



# NTFS 구조

1학년 권도윤

# 용어 설명



- 클러스터 : 컴퓨터 하드디스크에서 사용하는 논리적 단위.
- 파티션 : 하나의 하드디스크나 SSD 등 드라이브를 논리적으로 여러 부분으로 분할하는 것
- 파일 시스템 : 물리적인 디스크의 파티션 내에서 클러스터 단위 데이터를 배치하고 관리하기 위한 체계.
- NTFS : Microsoft Windows의 파일 시스템

# NTFS 구조



- NTFS 구조는 VBR + MFT + Data Area 로 구성
- 모든 데이터는 파일 형식으로 관리 하며 VBR은 고정 적으로 맨 앞자리에 위치
- MFT File 은 일반적으로 VBR 이후에 존재 하는데 데이터 영역의 어느곳에 와도 무관



# VBR(Volume Boot Record)

- NTFS 파티션이 처음 생성될 때, 파티션 정보들이 들어있는 볼륨을 VBR이라고 한다.
- VBR의 영역 크기는 일정하지 않고 클러스터의 크기에 따라 그 크기가 변한다.

Cluster Size (Byte)	VBR Size (Sector)
512	1
1K	2
2K	4
4K	8

# MFT(Master File Table)



- 볼륨에 존재하는 모든 파일과 디렉토리에 대한 정보를 가진 테이블
- windows에서 NTFS로 포맷할 경우 Windows는 MFT의 초기 크기를 작게 설정하여 파일이 많아지면 크기를 점점 늘려가게 된다. 하지만 한번 늘어난 MFT는 파일이 줄어든다고 해서 줄어들지는 않는다.

# MFT(Master File Table)의 위치 구하기



- HxD(16진수로 표현된 이진파일을 읽는 프로그램)를 통해 위치를 찾을 것.
- 디스크관리에 들어가서 VHD를 만들고 파일시스템은 NTFS로 설정하여 가상디스크를 만듦.
- HxD를 키고 도구-디스크열기로 새로 만든 가상디스크를 연결한다.

# MFT(Master File Table)의 위치 구하기

HxD - [새 볼륨 (D:)]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 16진수 0 of 2,091,008

새 볼륨 (D:)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	52	90	4E	54	46	53	20	20	20	00	02	08	00	00	00	#R.NIFS .....
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00	.....s..?y[.....
00000020	00	00	00	00	80	00	00	00	FF	E7	1F	00	00	00	00	00	.....E.E.yq.....
00000030	55	54	01	00	00	00	00	00	02	00	00	00	00	00	00	00	UI.....
00000040	F6	00	00	00	01	00	00	00	C8	B0	B8	3A	EC	B8	3A	F0	8.....E°,i,j;8
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	...d3A2B4.jhA.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.E°...f>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A°UI.r..0
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u..A..u.eY..fi
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..H5°...<ö..i.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	38	06	0B	00	75	DB	A3	YfA.2X.r&°;..u06
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..A....230°..+E
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fy.....2Ay...e
000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Ew1..wi.f#Au-
000000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.gTCpAuS.ü..r..
000000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h..hR..h..f5sf
00000100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h..fa..i.3A;.
00000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..°ö.ö°ep...f°.
00000120	06	66	Al	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.fj...f....fh...
00000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	..fP.Sh..h..B5..
00000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<öI.fY[2fYfY.
00000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fy.....2Ay
00000160	0E	16	00	75	BC	07	1F	66	61	C3	Al	F6	01	E8	09	00	...u..faA;ö.e...
00000170	Al	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	jü.e..öey&°<e.t.
00000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	OD	0A	41	20	64	69	..°...I.öA..A di
00000190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
000001A0	63	75	73	72	65	64	00	0D	00	63	6F	6F	56	2D	6F	63	sk read error oc

오프셋(h): 18 읽기전용 덮어쓰기

# MFT(Master File Table)의 위치 구하기

위치 값 = \$MFT클러스터 X 클러스터당 섹터 수 + VBR시작 섹터

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00007E00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	eR.NTFS .....
00007E10	00	00	00	00	00	F8	00	00	3F	00	FF	00	3F	00	00	00	.....e..y.?
00007E20	00	00	00	00	80	00	80	00	D8	A6	3F	01	00	00	00	00	.....e.e.0;?
00007E30	00	00	0C	00	00	00	00	00	6D	FA	13	00	00	00	00	00	.....má.....
00007E40	F6	00	00	00	01	00	00	00	0D	68	14	F4	7F	14	F4	52	ö.....h.ó.óR
00007E50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	B8	C0	07	...ú3ÀZD%. ú.ä.
00007E60	8E	D8	E8	16	00	B8	00	0D	8E	C0	33	DB	C6	06	0E	00	ž0é.....žÀ30ž...

Byte Per Sector	Not used by NTFS
Sectors Per Cluster	Not used by NTFS
Reserved Sectors	Total Sectors
Always 0	Logical Cluster Number for the file \$MFT
Not used by NTFS	Logical Cluster Number for the file \$MFTMirr
Media Descriptor	Clusters Per File Record Segment
Always 0	Clusters Per Index Buffer
Sectors Per Track	Not used by NTFS
Number Of Heads	Volume Serial Number
Hidden Sectors	Checksum



HxD - [새 볼륨 (D:)]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 16진수 섹터

새 볼륨 (D:)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	52	90	4E	54	46	53	20	20	20	00	02	08	00	00	00	ER.NTFS .....
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00	.....e..?.y.e...
00000020	00	00	00	00	80	00	80	00	FF	E7	1F	00	00	00	00	00	.....e.e.y.....
00000030	55	54	01	00	00	00	00	00	00	00	00	00	00	00	00	00	UT.....
00000040	F6	00	00	00	01	00	00	00	C8	B0	B8	3A	EC	B8	3A	F0	ö.....E°,i,:ð
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	...ú3ÄZD+.jûhÄ.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.E°....f.>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu."A"UI.r..û
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u..Ä..u.eY..fi
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	..h..H\$...<ö..i
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÿfÄ.zX.rá;...uÖe
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ü°. +E
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ZÄy...ë
000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Ewi,.,i.f\$Au-
000000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.üTCPAuö..ü.r..
000000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h..hR..h..fSfSf
00000100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h..fa..i.3Äj
00000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	...ö.üö*ëp...f.
00000120	06	66	Ä1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.fj..f.....fh...
00000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	..fP.Sh..h..B\$..
00000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<öi.fY[ZfYfY.
00000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ZÄy
00000160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u4..faÄjü.è..
00000170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	jü.è...öÿ<ö-<.t.
00000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	'..I..ëÄ..A di
00000190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
000001A0	63	75	72	72	65	64	00	0D	03	42	4E	4E	54	4D	47	52	sk read error oc

섹터 0

\$MTF클러스터 값  
0x015455 ->87125

HxD - [새 볼륨 (D:)]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 16진수 섹터

새 볼륨 (D:)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	52	90	4E	54	46	53	20	20	20	00	02	0B	00	00	00	æR.NTFS .....
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00	.....ø...?..y.€...
00000020	00	00	00	00	80	00	80	00	FF	E7	1F	00	00	00	00	00	....€.€..ÿç.....
00000030	55	54	01	00	00	00	00	00	02	00	00	00	00	00	00	00	UT.....
00000040	F6	00	00	00	01	00	00	00	C8	B0	B8	3A	EC	B8	3A	F0	ö.....Ë°.i,:ö
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ö3ÄZD+. öñÄ.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë'...f.>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A'*UI.r..ö
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u.+Ä..u.eÿ..fi
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'H\$...<ö..i.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÿfÄ.ËX.rä;...uöË
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ü+. +Ë
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ZÄy...ë
000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+ËwL...»i.f#Au-
000000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.öTCPAu\$.ü.r..
000000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..f\$F\$F
00000100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h..fa..i.3Ä¿
00000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..²ö.ó*ép...f'.
00000120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f;...f....fh...
00000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fp.Sh..h..'B\$..
00000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<öI.fY[ZfYfY.
00000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ZÄy
00000160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u4...faÄ;ö.e..
00000170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	jü.è...öÿ<ö-<.t.
00000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	'.»..i.öÄ..A di
00000190	73	6B	20	72	65	61	64	20	65	72	6F	72	20	6F	63		sk read error oc
000001A0	62	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	sk read error oc

클러스터당 섹터 수 = 8  
 VBR시작섹터 = 0  
 $87125 \times 8 + 0 = 697,000$

HxD - [새 볼륨 (D:)]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 16진수 섹터 697000

새 볼륨 (D:)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
15455000	46	49	4C	45	30	00	03	00	51	51	20	00	00	00	00	00	FILE.....
15455010	01	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00	.....
15455020	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00	.....
15455030	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	.....
15455040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
15455050	CB	B5	AC	B8	E7	05	D8	01	CB	B5	AC	B8	E7	05	D8	01	.....,.....,.....,.....
15455060	CB	B5	AC	B8	E7	05	D8	01	CB	B5	AC	B8	E7	05	D8	01	.....,.....,.....,.....
15455070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
15455080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	.....
15455090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	.....0...h...
154550A0	00	00	18	00	00	03	00	00	4A	00	00	00	18	00	01	00	.....J.....
154550B0	05	00	00	00	00	05	00	00	CB	B5	AC	B8	E7	05	D8	01	.....,.....,.....,.....
154550C0	CB	B5	AC	B8	E7	05	D8	01	CB	B5	AC	B8	E7	05	D8	01	.....,.....,.....,.....
154550D0	CB	B5	AC	B8	E7	05	D8	01	00	40	00	00	00	00	00	00	.....,.....,.....,.....
154550E0	00	40	00	00	00	00	00	00	06	00	00	00	00	00	00	00	.....@.....
154550F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00	...\$.M.F.T.....
15455100	80	00	00	00	48	00	00	00	01	00	40	00	00	00	06	00	...H.....@.....
15455110	00	00	00	00	00	00	00	00	3F	00	00	00	00	00	00	00	.....?.....
15455120	40	00	00	00	00	00	00	00	00	00	04	00	00	00	00	00	@.....
15455130	00	00	04	00	00	00	00	00	00	00	04	00	00	00	00	00	.....
15455140	31	40	55	54	01	00	00	00	B0	00	00	00	50	00	00	00	1@UT.....°...P...
15455150	01	00	40	00	00	00	05	00	00	00	00	00	00	00	00	00	..@.....
15455160	01	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
15455170	00	20	00	00	00	00	00	00	08	10	00	00	00	00	00	00	.....
15455180	08	10	00	00	00	00	00	00	31	01	54	54	01	31	01	D1	.....1.TT.1.N
15455190	AB	FE	00	00	00	00	00	00	FF	FF	FF	FF	00	00	00	00	<p.....yyyy...

MTF의 시그니처인 "FILE"을 확인할 수 있다.