

Activity XII : Computer Forensics

Instructors : Kunwadee Sripanidkulchai, Ph.D.

Part I. 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.

Because the file is still exist on disk. only the meta data that point to file is missing

2. How many objects can you find?

14

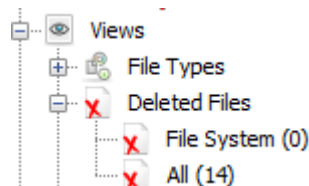
3. List all the objects here and report on whether or not the content is accessible or damaged/corrupted. Also note which files were actually already deleted.

All 14 files is available and may not be damaged

act12 > autopsy > Act12 > Export > 3-\$CarvedFiles >

<input type="checkbox"/> Name	Date modified
f0000281_Nick_is_a_pretty_man_with_...	3/11/2563 10:5
f0000321.wmv	3/11/2563 10:5
f0016021.wav	3/11/2563 10:5
f0016693.xls	3/11/2563 10:5
f0016741_Prudent_Engineering_Practic...	3/11/2563 10:5
f0019477.pdf	3/11/2563 10:5
f0019717.jpg	3/11/2563 10:5
f0019777.jpg	3/11/2563 10:5
f0020645.jpg	3/11/2563 10:5
f0020841.gif	3/11/2563 10:5
f0020853_moov.mov	3/11/2563 10:5
f0021929.wmv	3/11/2563 10:5
f0023957.ppt	3/11/2563 10:5
f0023981_wword60.zip	3/11/2563 10:5

All 14 files has been deleted (Unallocate)



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?

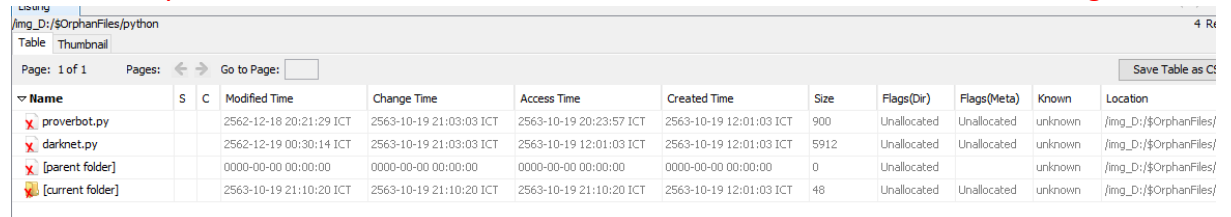
I'll use degaussing device. according to <https://www.drivedegausser.com/degauss-a-hard-drive>, it will take 4-60 seconds.

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

According to <https://www.forensicfocus.com/articles/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/>

Whether deleted files on SSD is depend on OS and available of TRIM command on the SSD hardware.

I tests on my own Drive and found some of deleted files. Notice the unallocated flag



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
proverbot.py			2562-12-18 20:21:29 ICT	2563-10-19 21:03:03 ICT	2563-10-19 20:23:57 ICT	2563-10-19 12:01:03 ICT	900	Unallocated	Unallocated	unknown	/img_Dr/\$OrphanFiles/
darknet.py			2562-12-19 00:30:14 ICT	2563-10-19 21:03:03 ICT	2563-10-19 12:01:03 ICT	2563-10-19 12:01:03 ICT	5912	Unallocated	Unallocated	unknown	/img_Dr/\$OrphanFiles/
[parent folder]			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	unknown	/img_Dr/\$OrphanFiles/
[current folder]			2563-10-19 21:10:20 ICT	2563-10-19 21:10:20 ICT	2563-10-19 21:10:20 ICT	2563-10-19 12:01:03 ICT	48	Unallocated	Unallocated	unknown	/img_Dr/\$OrphanFiles/