

0x38+04 -

Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F
035B3400	46 49 4C 45 30 00 03 00 9B 99 98 00 00 00 00 00
035B3410	02 00 01 00 38 00 01 00 A8 01 00 00 00 04 00 00
035B3420	00 00 00 00 00 00 00 00 04 00 00 00 A8 17 00 00
035B3430	03 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00
035B3440	00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00
035B3450	62 16 9B 68 0A 7C C9 01 BC 78 9D 68 0A 7C C9 01
035B3460	BC 78 9D 68 0A 7C C9 01 BC 78 9D 68 0A 7C C9 01
035B3470	20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
035B3480	00 00 00 00 09 01 00 00 00 00 00 00 01 00 00 00
035B3490	00 00 00 00 00 00 00 00 30 00 00 00 70 00 00 00
035B34A0	00 00 00 00 00 00 02 00 52 00 00 00 18 00 01 00
035B34B0	8A 00 00 00 00 00 01 00 62 16 9B 68 0A 7C C9 01
035B34C0	BC 78 9D 68 0A 7C C9 01 BC 78 9D 68 0A 7C C9 01
035B34D0	BC 78 9D 68 0A 7C C9 01 00 00 00 00 00 00 00 00
035B34E0	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
035B34F0	08 03 42 00 65 00 6E 00 31 00 2E 00 74 00 78 00
035B3500	74 00 00 00 00 00 00 00 40 00 00 00 28 00 00 00
035B3510	00 00 00 00 00 00 03 00 10 00 00 00 10 00 00 00
035B3520	F4 7C F1 27 DF E7 DD 11 A8 3F 00 22 18 D5 88 06
035B3530	80 00 00 00 70 00 00 00 00 00 18 00 00 00 01 00
035B3540	34 00 00 00 10 00 00 00 41 20 63 6F 75 6E 74 72
035B3550	79 6D 61 6E 20 62 65 74 77 65 65 6E 20 74 77 6F
035B3560	20 6C 61 77 79 65 72 73 20 69 73 20 6C 69 6B 65
035B3570	20 61 20 66 69 73 68 20 62 65 74 77 65 65 6E 20
035B3580	74 77 6E 20 63 61 74 73 2E 0D 0A 42 65 6E 6A 61
035B3590	6D 69 6E 20 46 72 61 6E 6B 6C 69 6E 00 00 00 00
035B35A0	FB FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00

- For the header of all MFT records, the record fields of interest are as follows:
 - At offset 0x00 - the MFT record identifier FILE
 - At offset 0x1C to 0x1F - size of the MFT record
 - At offset 0x14 - length of the header (indicates where the next attribute starts)
 - At offset 0x32 and 0x33 - the update sequence array, which stores the last 2 bytes of the first sector of the MFT record
- Attribute 0x10: Standard Information
 - At offset 0x38 from the beginning of the MFT record - The start of attribute 0x10
 - At offset 0x04 to 0x05 from the beginning of attribute 0x10 - size of the 0X10 attribute
 - At offset 0x18-0x1F - The file's create date and time
 - At offset 0x20 and 0x27 - the last modified date and time for the file
 - At offset 0x28 and 0x2F - the last access date and time
 - At offset 0x30 and 0x2F - the record access date and time
- Attribute 0x30: File_Name
- If the file name is shorter than eight characters, there are only one attribute 0x30
- If the file name is longer than eight characters, there are two attributes 0x30
 - At offset 0x04 to 0x05 from the beginning of attribute 0x30 - size of the 0x30 attribute
 - At offset 0x5A - short file name
 - At offset 0x20 to 0x27 - file create date and time
 - At offset 0x28 to 0x2F - file last modified date and time
 - At offset 0x30 to 0x37 - the last access date and time
 - At offset 0x38 to 0x3F - the record update date and time

- Attribute 0x40: Object_ID
 - At offset 0x04 to 0x05 from the beginning of attribute 0x40* - size of the 0x40 attribute
 - At offset 0x14* – starting offset position for GUID (global unique identifier) data
 - At offset 0x18 to 0x27* – starting position for GUID Object_ID data
- Attribute 0x80: Data for a Resident File
 - At offset 0x04 to 0x05 from the beginning of attribute 0x80* - size of the 0x80 attribute
 - At offset 0x08* – the resident/nonresident flag; for resident data, it is set to 0x00.
 - At offset 0x10* – Number of bytes in the data run.
 - At offset 0x18* – start of the resident data run
- Attribute 0x80: Data for a Nonresident File
 - At offset 0x04 to 0x05 from the beginning of attribute 0x80* - size of the 0x80 attribute
 - At offset 0x08* – the resident/nonresident flag; for nonresident data, it is set to 0x01.
 - At offset 0x40* – The start of the data run. The first run is the LCN.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F			
024C2E00	46	49	4C	45	30	00	03	00	0B	8A	AA	00	00	00	00	00	FILEO	...	
024C2E10	02	00	02	00	38	00	01	00	F0	01	00	00	00	04	00	00	...	8...@...	
024C2E20	00	00	00	00	00	00	00	00	05	00	00	00	A9	00	00	00	
024C2E30	05	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	
024C2E40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	...	H...	
024C2E50	DE	CE	75	56	E4	7C	C9	01	BC	BF	8C	18	26	66	C9	01	bluVä É.4&I.fé		
024C2E60	A4	85	50	45	E4	7C	C9	01	36	1E	BC	34	77	7D	C9	01	¶ PEs É.6.44w É		
024C2E70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...		
024C2E80	00	00	00	00	09	01	00	00	00	00	00	00	00	00	00	00	...		
024C2E90	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00	...	0...x...	
024C2EA0	00	00	00	00	00	00	00	03	00	5A	00	00	00	18	00	01	00	...	Z...
024C2EB0	8F	00	00	00	00	00	01	00	DE	CE	75	56	E4	7C	C9	01	I...	bluVä É	
024C2EC0	DE	CE	75	56	E4	7C	C9	01	DE	CE	75	56	E4	7C	C9	01	bluVä É.bluVä É		
024C2ED0	DE	CE	75	56	E4	7C	C9	01	00	00	00	00	00	00	00	00	bluVä É.....		
024C2EE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	...		
024C2EF0	0C	02	53	00	41	00	4E	00	54	00	45	00	46	00	7E	00	..S.A.N.T.E.F.~		
024C2F00	31	00	2E	00	4A	00	50	00	47	00	70	00	67	00	00	00	1...J.P.G.p.g...		
024C2F10	30	00	00	00	78	00	00	00	00	00	00	00	00	00	02	00	0...x.....		
024C2F20	5E	00	00	00	18	00	01	00	8F	00	00	00	00	00	01	00	^.....!...		
024C2F30	DE	CE	75	56	E4	7C	C9	01	DE	CE	75	56	E4	7C	C9	01	bluVä É.bluVä É		
024C2F40	DE	CE	75	56	E4	7C	C9	01	DE	CE	75	56	E4	7C	C9	01	bluVä É.bluVä É		
024C2F50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...		
024C2F60	20	00	00	00	00	00	00	00	0E	01	53	00	61	00	6E	00S.an		
024C2F70	74	00	65	00	46	00	65	00	30	00	30	00	31	00	2E	00	t.e.F.e.0.0.1...		
024C2F80	6A	00	70	00	67	00	00	00	00	00	00	00	60	00	00	00	j.p.g...!.....		
024C2F90	01	00	00	00	00	00	04	00	00	00	00	00	00	00	00	00	...	@...	
024C2FA0	AD	1A	00	00	00	00	00	00	40	00	00	00	00	00	00	00	-...@...		
024C2FB0	00	5C	35	00	00	00	00	00	35	5B	35	00	00	00	00	00	\\$5...5[5...		
024C2FC0	35	5B	35	00	00	00	00	00	32	B1	07	8C	8C	00	22	03	5[5...2±.!!."c		
024C2FD0	07	95	ED	32	BC	06	3C	36	00	22	35	03	02	FA	21	0B	.i124.<6."5..ú1.		
024C2FE0	6C	FE	22	4E	01	E9	04	00	FF	FF	FF	FF	82	79	47	11	1p"!é.yyyy!yg.		
024C2FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	05	00	00	...		
024C3000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...		

B A C D F G H I J E C