

NTFS

발 표 자 문 승 재



목 차

I

MFT

II

MFT Entry

III

\$STANDARD_INFORMATION



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	MR.NTFS 섹터 2,048
0000100010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00g...?y.....
0000100020	00	00	00	00	80	00	80	00	FF	A7	3C	3A	00	00	00	00ë.ë.ÿS<:....
0000100030	03	00	00	00	00	00	00	00	FF	04	47	07	00	00	00	00ÿ.G.....
0000100040	F6	00	00	00	01	00	00	00	F0	68	4F	0E	33	34	D6	01	ö.....ðhO.34Ö.
0000100050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07ü3AžB4.}ghÄ.
0000100060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.E'...f.>..N
0000100070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A*UI.r..ö
0000100080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u.+Ä..u.éÿ..fi
0000100090	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	00	00	.h..'HŠ...<ö..i.
00001000A0	C4	10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ÿfÄ.žX.rä;...uöÿ
00001000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ü*. +E
00001000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fy.....žÄÿ...ë
00001000D0	00	00	2B	C8	7F	FF	B8	00	00	00	00	00	00	00	00	00	K.+Ew1.,»I.f#Äu-
00001000E0	FB	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	f.@TCPAuš.ä..r..
00001000F0	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66	h.».hp..h..fSfSf
0000100100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h.,.fa..i.3Äž
0000100110	B9	D8	0F	00	00	00	00	00	00	00	00	00	00	00	00	00	(.'@.üö*ë...f'.
0000100120	A1	11	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.fj..f.....fh...
0000100130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..'BŠ..
0000100140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<öi.fÿ{zfÿÿÿ.
0000100150	16	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	...fy.....žÄÿ
0000100160	00	78	0F	00	00	00	00	00	00	00	00	00	00	00	00	00	...u4..faÄ s.ë..
0000100170	A0	FB	01	E8	03	00	F4	EB	FD	B4	01	8B	F0	AC	3C	00	ä.ë..öëÿ'.<ö-<.
0000100180	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	t.'.»..i.ëöÄ..A
0000100190	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	disk read error
00001001A0	63	75	00	00	00	00	00	00	00	00	00	00	00	00	00	00	occurred...BOOTM
00001001B0	47	52	20	69	73	20	6D	69	73	73	69	6E	67	00	0D	0A	GR is missing...
00001001C0	42	4F	4F	54	4D	47	52	20	69	73	20	63	6F	6D	70	72	BOOTMGR is compr
00001001D0	65	73	73	65	64	00	0D	0A	50	72	65	73	73	20	43	74	essed...Press Ct
00001001E0	72	6C	2B	41	6C	74	2B	44	65	6C	20	74	6F	20	72	65	rl+Alt+Del to re
00001001F0	73	74	61	72	74	0D	0A	00	8C	A9	BE	D6	00	00	55	AA	start...öÖ..U*

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

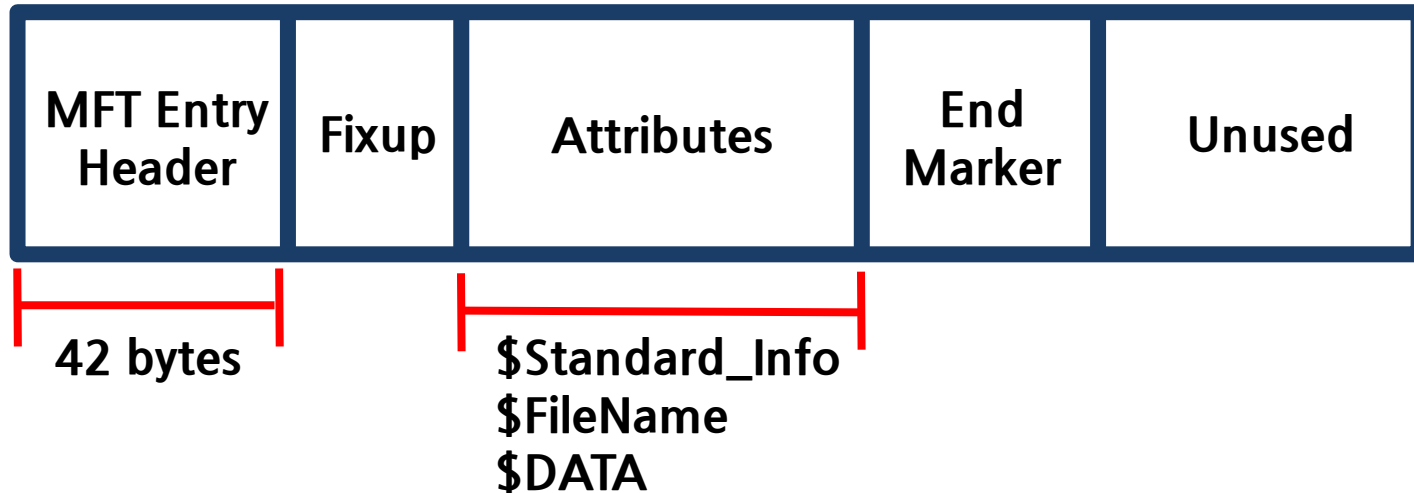
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
0000100000	EB	52	90	4E	54	4E	53	20	20	20	20	00	02	00	00	00	EB.NIFS	
0000100000	Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....	
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	008....°.....	
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	00H.....	
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8h0.340.8h0.340.	
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8h0.340.8h0.340.	
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	000...h...	
00001030A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00J.....	
00001030B0	05	00	00	00	00	00	05	00	F0	68	4F	0E	33	34	D6	018h0.340.	
00001030C0	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8h0.340.8h0.340.	
00001030D0	F0	68	4F	0E	33	34	D6	01	00	70	00	00	00	00	00	00	8h0.340..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	@.....δ.....	
0000103130	00	00	F4	0B	00	00	00	00	00	00	F4	0B	00	00	00	00	..δ.....δ.....	
0000103140	12	00	4F	03	32	00	17	F2	8D	4D	32	40	59	50	47	1C	..O.2...ð.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.Z0A1.ñ	
00001031A0	B2	CB	31	01	FD	73	03	00	FF	FF	FF	FF	00	00	00	00	°El.ýs..ýýýý....	
00001031B0	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	00	00	00	00	ýýýý....ýýýý....	
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	00	5B 01[.	

섹터 2,072

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	4E	53	20	20	20	20	00	02	00	00	00	EB.NIFS	
0000100000	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	008....°.....	
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	00H.....	
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.340.8hO.340.	
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.340.8hO.340.	
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	000...h...	
00001030A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00J.....	
00001030B0	05	00	00	00	00	00	05	00	F0	68	4F	0E	33	34	D6	018hO.340.	
00001030C0	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.340.8hO.340.	
00001030D0	F0	68	4F	0E	33	34	D6	01	00	70	00	00	00	00	00	00	8hO.340..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	@.....δ.....	
0000103130	00	00	F4	0B	00	00	00	00	00	00	F4	0B	00	00	00	00	..δ.....δ.....	
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.Z0A1.ñ	
00001031A0	B2	CB	31	01	FD	73	03	00	FF	FF	FF	FF	00	00	00	00	°El.ýs..ýýýý....	
00001031B0	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	00	00	00	00	ýýýý....ýýýý....	
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	00	5B	01[.

섹터 2,072

MFT Entry Structure



파일 시스템 구조 - MFT

\$STANDARD_INFO

\$FILE_NAME

\$DATA

\$Bitmap

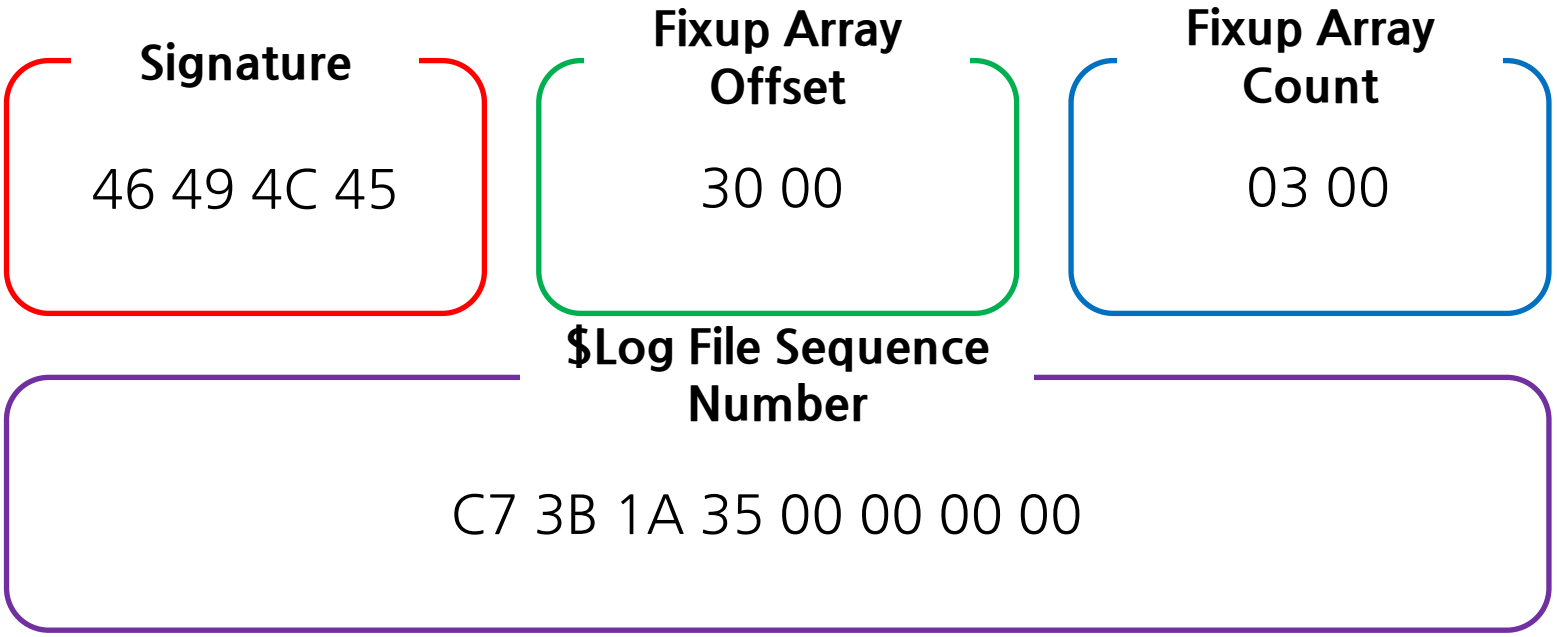
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000103000	46	49	4C	45	30	00	03	00	C7	3B	1A	35	00	00	00	00	FILE0...Ç;.5....
0000103010	01	00	01	00	38	00	01	00	B0	01	00	00	00	04	00	00	...8...°.....
0000103020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
0000103030	5B	01	00	00	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	00H.....
0000103050	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.34Ö.8hO.34Ö.
0000103060	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.34Ö.8hO.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	000...h...
00001030A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00J.....
00001030B0	05	00	00	00	00	00	05	00	F0	68	4F	0E	33	34	D6	018hO.34Ö.
00001030C0	F0	68	4F	0E	33	34	D6	01	F0	68	4F	0E	33	34	D6	01	8hO.34Ö.8hO.34Ö.
00001030D0	F0	68	4F	0E	33	34	D6	01	00	70	00	00	00	00	00	00	8hO.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..ô.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.Z0A1.ñ
00001031A0	B2	CB	31	01	FD	73	03	00	FF	FF	FF	FF	00	00	00	00	*El.ýs..ýýýý....
00001031B0	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	00	00	00	00	ýýýý....ýýýý....
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 2,072

- MFT Entry Header
- Fixup Array

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	008...°.....
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									[.....



Fixup

NTFS 파일 시스템

1개 이상의 섹터를 사용

마지막 2byte 값을 기록

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
.....									

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	008...°.....
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

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	008...°.....
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

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	48	00	00	00	18	00	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

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

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

STANDARD_INFO

Creation Time

F0 68 4F
33 34 D6

MFT alter Time

F0 68 4F
33 34 D6

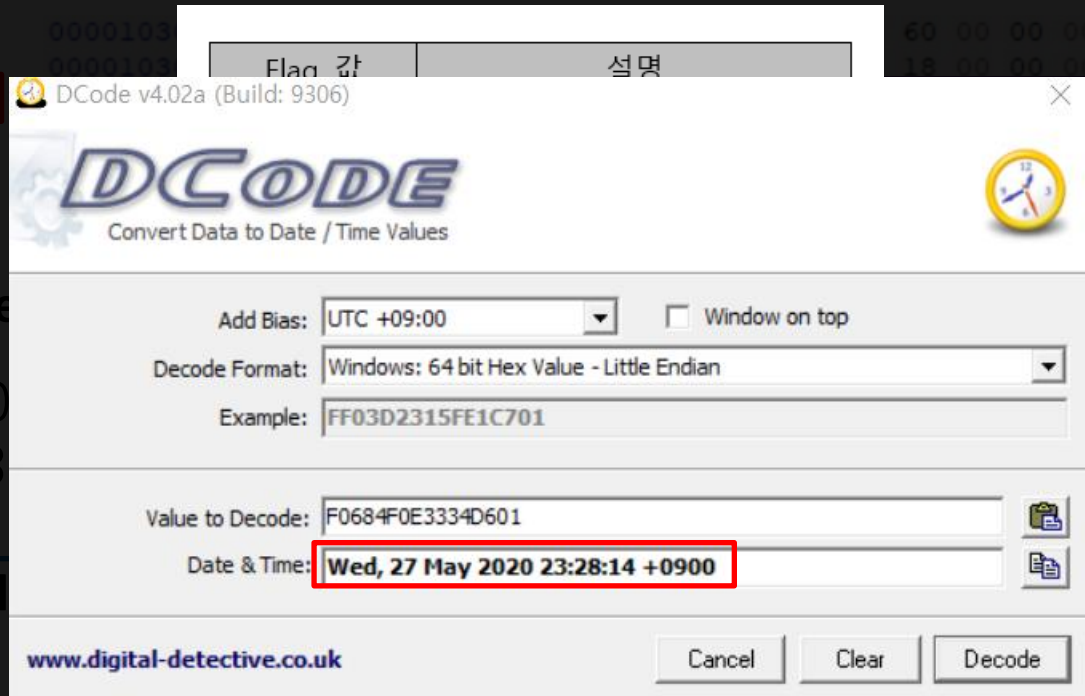
Flag 값	설명
0x0001	읽기 전용(Read only)
0x0002	숨김(Hidden)
0x0004	시스템
0x0020	아카이브
0x0040	장치(Device)
0x0080	일반(Normal)
0x0100	임시(Temporary)
0x0200	Sparse 파일
0x0400	재평가 지점
0x0800	압축
0x1000	오프라인
0x2000	인덱스에 담긴 내용이 아님
0x4000	암호화

60 00 00 00
18 00 00 00
33 34 D6 01
33 34 D6 01
00 00 00 00
00 00 00 00

Flag

06 00 00 00

STANDARD_INFO



0x4000	암호화
--------	-----

Q & A

