Homework 2 Report

Used software:

- OS Win10 64bit
- AccessData FTK Imager 4.2.0.13
- Autopsy 4.12

Task 1

Name: Alex Smith

File name: Alex_Smith.gif

Path: /root_folder/New Folder/Alex_Smith.gif

Creation timestamp: 13.10.2019 at 20:51:00

Modification timestamp: 13.10.2019 at 20:45:20

Size: 761945 bytes

Status: Nothing indicates the file itself was specifically deleted, but the parent folder ("New Folder") has been deleted. So we conclude that the file also was deleted.

Filename: Lucky_f_Bastard.jpg

Path: /root_folder/AGreat Dagain/Lucky_f_Bastard.jpg

Creation timestamp: 13.10.2019 at 20:51:27

Modification timestamp: 13.10.2019 20:49:14

Size: 50544

Status: Neither the file nor the parent folder are marked as deleted in the Hex, but Autopsy have it with the orphan files. So we conclude the file has been deleted.

Name: Owen Phelan

Filename: Owen_Phelan.jpg

Path: /root_folder/New Folder/Owen_Phelan.jpg

Creation timestamp: 13.10.2019 at 20:51:02

Modification timestamp: 13.10.2019 at 20:45:54

Size: 64278

Status: Same status as for “Alex Smith”

Name: Shawn Mendez

Filename: Shawn_Mendez.jpg

Path: /root_directory/?/New Folder/Shawn_Mendez.jpg

Creation timestamp: 13.10.2019 at 20:50:20

Modification timestamp: 13.10.2019 at 20:44:18

Size: 114877

Status: Once again, nothing explicit in the file metadata itself, but the parent folder was deleted. So the file behind was also deleted from a user point of view.

Name: Sylvester Stallone or Arnold Schwarzenegger

Filename: Silverster_Arn.jpg

Path: /root_folder/Silverster_Arn.jpg

Creation timestamp: 13.10.2019 at 20:50:37

Modification timestamp: 13.10.2019 20:46:48

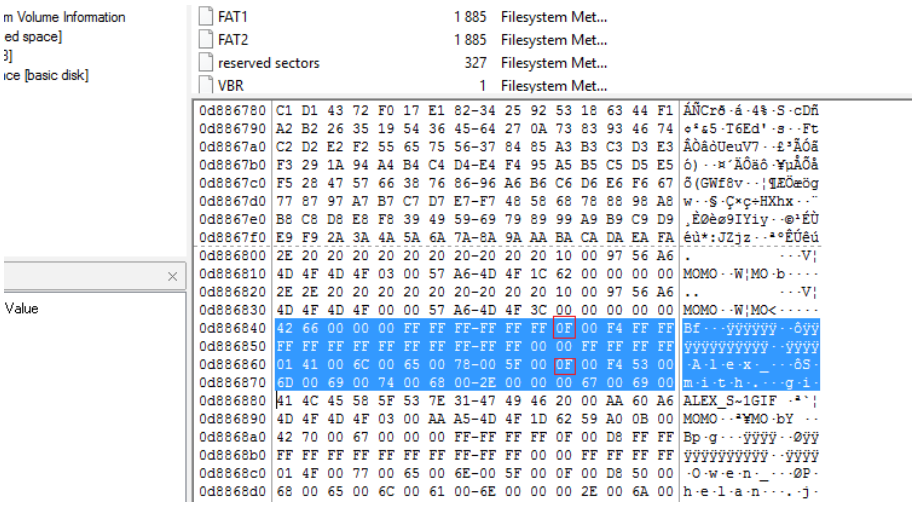
Size: 85083 bytes

Status: The filewas probably deleted, but the only evidence for that, is that it has been classed as an orphan file by Autopsy.

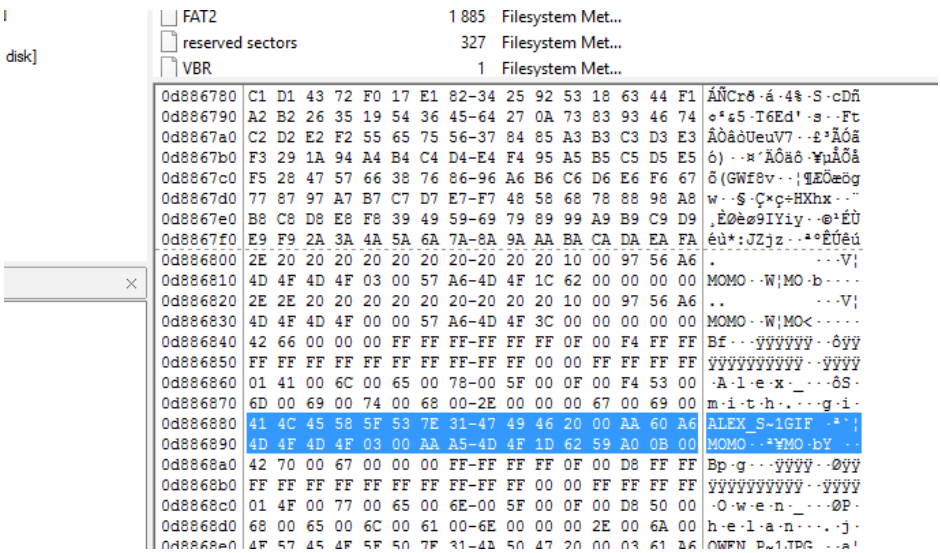
Methodology

I first start examining the image with Autopsy and look up different files. I mainly concentrate on picture files on the first partition. I bookmark the interesting files I found, in order to examine each one of them more in details and extract the required information. Autopsy already provides filename, creation and modification time and the file size.

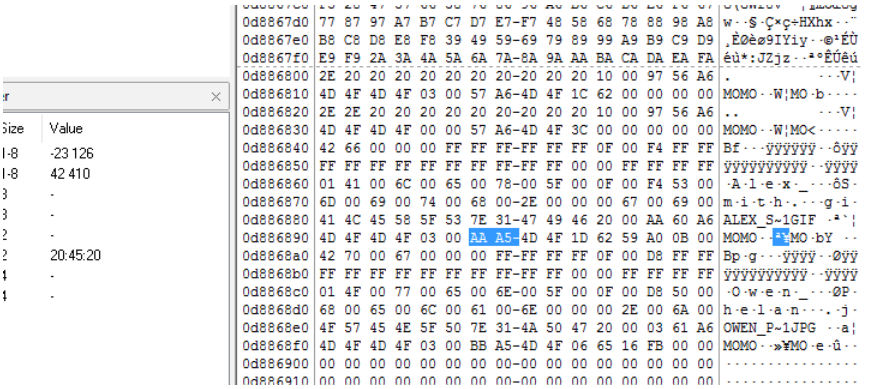
Then I use FTK Imager to find out the other missing information I'm looking for. Knowing the filename, or at least a part of it, I can find the Hex corresponding with a simple search.



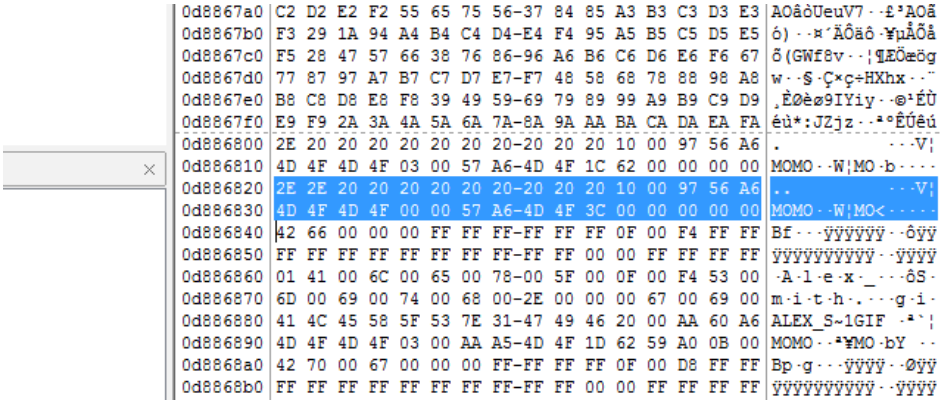
For "Alex Smith" for example, I first start by recovering the file name which is a LFN.



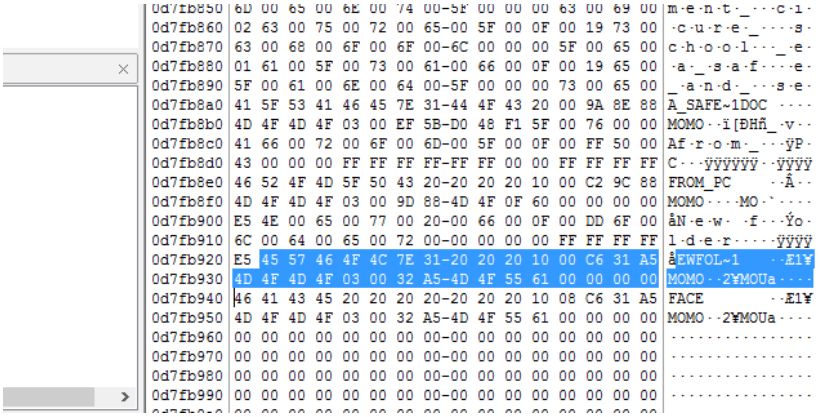
And then I look at the metadata, checking that this the right file, and looking for other information, such as a first bit changed to 0xE5.



Here for example, I can check the last modification time, which corresponds to the result already given by Autopsy. So I am indeed looking at the right file.



Then I reconstruct the path, step by step, by looking and the containing folder and its parent folder. I go up and I look again at its own parent folder … etc, until I reach the “root_folder”.



But by looking at the folder’s metadata, we can notice some details. For example here I see that “New Folder”, which is the parent folder for “Alex_Smith.gif”, has been deleted. That’s how I concluded for status of the file.

I also looked in the metadata to try to find a reason why modification timestamp is before creation timestamp (which is not logic), but I found nothing which could explain it.

Task 2

Filename: estonian_secret_airforce.jpg

Creation timestamp: 13.10.2019 at 17:28:49

Modification timestamp: 13.10.2019 at 20:13:54

Size: 48441

Status: The file was indicated by Autopsy as orphan, so I will assume it was deleted.

Filename: lethal_weapon.jpg

Creation timestamp: 13.10.2019 at 17:28:49

Modification timestamp: 13.10.2019 at 17:16:10

Size: 31385

Status: The file was indicated by Autopsy as orphan, so I will assume it was deleted.

Filename: locked_shields.jpg

Creation timestamp: 13.10.2019 at 17:28:49

Modification timestamp: 13.10.2019 at 17:17:08

Size: 37023

Status: The file was explicitly deleted (with the byte 0x41 found).

Filename: stolen_secret.jpg

Creation timestamp: 13.10.2019 at 17:28:49

Modification timestamp: 13.10.2019 at 17:15:32

Size: 44459

Status: The file was indicated by Autopsy as orphan, so I will assume it was deleted.