NTFS 시스템에서 파일 복구 1

김우종

NTFS 란?

NTFS란 윈도우 NT 계열 운영체제에 파일시스템이다.

NTFS의 특징으로는

1. 이론적으로 최대 볼륨 크기가 16TB 실질적 최대 크기 2TB
2. 복구성과 보안성
3. 대용량 파일의 저장이 가능

NTFS 파일 복구 전 알아두어야 할 것들

- 저장매체의 제일 첫 번째 섹터의 MBR에서 파티션 테이블
- VBR의 첫 번째 섹터에서 BPB영역
- NTFS 시스템에서 전체 레이아웃
- MFT Entry 포맷 구성

MBR(Master Boot Record)이란?

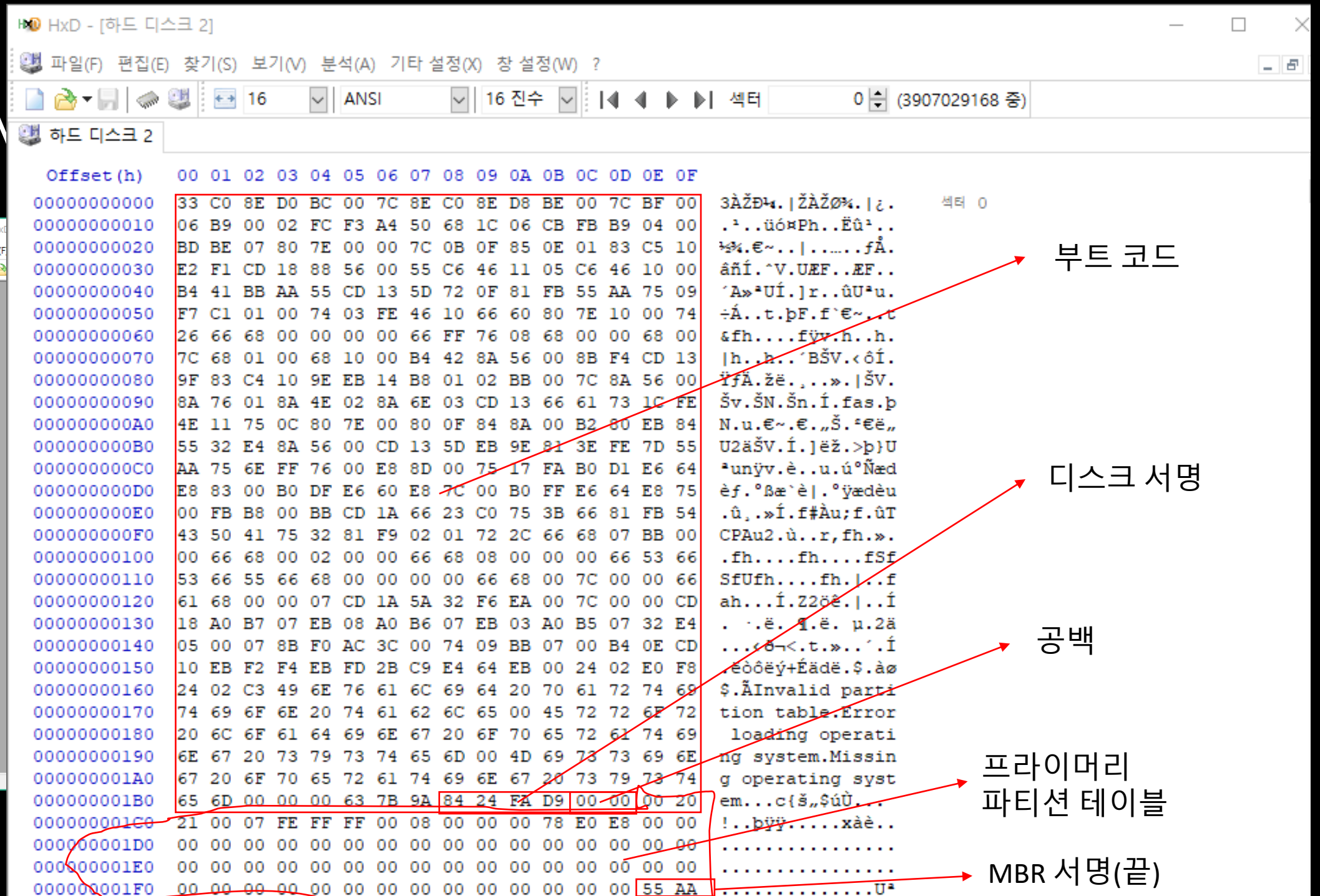
- MBR이란 데이터영역으로 분할된 기억장치[EX)하드디스크]의 첫 섹터 인 512Byte의 시동 섹터이다.

- MBR은 다음을 위해 사용 됨
  1. 디스크 프라이머리 파티션 테이블을 소유한다.
  2. 부트 스트래핑 운영 체제
  3. 32비트 디스크 서명이 있는 각 디스크 매체의 구별

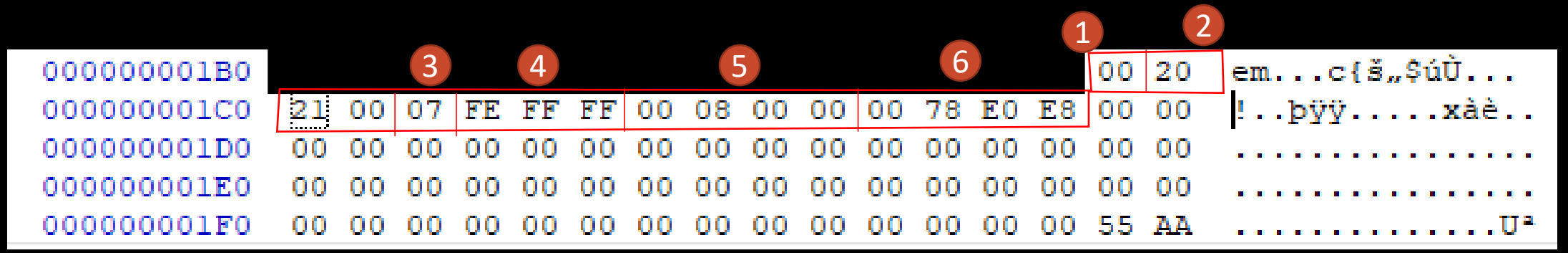
부트스트래핑:전원을 켜거나 재부팅 할 때 적재되는 프로그램

MBR의 구조

주소		설명		크기 (바이트)
십육진수	십진수			
0000	0	코드 영역		**440** 최대 446
01B8	440	디스크 서명		4
01BC	444	보통 없음(Null); 0x0000		2
01BE	446	**프라이머리 파티션 테이블** (4개의 16바이트 엔트리)		**64**
01FE	510	55h	MBR 서명; 0xAA55	**2**
01FF	511	AAh		
MBR, 전체 크기: 446 + 64 + 2 =				**512**


HxD - [하드 디스크 2]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
16
ANSI
16 진수
섹터
0
(3907029168 중)
하드 디스크 2
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000000 33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00 3ÀŽÐ¼.|ŽÀŽØ¾.|¿.
00000000010 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00 .¹..üó¤Ph..Ëû¹..
00000000020 BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10 ½¾.€~..|.....ƒÅ.
00000000030 E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00 âñÍ.ˆV.UÆF..ÆF..
00000000040 B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09 ´A»ªUÍ.]r..ûUªu.
00000000050 F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74 ÷Á..t.þF.f`€~..t
00000000060 26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00 &fh....fÿv.h..h.
00000000070 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13 |h..h..´BŠV.‹ôÍ.
00000000080 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00 ŸƒÄ.žë.¸..».|ŠV.
00000000090 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE Šv.ŠN.Šn.Í.fas.þ
000000000A0 4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84 N.u.€~.€.„Š.²€ë„
000000000B0 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55 U2äŠV.Í.]ëž.>þ}U
000000000C0 AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64 ªunÿv.è..u.ú°Ñæd
000000000D0 E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75 èƒ.°ßæ`è|.°ÿædèu
000000000E0 00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54 .û¸.»Í.f#Àu;f.ûT
000000000F0 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00 CPAu2.ù..r,fh.».
00000000100 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66 .fh....fh....fSf
00000000110 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66 SfUfh....fh.|..f
00000000120 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD ah...Í.Z2öê.|..Í
00000000130 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4 . ·.ë. ¶.ë. µ.2ä
00000000140 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD ...‹ð¬<.t.»..´.Í
00000000150 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8 .ëòôëý+Éädë.$.àø
00000000160 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69 $.ÃInvalid parti
00000000170 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72 tion table.Error
00000000180 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69 loading operati
00000000190 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E ng system.Missin
000000001A0 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 g operating syst
000000001B0 65 6D 00 00 00 63 7B 9A 84 24 FA D9 00 00 00 20 em...c{š„$úÙ...
000000001C0 21 00 07 FE FF FF 00 08 00 00 00 78 E0 E8 00 00 !..bÿÿ.....xàè..
000000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA ....Uª
부트 코드
디스크 서명
공백
프라이머리
파티션 테이블
MBR 서명(끝)

프라이머리 파티션 테이블 분석



	오프셋	설명
1	0x00	(1 바이트) 파티션 상태 (0x80 = 시동 가능, 0x00 = 부팅불가, 기타 = 비정상)
2	0x01	(3 바이트) 파티션의 첫 번째 섹터의 실린더-헤드-섹터 주소
3	0x04	(1 바이트) 파티션 종류[1]
4	0x05	(3 바이트) 파티션의 마지막 실린더-헤드-섹터 주소
5	0x08	(4 바이트) 파티션의 첫 번째 섹터의 LBA
6	0x0C	(4 바이트) 파티션의 크기 (단위: 섹터)

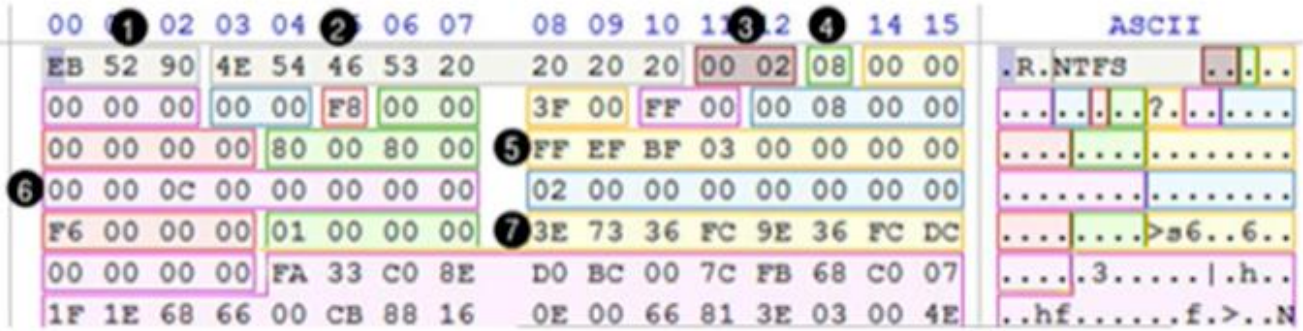
1. 파티션 상태 00 = 부팅 불가
2. CHS 시작 주소 <-여기서 사용 안함
3. 파티션 종류 07=NTFS
4. CHS 마지막 주소 <- 마찬가지로 사용 안함
5. 파티션테이블의 시작 위치 = 08 00 = 2048sector
6. 파티션의 크기 <- 사용 안함

볼륨의 전체 구성 (VBR/MFT)

- VBR
  - 운영체제가 NTFS를 인식하기 위한 시작점(XP = 63 sector 7 = 2048 sector)
  - 파일 시스템 구조의 레이아웃 정보 저장
  - 손상되면 NTFS 인식 불가
  - 파일 형태로 관리 ($boot)
- MFT : MFT Entry의 집합, 볼륨의 존재하는 파일과 디렉터리에 대한 정보를 갖고 있음
- Data Area : MFT에 포함되지 않는 정보가 저장됨

VBR의 첫번째 섹터에서 BPB영역

- VBR의 위치는 파티션테이블의 시작 위치에서 찾을 수 있음



00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	ASCII
EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	.R.NTFS ....
00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	....?....
00	00	00	00	80	00	80	00	FF	EF	BF	03	00	00	00	00	....
00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00	....
F6	00	00	00	01	00	00	00	3E	73	36	FC	9E	36	FC	DC	....>s6..6..
00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....3....|.h..
1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf....f.>..N

번호	필드 길이	데이터 값	필드 이름 및 정의
③	2bytes	00 02	섹터 당 바이트, 512바이트
④	1byte	08	클러스터 당 섹터 수, 8섹터 4096바이트
⑤	8bytes	FF D7 EF 0D 00 00 00 00	하드 디스크의 총 섹터 수(총 섹터 * 512 = 총 용량)
⑥	8bytes	00 00 0C 00 00 00 00 00	$MFT 파일의 클러스터 오프셋
⑦	8bytes	7E 39 EF 0E 60 EF 0E 14	볼륨 일련 번호

6번에서 MFT Entry 정보를 가지고 있는 섹터의 시작점을 알 수 있음

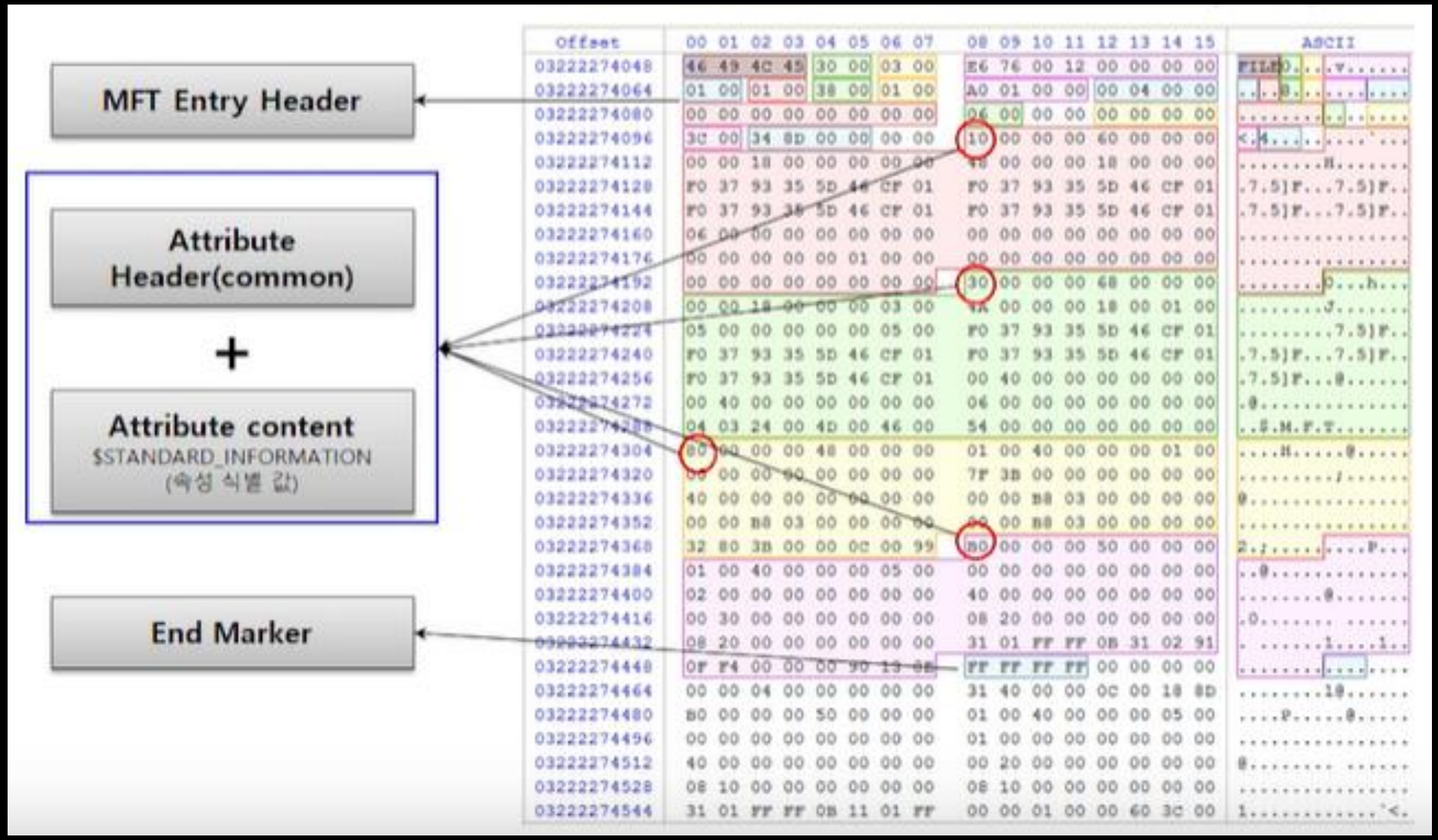
클러스터값 0C 00 00 = 786432(십진수)
(786432*8)+2048=MFT Entry 정보를 가진 섹터의 시작점

MFT 내부 구조

- MFT Entry 1024byte 구성

- 각 파일의 MFT Entry는 MFT Entry Header + 속성 구조를 통해 표현
  이름,시간정보,속성내용 등을 표현, 이를 메타정보라고 한다.
- 각 속성은 속성 헤더(Attribute Header)와 속성 내용(Attribute Content)을 가짐
- 일반적인 파일의 경우 아래 3개의 속성이 MFT Entry에 기록
  $STANDARD_INFORMATION : 모든 파일과 디렉터리 MFT Entry에 존재, 속성 중 맨 위에 위치, Base MFT Entry 에만 존재, 항상 resident (속성 값 : 0x10)
  $FILE_NAME : 파일이나 디렉터리 이름을 담은 속성 (속성 값 : 0x30)
  $DATA : 파일의 내용을 담고 있는 속성, 속성 헤더가 resident냐 non-resident냐에 따라 데이터 저장 위치가 달라짐 (속성 값 : 0x80)
- 위 3개 속성만으로 복구 분석 가능
- 그 외 알아야 하는 속성
  $BITMAP : 할당 정보를 관리, MFT와 인덱스에 할당 정보 관리하는 속성 (속성 값 : 0xB0)

MFT Entry 구조



0x10
$STANDATD_INFORMATION

0x30
$FILE_NAME

0x80
$DATA

0xB0
$BITMAP