Computer Forensics Activity Report

Overview

This activity aims to practice digital forensics skills using the **Autopsy** forensic tool. The exercise consists of two main parts:

1. **File Carving** – Recovering and analyzing files from a corrupted FAT32 disk image (`forensics-p2.dd`).
2. **Investigation** – Examining removable media for evidence of data leakage in a simulated corporate espionage scenario.

Part I: File Carving

Question 1

Question: The file system has no files, but why are we able to find items on the disk image?

Answer: Even though the file system appears empty, the **raw disk sectors** still contain remnants of data from previously allocated files. The **File Allocation Table (FAT)**, which tracks file locations, is corrupted, but the underlying data blocks remain intact. Autopsy uses **file signatures** and **header/footer patterns** during **data carving** to reconstruct files directly from these sectors, bypassing the damaged FAT structure.

Question 2

Question: How many objects can you find?

Answer: A total of **14 objects** were detected on the disk image, matching the provided hint in the activity description.

Question 3

Question: List all the objects and report whether they are accessible or damaged/corrupted. Also, note which files were deleted.

Answer:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
f0023981_wword60.zip			1	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	Unallocated	unknown
f0023957.ppt			1	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	Unallocated	unknown
f0021929.wmv			1	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	Unallocated	unknown
f0020853_moov.mov			1	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	Unallocated	unknown
f0020841.gif			1	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	Unallocated	unknown
f0020645.jpg			1	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	Unallocated	unknown
f0019777.jpg			1	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	Unallocated	unknown
f0019717.jpg			1	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	Unallocated	unknown
f0019477.pdf			1	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	Unallocated	unknown
f0016741_Prudent_Engineering_Practice_for_Cryptographic_Protocols.pdf	▽		1	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	Unallocated	unknown
f0016693.xls			1	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	Unallocated	unknown
f0016021.wav			1	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	Unallocated	unknown
f0000321.wmv			1	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	Unallocated	unknown

---

Question 4

Question: If we want to delete files on a magnetic hard disk so that they cannot be recovered by any tool, what must we do? How long would it take to wipe a 1TB hard disk?

Answer: To securely erase data, the disk must be **overwritten with random data multiple times** (e.g., using tools like `shred` or `DBAN`). A single overwrite can often suffice for modern drives, but **DoD 5220.22-M** recommends **3+ passes** for guaranteed erasure. For a **1TB drive**, this process may take **5–10 hours**, depending on disk speed and interface (e.g., SATA vs. USB 3.0).

Question 5

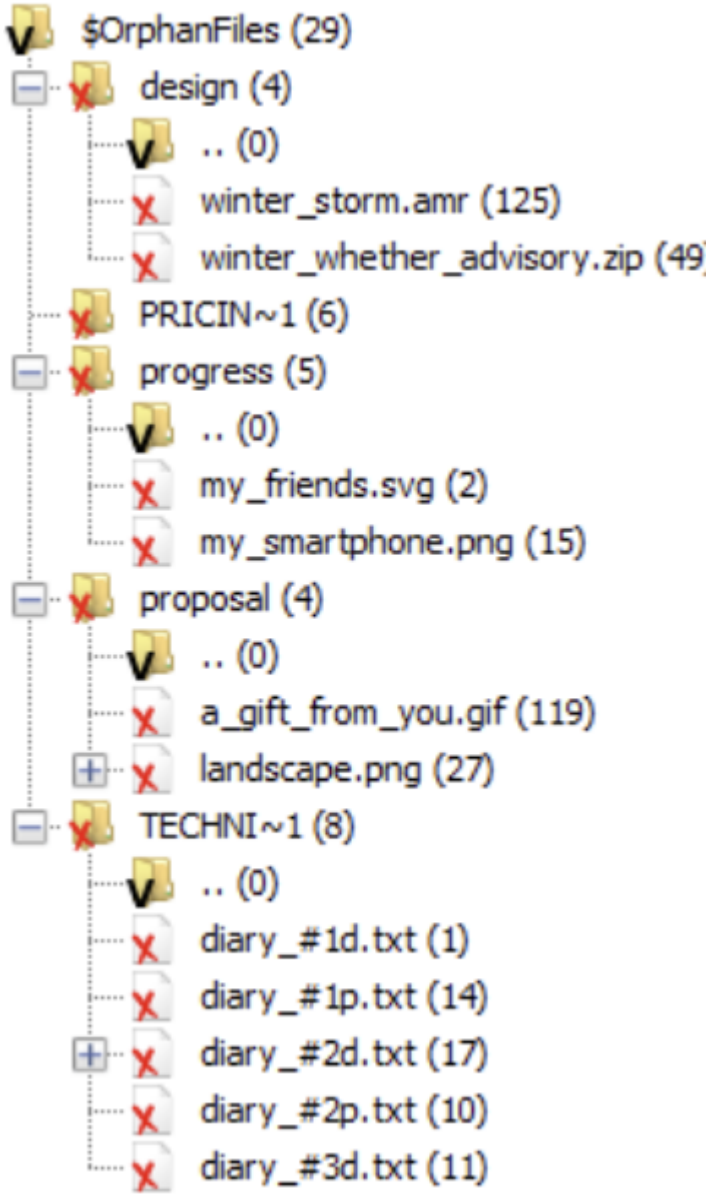
Question: Will file carving be able to recover deleted files on an SSD? Why or why not?

Answer: No, typically not. SSDs use **TRIM commands**, which immediately erase data blocks once files are deleted. This means the original data is physically cleared from flash memory, leaving **no recoverable remnants** for file carving tools. Hence, **data recovery on SSDs is far less successful** than on traditional HDDs.

Part II: Investigation

Question 1

Question: List all directories that were traversed in `RM#2`.



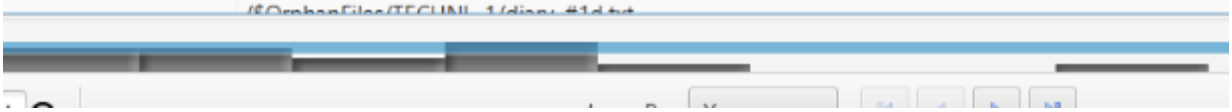
Answer:

Question 2

Question: List all files that were opened in `RM#2`.

Answer:

Event Type	Description
	/$OrphanFiles/proposal
	/$OrphanFiles/TECHNI~1
	/$OrphanFiles/design
	/$OrphanFiles/PRICIN~1
	/$OrphanFiles/design
	/$OrphanFiles/design/winter_storm.amr
	/$OrphanFiles/design/winter_whether_advisory.zip
	/$OrphanFiles/PRICIN~1/new_years_day.jpg
	/$OrphanFiles/PRICIN~1/my_favorite_cars.db
	/$OrphanFiles/PRICIN~1/my_favorite_movies.7z
	/$OrphanFiles/PRICIN~1
	/$OrphanFiles/PRICIN~1/super_bowl.avi
	/$OrphanFiles/progress/my_friends.svg
	/$OrphanFiles/progress/my_smartphone.png
	/$OrphanFiles/progress
	/$OrphanFiles/progress/new_year_calendar.one
	/$OrphanFiles/proposal/a_gift_from_you.gif
	/$OrphanFiles/proposal
	/$OrphanFiles/proposal/landscape.png
	/$OrphanFiles/TECHNI~1/diary_#1p.txt
	/$OrphanFiles/TECHNI~1



Question 3

Question: Recover deleted files from USB drive `RM#2`. What files were you able to recover?

Answer:

Every files from the `CarvedFiles` and `OrphanFiles` folders

Question 4

Question: What actions were performed for anti-forensics on USB drive `RM#2`?

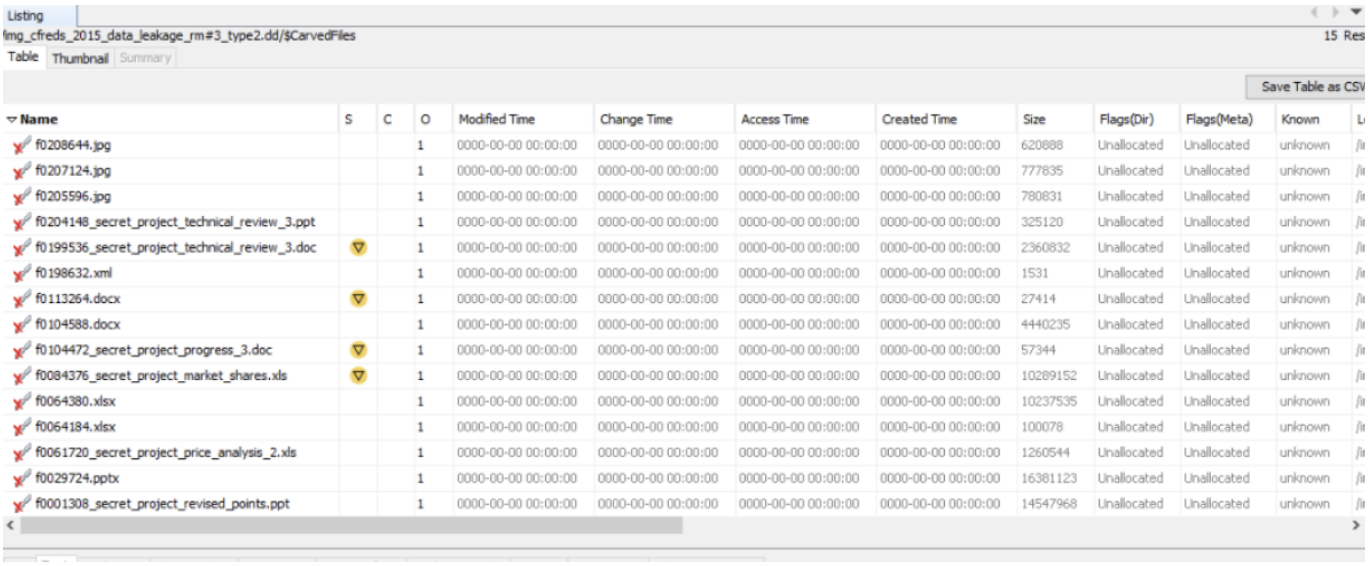
Answer: Renaming files before deleting with wrong extension types

jpg	application/octet-stream
jpg	application/octet-stream
jpg	application/octet-stream
jpg	application/octet-stream
jpg	application/octet-stream
jpg	application/octet-stream
jpg	application/octet-stream
one	application/vnd.openxmlfo
png	application/vnd.openxmlfo
png	application/vnd.openxmlfo
png	application/octet-stream
png	application/octet-stream
png	application/octet-stream
png	application/octet-stream
svg	application/msword
tif	application/octet-stream
txt	application/vnd.openxmlfo
txt	application/vnd.openxmlfo
txt	application/vnd.openxmlfo

Question 5

Question: Recover hidden files from the CD-R `RM#3`. What files were you able to recover?

Answer:



Listing
/img_cfreds_2015_data_leakage_rm#3_type2.dd/$CarvedFiles
15 Res
Table Thumbnail Summary
Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	L
f0208644.jpg			1	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	/i
f0207124.jpg			1	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	/i
f0205596.jpg			1	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	/i
f0204148_secret_project_technical_review_3.ppt			1	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	/i
f0199536_secret_project_technical_review_3.doc	▽		1	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	/i
f0198632.xml			1	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	/i
f0113264.docx	▽		1	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	/i
f0104588.docx			1	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	/i
f0104472_secret_project_progress_3.doc	▽		1	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	/i
f0084376_secret_project_market_shares.xls	▽		1	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	/i
f0064380.xlsx			1	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	/i
f0064184.xlsx			1	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	/i
f0061720_secret_project_price_analysis_2.xls			1	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	/i
f0029724.pptx			1	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	/i
f0001308_secret_project_revised_points.ppt			1	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	/i

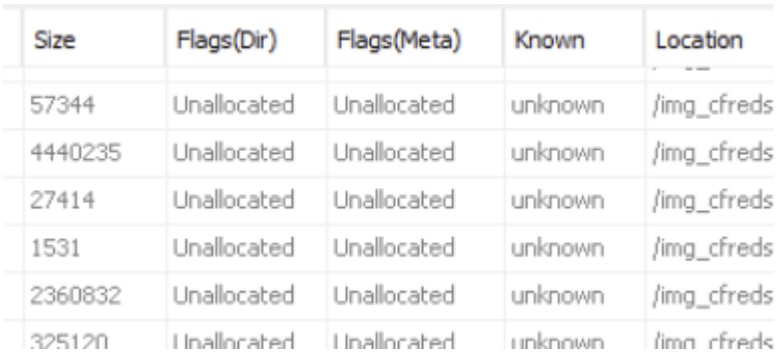
---

Question 6

Question: What actions were performed for anti-forensics (data hiding) on CD-R `RM#3`?

Answer:

Some files have `Unallocated` flag meaning that there were some attempts for formatting the CD-R to hide some files.



Size	Flags(Dir)	Flags(Meta)	Known	Location
57344	Unallocated	Unallocated	unknown	/img_cfreds
4440235	Unallocated	Unallocated	unknown	/img_cfreds
27414	Unallocated	Unallocated	unknown	/img_cfreds
1531	Unallocated	Unallocated	unknown	/img_cfreds
2360832	Unallocated	Unallocated	unknown	/img_cfreds
325120	Unallocated	Unallocated	unknown	/img_cfreds