Computer Forensics

Part 1 : File carving

1.Look at the data on the file system (Click on Data Sources and look at the hex values on the right). The file system has no files, but why are we able to find items on the disk image? Explain why the file system has no files but there are items that can be found on the disk image.

Ans : Because the files were deleted but not overwritten yet. The file system marks their space as unallocated, so it appears empty, but the contents still exist on the disk. Autopsy has capability to read directly from the disk image.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
f0000281_Nick_is_a_pretty_man_with_a_2003_dc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Unallocated
f0000321.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8037267	Unallocated
f0016021.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	318894	Unallocated
f0016693.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23040	Unallocated
f0016741_Prudent_Engineering_Practice_for_Cr			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1399508	Unallocated
f0019477.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122434	Unallocated
f0019717.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29885	Unallocated
f0019777.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	444314	Unallocated
f0020645.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	99298	Unallocated
f0020841.gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5498	Unallocated
f0020853_moov.mov				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	550653	Unallocated
f0021929.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1036994	Unallocated
f0023957.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11264	Unallocated
f0023981_wword60.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	78899	Unallocated

2. How many objects can you find?

Ans : 14 objects

3. List all the objects here and report on whether or not the content is accessible or damaged/corrupted. Also note which files were actually already deleted.

Ans : Since every file shows an “unallocated” flag, it means every file is already deleted. But every file is still accessible.

Here are some examples. others files I check through extract and open it in local

4. Think securely: If we want to delete files on a magnetic hard disk and not have them be recovered by any tool, what do we need to do? And how much time do you think you need to wipe a 1TB magnetic hard disk?

Ans : Based on Q1 the reason is “files were deleted but not over written yet”, so what we need to do is overwrite it with any data, time usage is fully based on the disk write speed, lets said 150 MB/s (avg HDD write speed) it will take around 1.85 hours.

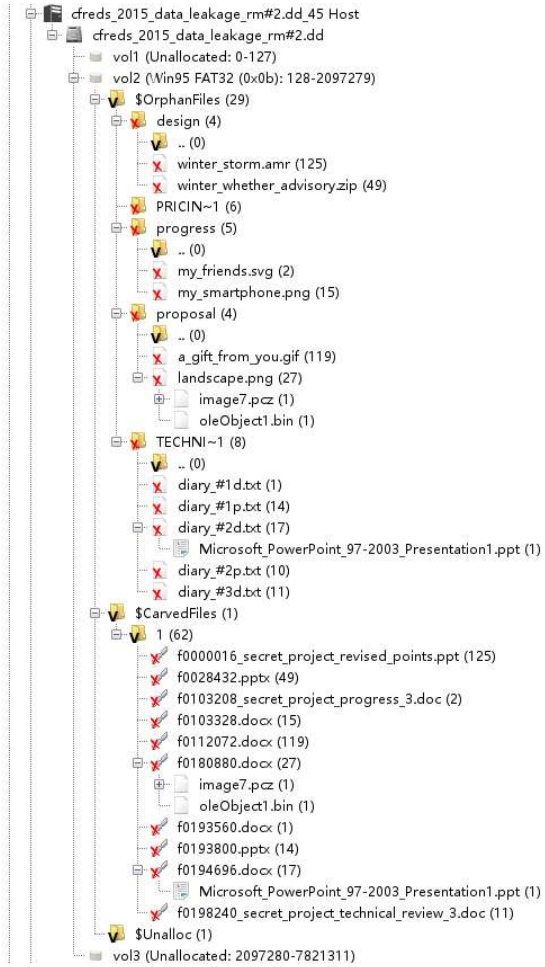
5. Will file carving be able to recover deleted files on an SSD? Why or why not?

Ans : Nope, while HDDs keep deleted data until overwritten, SSDs actively clear it after TRIM. As a result, carving tools find nothing left to reconstruct.

Part 2 : Investigation

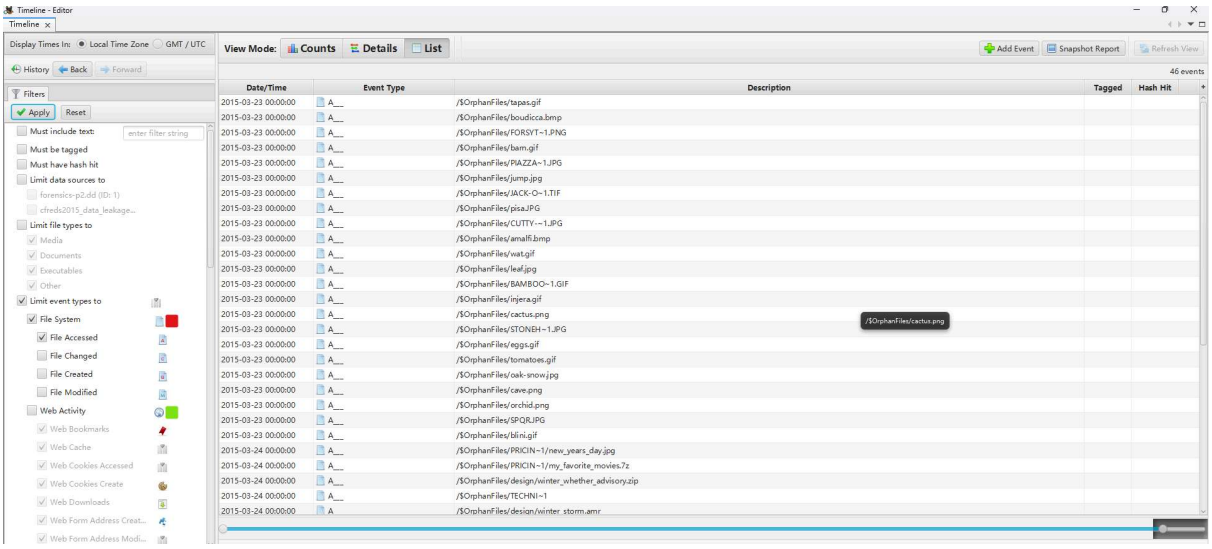
1. List all directories that were traversed in ‘RM#2’.

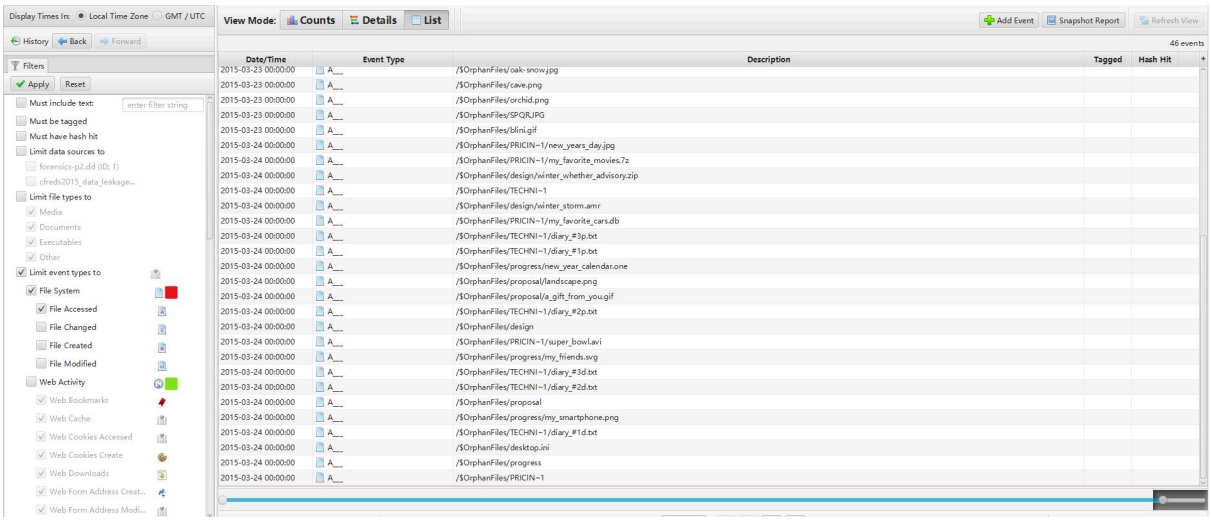
Ans : Picture shows below



2. List all files that were opened in 'RM#2'.

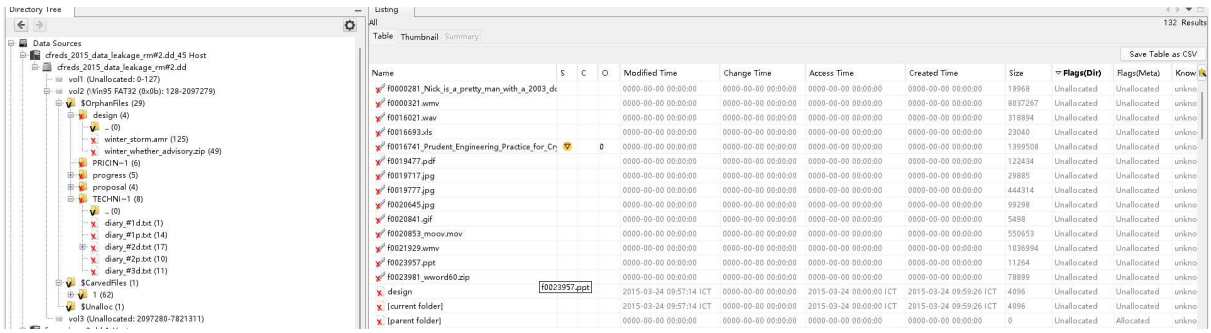
Ans : Showing below, Only filter file accessed operation





3. Recover deleted files from USB drive ‘RM#2’. What files were you able to recover?

Ans :



4. What actions were performed for anti-forensics on USB drive ‘RM#2’?

[Hint: this can be inferred from the results of the above question]

Ans :

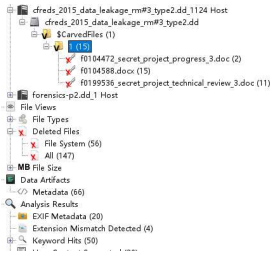
1. Delete file

2. Change file extension (make it even recover still human unreadable).

MIME Type	Extension
application/vnd.openxmlformats-officedocument.wordprocessingml.document	txt
application/vnd.openxmlformats-officedocument.presentationml.presentation	txt
application/vnd.openxmlformats-officedocument.wordprocessingml.document	txt
application/vnd.ms-powerpoint	txt
application/msword	txt
application/vnd.ms-powerpoint	txt

5. Recover hidden files from the CD-R 'RM#3'. What files were you able to recover?

Ans : these 15 files



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0001308_secret_project_revised_points.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14547968	Unallocated	Unallocated	unknown	/img_cfre
f0029724.pptx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16381123	Unallocated	Unallocated	unknown	/img_cfre
f0061720_secret_project_price_analysis_2.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1260544	Unallocated	Unallocated	unknown	/img_cfre
f0064184.xlsx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	100078	Unallocated	Unallocated	unknown	/img_cfre
f0064380.xlsx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10237535	Unallocated	Unallocated	unknown	/img_cfre
f0084376_secret_project_market_shares.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10289152	Unallocated	Unallocated	unknown	/img_cfre
f0104472_secret_project_progress_3.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Unallocated	Unallocated	unknown	/img_cfre
f0104588.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4440235	Unallocated	Unallocated	unknown	/img_cfre
f0113264.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27414	Unallocated	Unallocated	unknown	/img_cfre
f0198632.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1531	Unallocated	Unallocated	unknown	/img_cfre
f0199536_secret_project_technical_review_3.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2360832	Unallocated	Unallocated	unknown	/img_cfre
f0204148_secret_project_technical_review_3.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	325120	Unallocated	Unallocated	unknown	/img_cfre
f0205596.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	780831	Unallocated	Unallocated	unknown	/img_cfre
f0207124.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	777835	Unallocated	Unallocated	unknown	/img_cfre
f0208644.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	620888	Unallocated	Unallocated	unknown	/img_cfre

6. What actions were performed for anti-forensics (data hiding) on CD-R 'RM#3'?

Ans : 1. Delete files and 2. Change to random name so even recover can not easily said its leak sensitive information