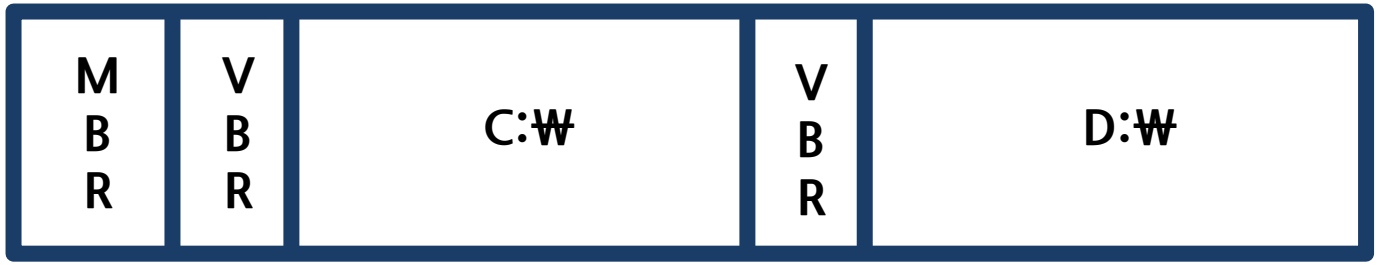
NTFS

발 표 자 문 승 재

목 차

파일 시스템 구조 - MFT

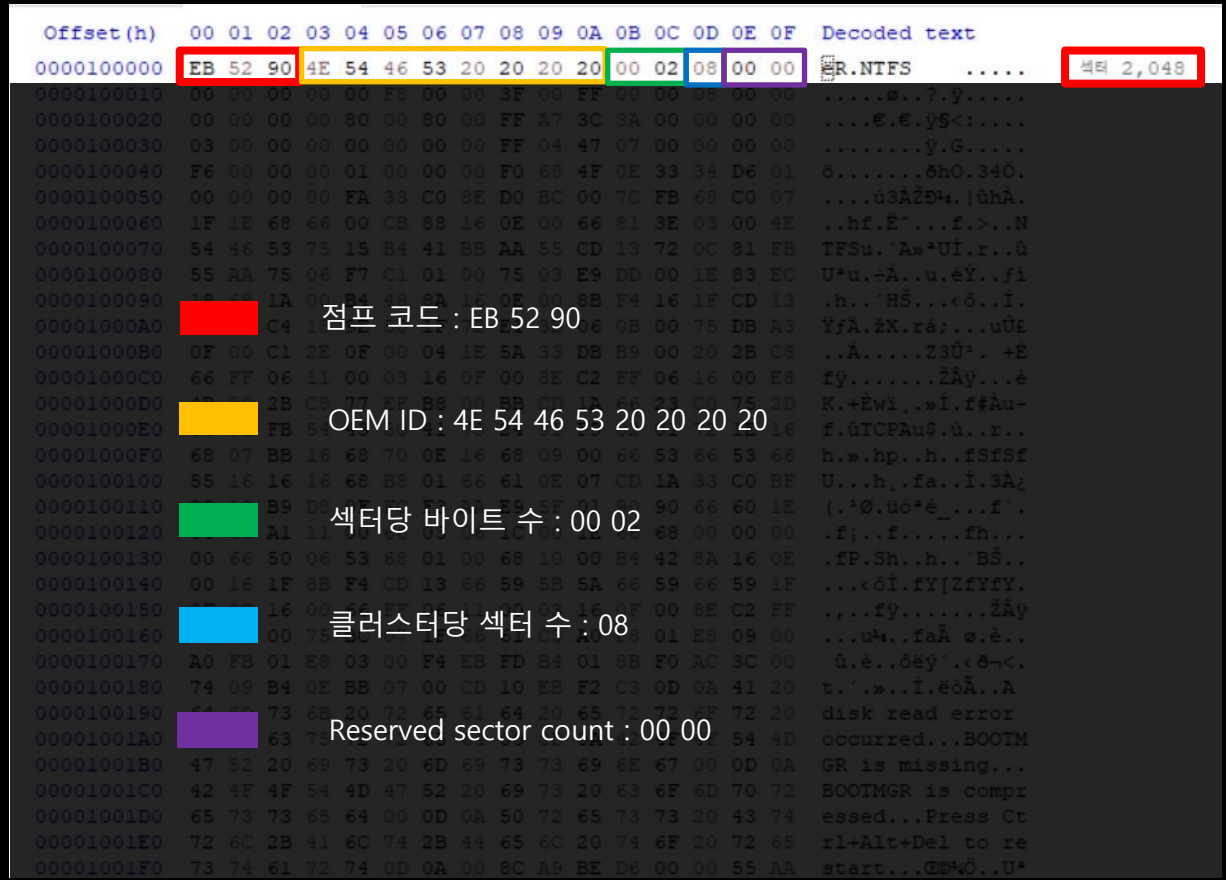


NTFS 파일시스템 구조

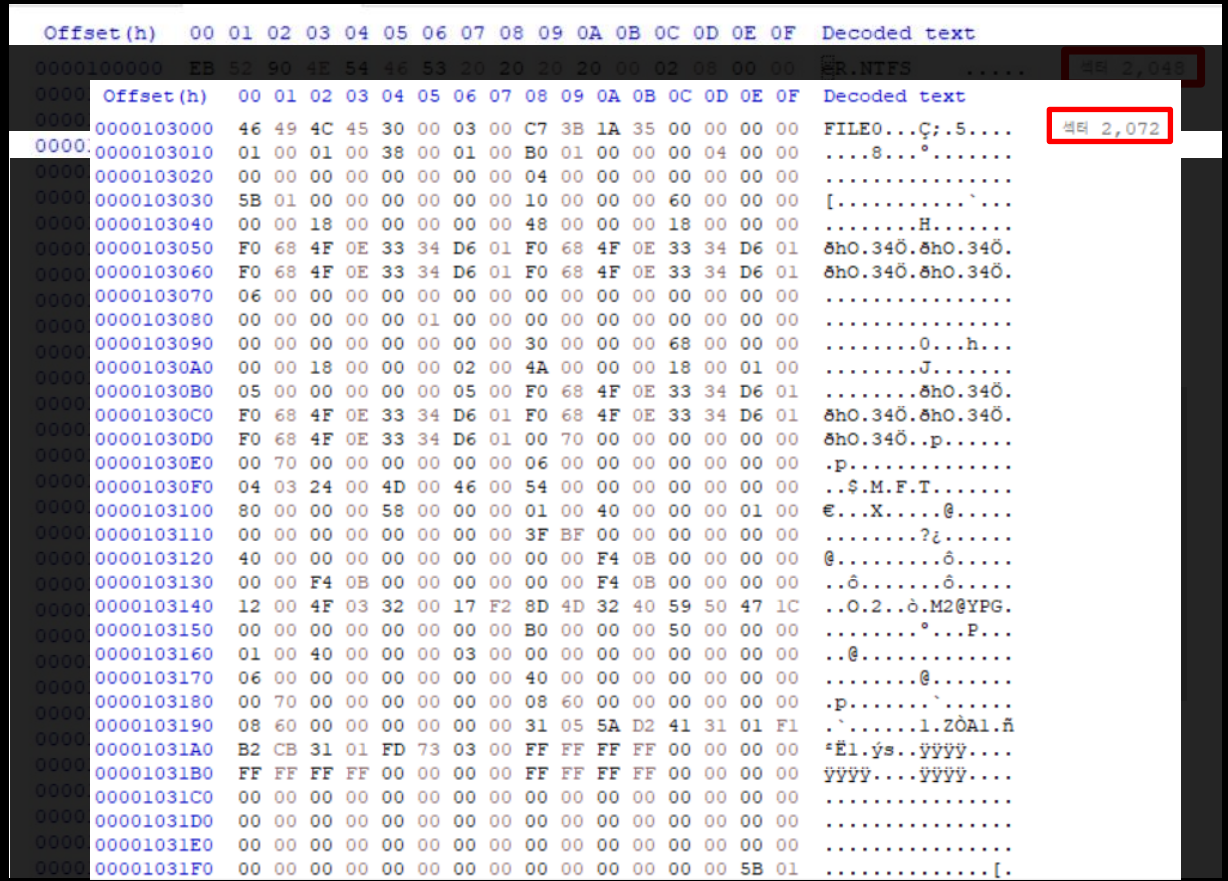
MFT

- 디렉토리나 파일 등을 관리하기 위해 존재하는 MFT Entry영역
- 파일과 디렉터리에 관한 정보가 있음

파일 시스템 구조 - VBR


Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0000100000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 ëR.NTFS .....
섹터 2,048
점프 코드 : EB 52 90
OEM ID : 4E 54 46 53 20 20 20 20
섹터당 바이트 수 : 00 02
클러스터당 섹터 수 : 08
Reserved sector count : 00 00

파일 시스템 구조 - MFT

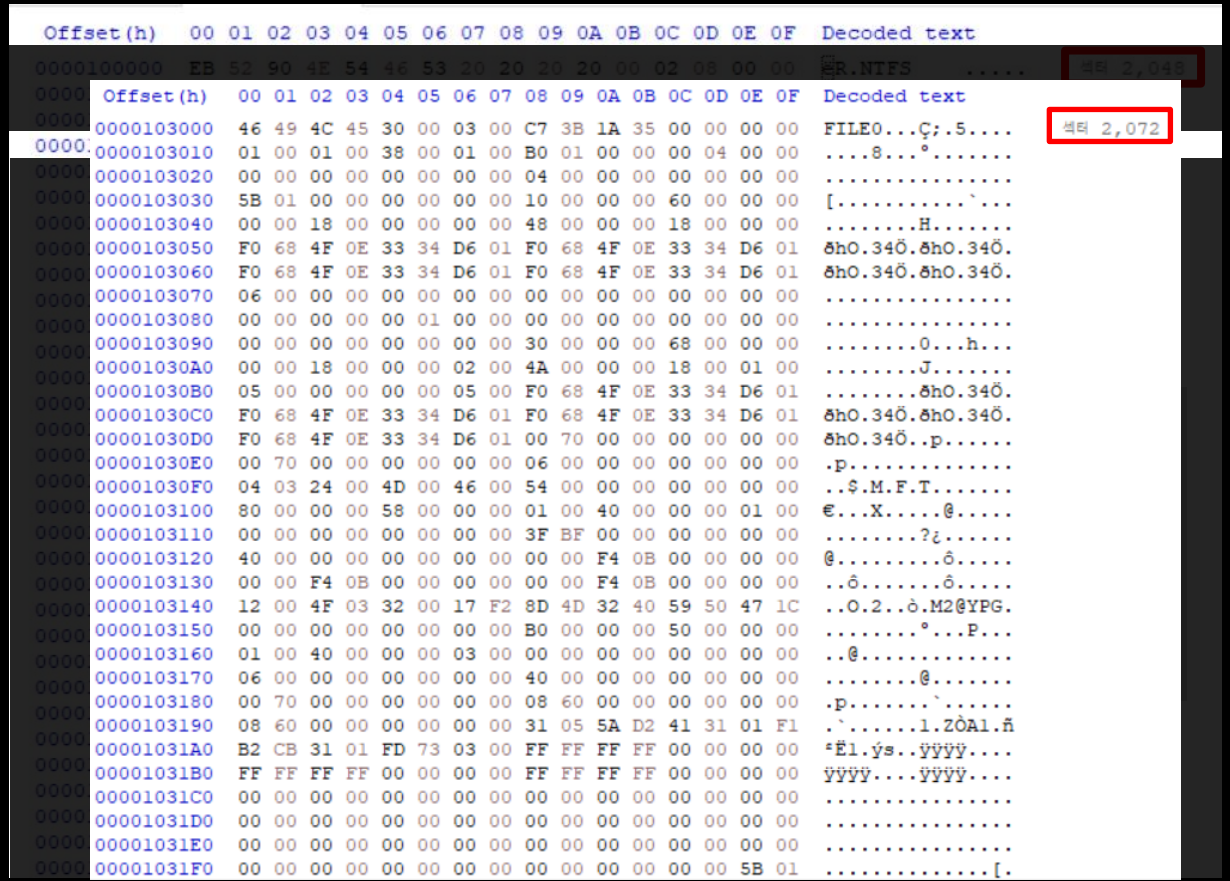


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	....8...°.....
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	.....
0000103030	5B	01	00	00	00	00	00	00	10	00	00	00	60	00	00	00	[.....`...
0000103040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
0000103070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000103080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	.....
0000103090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	.....0...h...
00001030A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00	.....J.....
00001030B0	05	00	00	00	00	00	05	00	F0	68	4F	0E	33	34	D6	01	.....ðhO.34Ö.
00001030C0	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
00001030D0	F0	68	4F	0E	33	34	D6	01	00	70	00	00	00	00	00	00	ðhO.34Ö..p.....
00001030E0	00	70	00	00	00	00	00	00	06	00	00	00	00	00	00	00	.p.....
00001030F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00	..$.M.F.T.....
0000103100	80	00	00	00	58	00	00	00	01	00	40	00	00	00	01	00	€...X.....@.....
0000103110	00	00	00	00	00	00	00	00	3F	BF	00	00	00	00	00	00	.....?¿.....
0000103120	40	00	00	00	00	00	00	00	00	00	F4	0B	00	00	00	00	@.....ô.....
0000103130	00	00	F4	0B	00	00	00	00	00	00	F4	0B	00	00	00	00	..ô.....ô.....
0000103140	12	00	4F	03	32	00	17	F2	8D	4D	32	40	59	50	47	1C	..O.2..ò.M2@YPG.
0000103150	00	00	00	00	00	00	00	00	B0	00	00	00	50	00	00	00	.....°...P...
0000103160	01	00	40	00	00	00	03	00	00	00	00	00	00	00	00	00	..@.....
0000103170	06	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
0000103180	00	70	00	00	00	00	00	00	08	60	00	00	00	00	00	00	.p.....`.....
0000103190	08	60	00	00	00	00	00	00	31	05	5A	D2	41	31	01	F1	.`.....1.ZÒA1.ñ
00001031A0	B2	CB	31	01	FD	73	03	00	FF	FF	FF	FF	00	00	00	00	²Ë1.ýs..ÿÿÿÿ....
00001031B0	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	00	00	00	00	ÿÿÿÿ....ÿÿÿÿ....
00001031C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	5B	01	.....[.

섹터 2,048

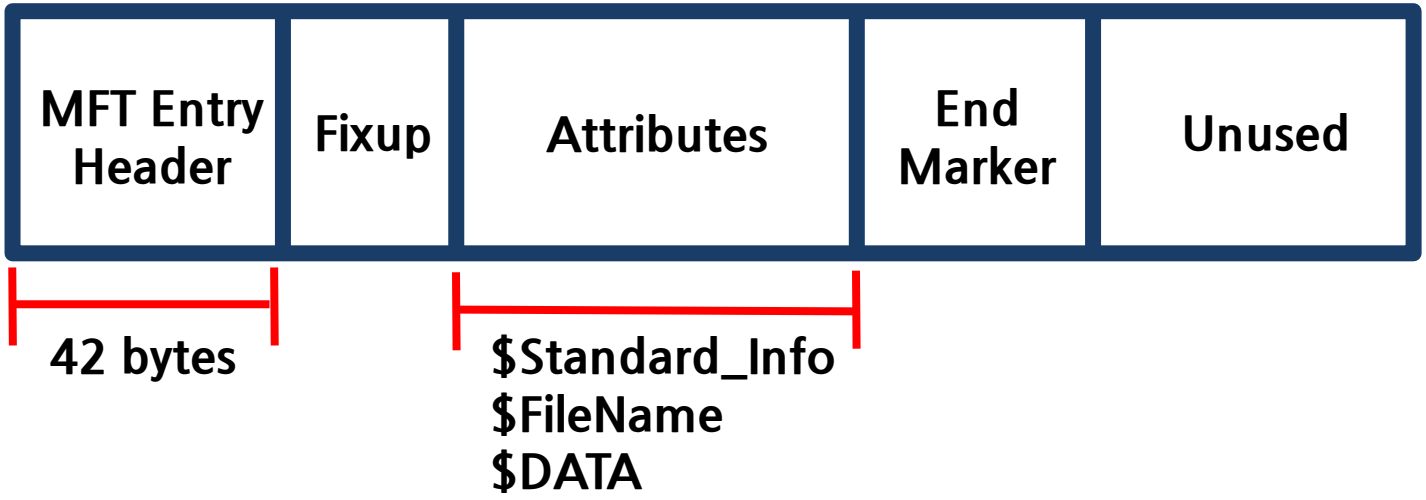
섹터 2,072

파일 시스템 구조 - MFT

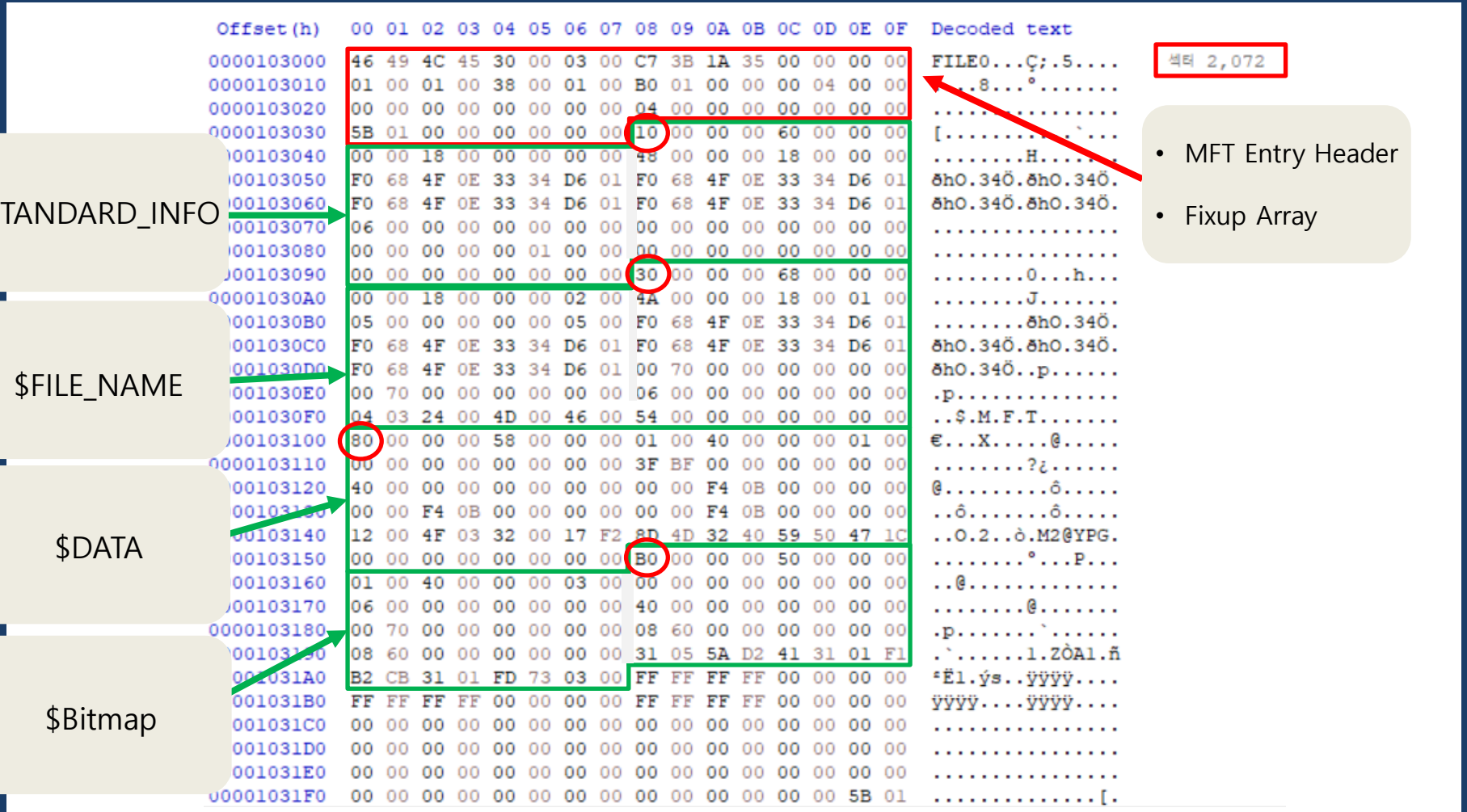


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	....8...°.....
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	.....
0000103030	5B	01	00	00	00	00	00	00	10	00	00	00	60	00	00	00	[.....`...
0000103040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
0000103070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000103080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	.....
0000103090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	.....0...h...
00001030A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00	.....J.....
00001030B0	05	00	00	00	00	00	05	00	F0	68	4F	0E	33	34	D6	01	.....ðhO.34Ö.
00001030C0	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	ðhO.34Ö.ðhO.34Ö.
00001030D0	F0	68	4F	0E	33	34	D6	01	00	70	00	00	00	00	00	00	ðhO.34Ö..p.....
00001030E0	00	70	00	00	00	00	00	00	06	00	00	00	00	00	00	00	.p.....
00001030F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00	..$.M.F.T.....
0000103100	80	00	00	00	58	00	00	00	01	00	40	00	00	00	01	00	€...X.....@.....
0000103110	00	00	00	00	00	00	00	00	3F	BF	00	00	00	00	00	00	.....?¿.....
0000103120	40	00	00	00	00	00	00	00	00	00	F4	0B	00	00	00	00	@.....ô.....
0000103130	00	00	F4	0B	00	00	00	00	00	00	F4	0B	00	00	00	00	..ô.....ô.....
0000103140	12	00	4F	03	32	00	17	F2	8D	4D	32	40	59	50	47	1C	..O.2..ò.M2@YPG.
0000103150	00	00	00	00	00	00	00	00	B0	00	00	00	50	00	00	00	.....°...P...
0000103160	01	00	40	00	00	00	03	00	00	00	00	00	00	00	00	00	..@.....
0000103170	06	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
0000103180	00	70	00	00	00	00	00	00	08	60	00	00	00	00	00	00	.p.....`.....
0000103190	08	60	00	00	00	00	00	00	31	05	5A	D2	41	31	01	F1	.`.....1.ZÒA1.ñ
00001031A0	B2	CB	31	01	FD	73	03	00	FF	FF	FF	FF	00	00	00	00	²Ë1.ýs..ÿÿÿÿ....
00001031B0	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	00	00	00	00	ÿÿÿÿ....ÿÿÿÿ....
00001031C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00001031F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	5B	01	.....[.

MFT Entry Structure



파일 시스템 구조 - MFT


Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0000103000 46 49 4C 45 30 00 03 00 C7 3B 1A 35 00 00 00 00 FILE0...Ç;.5....
0000103010 01 00 01 00 38 00 01 00 B0 01 00 00 00 04 00 00 ....8...°.......
0000103020 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ....
0000103030 5B 01 00 00 00 00 00 00 10 00 00 00 60 00 00 00 [...........`...
00103040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00 ....H.......
00103050 F0 68 4F 0E 33 34 D6 01 F0 68 4F 0E 33 34 D6 01 ðhO.34Ö.ðhO.34Ö.
00103060 F0 68 4F 0E 33 34 D6 01 F0 68 4F 0E 33 34 D6 01 ðhO.34Ö.ðhO.34Ö.
00103070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00103080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ....
00103090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 ....0...h...
001030A0 00 00 18 00 00 00 02 00 4A 00 00 00 18 00 01 00 ....J.......
001030B0 05 00 00 00 00 00 05 00 F0 68 4F 0E 33 34 D6 01 ....ðhO.34Ö.
001030C0 F0 68 4F 0E 33 34 D6 01 F0 68 4F 0E 33 34 D6 01 ðhO.34Ö.ðhO.34Ö.
001030D0 F0 68 4F 0E 33 34 D6 01 00 70 00 00 00 00 00 00 ðhO.34Ö..p......
001030E0 00 70 00 00 00 00 00 00 06 00 00 00 00 00 00 00 .p..............
001030F0 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00 ..$.M.F.T.......
00103100 80 00 00 00 58 00 00 00 01 00 40 00 00 00 01 00 €...X.....@.....
00103110 00 00 00 00 00 00 00 00 3F BF 00 00 00 00 00 00 ....?¿......
00103120 40 00 00 00 00 00 00 00 00 00 00 F4 0B 00 00 00 @.........ô.....
00103130 00 00 F4 0B 00 00 00 00 00 00 00 F4 0B 00 00 00 ..ô........ô.....
00103140 12 00 4F 03 32 00 17 F2 8D 4D 32 40 59 50 47 1C ..O.2..ò.M2@YPG.
00103150 00 00 00 00 00 00 00 00 B0 00 00 00 50 00 00 00 ....°...P...
00103160 01 00 40 00 00 00 03 00 00 00 00 00 00 00 00 00 ..@.............
00103170 06 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
00103180 00 70 00 00 00 00 00 00 08 60 00 00 00 00 00 00 .p.......`......
00103190 08 60 00 00 00 00 00 00 31 05 5A D2 41 31 01 F1 .`......1.ZÒA1.ñ
001031A0 B2 CB 31 01 FD 73 03 00 FF FF FF FF 00 00 00 00 ²Ë1.ýs..ÿÿÿÿ....
001031B0 FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00 ÿÿÿÿ....ÿÿÿÿ....
001031C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
001031D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
001031E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
001031F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5B 01 ....[.
섹터 2,072
• MFT Entry Header
• Fixup Array
$STANDARD_INFO
$FILE_NAME
$DATA
$Bitmap

파일 시스템 구조 - MFT Entry header

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	....8...°.......
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	....
0000103030	5B	01	00	00	00	00	00	00									[.......

Signature

46 49 4C 45

Fixup Array Offset

30 00

Fixup Array Count

03 00

$Log File Sequence Number

C7 3B 1A 35 00 00 00 00

Fixup

NTFS 파일 시스템

1개 이상의 섹터를 사용

마지막 2byte 값을 기록

파일 시스템 구조 - Fixup

오프셋	데이터								설명
0x0000	42byte								MFT Entry Header
0x002A	CD	AB	17	18	27	28	37	38	Fixup Array
.....									
0x1FB	11	12	13	14	15	16	CD	AB	End of Sector 1
.....									
0x3FB	21	22	23	24	25	26	CD	AB	End of Sector 2
.....									
0x5FB	31	32	33	34	35	36	CD	AB	End of Sector 3
.....									

파일 시스템 구조 - MFT Entry header

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	....8...°.....
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	....
0000103030	5B	01	00	00	00	00	00	00									[.......

Sequence Number

01 00

Hard link count

01 00

Offset to the first attribute

38 00

Flags

01 00

파일 시스템 구조 - MFT Entry header

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	....8...°.......
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	....
0000103030	5B	01	00	00	00	00	00	00									[.......

Used size of MFT Entry

B0 01 00 00

Allocated size of MFT Entry

00 04 00 00

File reference to base record

00 00 00 00
00 00 00 00

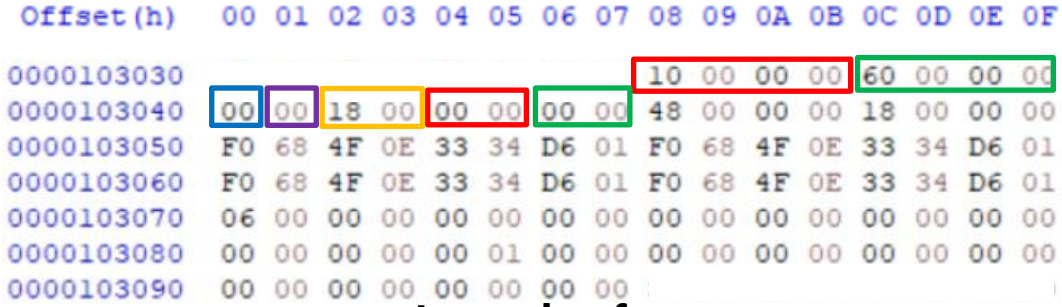
Next attribute ID

04 00

Attributes and fixup values

0x02A - 0x3FF

파일 시스템 구조 - $STANDARD_INFORMATION



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000103030									10	00	00	00	60	00	00	00
0000103040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000103080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
0000103090	00	00	00	00	00	00	00	00								

Attribute Type

10 00 00 00

Length of Attribute

60 00 00 00

Non-resident Flag

00

Length of Name

00

Offset to Name

18 00

Flag

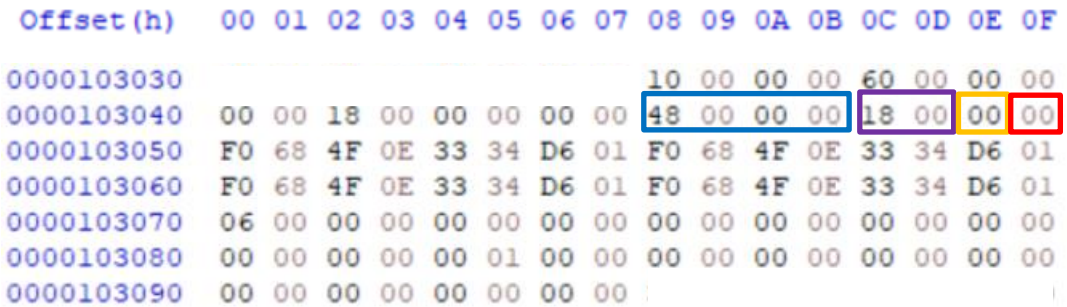
00 00

Attribute Identifier

00 00

파일 시스템 구조 - $STANDARD_INFORMATION

resident



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000103030									10	00	00	00	60	00	00	00
0000103040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000103080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
0000103090	00	00	00	00	00	00	00	00								

Size of Content

48 00 00 00

Offset to Content

18 00

Indexed Flag

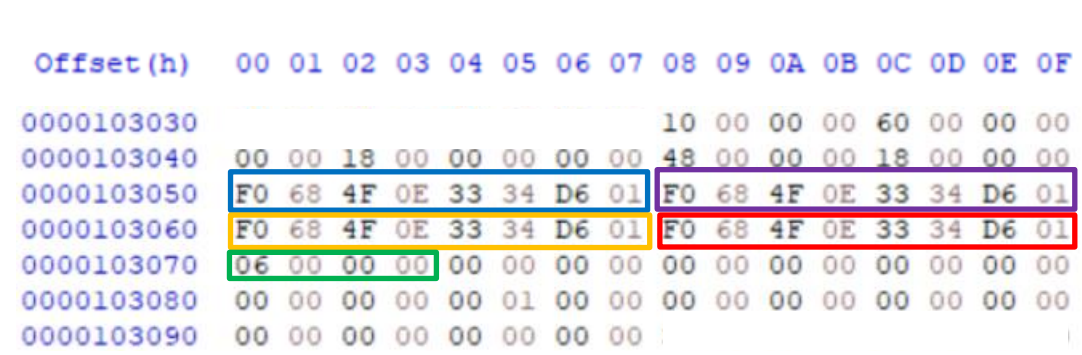
00

Unused

00

파일 시스템 구조 - $STANDARD_INFORMATION

STANDARD_INFO



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000103030									10	00	00	00	60	00	00	00
0000103040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01
0000103070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000103080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
0000103090	00	00	00	00	00	00	00	00								

Creation Time

F0 68 4F 0E
33 34 D6 01

File altered Time

F0 68 4F 0E
33 34 D6 01

MFT altered Time

F0 68 4F 0E
33 34 D6 01

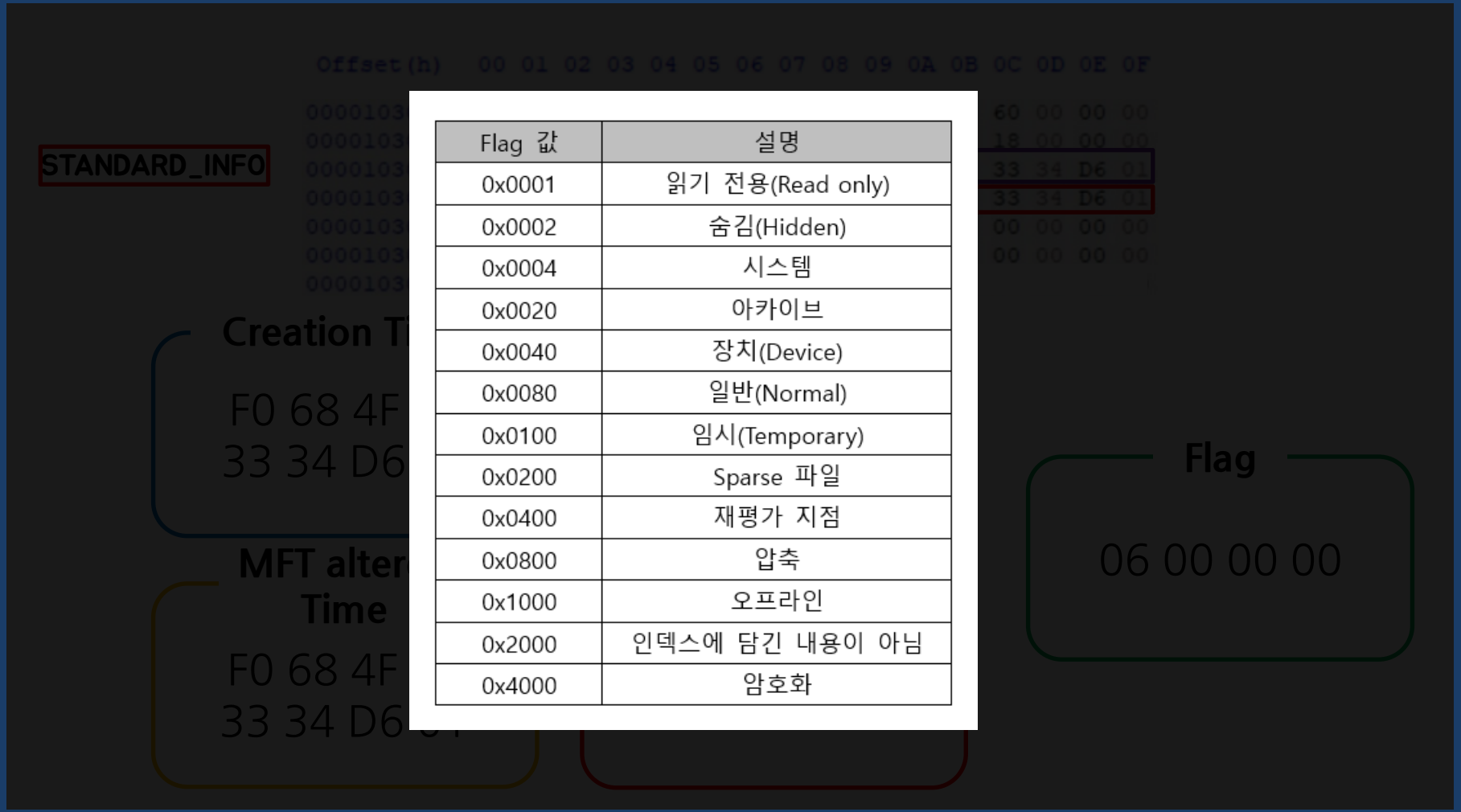
File accessed Time

F0 68 4F 0E
33 34 D6 01

Flag

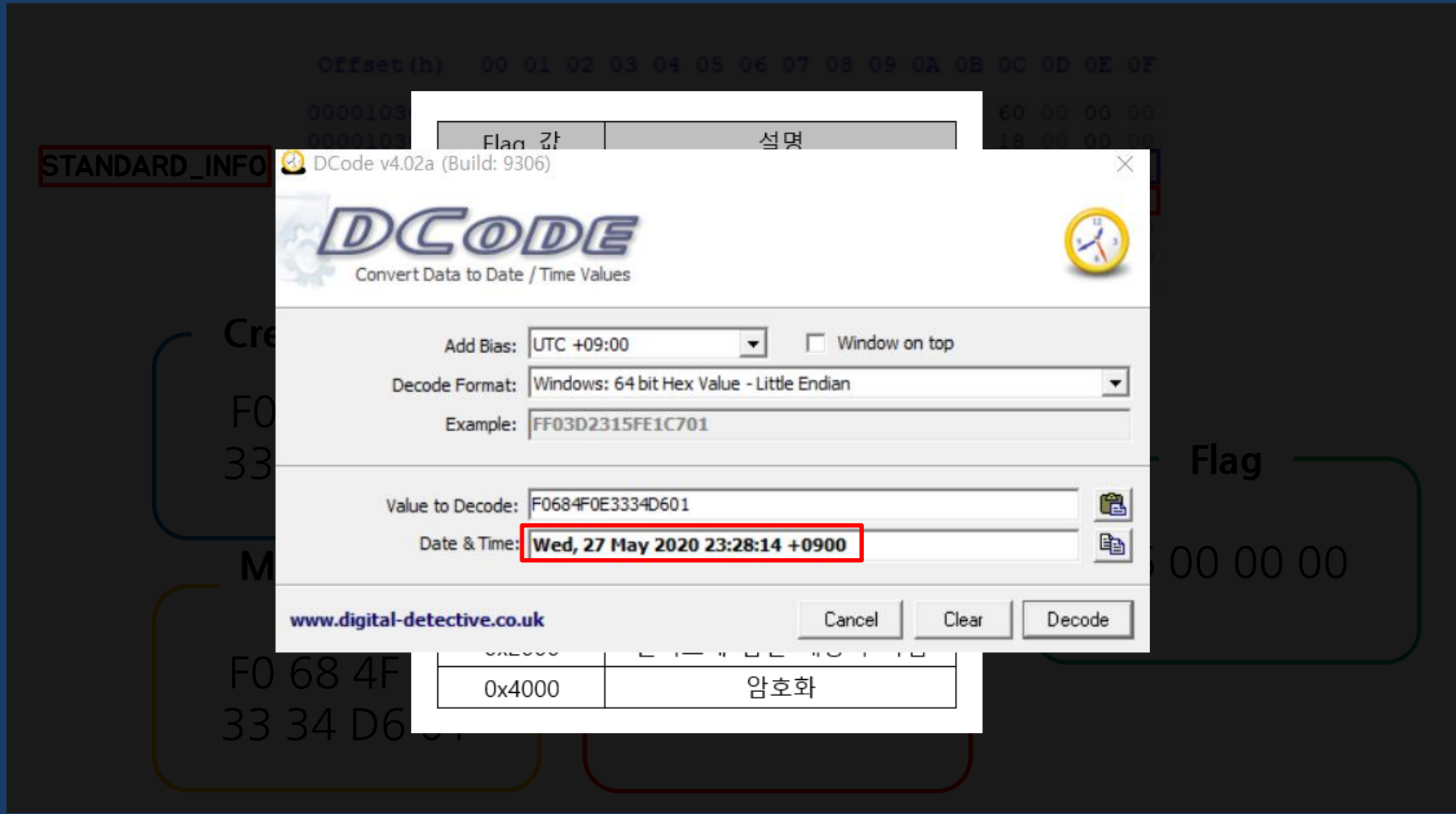
06 00 00 00

파일 시스템 구조 - $STANDARD_INFORMATION



Flag 값	설명
0x0001	읽기 전용(Read only)
0x0002	숨김(Hidden)
0x0004	시스템
0x0020	아카이브
0x0040	장치(Device)
0x0080	일반(Normal)
0x0100	임시(Temporary)
0x0200	Sparse 파일
0x0400	재평가 지점
0x0800	압축
0x1000	오프라인
0x2000	인덱스에 담긴 내용이 아님
0x4000	암호화

파일 시스템 구조 - $STANDARD_INFORMATION



Q & A