Expt. No.

Name : Piyush Pandurang Burate. Class : TYCS Roll No.: 523

Title of Experiment : Recovering and inspecting deleted Files.

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- Recovering and inspecting deleted Files ;
- Check for deleted files.
- Analyzing and inspecting the recovered Files perform the using recovery option in Encase and perform manually through command line.

S/W / H/W Requirement :- FTK imager, computer, printer.

Theory :-

Types of attempts in destroying Files.

Modern computer hard drives contain an assartment of data including an operating system application of programs and user data stored in files. Drives also contain backing store of memory and OS meta information such as directory files, attributes and allocation to beets drivers includes directory blocks startup of S/W.

Remark

Signature

Level	Where Found	Description
Level 0	Regular Files	Info. contained in the file system. Includes a file name the attributes and file contents one can directly access system.
Level 1	Temporary Files	Temporary files include print spooler browser cache files, helper and recycle bin files.
Level 2	Deleted Files	When a file is deleted from a file system, most OS do not overwrite the blocks on the hard disk the file most directory Morton utilities.
Level 3	Retained data blocks	Data that can be recovered from a disk but which does not obviously belong to named file level 3 data include info. in slack space backing tools level 3.
Level 4	Vendor hidden blocks	This level consists of data blocks that can only be accessed using vendor specific commands This level and blocks management.

Level 5	Overwritten data	Many individuals maintain that information can be recovered from a hard drive even after, it overwritten we reserve 5 level info.

Technique to Recover –

The tools technique and methodology of electronic gathering and analysis have been tried and proven and are accepted in many countries through out the investigation.

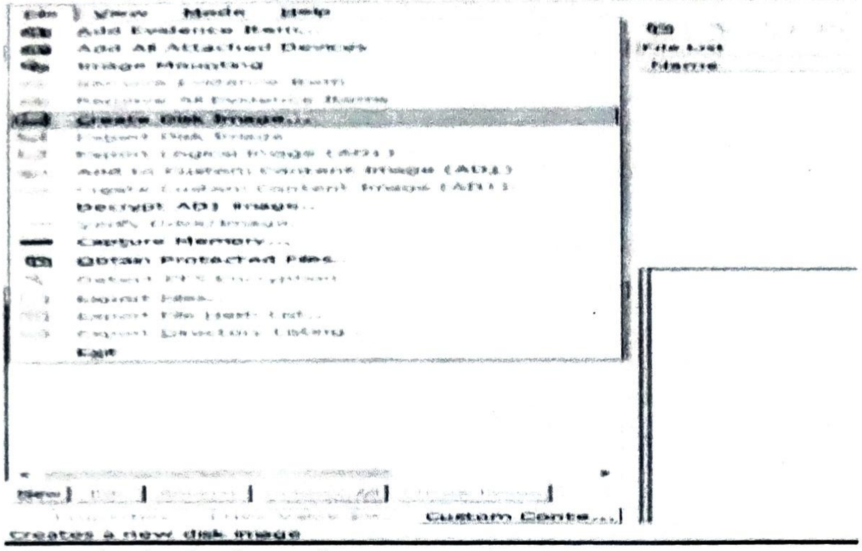
Tools	Platform	Nature
Drives	DOS/Windows	Inspect stack space and deleted File metadata.
Forensic toolkit	Windows	Graphic search and preview of forensic info ~~on~~ of including searches for JPEG images and internet text.
Ilook	Window	Handles dozens of Files system to available to us goverement agencies.
Norton utilities	Window	Handles dozens of File system explorer interface to deleted Files generates law agencies.

Conclusion :-

We recovered deleted Files using Access data FTK imager.

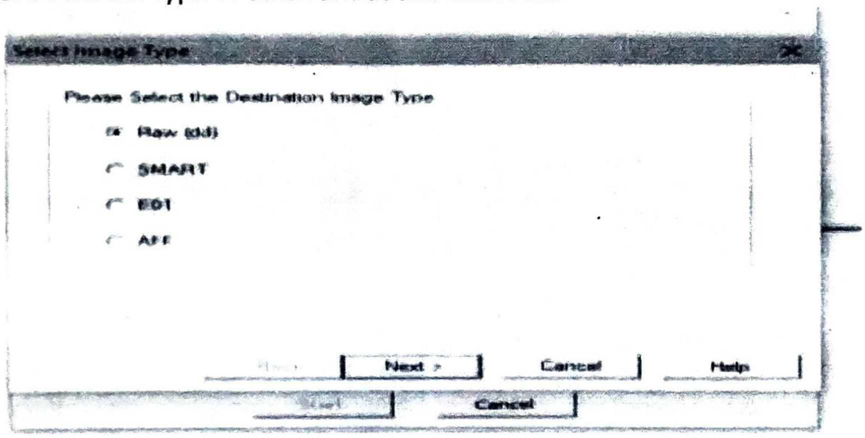
Practical 6

1.Open AccessData FTK Imager. Click on File > Create Disk Image



1.

2. Type the destination path.
3. Click on Logical drive.
4. Click on Add > Browse
5. Select the type of data format and click next


Select Image Type

Please Select the Destination Image Type

- ● Raw (dd)
- ○ SMART
- ○ E01
- ○ AFF

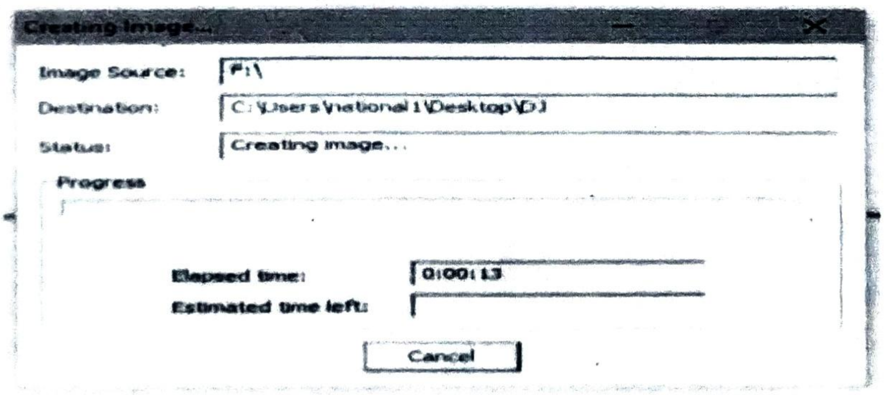

Creating Image...

Image Source: F:\

Destination: C:\Users\national 1\Desktop\D\

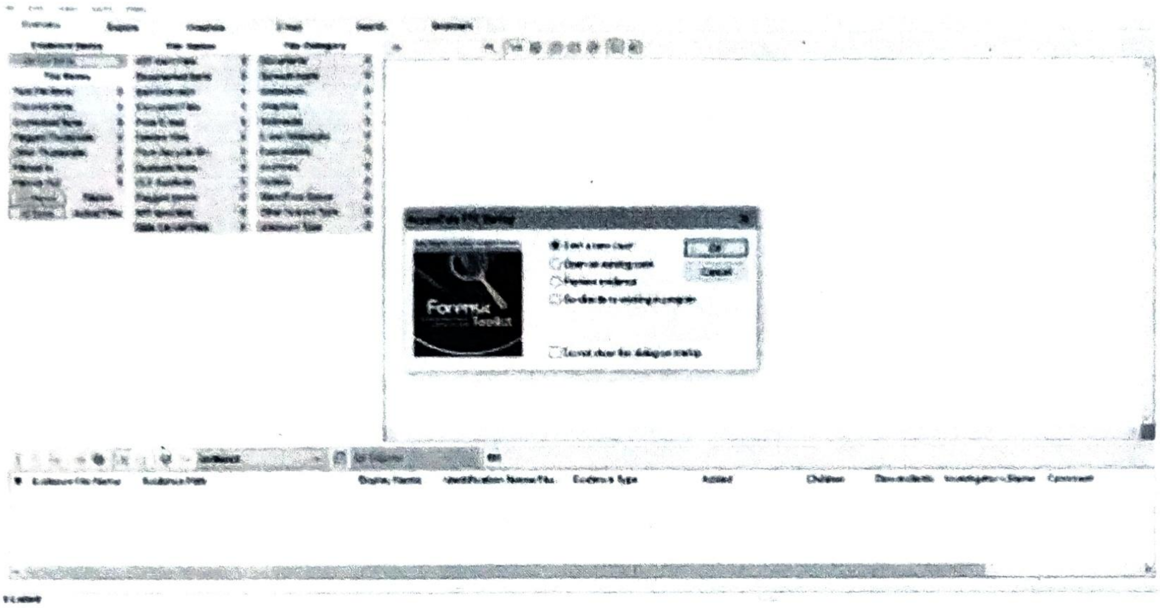
Status: Creating image...

Progress

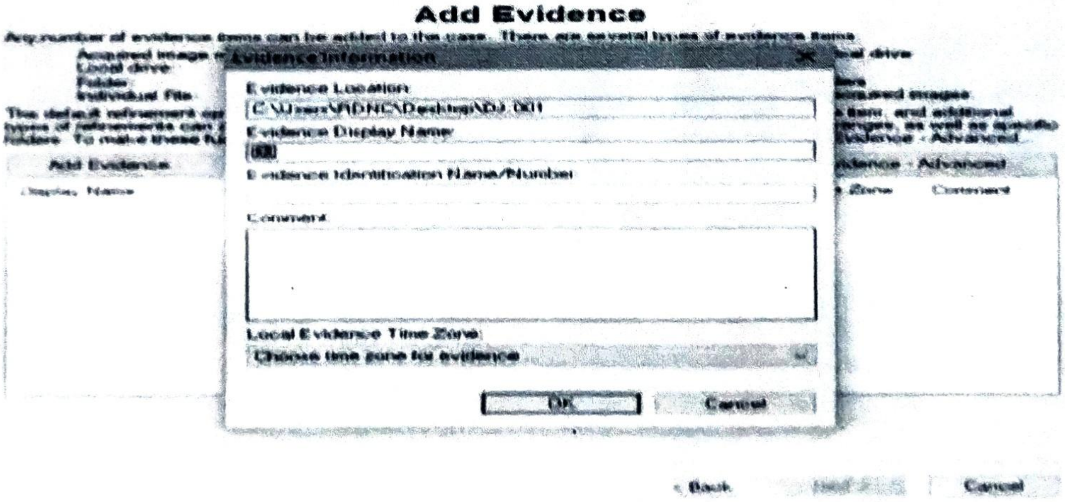
Elapsed time: 0:00:13

Estimated time left:

6. Open the Forensic toolkit and click on file > new case



7. Enter the details and click on next
8. Click on next
9. Click on next
10. Click on next
11. Click on Add Evidence > Acquired Image of Drive > Continue
12. Select the image file
13. Click on OK



Add Evidence

Evidence Information

Evidence Location:
C:\Users\RDNC\Desktop\DJ.001

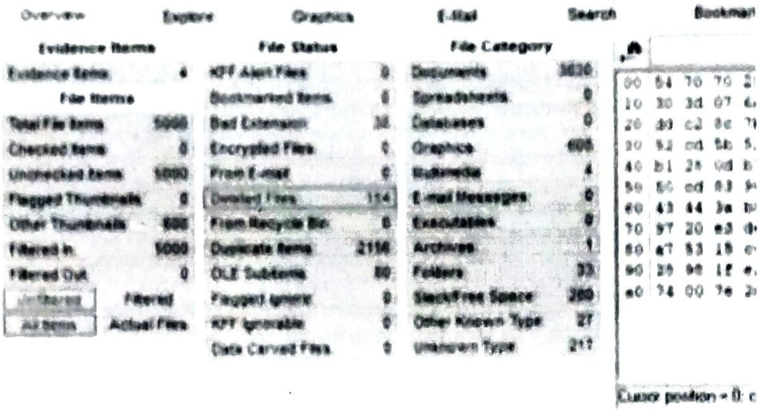
Evidence Display Name:

Evidence Identification Name/Number

Comment

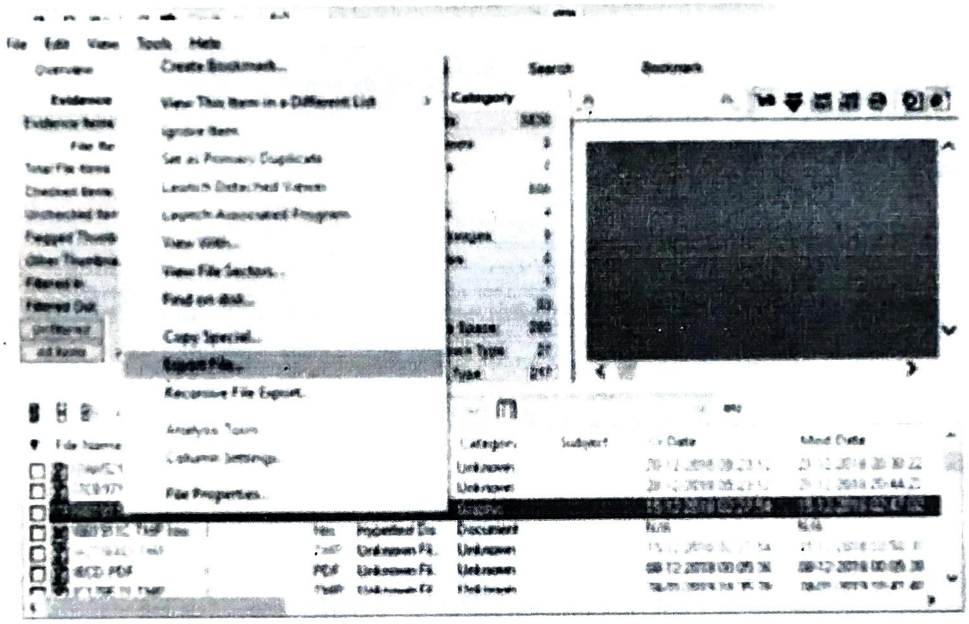
Local Evidence Time Zone:
Choose time zone for evidence

14. Click on next
15. Click on Finish
16. Files are being carving.
17. In the left panel you can see all the recovered files.
18.Click on the Deleted file tab-> Right click on any deleted file to export it

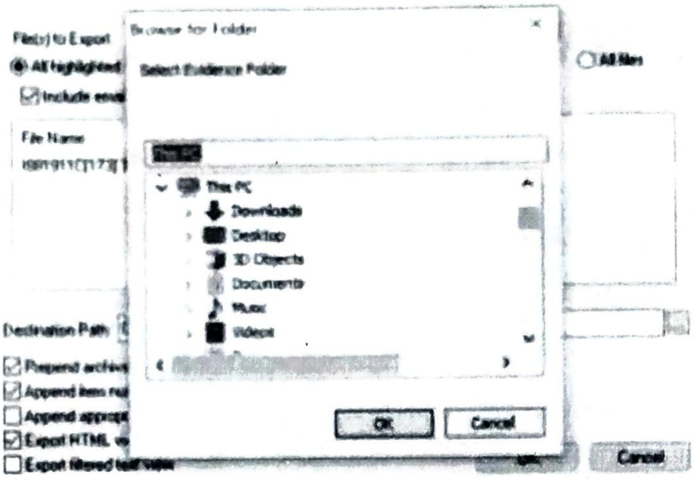


Evidence Items		File Status		File Category	
Evidence Items	4	KFF Alert Files	0	Documents	3830
File Items		Bookmarked Items	0	Spreadsheets	0
Total File Items	5000	Bad Extension	38	Databases	0
Checked Items	0	Encrypted Files	0	Graphics	608
Unchecked Items	5000	From E-mail	0	Multimedia	4
Flagged Thumbnails	0	Deleted Files	114	E-mail Messages	0
Other Thumbnails	608	From Recycle Bin	0	Executables	0
Filtered In	5000	Duplicate Items	2156	Archives	1
Filtered Out	0	OLE Subitems	80	Folders	33
Filtered		Flagged Ignore	0	Slack/Free Space	280
Actual Files		KFF Ignorable	0	Other Known Type	27
		Data Carved Files	0	Unknown Type	217

```
00 54 70 70 2
10 30 3d 07 6
20 d0 c2 8c 7
30 52 cd 5b 5
40 b1 28 0d b
50 56 cd 83 9
60 43 44 3a b
70 97 20 e3 d
80 a7 53 18 c
90 39 98 1f e
a0 74 00 7e 2
```



19.Browse and choose the destination folder to export the deleted file



File(s) to Export

● All highlighted ○ All files

☑ Include email

File Name

@B1911C[173][1

Destination Path

☑ Prepend archive

☑ Append item na

☐ Append appropr

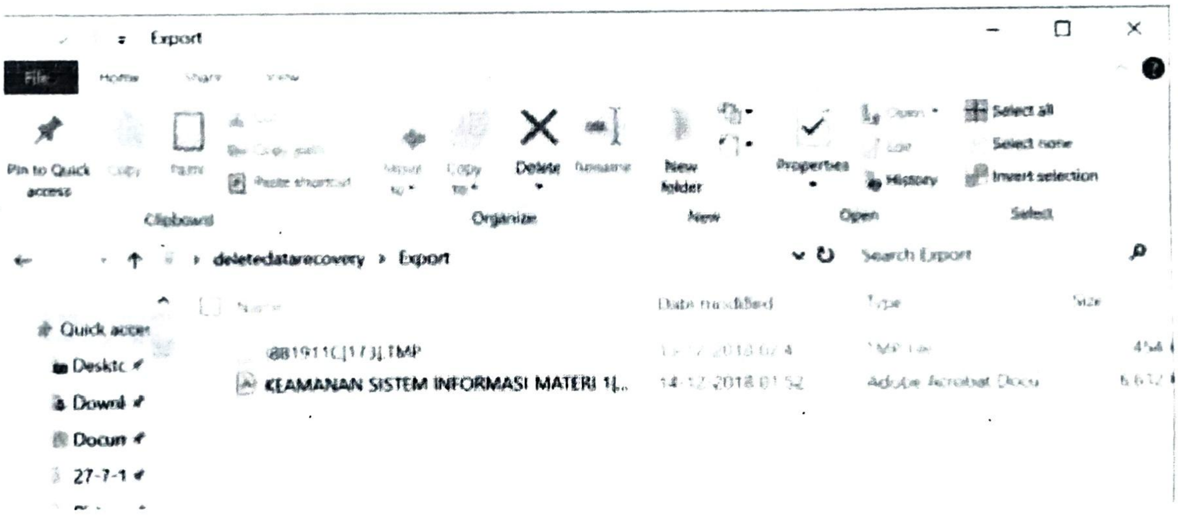
☑ Export HTML vi

☐ Export filtered text view

Browse for Folder

Select Evidence Folder

This PC



Export

deletedatarecovery > Export

Name	Date modified	Type	Size
@B1911C[173].TMP	14-12-2018 02:4	TMP File	454
KEAMANAN SISTEM INFORMASI MATERI 1[...	14-12-2018 01:52	Adobe Acrobat Docu	6.612