



CY2002

Digital Forensics

Assignment 04 **ADS and EFS files**

Submitted by: Abdul Sami Qasim

Roll number: 22i-1725

Date: October 25, 2024

Table of Contents

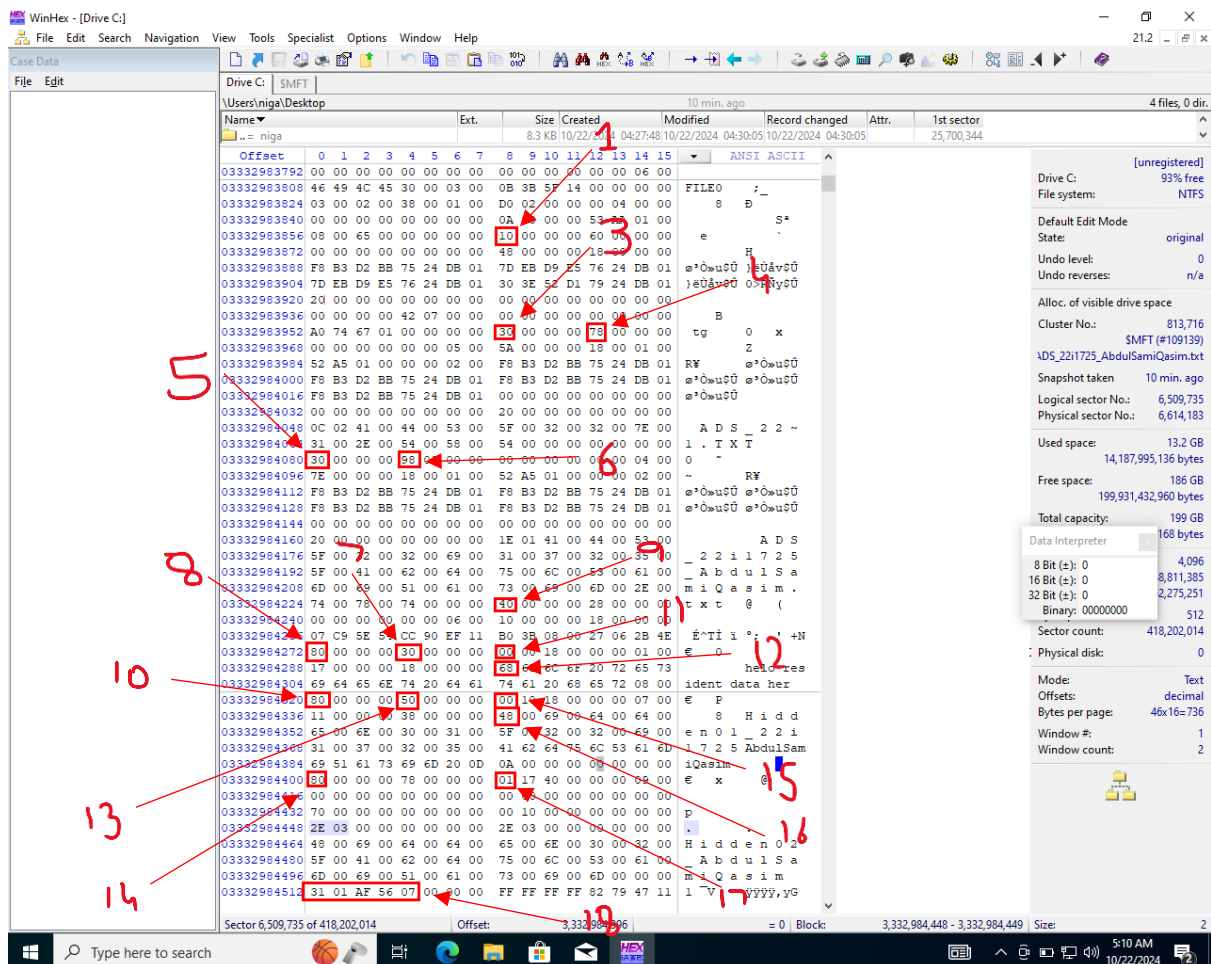
• Introduction	2
• Details and Steps	2
Question 1.....	2
Question 2.....	6
Question 3.....	9
• Summary	11
• References	11

• Introduction

The assignment revolves around the use of winhex to read the MFT entries for ADS file streams and EFS encrypted files.

• Details and Steps

Question 1



1. Attribute 0x10
2. -
3. Attribute 0x30
4. Size of 0x30 (0x78h bytes)
5. Attribute 0x30
6. Size of 0x30 (0x98h bytes)
7. Size of Attribute 0x80 (0x30h bytes)
8. Attribute 0x80
9. Attribute 0x40
10. Attribute 0x80
11. Flag for resident/non-resident (resident here as it is 00)
12. Start of data
13. Size of 0x80 attribute (0x50h bytes)

14. Attribute 0x80
15. Flag for resident/non-resident (resident as it is 00)
16. Start of data
17. Flag for resident/non-resident (non-resident as it is 01)
18. Datarun

This datarun has 3 components,

1. The first byte representing size of total datarun after that byte and individual sizes of second and third components.
2. The next component (size 01) represents the total cluster numbers
3. The last component (size 03) represents the LCN (logical cluster number) of the file content

WinHex - [Drive C:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

Drive C:

\\$Recycle.Bin\S-1-5-21-3557107667-3964680910-433341467-1001

8 min. ago

1+1=2 files, 0 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
..	Bin	0.6 KB	12/07/2019 02:14:52	10/22/2024 04:28:47	10/22/2024 04:28:47	SH	6,291,578

Offset: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

ANSI ASCII

FILE0 Eä0B

S p

*8

H

ä°öuüü ää üüüü

ä..äüüü üüüü/äü

B

Pée 0 x

Z

RW ä°öuüü

Ääüüü Ääüüü

Ääüüü Ääüüü

E F S ~ 2 2 ~

1 . T X T

0 ~

RW

ä°öuüü Ääüüü

Ääüüü Ääüüü

E F S

2 2 i 1 7 2 5

A b d u l S a

m i Q a s i m .

t x t @ (

É~TÍ i °; ' +N

€ H @

1 ä7 P

H

°

* \$ E F S

1 57 üüüü,yG

1 e7 P

H

ø

\$ E F S

Sector 6,511,700 of 418,202,014

Offset: 3,333,990,512

= 32 Block: 14,971,584,467 - 14,971,584,483

Size: 17

Activate Windows
Go to Settings to activate Windows.

Drive C: [unregistered]
File system: NTFS

Default Edit Mode: original

State: original

Undo level: 0

Undo reverses: n/a

Alloc. of visible drive space

Cluster No.: 813,962

SMFT (#110122)

EFS_2211725_AbdulSamiQasim.txt

Snapshot taken: 11 min. ago

Logical sector No.: 6,511,700

Physical sector No.: 6,616,148

Used space: 22.1 GB

23,692,075,008 bytes

Free space: 177 GB

190,427,353,088 bytes

Total capacity: 199 GB

214,119,431,168 bytes

Bytes per cluster: 4,096

Free clusters: 46,491,053

Total clusters: 52,275,251

Bytes per sector: 512

Sector count: 418,202,014

Physical disk: 0

Mode: hexadecimal

Offsets: decimal

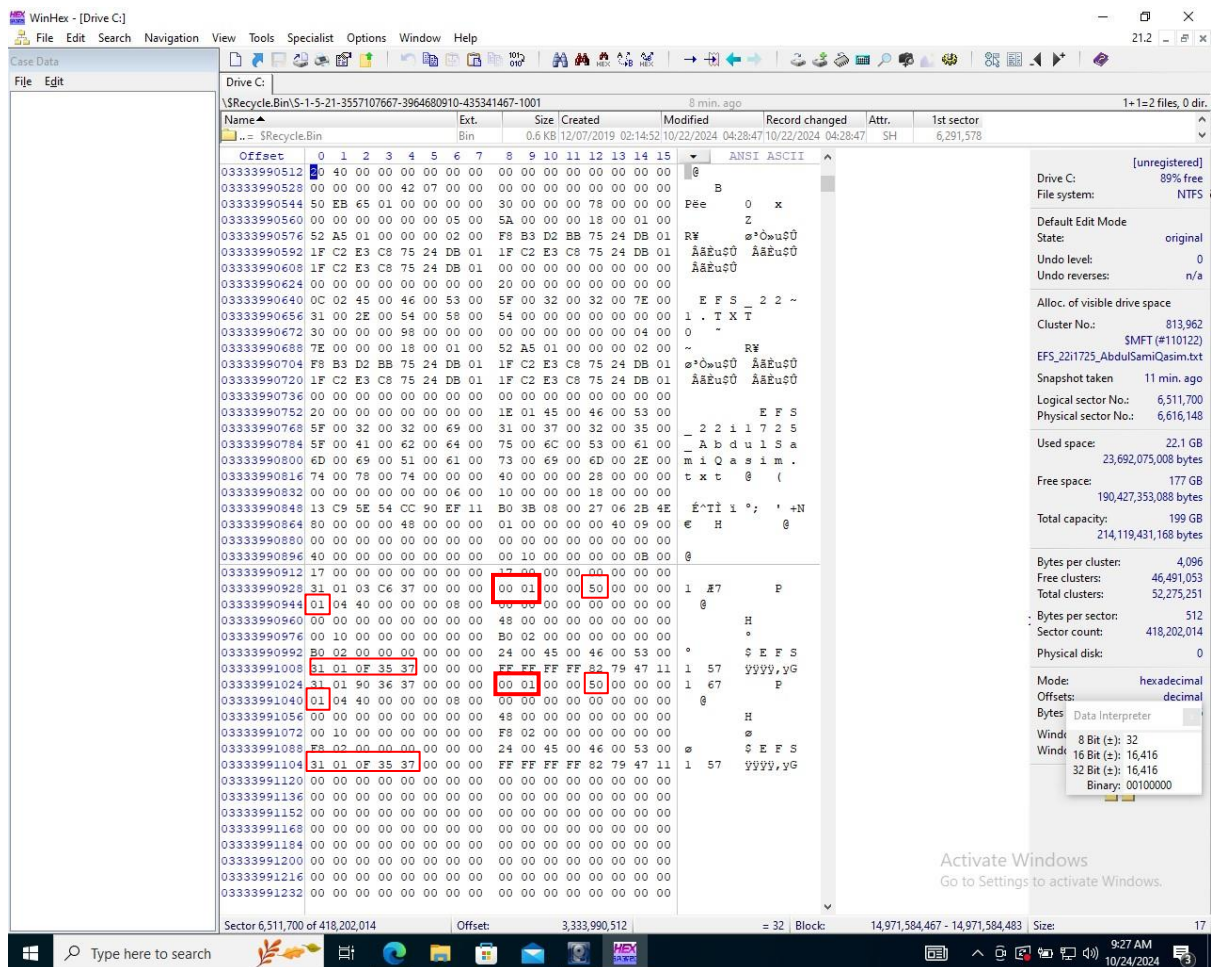
Bytes: Data Interpreter

Windo: 8 Bit (±): 32

Windo: 16 Bit (±): 16,416

Windo: 32 Bit (±): 16,416

Binary: 00100000



There are two 0x100 attributes, one is the DDF (Data Decryption Field) and the other is the DRF (Data Recovery Field). The FEK and FEKI both are non-resident, as suggested by the 01 flag on the 8th offset byte from the start of the attribute.

THE FEK is located here (highlighted in light blue is the FEK):

The hexes highlighted in red mark the start of the FEK1 which goes on till the beginning of the FEK (the block highlighted in blue)

WinHex - [Drive C:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

Drive C: EFS_221725_AbdulSamiQasim\...

0 min. ago

13 files, 13+0=14 dir.

Name▲	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Path unknown							
Offset	0	1	2	3	4	5	6
03332983792	00	00	00	00	00	00	00
03332983808	46	49	4C	45	30	03	00
03332983824	03	00	01	00	38	00	01
03332983840	00	00	00	00	00	00	00
03332983856	10	00	64	00	00	00	00
03332983872	00	00	00	00	00	00	00
03332983888	F8	B3	D2	BB	75	24	DB
03332983904	B5	72	14	73	2F	26	DB
03332983920	20	00	00	00	00	00	00
03332983936	00	00	00	00	2E	0B	00
03332983952	F8	23	43	10	00	00	00
03332983968	00	00	00	00	00	0A	00
03332983984	0F	AC	01	00	00	02	00
03332984000	7D	EB	D9	E5	76	24	DB
03332984016	2D	A9	E3	80	28	26	DB
03332984032	17	00	00	00	00	00	00
03332984048	0C	03	24	00	52	00	00
03332984064	57	00	2E	00	74	00	78
03332984080	40	00	00	00	28	00	00
03332984096	10	00	00	00	18	00	00
03332984112	80	B3	08	00	27	06	2B
03332984128	00	00	18	00	00	01	00
03332984144	68	65	6C	6F	20	72	65
03332984160	76	61	20	68	65	72	65
03332984176	00	10	18	00	00	00	07
03332984192	48	00	69	00	64	00	64
03332984208	5F	00	32	00	32	00	69
03332984224	41	62	64	75	6C	53	61
03332984240	0A	00	00	00	00	00	00
03332984256	01	17	40	00	00	00	09
03332984272	00	00	00	00	00	00	00
03332984288	00	10	00	00	00	00	00
03332984304	2E	03	00	00	00	00	00
03332984320	65	00	6E	00	30	00	32
03332984336	75	00	6C	00	53	00	61
03332984352	73	00	69	00	6D	00	00
03332984368	FF	FF	FF	FF	82	79	47
03332984384	69	51	61	73	69	6D	20
03332984400	80	00	00	00	78	00	00
03332984416	00	00	00	00	00	00	00
03332984432	70	00	00	00	00	00	00
03332984448	2E	03	00	00	00	00	00
03332984464	48	00	69	00	64	00	64
03332984480	5F	00	41	00	62	00	61
03332984496	6D	00	69	00	51	00	61
03332984512	31	01	AF	56	07	00	00

Sector 6,509,734 of 418,202,014 Offset: 3,332,984,296 = 46 Block: 14,971,584,467 - 14,971,584,483 Size: 17

[unregistered]
Drive C:
File system: NTFS
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Alloc. of

1. Second 0x30 attribute is removed
2. Name of the .txt changed
3. Resident data remained the same and the hidden files are still intact
4. There are two same 0x80 attributes

WinHex - [Drive C:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

Drive C:

\\\$Recycle.Bin\\S-1-5-21-3557107667-3964680910-435341467-1001 1 min. ago 3 files, 0 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
..	Bin	0.6 KB	12/07/2019 02:14:52	10/22/2024 04:28:47	10/22/2024 04:28:47	SH	6,291,578
..	Bin	376 B	10/22/2024 04:28:47	10/24/2024 11:27:26	10/24/2024 11:27:26	SH	6,510,622
SRPE0HD.txt	txt	134 B	10/24/2024 11:27:26	10/24/2024 11:27:26	10/24/2024 11:27:26	A	6,504,604
SRPE0HD.txt	txt	23 B	10/22/2024 04:30:01	10/22/2024 04:30:52	10/24/2024 11:27:26	EAI	29,241,368
desktop.ini	ini	129 B	10/22/2024 04:28:47	10/22/2024 04:28:47	10/22/2024 04:28:47	SHA	6,510,624

Offset: 0 1 2 3 4 5 6 7 8 9 A B C D E F

ANSI ASCII

037C602FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

037C602FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

037C602FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

037C603000 D9 54 39 1A 47 2B A1 2F BB 39 3E 07 C2 58 7F 54

037C603010 89 09 3A B6 BC 37 6C E2 60 0A D7 A4 CA F3 E2 9D

037C603020 81 BD 6F 97 4C EB 7C BA 00 D2 09 77 16 02 4C 44

037C603030 7A BD 18 80 4A 43 C1 23 B4 2E D2 36 31 4B 0C D6

037C603040 85 60 5D 0A D8 79 46 94 AE AE 71 06 5A C7 7F B2

037C603050 57 A7 CC 54 1D 1E AF FD 8A 3F 3B 9F FC 45 AA AB

037C603060 C7 04 CB 8B 1C 59 F6 0E 69 C0 43 F9 B7 35 32 AC

037C603070 C2 0B 33 D9 87 80 64 FC 83 42 40 E4 0E FF F4 AB

037C603080 71 5E 77 4E C7 5E 9D 46 B4 93 3C 21 09 F6 04 D3

037C603090 98 2F E1 86 13 2E F1 B1 6F C6 C5 26 F2 E0 5C 65

037C6030A0 69 DB 67 D9 8B ED 9E 05 73 94 38 5A D9 DA 64 84

037C6030B0 71 8C F5 D4 50 3C 88 0A A6 BE 5D 3A 1B 3A E0 E8

037C6030C0 13 BA C9 67 7F 20 2C 50 F1 0B EF 8D 60 AC 8D A4

037C6030D0 DB F9 B4 EE 9E FB 62 06 1F CF A4 82 D1 31 8A 1D

037C6030E0 9B 38 8E 61 E0 50 9C C7 E7 53 6B 0F 6E 74 5A 3A

037C6030F0 68 8A 7E 13 E4 C0 FE F8 55 84 80 90 E9 E8 01 59

037C603100 D4 44 96 32 11 50 C2 85 5D 94 C4 D0 80 D4 84 2B

037C603110 9C 40 CC 2C 0A 20 EB 48 67 74 5B 55 63 02 BC 54

037C603120 13 79 C9 6F 0D 05 AA C1 C5 EA 7F C1 5E F0 B6 0A

037C603130 9E 8C 0F C1 6A 69 E2 DB BD 46 28 E0 24 72 25 66

037C603140 32 C4 F3 24 A8 DC 06 07 C8 EF BA 77 FB DE EF 41

037C603150 24 57 50 DD 4C C6 0A 5B 9C 7B 11 CD A3 4A 62 E6

037C603160 80 B8 3F A5 B8 E6 90 F1 A8 32 89 5A 9E F9 C8 01

037C603170 86 2B DD 98 0E 69 AD 86 B8 FC AD 9F C7 71 94 09

037C603180 2E 69 DE 09 0A FB 0D 31 69 11 29 3D 68 84 7C EF

037C603190 4E 5F EC 58 52 E0 40 48 FB 86 35 F9 E8 DD 36 1D

037C6031A0 3F B9 B4 BE B4 65 66 B0 7B E3 1A 99 44 66 18 FB

037C6031B0 3A 59 AA AD A2 8E 9E 55 F9 FF 2E 99 95 DB 50 26

037C6031C0 7C 6B 52 9C 41 92 A1 96 3C 87 27 10 2B D1 44 D5

037C6031D0 38 29 EB 8D 85 77 2A 00 2E AB 68 FA 39 A0 80 1E

037C6031E0 A9 BF 7E 7C 7A C3 88 AB CA EC 88 8E FA 2F 23 E9

037C6031F0 40 C7 AF A0 85 8E 0E E5 24 BC 23 37 8D 07 C5 E3

037C603200 36 85 3A 85 42 D1 F9 87 9C 01 9C A2 AC D8 64 41

037C603210 3E 2C BF 06 BF 90 CE F6 9D E6 B8 9A 7F 1E 83 E6

037C603220 8E 49 C8 47 96 1F 37 D3 3D 63 2F 33 69 FD 28 2C

037C603230 41 F1 53 23 77 E6 03 90 C0 88 48 84 B7 F3 57 59

037C603240 8A 41 72 8F 53 EF 6E 66 36 F3 DF 93 6D E8 06 72

037C603250 63 24 58 15 64 CB D0 6E 43 8E 56 B9 BC 90 37 67

Activate Windows
Go to Settings to activate Windows.

Drive C: [unregistered]
89% free
File system: NTFS

Default Edit Mode: original
State: original
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space
Cluster No.: 3,655,171
SRPE0HD.txt
667-3964680910-435341467-1001
Snapshot taken: 2 min. ago
Logical sector No.: 29,241,368
Physical sector No.: 29,345,816

Used space: 22.1 GB
23,719,538,688 bytes

Free space: 177 GB
190,399,889,408 bytes

Total capacity: 199 GB
214,119,431,168 bytes

Bytes per cluster: 4,096
Free clusters: 46,484,348
Total clusters: 52,275,251

Bytes per sector: 512
Sector count: 418,202,014

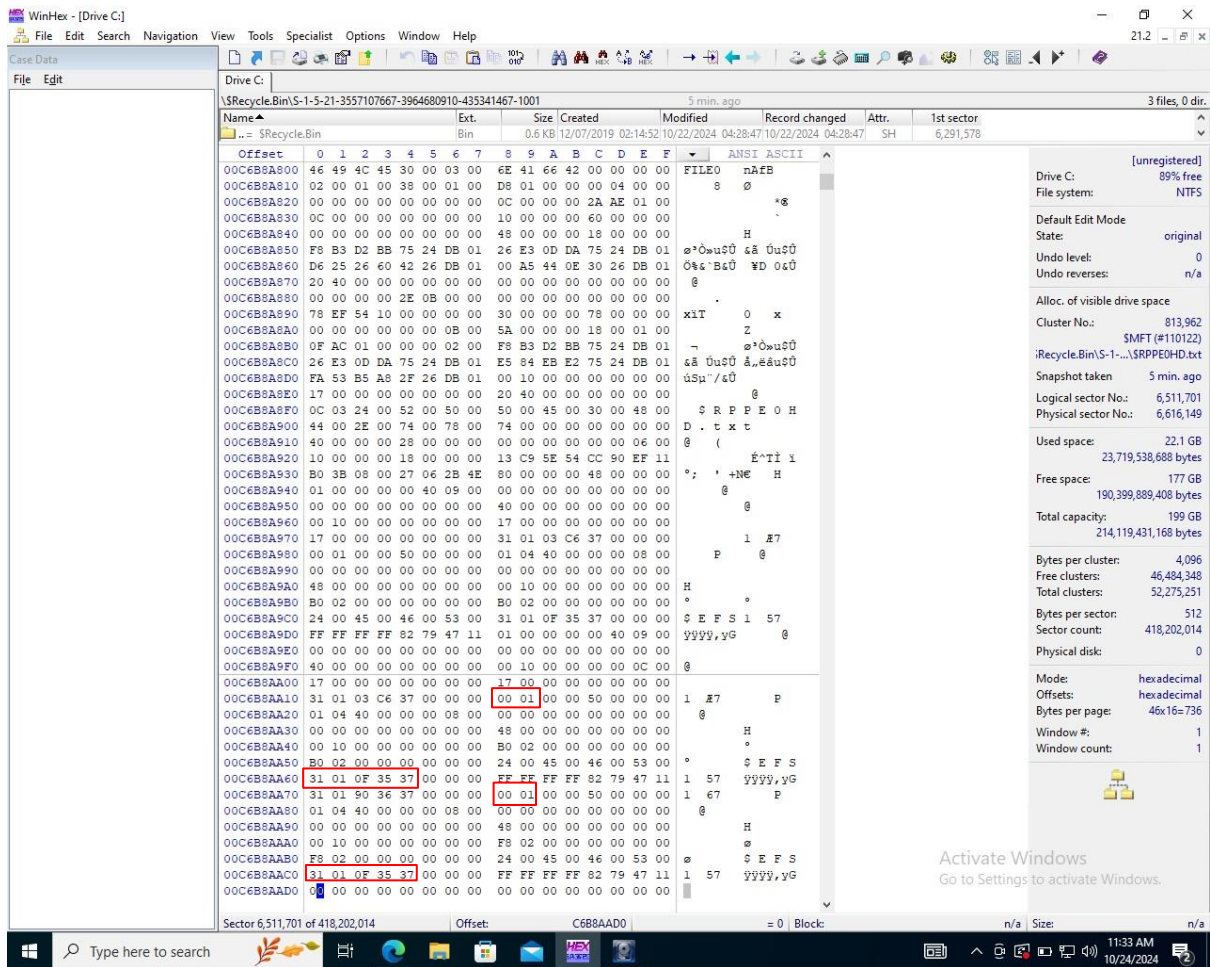
Physical disk: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 41x16=656

Window #: 1
Window count: 1

Sector 29,241,368 of 418,202,014 Offset: 37C603167 = 241 Block: n/a Size: n/a

Data remains encrypted even after deletion.



Changes:

1. One 0x30 attribute got deleted
2. Name changed

WinHex - [Drive C:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

Drive C: EFS_221725_AbdulSamiQasim...

0 min. ago

13 files, 13+0+1=14 dir.

Name▲	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Path unknown							

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
03332983744	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03332983760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03332983776	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03332983792	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03332983808	46	49	4C	45	30	00	03	00	4F	B8	2F	42	00	00	00	00
03332983824	04	00	01	00	38	00	00	00	38	02	00	00	00	04	00	00
03332983840	00	00	00	00	00	00	00	00	00	00	00	00	53	AA	01	00
03332983856	11	00	64	00	00	00	00	00	10	00	00	00	60	00	00	00
03332983872	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
03332983888	F8	B3	D2	BB	75	24	DB	01	7D	EB	D9	E5	76	24	DB	01
03332983904	B5	72	14	73	2F	26	DB	01	AD	FA	62	CF	2B	26	DB	01
03332983920	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03332983936	00	00	00	00	2E	0B	00	00	00	00	00	00	00	00	00	00
03332983952	F8	23	43	10	00	00	00	00	30	00	00	00	78	00	00	00
03332983968	00	00	00	00	00	00	0A	00	SA	00	00	00	18	00	01	00
03332983984	0F	AC	01	00	00	00	02	00	F9	B3	D2	BB	75	24	DB	01
03332984000	7D	EB	D9	E5	76	24	DB	01	7D	EB	D9	E5	76	24	DB	01
03332984016	2D	A9	E3	80	28	26	DB	01	18	00	00	00	00	00	00	00
03332984032	17	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
03332984048	0C	03	24	00	52	00	52	00	54	00	53	00	4A	00	47	00
03332984064	57	00	2E	00	74	00	78	00	74	00	00	00	00	00	00	00
03332984080	50	00	00	28	00	00	00	00	00	00	00	00	00	00	00	00
03332984096	10	00	00	18	00	00	00	00	00	00	00	00	00	00	00	00
03332984112	30	3B	08	00	27	06	2B	4E	80	00	00	00	30	00	00	00
03332984128	00	00	18	00	00	00	01	00	17	00	00	00	18	00	00	00
03332984144	68	65	6C	6F	20	72	65	73	60	64	65	6E	74	20	64	61
03332984160	70	61	20	68	65	72	65	00	80	00	00	00	50	00	00	00
03332984176	70	10	18	00	00	00	07	00	11	00	00	38	00	00	00	00
03332984192	48	00	69	00	64	00	64	00	65	00	6E	00</				

Page 9 of 11

WinHex - [Drive C:]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

Drive C:

0 min. ago 13 files, 13+0+1=14 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Path unknown							

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00C6B8A7D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A7E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A7F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A800	46	49	4C	45	30	00	03	00	73	16	73	42	00	00	00	00	FILE0	a B
00C6B8A810	03	00	01	00	38	00	00	00	D8	01	00	00	00	04	00	00	8	0
00C6B8A820	00	00	00	00	00	00	00	00	0C	00	00	00	2A	AE	01	00		*S
00C6B8A830	0D	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00		H
00C6B8A840	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00		
00C6B8A850	F8	B3	D2	BB	75	24	DB	01	26	E3	0D	DA	75	24	DB	01	a*0wu\$0	4\$ 0u\$0
00C6B8A860	D6	25	26	60	42	26	DB	01	00	A5	44	0E	30	26	DB	01	0%4 B\$0	YD 0\$0
00C6B8A870	20	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A880	00	00	00	00	2E	0B	00	00	00	00	00	00	00	00	00	00		
00C6B8A890	78	EF	54	10	00	00	00	00	30	00	00	00	78	00	00	00	xIT	0 x
00C6B8A8A0	00	00	00	00	00	00	0B	00	5A	00	00	00	18	00	01	00		Z
00C6B8A8B0	0F	AC	01	00	00	00	02	00	F8	B3	D2	BB	75	24	DB	01	-	a*0wu\$0
00C6B8A8C0	26	E3	0D	DA	75	24	DB	01	E5	84	EB	E2	75	24	DB	01	4\$ 0u\$0	4\$ 0u\$0
00C6B8A8D0	FA	53	B5	A8	2F	26	DB	01	00	10	00	00	00	00	00	00	4\$u-/\$0	
00C6B8A8E0	17	00	00	00	00	00	00	00	20	40	00	00	00	00	00	00		
00C6B8A8F0	0C	03	24	00	52	00	50	00	50	00	45	00	30	00	48	00	\$ R P P E 0 H	
00C6B8A900	44	00	2E	00	74	00	78	00	74	00	00	00	00	00	00	00	D . t x t	
00C6B8A910	40	00	00	00	28	00	00	00	00	00	00	00	00	00	06	00	@	
00C6B8A920	10	00	00	00	18	00	00	00	13	C9	5E	54	CC	90	EF	11	@	(
00C6B8A930	B0	3B	08	00	27	06	2B	4E	80	00	00	00	48	00	00	00	°; ' +NE	H
00C6B8A940	01	00	00	00	00	40	09	00	00	00	00	00	00	00	00	00	@	
00C6B8A950	00	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	@	
00C6B8A960	00	10	00	00	00	00	00	00	17	00	00	00	00	00	00	00		
00C6B8A970	17	00	00	00	00	00	00	00	31	01	03	C6	37	00	00	00	1	87
00C6B8A980	00	01	00	00	50	00	00	00	01	04	40	00	00	00	08	00	P	@
00C6B8A990	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A9A0	48	00	00	00	00	00	00	00	00	10	00	00	00	00	00	00	H	
00C6B8A9B0	B0	02	00	00	00	00	00	00	B0	02	00	00	00	00	00	00	°	
00C6B8A9C0	24	00	45	00	46	00	53	00	31	01	0F	35	37	00	00	00	\$ E F S 1	57
00C6B8A9D0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	yyy9, yG	
00C6B8A9E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8A9F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0D	00		
00C6B8AA00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AA90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00C6B8AAA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

Sector 6,511,700 of 418,202,014 Offset: C6B8A9FF = 0 Block: n/a Size: n/a

Activate Windows
Go to Settings to activate Windows.

11:38 AM 10/24/2024

One 0x100 attribute got deleted.

- ## Summary

To summarize the assignment, we've manually seen how to find the data in a file, how to locate dataruns and we saw how to find information about an EFS file.

- ## References

attribute-encrypted-files. (n.d.). Retrieved from ntfs.com: <https://ntfs.com/attribute-encrypted-files.htm>

logged_utility_stream.html. (n.d.). Retrieved from flatcap.github.io: https://flatcap.github.io/linux-ntfs/ntfs/attributes/logged_utility_stream.html

Maningo, J. (2015). *efs-protecting-files-at-rest*. Retrieved from quickstart.com: <https://www.quickstart.com/data-science/efs-protecting-files-at-rest/>

Nelson, B., Philips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations 6th ed.* Cengage.