vol2/$Boot	2019
$ObjId			/img_Scenario 003.001/vol_vol2/$Extend/$ObjId	2019
$Quota			/img_Scenario 003.001/vol_vol2/$Extend/$Quota	2019
$Reparse			/img_Scenario 003.001/vol_vol2/$Extend/$Reparse	2019
$Repair			/img_Scenario 003.001/vol_vol2/$Extend/$RmMetadata/$...	2019

Figure 7: Snapshot of Analysis and Extraction of data from Sample C using Autopsy

Table 2: Comparison between performance of proprietary and open-source tool based on result analysis of Sample C

Parameters	Proprietary Tool (FTK 7.0)	Open-Source Tool (Autopsy)
Number of original data items recovered	0	0
Number of data items recovered from slack space	162	17
Number of data items recovered from unallocated space	31	0

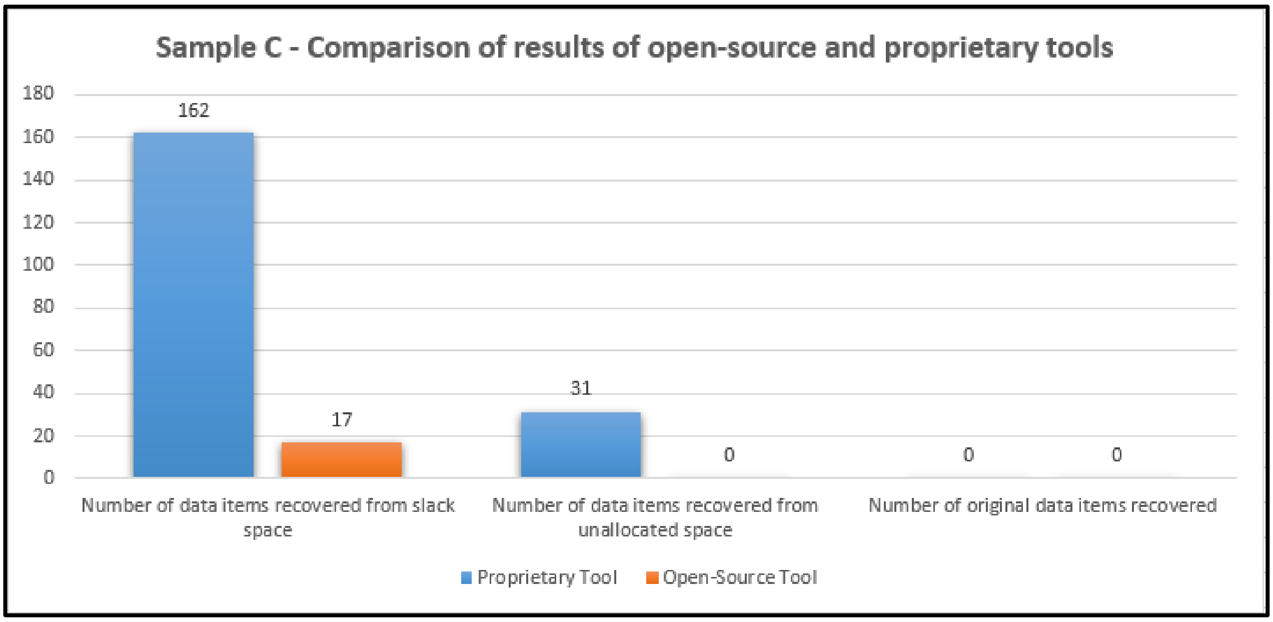
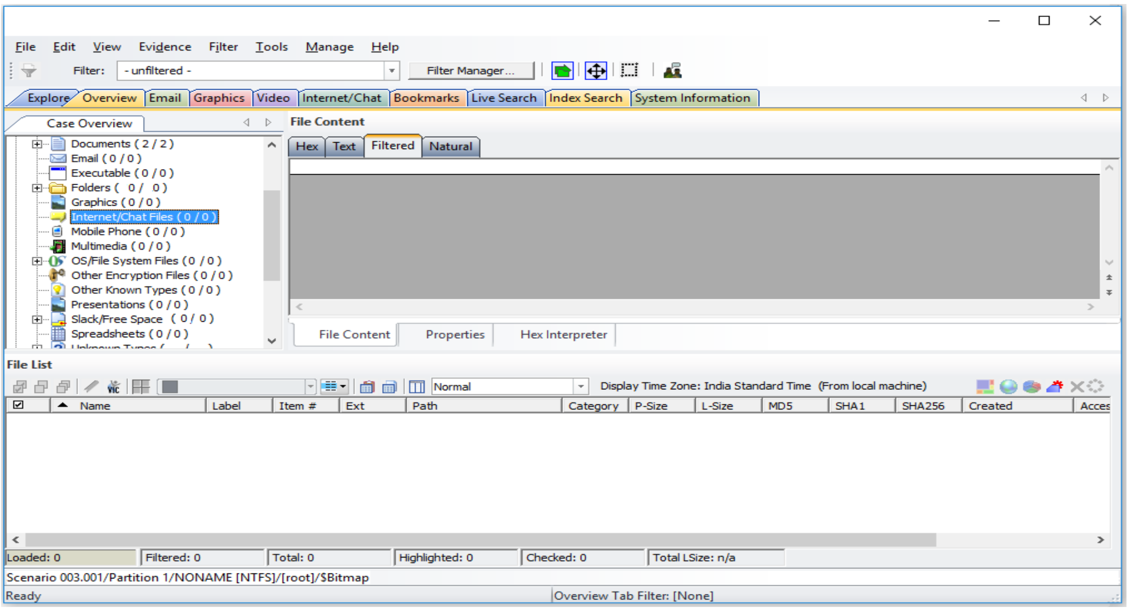


Figure 8: Comparison Graph between results of Proprietary and Open-source tool in analysis of Sample C

On analyzing the results shown in Table 3 and interpretation of the graph, it can be inferred that the proprietary tool is able to recover more data from the slack space and unallocated space as compared to that of open-source tool. However, original data items could not be recovered from the exhibit. Hence, on the basis of comparison and analysis of the results, it can be said the proprietary tool shows a relatively better performance in comparison to open-source tool, when recovery of data is to be done from a storage device that has been formatted.

5.4 Data Extraction and Forensic Analysis of Sample D

Sample D has been prepared by performing a wiping operation on the exhibit multiple times, using specialized wiping software. After wiping the exhibit, it is forensically imaged using the software FTK Imager and the image is analyzed using both proprietary tools i.e. FTK 7.0 and open-source tool i.e. Autopsy. The snapshots of the analysis performed on the image of the exhibit using different tools, are shown in Fig. 9 and Fig. 10 respectively.


File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information
Case Overview
Documents (2 / 2)
Email (0 / 0)
Executable (0 / 0)
Folders (0 / 0)
Graphics (0 / 0)
Internet/Chat Files (0 / 0)
Mobile Phone (0 / 0)
Multimedia (0 / 0)
OS/File System Files (0 / 0)
Other Encryption Files (0 / 0)
Other Known Types (0 / 0)
Presentations (0 / 0)
Slack/Free Space (0 / 0)
Spreadsheets (0 / 0)
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Acces

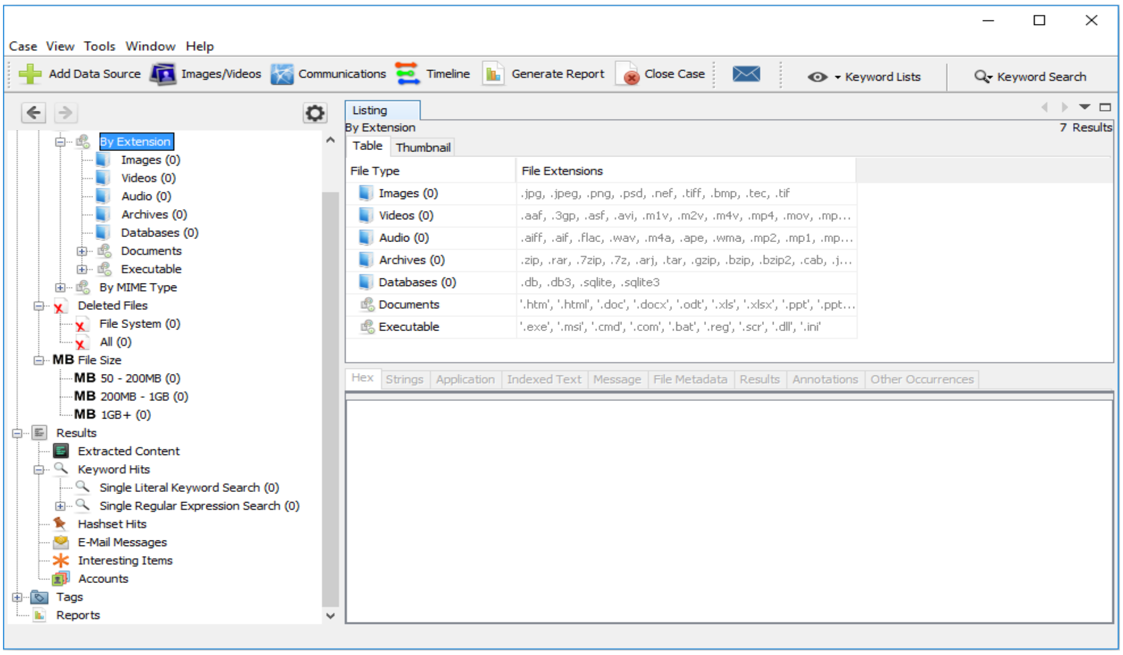
Display Time Zone: India Standard Time (From local machine)

Loaded: 0 | Filtered: 0 | Total: 0 | Highlighted: 0 | Checked: 0 | Total LSize: n/a

Scenario 003.001/Partition 1/NONAME [NTFS]/[root]/$Bitmap

Ready | Overview Tab Filter: [None]

Figure 9: Snapshot of Analysis and Extraction of data from sample D using FTK 7.0



By Extension — 7 Results

File Type	File Extensions
Images (0)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif
Videos (0)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mp...
Audio (0)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp...
Archives (0)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .j...
Databases (0)	.db, .db3, .sqlite, .sqlite3
Documents	'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.ppt...
Executable	'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'

Figure 10: Snapshot of Analysis and Extraction of data from sample D using Autopsy

From the results given by both the proprietary and open-source tools, it is observed that data recovery is not possible once the storage media is wiped several times. The reason for such a result is attributed to the fact that wiping erases both the data as well as the file-system from the exhibit. It should be noted that the word 'erase' is used instead of 'delete' because here, the data is not deleted, which is the reason it is not recoverable. The data along with the in-built file-system of the storage media are erased beyond recovery.

6 CONCLUSIONS

This research work has been carried out with the objective of performing a comparative study among the results of analysis and extraction of evidences (data files) from different prepared samples of digital exhibits, using open-source as well as proprietary forensic tools. Four different samples were prepared with test data for conducting the experiment. All the samples were prepared using the same set of test data. The first sample consisted of data in an active state, while data in the second sample was deleted partially and overwritten with new data. In the third sample, the exhibit was formatted using the in-built feature of the operating system and the fourth sample consisted of exhibit, which was wiped using wiping software.

After conducting the experiments, it has been observed that both proprietary and open-source tools show similar performances when used to analyze active data files (Sample A) i.e. all the data could be recovered easily from the forensic image of the exhibit. However, when data is deleted and new data is added (Sample B) or the exhibit is formatted (Sample C), proprietary tool showed a relatively better performance as compared to open-source tool. In the final sample (Sample D), when the exhibit was wiped, both forensic tools again showed similar performances i.e. data could not be recovered from the exhibit by using either tool.

Hence, based on the experimentation process in the research work, several conclusions have been drawn, as follows:

i. Deleted data can be recovered from exhibit using either proprietary or open-source tool. However, if new data is added, chances of complete data recovery would reduce considerably. The old data can be recovered partially or traces of it can also be extracted from the slack spaces or unallocated spaces depending upon the type of tool used. A proprietary tool performs better as compared to open-source tool.

ii. Data recovery becomes a difficult task when the exhibit is formatted. Both proprietary and open-source tools would not be able to recover any originally stored data in the exhibit, except traces of data from the slack spaces or unallocated spaces. A proprietary tool, however, shows better performance in both cases, as it can extract larger number of data items from the slack or unallocated spaces.

iii. An open-source tool recovers less amount of deleted data or data from formatted disk, as compared to proprietary tool. A scientific can technical reason to this can be attributed to the fact that the number of modules or libraries available in an open-source tool like Autopsy is less as compared to that of a proprietary tool like FTK Analyzer, when freshly installed in a computer system. Due to the availability of lesser data recovery modules, the amount of data that can be acquired from the storage media by open-source tool is less than the amount of data recovered by proprietary tool.

iv. Wiping an exhibit leaves data recovery impossible from any location, including even slack and unallocated spaces, either by proprietary or open-source tool. Therefore, both proprietary and open-source tools can be used depending upon the case, for analyzing and extracting data while examination of seized digital exhibits.

7 REFERENCES

1. Naser A., Majid M.A., Zolkipli M.F., Anwar S.: Trusting Cloud Computing for personal files. In International Conference on Information and Communication Technology Convergence (ICTC), IEEE South Korea (2014).

2. Beer R., Stander A., Belle JP.: Anti-Forensics: A Practitioner Perspective. In: International Journal of Cyber-Security and Digital Forensics, vol. 4, issue 2, pp 390-403, SDIWC (2015).

3. Angelopoulou A., Jones A., Vldalls S., Janlcke H.: The 2016 Hard Disk Study on Information Available on the Second-Hand Market in the UK. In: Proc. 16th European Conference on Cyber Warfare and Security (ECCWS), ResearchGate (2017).

4. Lyle J.: Testing Disk Imaging Tools. In (Proc). 2002 Digital Forensic Research Conference (DFRWS), Syracuse, NY (2002).

5. AccessData FTK Imager, User Guide, https://ad-pdf.s3.amazonaws.com/ Imager% 203_1_4_UG.pdf

6. Open Source Digital Forensics, https://www.sleuthkit.org

7. Boddington R.: A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial. In (Proc). Annual ADFSL Conference on Digital Forensics, Security and Law (ADFSL), pp. 155-172, (2012).

8. Naqvi S.: Digital Investigations and Forensic Analysis: Practices and Technologies. In Sixth

International Conference on Digital Society (ICDS), Valencia (2012).

9. The Leftovers: A Data Recovery Study, http://info.blancco.com/en-rs-leftovers-a-data-recovery-study

10. Garfinkel S., Shelat A.: Remembrance of data passed: A study of disk sanitization practices. IEEE Security and Privacy, vol. 1, issue 1, pp. 17-27, (2003)

11. Lawon D., Stacey R., Dodd G.: eDiscovery in Digital Forensic Investigations. CAST Publications Number 32/14, Metropolitan Police Service, (2014).

12. File Shredder, http://www.fileshredder.org/

13. Police Central e-Crime Unit.: ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers, (2012).

14. Nelson B., Philips A. and Steuart C.: Guide to Computer Forensics and Investigations, 4th Edition. Cengage Learning, (2013).

15. Meshram B., Patil D.: Digital Forensic Analysis of Hard Disk for Evidence Collection. In: International Journal of Cyber-Security and Digital Forensics, vol. 7, issue 2, pp 100-110, SDIWC (2018).

16. Formatting- Formatting a Hard Drive, www.http://www.idc-online.com

17. Karie M., Kebande V.: Building Ontologies for Digital Forensic Terminologies. In: International Journal of Cyber-Security and Digital Forensics, vol. 5, issue 2, pp 75-82, SDIWC (2016).