Phatcharapon Jumruspun 6031040921

Activity XII: Computer Forensics Part I

1. Explain why the file system has no files but there are items that can be found on the disk image.

With the nature of the deletion in hard disk drives, the files do not actually get deleted, instead the metadata is changed to unallocated the supposed deleted area, but the deleted content is still there. The autopsy tool allows user to extract deleted files from unallocated area, and even the data is being completely deleted, the Autopsy tool has a technique called “Carving” to extract the remaining data from the overwritten block as long as it did not completely get overwritten.

2. How many objects can you find?

14 files (objects?) which also contains 2 email addresses

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

File name	Application	Accessibility	Deletion Status
f0019717.jpg	Image	Accessible	Deleted
f0019777.jpg	image	Accessible	Deleted
f0020645.jpg	Image	Accessible	Deleted
f0020853_moov.mov	Video	Corrupted (Encoding not supported 0xc00d5212)	Deleted
f0000321.wmv	Video	Accessible	Deleted
f0021929.wmv	Video	Accessible	Deleted
f0016021.wav	Audio	Accessible	Deleted
f0000281_Nick_is_a_pretty_man_with_a_2003_document.doc	MS Word document	Accessible	Deleted
f0016693.xls	MS Excel document	Accessible	Deleted
f0016741_Prudent_Engineering_Practice_for_Cryptographic_Protocols.pdf	PDF	Accessible	Deleted
f0019477.pdf	PDF	Accessible	Deleted
f0020841.gif	Image	Accessible	Deleted
f0023957.ppt	MS Powerpoint Document	Accessible	Deleted
f0023981_wword60.zip	Zip file	Accessible	Deleted

4. Think securely: If we want to delete files on a magnetic hard disk and not having 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?

We have to overwrite the whole HDD in total of 7 times just to be safe. With the size being 1TB that means we need to overwrite 7TB in total. Assuming the write speed of the HDD is 100 megabytes per second, that would take us $\frac{7 \times 2^{10} \times 2^{10}}{100} = 73400.32\ seconds$ (20.38 hours) in total to overwrite the HDD 7 times.

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

Since SSD does not leave the deleted data like HDD do by automatically wiping “trimmed” data. Which is also is really hard to stop as the SSD will attempt to wipe the data at the moment the SSD is powered. The traditional data carving technique won’t be usable with SDD. But that does not mean extracting deleted data from SSD is impossible, we still can use factory access mode to extract deleted data from SSD, according to this piece of information:

“Generally speaking, SSD imaging via factory access mode requires the following steps.

1. *Prevent SSD controller from booting into “standard” mode by blocking controller’s access to NAND flash chips. This prevents the controller from loading firmware and ensures that no background process can destroy evidence.*
2. *Switch the SSD drive to factory access mode.*
3. *Read SSD firmware and system areas. If necessary, reconstruct damaged translation tables.*
4. *Upload microcode into the SSD controller RAM. Upload translation tables and other system data.*
5. *Boot SSD controller to the code in RAM.*
6. *Use factory access modes to access information on the SSD drive.”*

Source: https://blog.elcomsoft.com/2019/01/life-after-trim-using-factory-access-mode-for-imaging-ssd-drives/