

Part 1

Observation – The headers for a certain program are the same. In this case the older format of Microsoft Office programs (doc, xls) have the same header, as do docx and.xlsx. The .jpg and .png have different headers. This would be useful in a forensic investigation because it can narrow down the type of software you might need to interpret some data.

Headers - Notepad

File	Edit	Format	View	Help													
(.doc)																	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	D0	CF	11	E0	A1	B1	1A	E1									ËÏ à¡± á
(.xls)																	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	D0	CF	11	E0	A1	B1	1A	E1									ËÏ à¡± á
(.docx)																	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	14	00	06	00									PK
(.xlsx)																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	50	4B	03	04	14	00	06	00									PK
(.jpg)																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	FF	D8	FF	E0	00	10	4A	46									ÿøÿà JF
(.png)																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A									PNG

Part 2

1. According to the data interpreter, what is the file create date and time for the file lab1par2t.txt?
According to the data interpreter the file was created at 20:57:59 on 10/25/2019

The screenshot shows a file explorer window with a list of files. The file 'lab1part2.txt' is selected. A right-click context menu is open, showing the 'Date created' as 'Friday, October 25, 2019, 1:57:59 PM'. A 'Data Interpreter' window is also open, showing a hex dump and a timestamp of '10/25/2019 20:57:59'.

Using File Explorer and go to the folder where the lab1part2.txt located, right click on the arrow near "Size" or "Name", and select the "Date created". Now the "Date created" time is also displayed.

The screenshot shows a file explorer window with a list of files. The file 'lab1part2.txt' is selected. A right-click context menu is open, showing the 'Date created' as 'Friday, October 25, 2019, 1:57:59 PM'.

3. Compare this time and the time you got from data interpreter. Are they the same? If not, why (You may google online to get the answer)? The date and time created are different than the actual time created because (see picture below)

X-Ways Forensics employs its own, not Windows' logic to convert UTC timestamps to a freely chosen time zone for display in the directory browser, in report tables and exported lists. It displays timestamps independently of the time zone selected in the examiner's system's Control Panel. The display of timestamps in X-Ways Forensics may differ from Windows because in Windows a timestamp in daylight saving time is not displayed based on daylight saving time if daylight saving time is not active when looking at that timestamp.

4. What is the size of the MFT record? The size of the MFT record is 400 bytes and is located at offset 0x1C to 0x1F

The screenshot displays the X-Ways Forensics interface. The top pane shows a file list for 'C:\Users\Curti\Desktop'. The file 'lab1part2.txt' is selected, showing a size of 259 B and a timestamp of 10/25/2019 13:57:59. The bottom pane shows a hex view of the file's content, starting at offset 0x1C. The hex data is as follows:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
35655B800	46	49	4C	45	30	00	03	00	63	94	0F	1C	01	00	00	00
35655B810	0F	00	02	00	38	00	01	00	D8	02	00	00	00	04	00	00
35655B820	00	00	00	00	00	00	00	00	05	00	00	00	0E	CF	02	00
35655B830	05	00	20	74	00	00	00	00	10	00	00	00	60	00	00	00
35655B840	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
35655B850	BC	ED	41	E2	76	8B	D5	01	24	92	55	E2	76	8B	D5	01
35655B860	4C	FE	59	E2	76	8B	D5	01	24	92	55	E2	76	8B	D5	01
35655B870	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
35655B880	00	00	00	00	3F	06	00	00	00	00	00	00	00	00	00	00
35655B890	38	7F	45	34	00	00	00	00	30	00	00	00	78	00	00	00
35655B8A0	00	00	00	00	00	00	03	00	5A	00	00	00	18	00	01	00
35655B8B0	49	3E	01	00	00	00	01	00	BC	ED	41	E2	76	8B	D5	01
35655B8C0	18	6B	55	E2	76	8B	D5	01	18	6B	55	E2	76	8B	D5	01
35655B8D0	18	6B	55	E2	76	8B	D5	01	00	00	00	00	00	00	00	00
35655B8E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
35655B8F0	0C	02	4C	00	41	00	42	00	31	00	50	00	41	00	7E	00
35655B900	31	00	2E	00	54	00	58	00	54	00	00	00	00	00	00	00
35655B910	30	00	00	00	78	00	00	00	00	00	00	00	00	00	02	00
35655B920	5C	00	00	00	18	00	01	00	49	3E	01	00	00	00	01	00
35655B930	BC	ED	41	E2	76	8B	D5	01	18	6B	55	E2	76	8B	D5	01
35655B940	18	6B	55	E2	76	8B	D5	01	18	6B	55	E2	76	8B	D5	01
35655B950	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

The right pane shows a 'Data Interpreter' window with the following information:

- 8 Bit (±): 0
- 16 Bit (±): 0
- 32 Bit (±): 0
- FILETIME: ?

The status bar at the bottom indicates the current offset is 85655B81F, which is 400 bytes (0x1C to 0x1F) from the start of the file.

5. What is the length of the header for the MFT record? The length of the header is 38 and is located at offset 0x14 – 0x15

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

085655B800 46 49 4C 45 30 00 03 00 63 94 0F 1C 01 00 00 00

085655B810 0F 00 02 00 38 00 01 00 D8 02 00 00 00 04 00 00

085655B820 00 00 00 00 00 00 00 00 05 00 00 00 0E CF 02 00

085655B830 09 00 20 74 00 00 00 00 10 00 00 00 60 00 00 00

085655B840 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00

085655B850 BC ED 41 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B860 4C FE 59 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B870 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00

085655B880 00 00 00 00 3F 06 00 00 00 00 00 00 00 00 00

085655B890 38 7F 45 34 00 00 00 00 30 00 00 00 78 00 00 00

085655B8A0 00 00 00 00 00 00 03 00 5A 00 00 00 18 00 01 00

085655B8B0 49 3E 01 00 00 00 01 00 BC ED 41 E2 76 8B D5 01

085655B8C0 18 6B 55 E2 76 8B D5 01 18 6B 55 E2 76 8B D5 01

085655B8D0 18 6B 55 E2 76 8B D5 01 00 00 00 00 00 00 00

085655B8E0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00

085655B8F0 0C 02 4C 00 41 00 42 00 31 00 50 00 41 00 7E 00

085655B900 31 00 2E 00 54 00 58 00 54 00 00 00 00 00 00

085655B910 30 00 00 00 78 00 00 00 00 00 00 00 00 02 00

085655B920 5C 00 00 00 18 00 01 00 49 3E 01 00 00 01 00

085655B930 BC ED 41 E2 76 8B D5 01 18 6B 55 E2 76 8B D5 01

085655B940 18 6B 55 E2 76 8B D5 01 18 6B 55 E2 76 8B D5 01

085655B950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Sector 69937884 of 487073792 Offset: 85655B815 = 0 | Block: 85655B814 - 85655B815 Size: 2

6. What is the file's last modified date and time? Take a screenshot with data interpreter to prove your answer.

According to the data interpreter the file was last modified at 20:57:59 on 10/25/2019

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

085655B800 46 49 4C 45 30 00 03 00 63 94 0F 1C 01 00 00 00

085655B810 0F 00 02 00 38 00 01 00 D8 02 00 00 00 04 00 00

085655B820 00 00 00 00 00 00 00 00 05 00 00 00 0E CF 02 00

085655B830 09 00 20 74 00 00 00 00 10 00 00 00 60 00 00 00

085655B840 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00

085655B850 BC ED 41 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B860 4C FE 59 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B870 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00

085655B880 00 00 00 00 3F 06 00 00 00 00 00 00 00 00 00

085655B890 38 7F 45 34 00 00 00 00 30 00 00 00 78 00 00 00

085655B8A0 00 00 00 00 00 00 03 00 5A 00 00 00 18 00 01 00

085655B8B0 49 3E 01 00 00 00 01 00 BC ED 41 E2 76 8B D5 01

085655B8C0 18 6B 55 E2 76 8B D5 01 18 6B 55 E2 76 8B D5 01

085655B8D0 18 6B 55 E2 76 8B D5 01 00 00 00 00 00 00 00

085655B8E0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00

085655B8F0 0C 02 4C 00 41 00 42 00 31 00 50 00 41 00 7E 00

Sector 69937884 of 487073792 Offset: 85655B815 = 0 | Block: 85655B814 - 85655B815 Size: 2

7. What is the file name? In which attribute and at what position can you find it? The short file name is at offset 0x5A from the beginning of attribute 0x30

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

085655B800 46 49 4C 45 30 00 03 00 63 94 0F 1C 01 00 00 00

085655B810 0F 00 02 00 38 00 01 00 D8 02 00 00 00 04 00 00

085655B820 00 00 00 00 00 00 00 00 05 00 00 00 0E CF 02 00

085655B830 09 00 20 74 00 00 00 00 10 00 00 00 60 00 00 00

085655B840 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00

085655B850 BC ED 41 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B860 4C FE 59 E2 76 8B D5 01 24 92 55 E2 76 8B D5 01

085655B870 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00

085655B880 00 00 00 00 3F 06 00 00 00 00 00 00 00 00 00

085655B890 38 7F 45 34 00 00 00 00 30 00 00 00 78 00 00 00

085655B8A0 00 00 00 00 00 00 03 00 5A 00 00 00 18 00 01 00

085655B8B0 49 3E 01 00 00 00 01 00 BC ED 41 E2 76 8B D5 01

085655B8C0 18 6B 55 E2 76 8B D5 01 18 6B 55 E2 76 8B D5 01

085655B8D0 18 6B 55 E2 76 8B D5 01 00 00 00 00 00 00 00

085655B8E0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00

085655B8F0 0C 02 4C 00 41 00 42 00 31 00 50 00 41 00 7E 00

Sector 69937884 of 487073792 Offset: 85655B8F2 = 76 | Block: 85655B899 - 85655B8F2 Size: 5A

The full file name is at 0xD2 from the beginning of attribute 0x30

085655B860	4C FE 59 E2 76 8B D5 01	24 92 55 E2 76 8B D5 01	LpYävIÖ s'UävIÖ
085655B870	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	?
085655B880	00 00 00 00 3F 06 00 00	00 00 00 00 00 00 00 00	8 E4 0 x
085655B890	38 7F 45 34 00 00 00 00	30 00 00 00 78 00 00 00	Z
085655B8A0	00 00 00 00 00 03 00	5A 00 00 00 18 00 01 00	I> kUävIÖ
085655B8B0	49 3E 01 00 00 01 00	BC ED 41 E2 76 8B D5 01	kUävIÖ kUävIÖ
085655B8C0	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	I A B 1 P A ~
085655B8D0	18 6B 55 E2 76 8B D5 01	00 00 00 00 00 00 00 00	1 . T X T
085655B8E0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	0 x
085655B8F0	0C 02 4C 00 41 00 42 00	31 00 50 00 41 00 7E 00	\ I>
085655B900	31 00 2E 00 54 00 58 00	54 00 00 00 00 00 00 00	kUävIÖ kUävIÖ
085655B910	30 00 00 00 78 00 00 00	00 00 00 00 00 00 02 00	l a b
085655B920	5C 00 00 00 18 00 01 00	49 3E 01 00 00 00 01 00	1 p a r t 2 . t
085655B930	BC ED 41 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	x t @ (
085655B940	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	/U 'Iöé IG PVÅ
085655B950	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	I
085655B960	20 00 00 00 00 00 00 00	0D 01 6C 00 61 00 62 00	
085655B970	31 00 70 00 61 00 72 00	74 00 32 00 2E 00 74 00	
085655B980	78 00 74 00 00 00 00 00	40 00 00 00 28 00 00 00	
085655B990	00 00 00 00 00 04 00	10 00 00 00 18 00 00 00	
085655B9A0	2F 55 04 91 95 F6 E9 11	97 47 00 50 56 C0 00 08	
085655B9B0	80 00 00 00 20 01 00 00	00 00 18 00 00 00 01 00	

Sector 69937884 of 487073792 Offset: 85655B96A = 108 | Block: 85655B899 - 85655B96A | Size: D2

Data Interpreter

8 Bit (±): 108
16 Bit (±): 108
32 Bit (±): 6357100
FILETIME: 09/15/1644 18:24:37

Hard disk 0, Partition 46% free
File system: NTFS
[Read-only mode]

Alloc. of visible drive space:
Cluster No.: 8742235
\$MFT (#184078)
Users\Curti\De...lab1part2.txt
Snapshot taken 3 days ago
Physical sector No.: 71260892
Logical sector No.: 69937884

Used space: 55.1 GB
59,125,649,408 bytes
Free space: 177 GB
190,256,128,000 bytes
Total capacity: 232 GB
249,381,781,504 bytes

Bytes per cluster: 4,096
Free clusters: 46,449,250

8. Is this file a resident file or nonresident file? Where can you find the evidence? The file is a resident file. You can find the resident/nonresident flag at offset 0x08 from the beginning of the attribute 0x80. The flag for this particular file is 00 which indicates a resident file.

85655B8C0	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B8D0	18 6B 55 E2 76 8B D5 01	00 00 00 00 00 00 00 00	kUävIÖ
85655B8E0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	
85655B8F0	0C 02 4C 00 41 00 42 00	31 00 50 00 41 00 7E 00	I A B 1 P A ~
85655B900	31 00 2E 00 54 00 58 00	54 00 00 00 00 00 00 00	1 . T X T
85655B910	30 00 00 00 78 00 00 00	00 00 00 00 00 00 02 00	0 x
85655B920	5C 00 00 00 18 00 01 00	49 3E 01 00 00 00 01 00	\ I>
85655B930	BC ED 41 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B940	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B950	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
85655B960	20 00 00 00 00 00 00 00	0D 01 6C 00 61 00 62 00	l a b
85655B970	31 00 70 00 61 00 72 00	74 00 32 00 2E 00 74 00	1 p a r t 2 . t
85655B980	78 00 74 00 00 00 00 00	40 00 00 00 28 00 00 00	x t @ (
85655B990	00 00 00 00 00 04 00	10 00 00 00 18 00 00 00	
85655B9A0	2F 55 04 91 95 F6 E9 11	97 47 00 50 56 C0 00 08	/U 'Iöé IG PVÅ
85655B9B0	80 00 00 00 20 01 00 00	00 00 18 00 00 00 01 00	
85655B9C0	03 01 00 00 18 00 00 00	41 20 63 6F 75 6E 74 72	A countr
85655B9D0	79 6D 61 6E 20 62 65 74	77 65 65 6E 20 74 77 6F	ymen between two
85655B9E0	20 6C 61 79 65 72 73 20	69 73 20 6C 69 6B 65 20	layers is like
85655B9F0	61 20 66 69 73 68 20 62	65 74 77 65 65 6E 09 00	a fish between
85655BA00	77 6F 20 63 61 74 73 2E	0D 0A 41 20 73 6C 69 70	wo cats. A slip
85655BA10	20 6F 66 20 74 68 65 20	66 6F 6F 74 20 79 6F 75	of the foot you

Sector 69937884 of 487073792 Offset: 85655B9B8 = 0 | Block: 85655B9B1 - 85655B9B8 | Size: 8

Data Interpreter

8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 1572864
FILETIME: 11/22/1601 18:44:57

Hard disk 0, Partition 46% free
File system: NTFS
[Read-only mode]

Alloc. of visible drive space:
Cluster No.: 8742235
\$MFT (#184078)
Users\Curti\De...lab1part2.txt
Snapshot taken 3 days ago
Physical sector No.: 71260892
Logical sector No.: 69937884

Used space: 55.1 GB
59,125,649,408 bytes
Free space: 177 GB
190,256,128,000 bytes
Total capacity: 232 GB
249,381,781,504 bytes

Bytes per cluster: 4,096
Free clusters: 46,449,250

9. In which attribute can you find the data run? Where is the start of the data run? The data run is in attribute 0x80. The start of the data run for the file is located at offset 0x18 from the beginning of attribute 0x80

85655B8C0	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B8D0	18 6B 55 E2 76 8B D5 01	00 00 00 00 00 00 00 00	kUävIÖ
85655B8E0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	
85655B8F0	0C 02 4C 00 41 00 42 00	31 00 50 00 41 00 7E 00	I A B 1 P A ~
85655B900	31 00 2E 00 54 00 58 00	54 00 00 00 00 00 00 00	1 . T X T
85655B910	30 00 00 00 78 00 00 00	00 00 00 00 00 00 02 00	0 x
85655B920	5C 00 00 00 18 00 01 00	49 3E 01 00 00 00 01 00	\ I>
85655B930	BC ED 41 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B940	18 6B 55 E2 76 8B D5 01	18 6B 55 E2 76 8B D5 01	kUävIÖ kUävIÖ
85655B950	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
85655B960	20 00 00 00 00 00 00 00	0D 01 6C 00 61 00 62 00	l a b
85655B970	31 00 70 00 61 00 72 00	74 00 32 00 2E 00 74 00	1 p a r t 2 . t
85655B980	78 00 74 00 00 00 00 00	40 00 00 00 28 00 00 00	x t @ (
85655B990	00 00 00 00 00 04 00	10 00 00 00 18 00 00 00	
85655B9A0	2F 55 04 91 95 F6 E9 11	97 47 00 50 56 C0 00 08	/U 'Iöé IG PVÅ
85655B9B0	80 00 00 00 20 01 00 00	00 00 18 00 00 00 01 00	
85655B9C0	03 01 00 00 18 00 00 00	41 20 63 6F 75 6E 74 72	A countr
85655B9D0	79 6D 61 6E 20 62 65 74	77 65 65 6E 20 74 77 6F	ymen between two
85655B9E0	20 6C 61 79 65 72 73 20	69 73 20 6C 69 6B 65 20	layers is like
85655B9F0	61 20 66 69 73 68 20 62	65 74 77 65 65 6E 09 00	a fish between
85655BA00	77 6F 20 63 61 74 73 2E	0D 0A 41 20 73 6C 69 70	wo cats. A slip
85655BA10	20 6F 66 20 74 68 65 20	66 6F 6F 74 20 79 6F 75	of the foot you

Sector 69937884 of 487073792 Offset: 85655B9C8 = 65 | Block: 85655B9B1 - 85655B9C8 | Size: 18

Data Interpreter

8 Bit (±): 65
16 Bit (±): 8257
32 Bit (±): 1868767297
FILETIME: 10/11/27735 09:40:28

Hard disk 0, Partition 46% free
File system: NTFS
[Read-only mode]

Alloc. of visible drive space:
Cluster No.: 8742235
\$MFT (#184078)
Users\Curti\De...lab1part2.txt
Snapshot taken 3 days ago
Physical sector No.: 71260892
Logical sector No.: 69937884

Used space: 55.1 GB
59,125,649,408 bytes
Free space: 177 GB
190,256,128,000 bytes
Total capacity: 232 GB
249,381,781,504 bytes

Bytes per cluster: 4,096
Free clusters: 46,449,250