**CS483 – Digital Forensics**

**File System Forensics Exercise**

Break off into teams of 2 students. Each team will conduct forensic analysis on a suspect’s drive. Your goal is to search for evidence and develop a hypothesis on what happened. Document your steps and your evidence.

**Scenario**: A NIST employee, the suspect, resigned under suspicious circumstances. It is suspected that the employee extracted sensitive classified information from a secret project. The project was conveniently code named as ***secret project***. Specifically, a secret document from this project was renamed and released as a **.jpg** file with an otherwise inconspicuous name. It is unknown how the secrets were removed.

Things you should look for:

* Use of anti-forensics tools
* Evidence of accessing secret documents
* Evidence of exfiltration

**Part 1 – Extract the MBR**

Extract the MBR from the drive image. Recall that the MBR should be in the first sector of the drive (first 512 Bytes). Save the extracted MBR as a separate file and record the hash (SHA256) of the MBR. Using **xxd**, show the raw contents of the MBR and the SHA256 here. Do some quick checks to verify the MBR structure looks correct. What is the disk signature?

**Part 2 – Examine the Partition Table**

Using **mmls**, examine the partition table. Make sure to observe the sector sizes. Screenshot the partition table here:

In the partition table, you should observe two NTFS partitions, and 2 unallocated regions. That first entry, the *Primary Table*, is the MBR you extracted earlier. Using the **dd** utility, carve out each unallocated region and the two partitions such that you now have 5 files: the MBR, two files containing the data in the unallocated space, and two NTFS file systems.

Run the **file** command on each of the extracted partition files to see which operating system was installed.

**Part 3 – Extract Basic Information**

Use **fsstat** to collect some basic information from the volumes.

What is the Volume Serial Number?

Which cluster starts the Master File Table (MFT)?

What is the sector size?

What is the cluster size?

**Part 4 – Mount the File Systems**

**Before you mount anything**, verify you carved them properly using the **file** command and **xxd | head** for a sanity check. For example, one of the partitions should be carved at an offset of **206848** if you set **bs=512** (when bs=1, offsets need to be converted to bytes). Now that the two partitions are carved, you can mount them to your live Linux system. This will allow you to navigate the file system to explore the contents of the suspect’s machine.

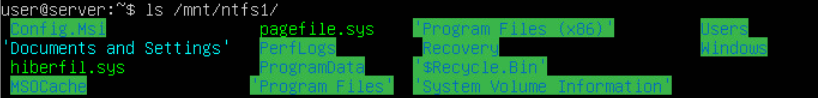
First, create two new directories to serve as mount points:



Next, mount each partition. Here is an example:



Now you can explore the file structure of each partition. One of them does not contain any information. One does contain information. You should be able to quickly identify which partition was the primary one used by the suspect.



Spend some time navigating the files in the interesting partition.

Any interesting user accounts?

**Part 5 – Find the Resignation Letter**

Find the resignation letter. Since it is a doc file, you need to use **pandoc** to view the contents of a doc file in the terminal. Here is a usage example:

**pandoc document.docx | lynx --stdin**

Once you find the resignation letter, you know you’re in the correct user profile. Paste a screenshot of the resignation letter here:

**Part 6 – Evidence of Program Execution**

To find recent applications that were executed, you can consult the Windows Prefetch buffer. Prefetch contains a list of recently executed applications. Its purpose is to increase application load time the next time the application is executed, but it also contains forensic value because it tells you which applications were recently execute. It is located in /Windows/Prefetch



Do you see any interesting programs that were executed that suggest the suspect may have been trying to hide something?

You can corroborate your findings by looking in the user’s **Downloads** folder, and inside the user’s **AppData/Local**. Finally, check the user’s **Recents** folder for recently accessed files.

**Part 7 – Enumerating the File System**

To list all files in the file system use fls. Run this tool against the original dd file (not the carved one), and you need to specify the offset (the first sector of the partition of interest).



The output is very long (a lot of files), so **grep** is helpful if you want to look for specific patterns.

**Part 8 – Finding Deleted Files**

As discovered earlier, the suspect used some anti-forensics tools. As such, they probably deleted incriminating evidence. However, you can still find file names of recently deleted files thanks to the **$FILE\_NAME** attribute in the Master File Table (MFT). Simply add the **-d** flag on **fls** to include deleted files. Again, it is helpful to **grep** to limit your search space. Hopefully your investigation thus far has provided you some intel to tailor your searches.

**Part 9 – Timelining**

You can include the **-l** option on **fls** to include file metadata, including helpful time stamps. If the file was security deleted, then the timelining information is removed. However, you can try to find some evidence surrounding the deleted files to create a hypotheses on when files were accessed and deleted.

**Part 10 – Conclusions**

Based on the evidence you observed, what do you think happened here? Write a paragraph to summarize your findings.

**Part 11 – Optional**

Is there anything interesting in the unallocated drive space?