

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 file was 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.

m Volume Information	<input type="checkbox"/> FAT1	1 885	Filesystem Met...	
ed space]	<input type="checkbox"/> FAT2	1 885	Filesystem Met...	
3]	<input type="checkbox"/> reserved sectors	327	Filesystem Met...	
ice [basic disk]	<input type="checkbox"/> VBR	1	Filesystem Met...	
	0d886780	C1 D1 43 72 F0 17 E1 82-34 25 92 53 18 63 44 F1	ÃÑCr8-á-4\$-S-0dñ	
	0d886790	A2 B2 26 35 19 54 36 45-64 27 0A 73 83 93 46 74	e+5-76Ed'-s'-Ft	
	0d8867a0	C2 D2 E2 F2 55 65 75 56-37 84 85 A3 B3 C3 D3 E3	Ã0ã0Ueu7'-s'Ã0ã	
	0d8867b0	F3 29 1A 94 A4 B4 C4 D4-E4 F4 95 A5 B5 C5 D5 E5	6)-*-Ã0ã0-Ã0ã0	
	0d8867c0	F5 28 47 57 66 38 76 86-96 A6 B6 C6 D6 E6 F6	ðGWF8v-..ðGWF8g	
	0d8867d0	77 87 97 A7 B7 C7 D7 E7-F7 48 58 68 78 88 98 A8	w-..S-Cç+HXhx-..	
	0d8867e0	B8 C8 D8 E8 F8 39 49 59-69 79 89 99 A9 B9 C9 D9	E0e9I1iy-@EÜ	
	0d8867f0	E9 F9 2A 3A 4A 5A 6A 7A-8A 9A AA BA CA EA FA	éú+;Jzj-..*EÜéú	
	0d886800	2E 20 10 20 20 20 20 20-20 20 10 00 97 56 A6	..-V-	
	0d886810	4D 4F 4D 4F 03 00 57 A6-4D 4F 1C 62 00 00 00 00	MOMO-·WjMO·b-·	
	0d886820	2E 2E 20 20 20 20 20 20-20 20 10 00 97 56 A6	..-V-	
	0d886830	4D 4F 4D 4F 00 00 57 A6-4D 4F 3C 00 00 00 00 00	MOMO-·WjMO<-·	
	0d886840	42 66 00 00 00 FF FF FF-FF FF FF 0F 0F 0F F4 FF FF	Bf-·yyyyyy-6yy	
	0d886850	FF FF FF FF FF FF FF FF-FF FF FF 0F 0F FF FF FF	yyyyyyyyyy-·yyyy	
	0d886860	01 41 00 6C 00 65 00 78-00 5F 00 0F 0F F4 53 00	-A-l-e-x-·-6S	
	0d886870	6D 00 69 00 74 00 68-0E 2E 00 00 67 00 69 00	m-i-t-h-·-g-i	
	0d886880	11 4C 45 58 5F 53 7E 31-47 49 46 20 00 AA 60 A6	ALEX-S-IGIF-·*!	
	0d886890	4D 4F 4D 4F 03 00 AA A5-4D 4F 1D 62 59 A0 0B 00	MOMO-·*YMO·bY-·	
	0d8868a0	42 70 00 67 00 00 FF FF-FF FF FF 0F 0F D8 FF FF	Bp-g-·yyyy-0yy	
	0d8868b0	FF FF FF FF FF FF FF FF-FF FF FF 0F 0F FF FF FF	yyyyyyyyyy-·yyyy	
	0d8868c0	01 4F 00 77 00 65 00 6E-00 5F 00 0F 0F D8 50 00	-O-w-e-n-·-0P-	
	0d8868d0	68 00 65 00 6C 00 61 00-6E 00 00 00 2E 00 6A 00	h-e-l-a-n-·-l-	

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

	FAT2	1885	Filesystem Met...	
	reserved sectors	327	Filesystem Met...	
	VBR	1	Filesystem Met...	
disk]				
	0d886780	C1 D1 43 72 F0 17 E1 82-34 25 92 53 18 63 44 F1	ÃÑCrð-á-4%-S-cDñ	
	0d886790	A2 B2 26 35 19 54 36 45-64 27 0A 73 83 93 46 74	e's5-T6Ed' s-Ft	
	0d8867a0	C2 D2 E2 F2 55 65 75 56-37 84 85 A3 B3 C3 D3 E3	ÃôâðUeuV7-z*Ãôâ	
	0d8867b0	F3 29 1A 94 A4 B4 C4 D4-E4 F4 95 A5 B5 C5 D5 E5	ò)-x'Ãôâð-VnÃôÂ	
	0d8867c0	F5 28 1F 57 66 38 76 86-96 A6 B6 C6 D6 E6 F6	ð(GWfëv-..ÏEÖèBg	
	0d8867d0	77 87 97 A7 B7 C7 D7 E7-F7 48 58 68 78 88 98 A8	w-S-Ç×ç-HXhx..	
	0d8867e0	B8 C8 D8 E8 F8 39 49 59-69 79 89 99 A9 B9 C9 D9	EöèøIYiyi-y·EU	
	0d8867f0	E9 F9 2A 3A 4A 5A 6A 7A-8A 9A AA BA CA DA EA FA	éú*:JZjz-z·EÜéú	
	0d886800	2E 20 20 20 20 20 20 20-20 20 20 10 00 97 56 A6	.-...-V!	
	0d886810	4D 4F 4D 4F 03 00 57 A6-4D 4F 1C 62 00 00 00 00	MOMO-W!M0-b-...	
	0d886820	2E 2E 20 20 20 20 20 20-20 20 20 10 00 97 56 A6	..-...-V!	
	0d886830	4D 4F 4D 4F 00 00 57 A6-4D 4F 3C 00 00 00 00 00	MOMO-W!M0<-...	
	0d886840	42 66 00 00 00 FF FF FF-FF FF FF 0F 00 F4 FF FF	Bf--yyyyyyy-ðyy	
	0d886850	FF FF FF FF FF FF FF FF-FF 00 00 FF FF FF FF	yyyyyyyyyyy-yyy	
	0d886860	01 41 00 6C 00 65 00 78-0F 5F 0F 0F 0F F4 53 00	-A-l-e-x-...-ðS-	
	0d886870	6D 00 69 70 04 70 68 00-2E 00 00 00 67 00 69 00	m-i-t-h-...-g-l-	
	0d886880	41 4C 45 58 5F 53 7E 31-47 49 46 20 00 AA 60 A6	ALEX_S-IGF-*!	
	0d886890	4D 4F 4D 4F 03 00 AA A5-4D 4F 1D 62 59 A0 0B 00	MOMO~*yMO-by ..	
	0d8868a0	42 70 00 67 00 00 00 FF-FF FF FF 0F 00 D8 FF FF	Bp-g-...yyyy-Øyy	
	0d8868b0	FF FF FF FF FF FF FF FF-FF 00 00 FF FF FF FF	yyyyyyyyyyy-yyy	
	0d8868c0	01 4F 00 77 00 65 00 6E-00 5F 0F 0F 0F D8 50 00	-O-w-e-n-...-ØP-	
	0d8868d0	68 00 65 00 6C 00 61 01-6E 00 00 00 2E 00 6A 00	he-l-a-n-...-j-	
	0d8868e0	4F 57 45 4F 5F 50 7E 31-4E 50 47 20 00 03 61 26	OWN-P-1-IDC-...-l	

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

	r	Size	Value	
1-8	-23	126		
1-8	42	410		
3	.			
3	.			
2	.			
2	.			
1	20:45:20			
1	.			
1	.			

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.

	0d8867a0	C2 D2 E2 F2 55 65 75 56-37 84 85 A3 B3 C3 D3 E3	A0A0UeuV7·-f·AOA
	0d8867b0	F3 29 1A 94 A4 B4 C4 D4-E4 F4 95 A5 B5 C5 D5 E5	ò)·-·AOA0-YnAOA
	0d8867c0	F5 28 47 57 66 38 76-86 A6 B6 C6 D6 E6 F6 67	d(GWfev···LEOag
	0d8867d0	77 87 97 A7 B7 C7 D7 E7-F7 48 58 68 78 88 98 A8	w·-S·C·c-HXhx·
	0d8867e0	B8 C8 D8 E8 F8 39 49 59-69 79 89 9A 9B 9C 9D 9E	,EOe09IYiy·@·EU
	0d8867f0	E9 F9 2A 3A 4A 5A 6A 7A-8A 9A AA BA CA DA FA	éú*:JzJz·-*Éúéú
	0d886800	2E 20 20 20 20 20 20-20 20 20 10 00 97 56 A6	. ····V;
	0d886810	4D 4F 4D 4F 03 00 57 A6-4D 4F 1C 62 00 00 00 00	MOMO·-W;MO·b·
x	0d886820	2E 2E 20 20 20 20 20-20 20 20 10 00 97 56 A6	...·-·V;
	0d886830	4D 4F 4D 4F 00 00 57 A6-4D 4F 3C 00 00 00 00 00	MOMO·-W;MO<·-
	0d886840	42 66 00 00 00 FF FF FF-FF FF FF 0F 00 F4 FF FF	Bf···YyyyYyY·ôyy
	0d886850	FF FF FF FF FF FF FF FF-FF FF FF 00 FF FF FF FF	YyyYyyYyyYy·YyyY
	0d886860	01 41 00 6C 00 65 00 78-00 5F 00 0F 00 F4 53 00	-A-l-e-x···ôS
	0d886870	6D 00 69 00 74 00 68-00-2E 00 00 67 00 69 00	m-i-t-h···g-i
	0d886880	41 4C 45 58 5F 53 7E 31-47 49 46 20 00 AA 60 A6	ALEX_S-1GIF·^;
	0d886890	4D 4F 4D 4F 03 00 AA A5-4D 4F 1D 62 59 A0 0B 00	MOMO·-YMO-by·
	0d8868a0	42 70 00 67 00 00 00 FF-FF FF FF 0F 00 D8 FF FF	Bp·g··YyyY·ôYy
	0d8868b0	FF FF FF FF FF FF FF FF-FF FF FF 00 FF FF FF FF	YyyYyyYyyYy·YyyY

Then I reconstruct the path, step by step, by looking at 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”.

	0d7fb890	6D 00 65 00 6E 00 74 00-5F 00 00 00 63 00 69 00	m-e-n-t-...c-l
	0d7fb8b0	02 63 00 75 00 72 00 65-00 5F 00 0F 00 19 73 00	c-o-u-r-...e-
	0d7fb8f0	63 00 68 00 6F 00 6F 00-6C 00 00 5F 0F 65 00	c-h-o-o-l-...s-
	0d7fb880	01 61 00 5F 00 73 00 61-00 66 00 0F 00 19 65 00	a-s-a-f-e-...
	0d7fb890	5F 00 61 00 6E 00 64 00-5F 00 00 73 00 65 00	_and...se-
	0d7fb8a0	41 5F 53 41 46 45 7E 31-44 4F 43 20 00 9A 8E 88	A_SAFE-1DOC ...
	0d7fb8b0	4D 4F 4D 4F 03 00 EF 5B-0D 48 F1 5F 00 76 00 00	MOMO - i[BHA] v...
	0d7fb8c0	41 66 00 72 00 6F 00 6D-00 5F 00 0F 00 FF 50 00	Af-x-o-m-...yp-
	0d7fb8d0	43 00 00 00 FF FF FF FF-FF FF 00 0F FF FF FF C	C-yyy-yyyy-yy-y
	0d7fb8e0	46 52 4F 4D 5F 50 43 20-20 20 20 00 C2 9C 88	FROM_PC ...Ä
	0d7fb8f0	4D 4F 4D 4F 03 00 9D 88-4D 4F 0F 60 00 00 00 00	MOMO-...MO...
	0d7fb900	E5 4E 00 65 00 77 00 20-00 66 00 0F 00 DD 6F 00	än-e-w- f-...Yo
	0d7fb910	6C 00 64 00 65 00 72 00-00 00 00 00 FF FF FF FF	l-d-e-r-...yy-y
	0d7fb920	E5 45 57 46 4F 4C 7E 31-20 20 20 10 00 C6 31 A5	ÄEWOL-1 ...ELY
	0d7fb930	4D 4F 4D 4F 03 00 32 A5-4D 4F 55 61 00 00 00 00	MOMO - 2YMODa...
	0d7fb940	46 41 43 45 20 20 20 20-20 20 20 20 10 08 C6 31 A5	FACE ...ELY
	0d7fb950	4D 4F 4D 4F 03 00 32 A5-4D 4F 55 61 00 00 00 00	MOMO - 2YMODa...
	0d7fb960	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
	0d7fb970	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
	0d7fb980	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
	0d7fb990	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

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.