[Kevin's Attic for Security Research]

NTFS Fundamentals

kevinkoo001@gmail.com

What to Cover

1. Information with Tools
2. NTFS Layout
3. MBR
4. VBR
5. MFT

   MFT Entry and MFT Attributes

   Cluster Runs

   LCN&VCN

   Sparse/Compression

   Resident/Non-Resident File

NTFS Fundamentals

NTFS > Information with Tools

- (Sysinternals) ntfsinfo.exe c:\

```
D:¥Tools¥SysinternalsSuite>ntfsinfo.exe c:

NTFS Information Dump V1.01
Copyright (C) 1997 Mark Russinovich
http://www.sysinternals.com

Volume Size
-----------
Volume size              : 52100 MB
Total sectors            : 106701776
Total clusters           : 13337722
Free clusters            : 551042
Free space               : 2152 MB (4% of drive)

Allocation Size
---------------
Bytes per sector         : 512
Bytes per cluster        : 4096
Bytes per MFT record     : 1024
Clusters per MFT record: 0

MFT Information
--------------
MFT size                 : 199 MB (0% of drive)
MFT start cluster        : 786432
MFT zone clusters        : 11478144 - 11478784
MFT zone size            : 2 MB (0% of drive)
MFT mirror start         : 6668861
```

Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.

[References]
http://technet.microsoft.com/en-us/sysinternals/bb545027.aspx

NTFS Fundamentals

NTFS > Information with Tools

- (TSK) mmls \\.\PhysicalDrive0

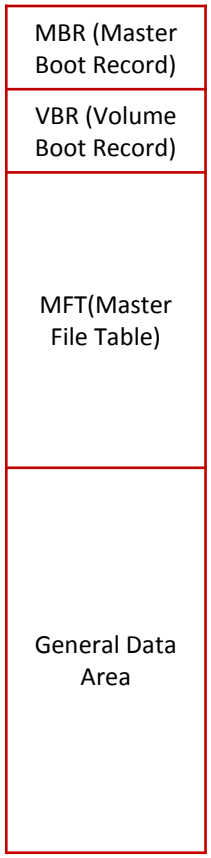
```
D:₩Tools₩Digital Forensic₩Integrated Toolkit₩sleuthkit-win32-4.0.2₩bin>mmls ₩₩.₩
PhysicalDrive0
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0106701839   0106701777   NTFS (0x07)
03:  Meta    0106701840   0250069679   0143367840   Win95 Extended (0x0f)
04:  Meta    0106701840   0106701840   0000000001   Extended Table (#1)
05:  -----   0106701840   0106701902   0000000063   Unallocated
06:  01:00   0106701903   0250069679   0143367777   NTFS (0x07)
```

- FSUTIL
  c:\fsutil fsinfo ntfsinfo [Drive]

```
C:₩Users₩Mr.Koo>fsutil fsinfo ntfsinfo c:
NTFS 볼륨 일련 번호:              0xdc8429c184299ed0
버전:                             3.1
섹터 개수:                        0x00000000065c23d0
전체 클러스터 개수:               0x0000000000cb847a
사용 가능한 클러스터:             0x0000000000004bcc7
예약된 개수:                      0x00000000000007c0
섹터당 바이트:                    512
실제 섹터당 바이트:               512
클러스터당 바이트:                4096
FileRecord 세그먼트당 바이트:     1024
FileRecord 세그먼트당 클러스터:   0
Mft 올바른 데이터 길이:           0x000000000c7c0000
Mft 시작 Lcn:                     0x0000000000c0000
Mft2 시작 Lcn:                    0x000000000065c23d
Mft 영역 시작:                    0x0000000000af2480
Mft 영역 끝:                      0x0000000000af2700
RM 식별자:          B8171DCB-6FD7-11E1-9FCD-806E6F6E6963
```

[References]
http://www.sleuthkit.org/sleuthkit/

- NTFS Layout



❖ 모든 Data를 File 형태로 관리함: 파일 시스템 관리 데이터, 사용자 데이터

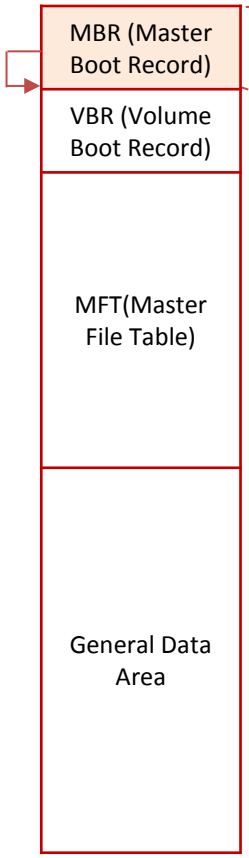
❖ 관리 데이터 역시 물리적 위치와 독립적임

❖ 단, VBR은 BPR(BIOS Parameter Block)으로 고정 위치에 존재함

- Volume 설정값, 실행코드

[References]
http://

- MBR(Master Boot Record)

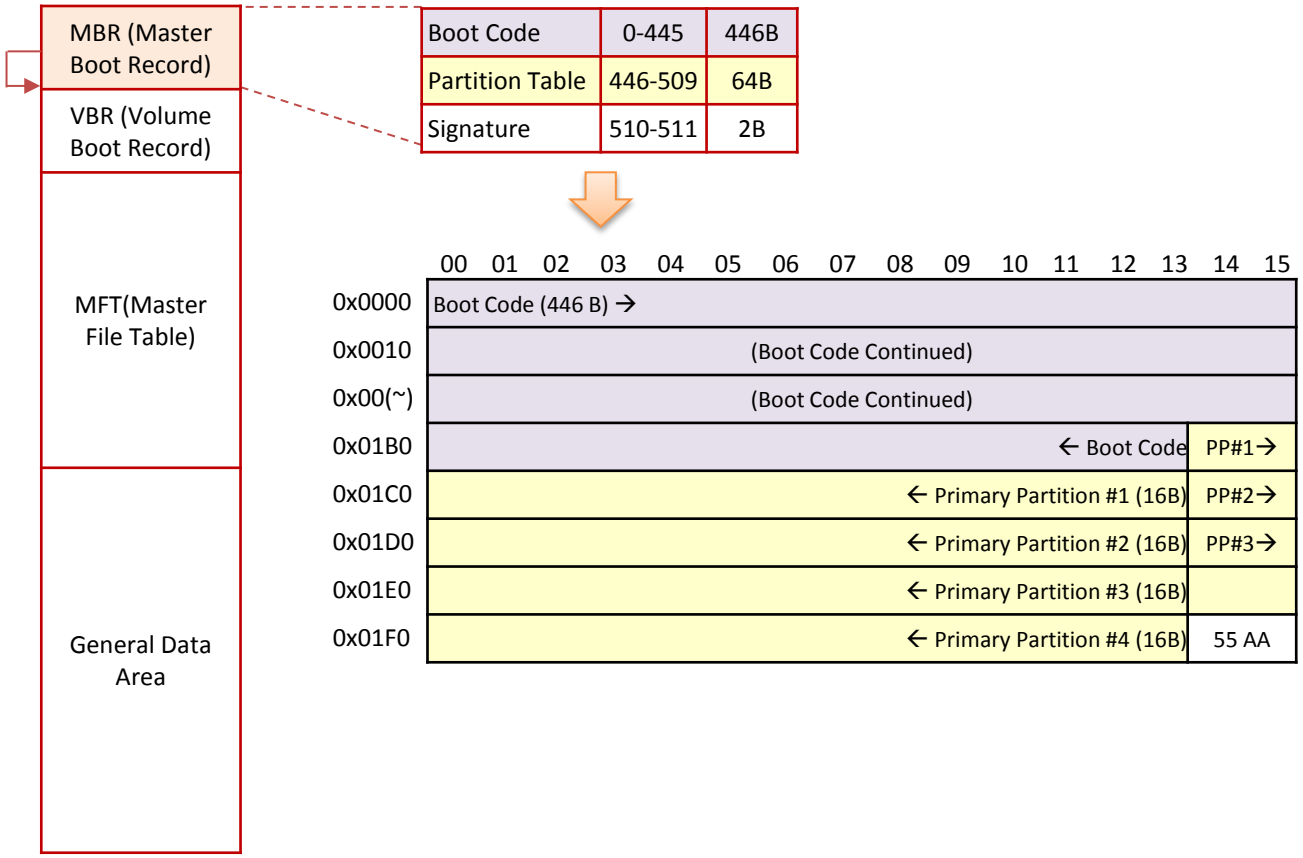


Boot Code	0-445	446B
Partition Table	446-509	64B
Signature	510-511	2B

- ❖ 저장매체의 가장 첫 번째 Sector(LBA 0)에 위치함
- ❖ Boot Code는 기계어로 Booting 가능한 Partition을 지정하며, 없을 경우 오류 메시지 출력
- ❖ Partition Table은 주 파티션 4개 정보를 가지며, Table 당 16B임
- ❖ MBR은 VBR의 시작점을 가리킴
- ❖ Cluster (512 Byte) 크기
- ❖ Signature: 0x55AA

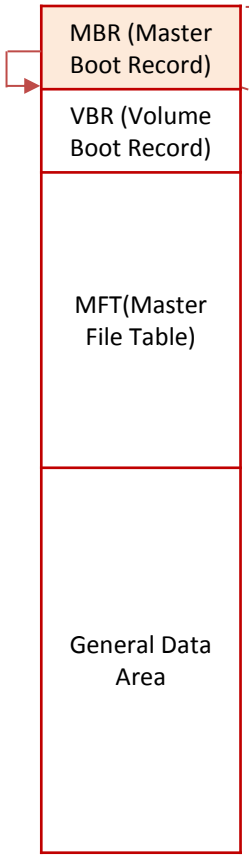
[References]
http://

- MBR(Master Boot Record)

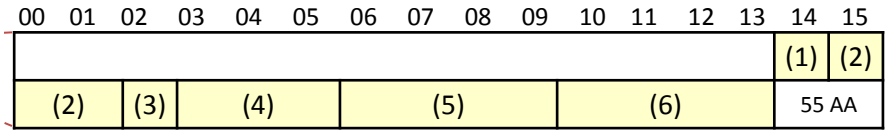


[References]
http://

- MBR(Master Boot Record): Partition Table Structure



Boot Code	0-445	446B
Partition Table	446-509	64B
Signature	510-511	2B



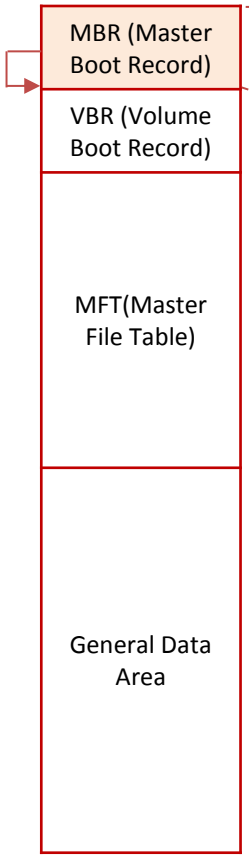
Field	Size	Description	Note
(1) Boot flag	1B	0x80 (부팅가능), 0x00(부팅불가)	
(2) Starting CHS Address	3B	CHS 방식일 경우 Partition 시작 CHS 주소	
(3) Partition Type (0x00 – 0xFF)	1B	Wiki 참조	0x07
(4) Ending CHS Address	3B	CHS 방식일 경우 Partition 마지막 CHS 주소	
(5) Starting LBA Address	4B	LBA 방식일 경우 Partition 시작 LBA 주소	
(6) Size in Sector	4B	Partition에 할당한 Sector 수	

[References]
http://en.wikipedia.org/wiki/Partition_type

NTFS Fundamentals

NTFS > MBR(Master Boot Record)

- MBR(Master Boot Record)

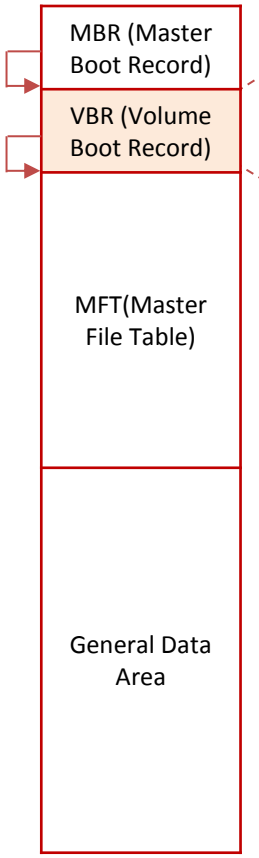


Boot Code	0-445	446B
Partition Table	446-509	64B
Signature	510-511	2B

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
0000000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
0000000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
0000000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
0000000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
0000000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
0000000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
0000000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
0000000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
0000000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
00000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
00000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
00000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
00000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
00000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
00000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
0000000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
0000000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
0000000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
0000000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
0000000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
0000000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
0000000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
0000000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
0000000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
0000000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
00000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
00000001B0	65	6D	00	00	00	63	7B	9A	0F	27	10	27	00	00	80	01
00000001C0	01	00	07	EF	FF	FF	3F	00	00	00	D1	23	5C	06	00	EF
00000001D0	FF	FF	0F	EF	FF	FF	10	24	5C	06	A0	9E	8B	08	00	00
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

[References]
http://en.wikipedia.org/wiki/Partition_type

- VBR(Volume Boot Record) or BPB(Boot Parameter Block)

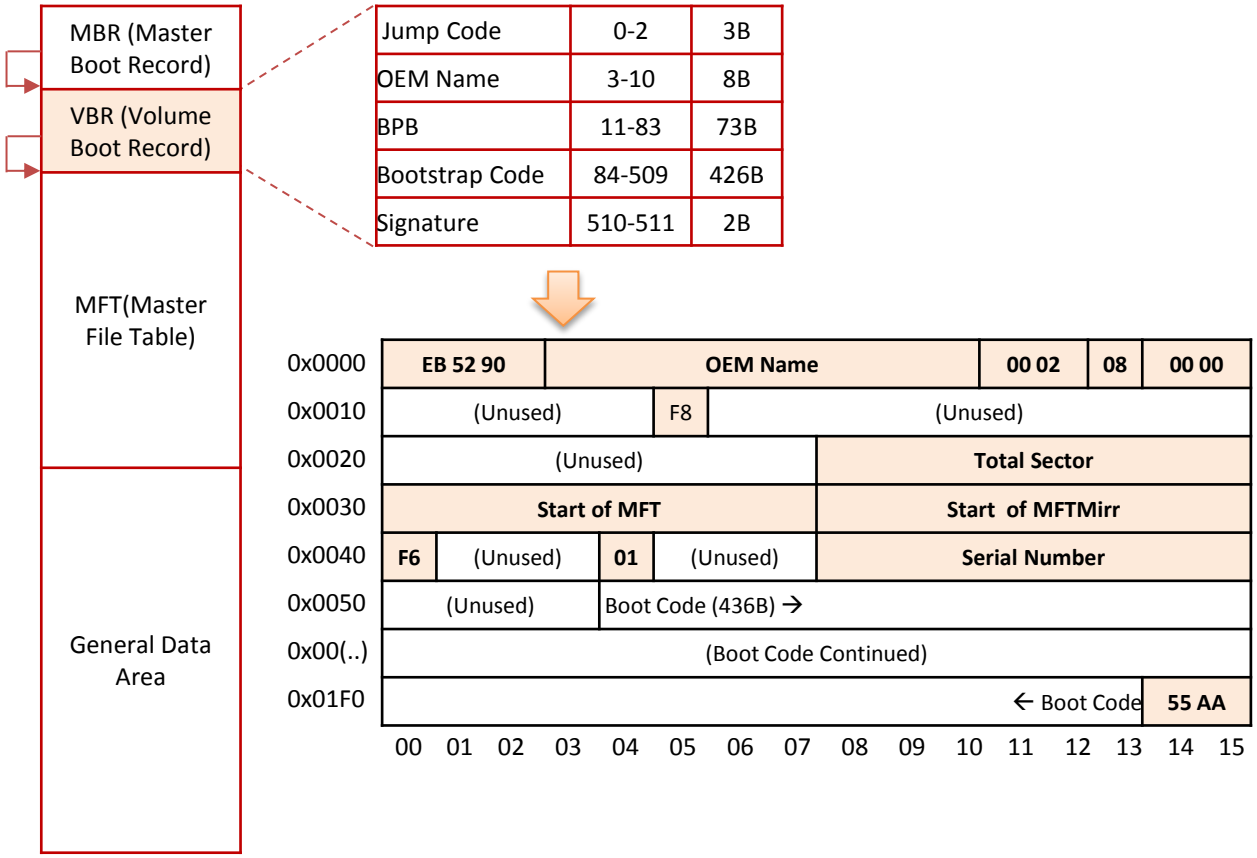


Jump Code	0-2	3B
OEM ID	3-10	8B
BPB	11-83	73B
Bootstrap Code	84-509	426B
Signature	510-511	2B

- ❖ NTFS Partition의 가장 첫 번째 Sector에 위치함
- ❖ Boot Sector, NTLDR 위치, Boot Code 정보를 포함하며 BPB(Boot Parameter Block)이라고도 함
- ❖ VBR은 MFT의 시작점을 가리킴
- ❖ Cluster (512 Byte) 크기
- ❖ Signature: 0x55AA

[References]
http://

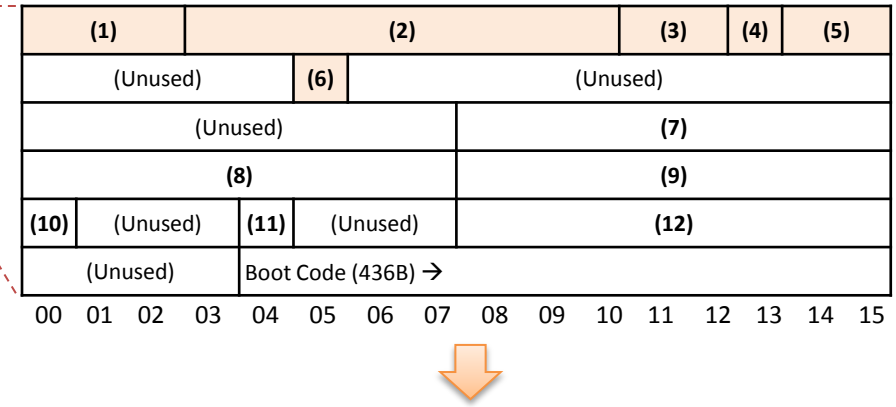
- VBR(Volume Boot Record) or BPB(Boot Parameter Block)



[References]
http://

- VBR(Volume Boot Record) or BPB(Boot Parameter Block)

Jump Code	0-2	3B
OEM Name	3-10	8B
BPB	11-83	73B
Bootstrap Code	84-509	426B
Signature	510-511	2B

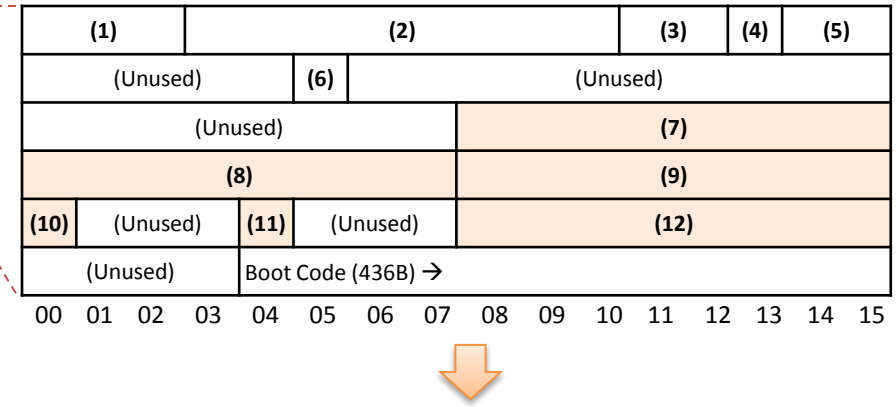


Field	Size (Offset)	Description	Note
(1) Jump Boot Code	3B (0-2)	부트 코드로 점프하는 기계어 Instruction	0xEB5290
(2) OEM ID	8B (3-10)	제조회사를 나타냄, 윈도우는 “NTFS “로 표기	
(3) Bytes Per Sector	2B (11-12)	Sector 당 Byte 수 (512,1024,2048,4096 중 하나)	512 (0xF6)
(4) Sectors Per Cluster	1B (13)	Cluster 당 Sector 수 (0보다 크고 2의 배수)	8
(5) Reserved Sector Count	2B (14-15)	NTFS는 Reserved 영역이 없고 Partition 앞에 Boot Sector가 존재하므로 0x00	0
(6) Media	1B (21)	Volume을 어떤 Media에 저장하는지 기록, 최신 윈도우는 이 항목을 참조하지 않음	0xF8 (고정disk)

[References]
http://

- VBR(Volume Boot Record) or BPB(Boot Parameter Block)

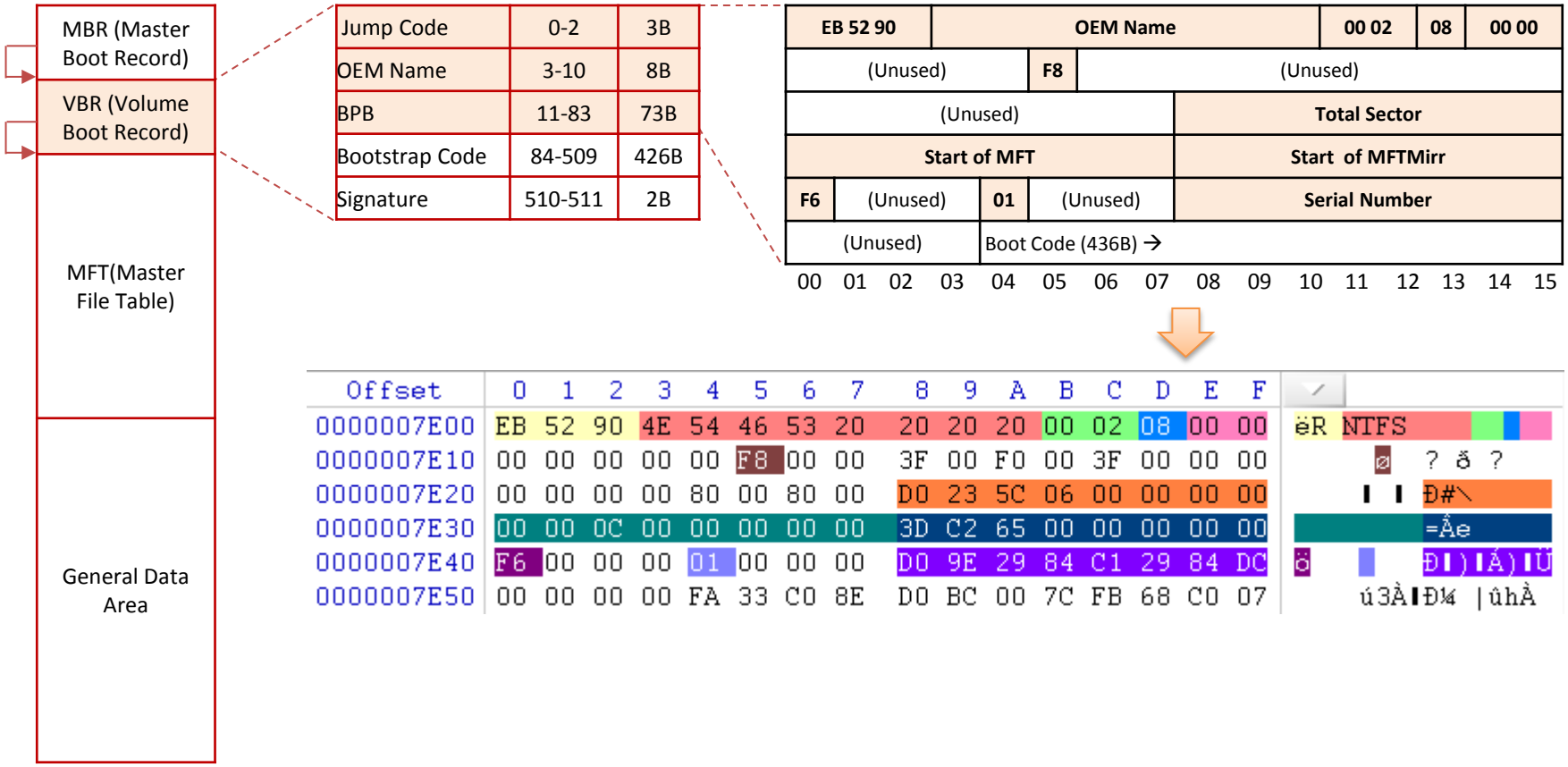
Jump Code	0-2	3B
OEM Name	3-10	8B
BPB	11-83	73B
Bootstrap Code	84-509	426B
Signature	510-511	2B



Field	Size (Offset)	Description	Note
(7) Total Sectors	8B (40-47)	Volume에 있는 전체 Sector 수	
(8) Start Cluster of $MFT	8B (48-55)	MFT의 시작 Cluster 주소	
(9) Start Cluster of $MFTMirr	8B (56-63)	MFT 복사본 MFTMirr의 Cluster 주소	
(10) MFT Entry Size	1B (64)	MFT Entry 크기 (2^(-10)=1,024)	0xF6
(11) Index Record Size	1B (68)	Index Record의 크기	0x01
(12) Serial Number	8B (72-79)	Volume의 Serial Number	

[References]
http://

- VBR(Volume Boot Record) or BPB(Boot Parameter Block) Example

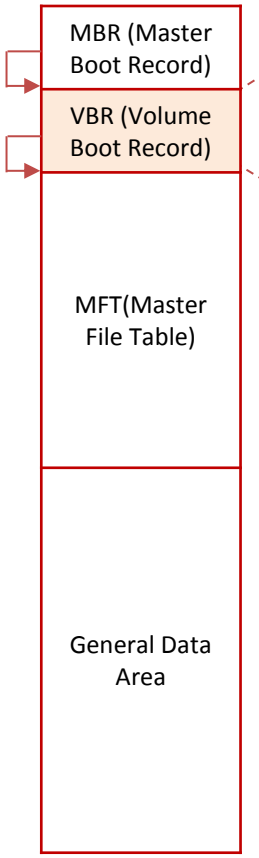


[References]
http://

NTFS Fundamentals

NTFS > VBR(Volume Boot Record)

- VBR(Volume Boot Record) or BPB(Boot Parameter Block) Example

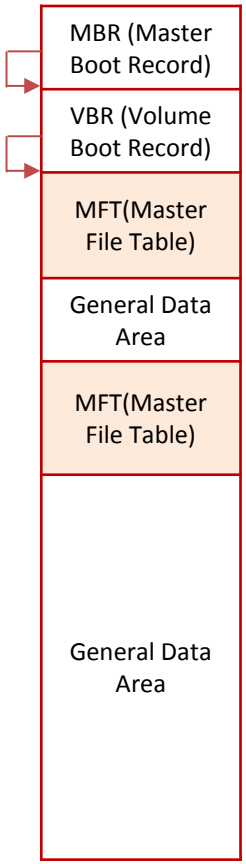


Jump Code	0-2	3B
OEM Name	3-10	8B
BPB	11-83	73B
Bootstrap Code	84-509	426B
Signature	510-511	2B

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000007E00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
0000007E10	00	00	00	00	00	F8	00	00	3F	00	F0	00	3F	00	00	00
0000007E20	00	00	00	00	80	00	80	00	D0	23	5C	06	00	00	00	00
0000007E30	00	00	0C	00	00	00	00	00	3D	C2	65	00	00	00	00	00
0000007E40	F6	00	00	00	01	00	00	00	D0	9E	29	84	C1	29	84	DC
0000007E50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
0000007E60	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E
0000007E70	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB
0000007E80	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC
0000007E90	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13
0000007EA0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3
0000007EB0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8
0000007EC0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8
0000007ED0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D
0000007EE0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16
0000007EF0	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66
0000007F00	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF
0000007F10	28	10	B9	D8	0F	FC	F3	AA	E9	5F	01	90	90	66	60	1E
0000007F20	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00
0000007F30	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E
0000007F40	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F
0000007F50	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF
0000007F60	0E	16	00	75	BC	07	1F	66	61	C3	A0	F8	01	E8	09	00
0000007F70	A0	FB	01	E8	03	00	F4	EB	FD	B4	01	8B	F0	AC	3C	00
0000007F80	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20
0000007F90	64	69	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20
0000007FA0	6F	63	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D
0000007FB0	47	52	20	69	73	20	6D	69	73	73	69	6E	67	00	0D	0A
0000007FC0	42	4F	4F	54	4D	47	52	20	69	73	20	63	6F	6D	70	72
0000007FD0	65	73	73	65	64	00	0D	0A	50	72	65	73	73	20	43	74
0000007FE0	72	6C	2B	41	6C	74	2B	44	65	6C	20	74	6F	20	72	65
0000007FF0	73	74	61	72	74	0D	0A	00	8C	A9	BE	D6	00	00	55	AA

[References]
http://

- MFT (Master File Table)

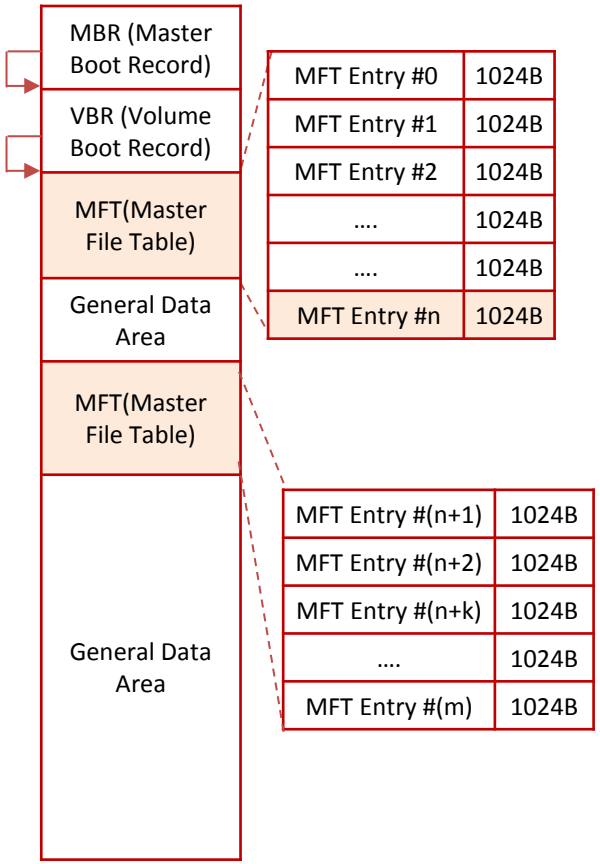


- ❖ Includes the information for all files and directories
- ❖ Increases the size as the number of entries grow gradually
- ❖ Grows only and never shrinks as MFT Entry is not removed when a file is deleted

- ❖ Each cluster can contain 4 MFT Entries when the cluster size of 4KB.
- ❖ Each file may have more than a single MFT entry.
- ❖ What would be the size of MFT if the number of files in the volume is 100,000?

[References]
http://

- MFT (Master File Table) Entry



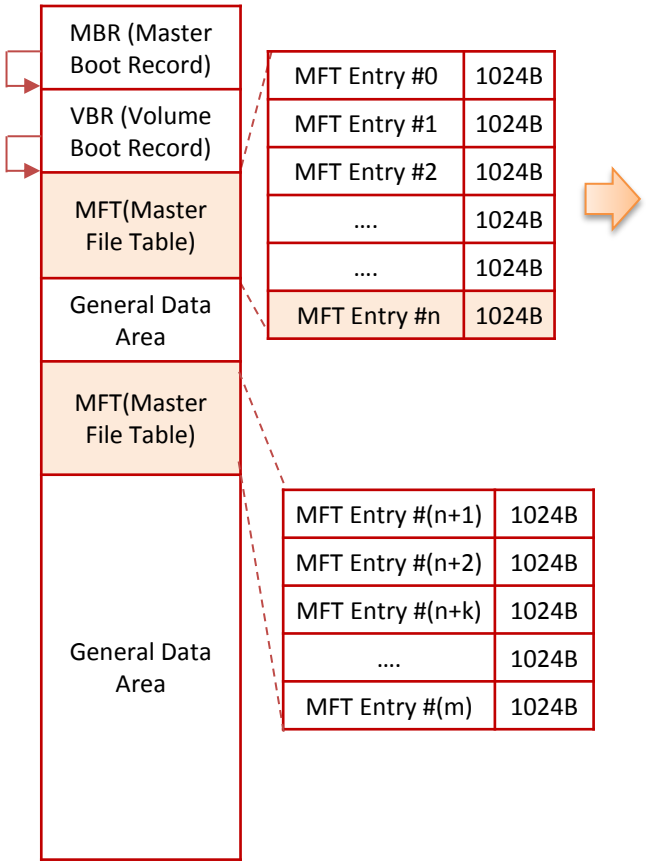
- ❖ MFT Entry consists of MFT Entry Header and multi-Attributes.
- ❖ An attribute consists of Attribute Header and Content.
- ❖ Signature: 0x46494c45 or FILE
- ❖ Each MFT Entry has 1KB (= 1024 Bytes) in size.
- ❖ Sometimes this is called File Record.

[References]
http://

NTFS Fundamentals

NTFS > MFT(Master File Table)

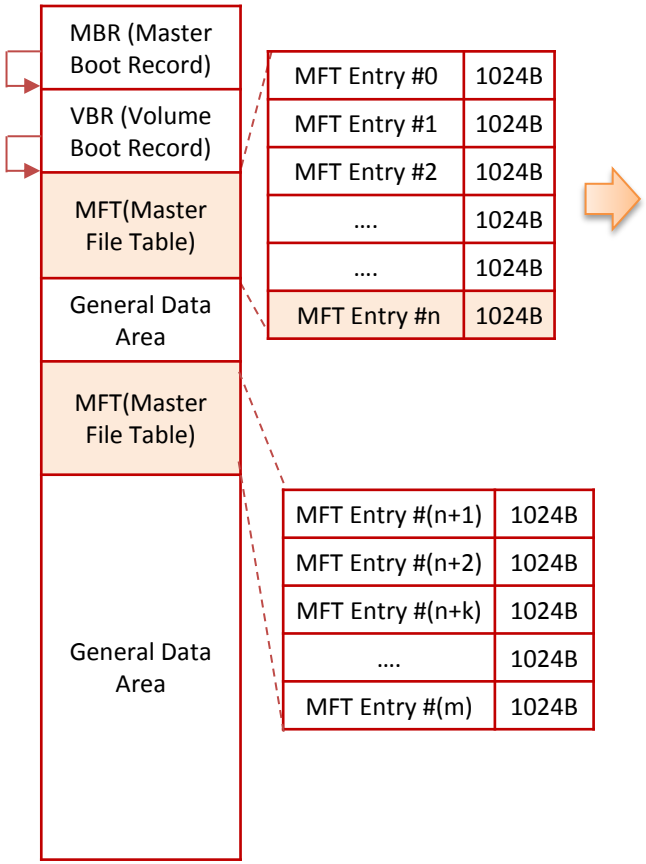
- MFT (Master File Table) Entry 0-15 : Meta Data Files (Reserved)



MFT Entry #	Filename	Description
0	$MFT	MFT 자체 정보를 담은 파일
1	$MFTMirr	MFT 파일 백업
2	$LogFile	Transaction Journal 기록
3	$Volume	Volume에 관한 정보
4	$AttrDef	인자 값, 이름, 크기 속성 정보
5	.	File System Root directory
6	$Bitmap	File System Cluster 할당 관리 정보
7	$Boot	Boot Record 영역 정보
8	$BadClus	Bad Cluster 관련 정보
9	$Secure	File 보안과 접근 권한 정보
10	$Upcase	모든 Unicode 대문자
11	$Extend	추가적인 확장 directory
12~23	Unused	사용하지 않음
24~	General Files	일반 File, Directory 저장
Not specified	$ObjId	파일 고유의 Object ID (Win2K 이상)
Not specified	$Quota	사용량 정보 (Win2K 이상)
Not specified	$Reparse	Reparse Point 정보 (Win2K 이상)
Not specified	$UsnJrnl	File, Directory 변경 시 기록 (Win2K 이상)

[References]
http://

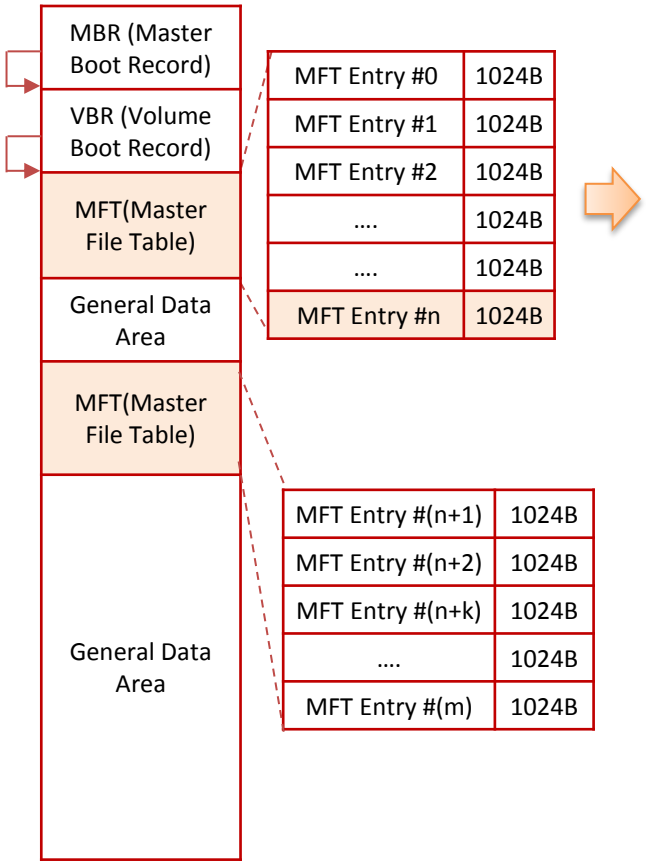
- MFT (Master File Table) Entry : File Reference Address (File Record Number)

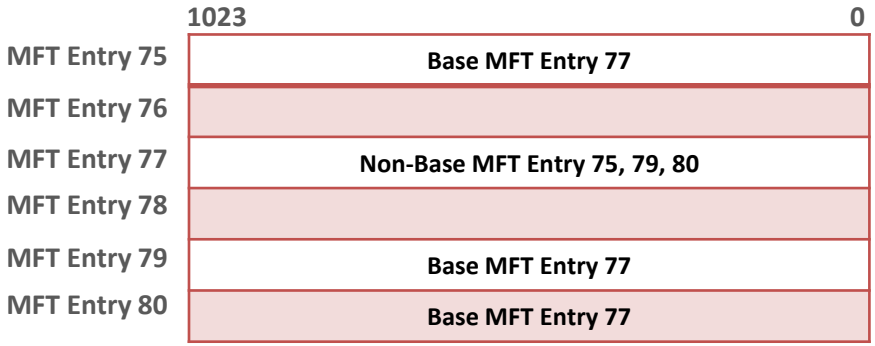


- What if MFT Entry number is 2,048?
- MFT Entry Address: 0x000000000800
- Sequence Value: 0x0020

[References]
http://

- MFT (Master File Table) Entry : Base / Non-base





- In case of 4 MFT Entries:

  Whole MFT Entries: 75, 77, 79, 80

  Base MFT Entry: 77

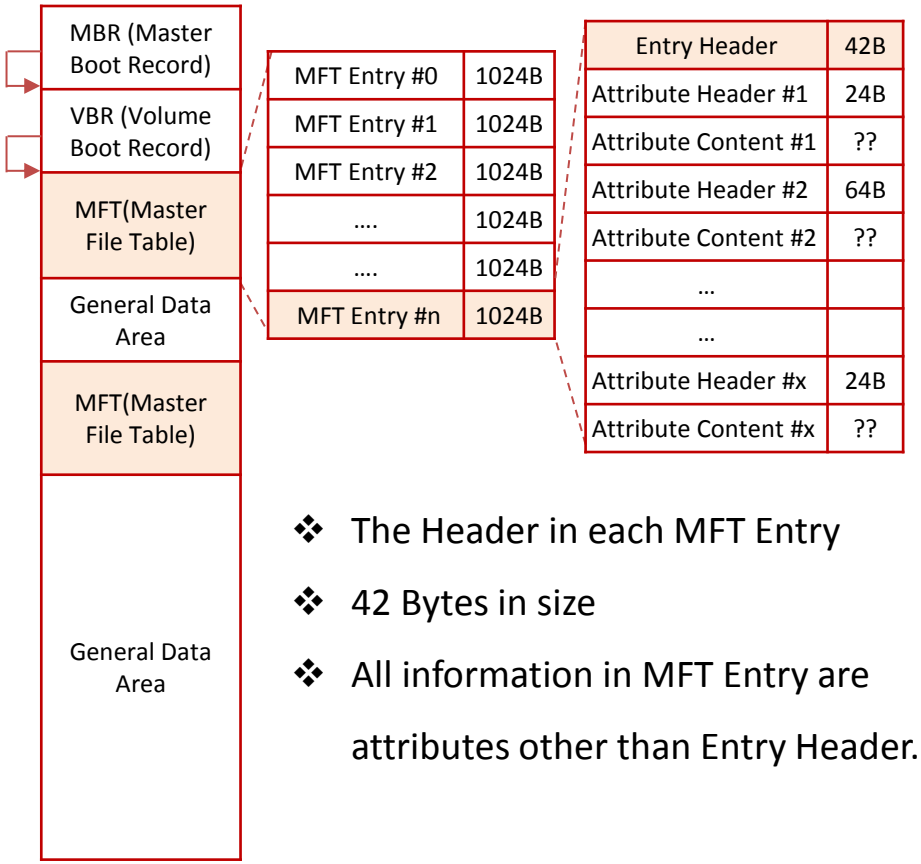
  Non-Base MFT Entries: 75, 79, 80

- Non-base Entry has a value for

  "*File Reference to base MFT Entry*" item in MFT Header

[References]
http://

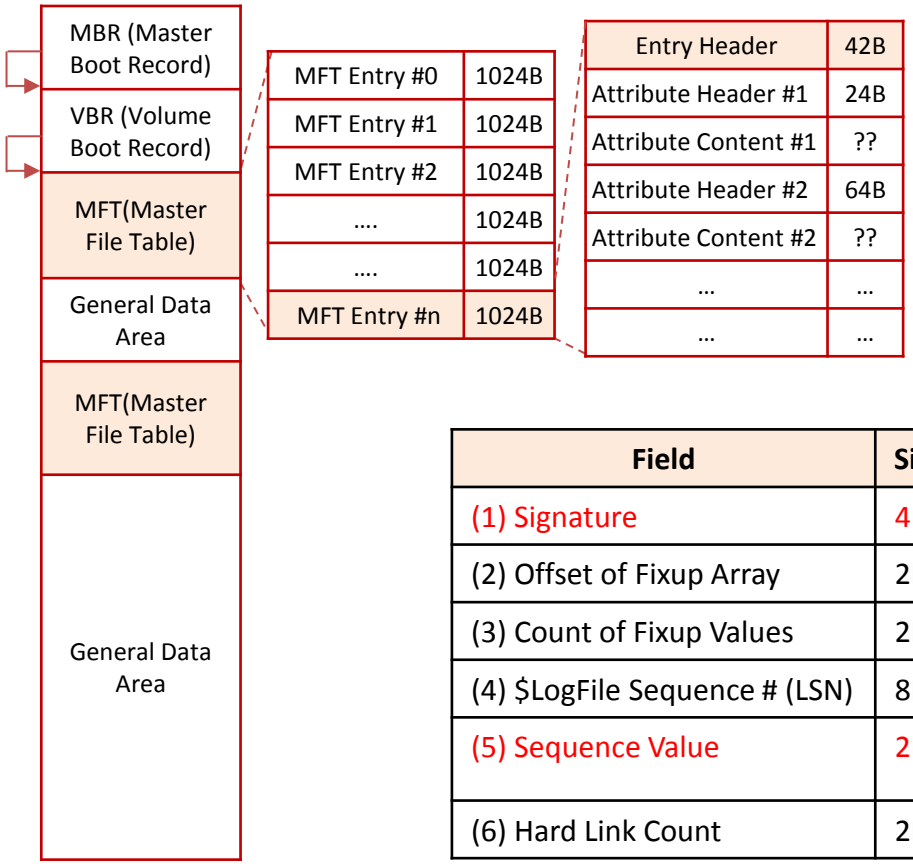
- MFT (Master File Table) Entry Header

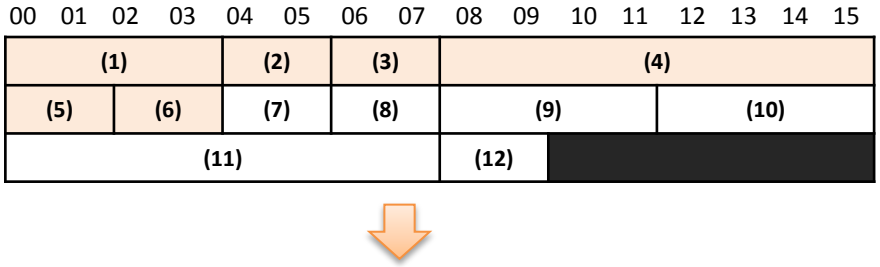


- ❖ The Header in each MFT Entry
- ❖ 42 Bytes in size
- ❖ All information in MFT Entry are attributes other than Entry Header.

[References]
http://

- MFT (Master File Table) Entry Header

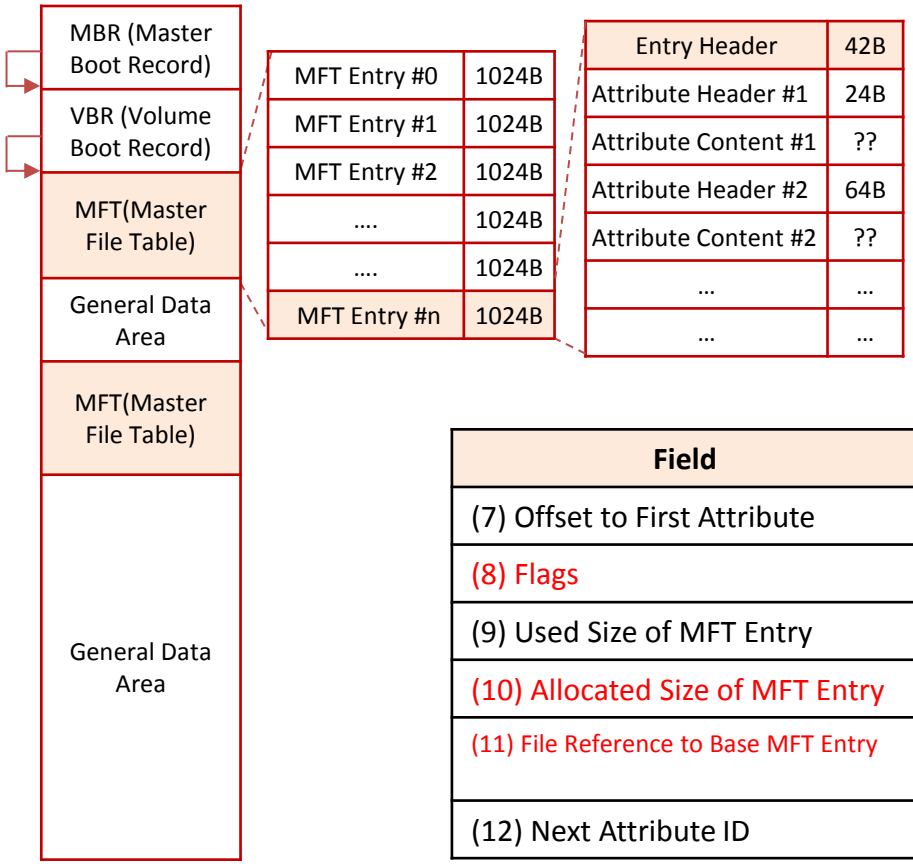


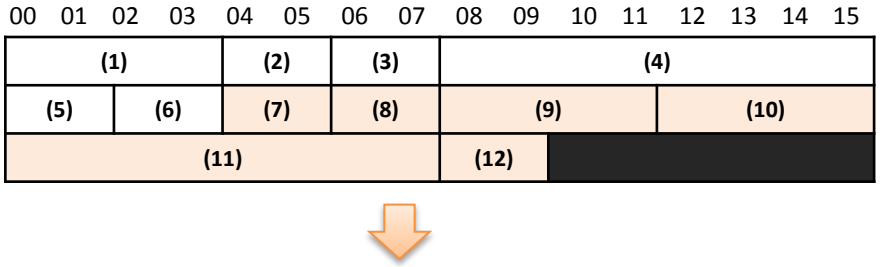


Field	Size (Offset)	Description	Note
(1) Signature	4B (0-3)	단순 문자열로 보통 'FILE' 문자열로 구성	0x46494c45
(2) Offset of Fixup Array	2B (4-5)	MFT Entry 내 Fixup 배열 위치 정보	0x0030 (48)
(3) Count of Fixup Values	2B (6-7)	Fixup 배열 항목 개수	0x0003 (3)
(4) $LogFile Sequence # (LSN)	8B (8-15)	$LogFile에 data 의 마지막 Transaction 위치	
(5) Sequence Value	2B (16-17)	MFT Entry 할당/해제시 File Reference Addr. 주소 생성, 항상 값이 증가함	
(6) Hard Link Count	2B (18-19)	MFT Entry에 연결되어 있는 Hard Link 수	0x0001 (1)

[References]
http://

- MFT (Master File Table) Entry Header

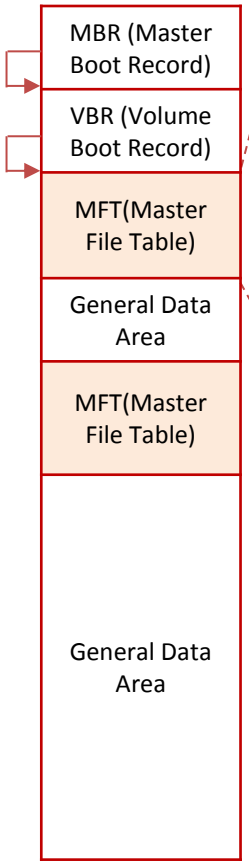




Field	Size (Offset)	Description	Note
(7) Offset to First Attribute	2B (20-21)	첫 번째 속성의 Offset	0x0038 (56)
(8) Flags	2B (22-23)	0x01 (사용중), 0x02 (디렉토리)	
(9) Used Size of MFT Entry	4B (24-27)	MFT Entry가 사용하는 실제 Byte수	
(10) Allocated Size of MFT Entry	4B (28-31)	MFT Entry 크기 (항상 1 KB = 1,024B)	1024
(11) File Reference to Base MFT Entry	8B (32-39)	Non-base MFT Entry일 경우 base MFT Entry 위치의 File Reference Address	
(12) Next Attribute ID	2B (40-41)	미래에 생성할 속성이 가질 속성 ID	

[References]
http://

- MFT (Master File Table) Entry Header Example



MFT Entry #0	1024B
MFT Entry #1	1024B
MFT Entry #2	1024B
....	1024B
....	1024B
MFT Entry #n	1024B

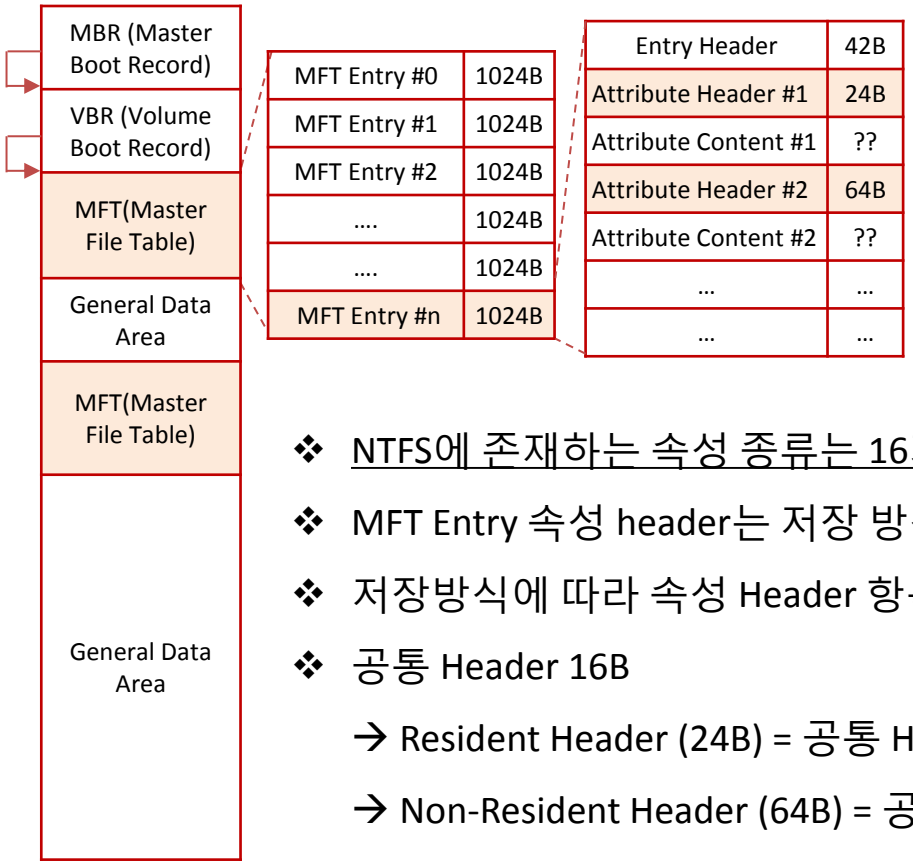
Entry Header	42B
Attribute Header #1	24B
Attribute Content #1	??
Attribute Header #2	64B
Attribute Content #2	??
...	...
...	...

00 01	02 03	04 05	06 07	08 09 10 11	12 13 14 15
Signature		Offset of Fixup Array	Count of Fixup Values	$LogFile Sequence Number (LSN)	
Sequence Value	Hard Link Count	Offset to First Attr.	Flags	Used Size of MFT Entry	Allocated Size of MFT Entry
File Reference to Base MFT Entry				Next Attr. ID	

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	46	49	4C	45	30	00	03	00	83	E1	72	4A	10	00	00	00
00000010	01	00	01	00	38	00	01	00	E8	01	00	00	00	04	00	00
00000020	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00

[References]
http://

- MFT (Master File Table) Entry Attribute Header



❖ NTFS에 존재하는 속성 종류는 16가지임

❖ MFT Entry 속성 header는 저장 방식에 따라 Resident, Non-Resident로 나눔

❖ 저장방식에 따라 속성 Header 항목이 다름

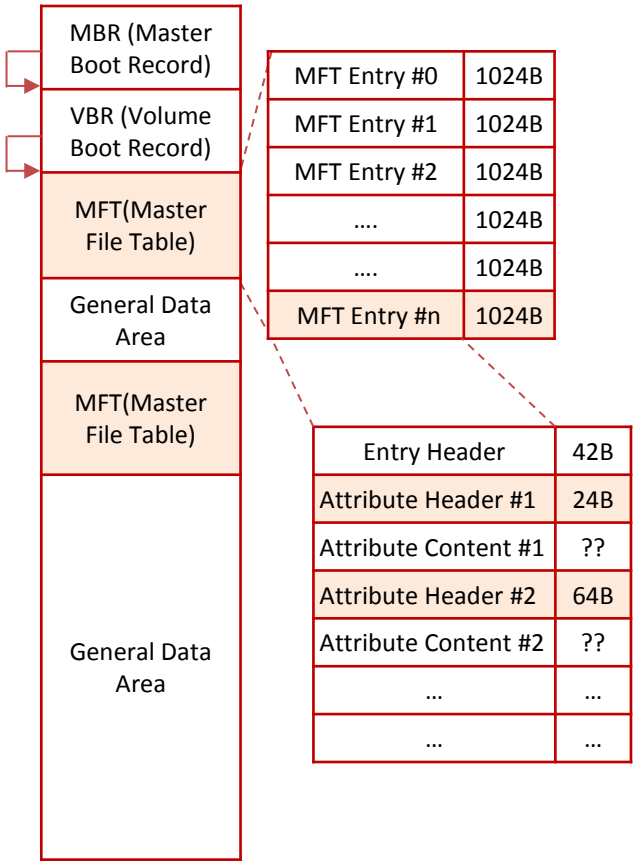
❖ 공통 Header 16B

→ Resident Header (24B) = 공통 Header (16B) + 전용 Header (8B)

→ Non-Resident Header (64B) = 공통 Header (16B) + 전용 Header (48B)

[References]
http://

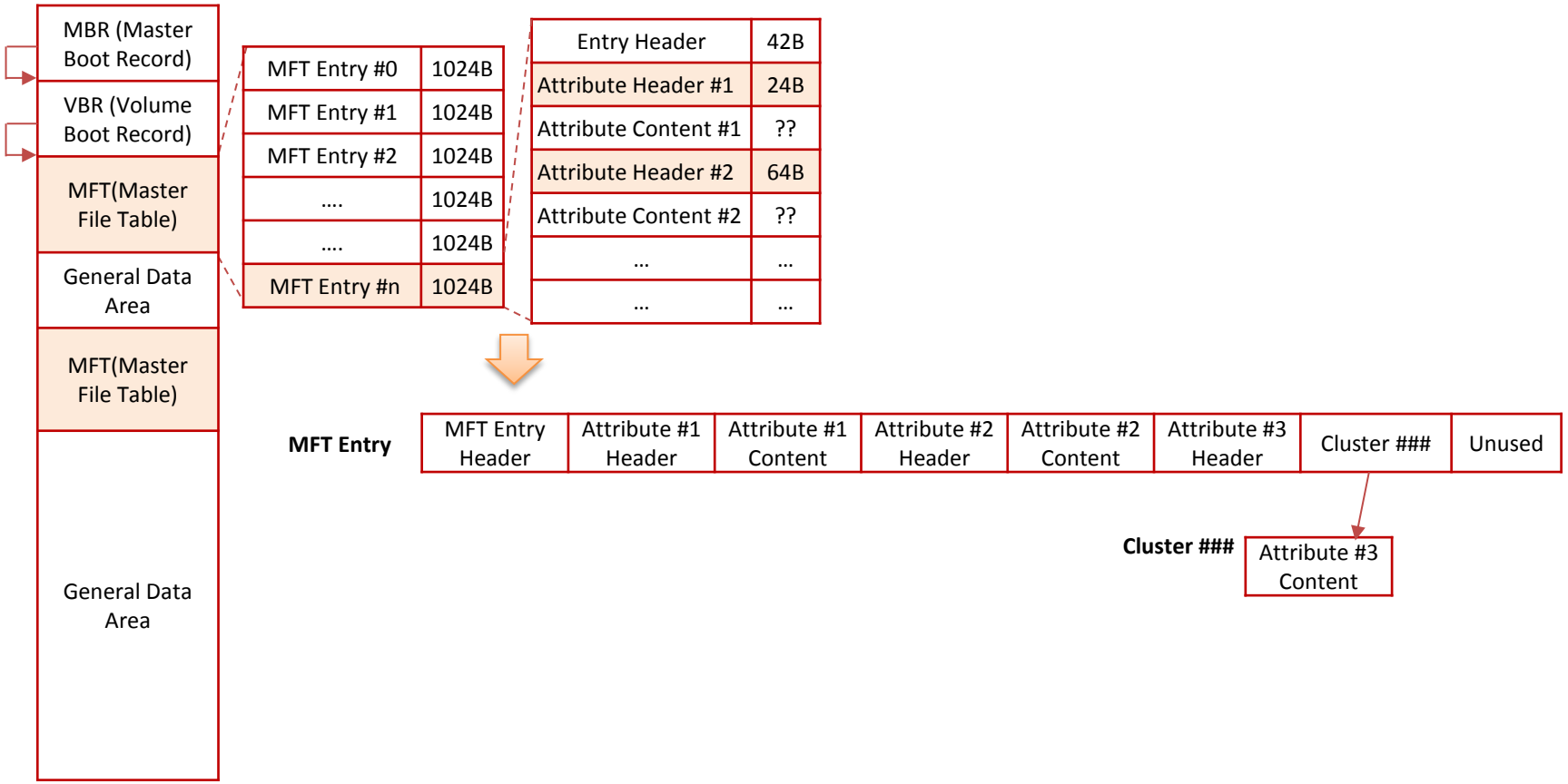
- MFT (Master File Table) Entry Attribute Kinds



Attr Type ID	Attr Name	Description
0x10 (16)	$STANDARD_INFORMATION	최근접근시간, 생성시간, 소유자
0x20 (32)	$ATTRIBUTE_LIST	속성 리스트
0x30 (48)	$FILE_NAME	유니코드 형식의 파일명
0x40 (64)	$VOLUME_VERSION	Volume 정보 (이전 버전)
0x40 (64)	$OBJECT_ID	File, Directory 고유 값
0x50 (80)	$RECURITY_DESCRIPTOR	File 접근 제어와 보안 속성
0x60 (96)	$VOLUME_NAME	Volume명
0x70 (112)	$VOLUME_INFORMATION	File System 버전과 Flag
0x80 (128)	$DATA	File 내용
0x90 (144)	$INDEX_ROOT	Index Tree의 Root node
0xa0 (160)	$INDEX_ALLOCATION	Index Tree와 연결된 node
0xb0 (176)	$BITMAP	할당 정보 관리 속성
0xc0 (192)	$SYMBOLIC_LINK	Soft Link 정보 (이전 버전)
0xc0 (192)	$REPARSE_POINT	Reparse 위치 정보
0xd0 (208)	$EA_INFORMATION	OS/2 호환용
0xe0 (224)	$EA	OS/2 호환용
0xf0 (256)	$LOGGED_UTILITT_STREAM	암호화 속성 정보와 Key

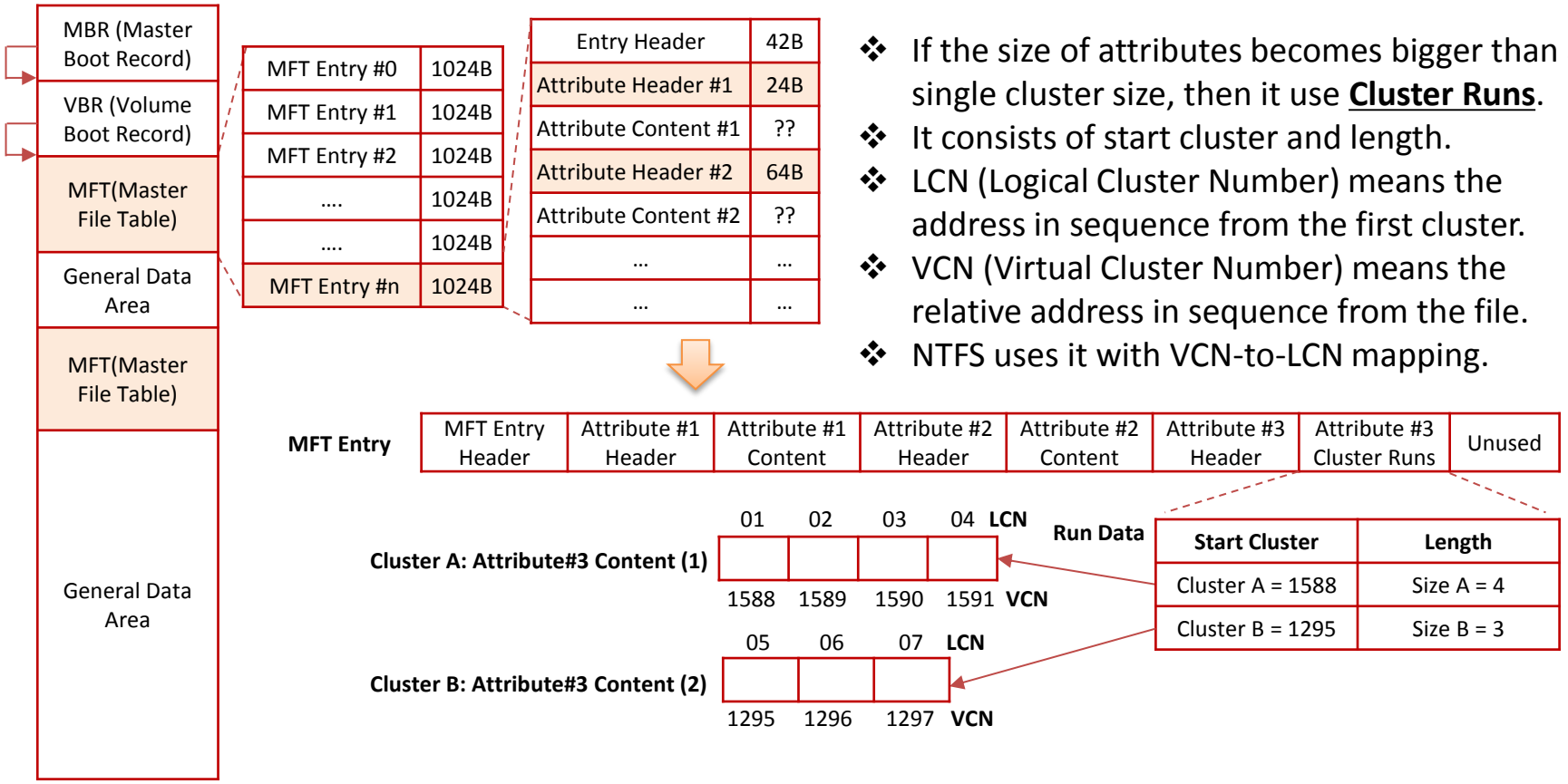
[References]
http://

- MFT (Master File Table) Entry Structure Overview



[References]
http://

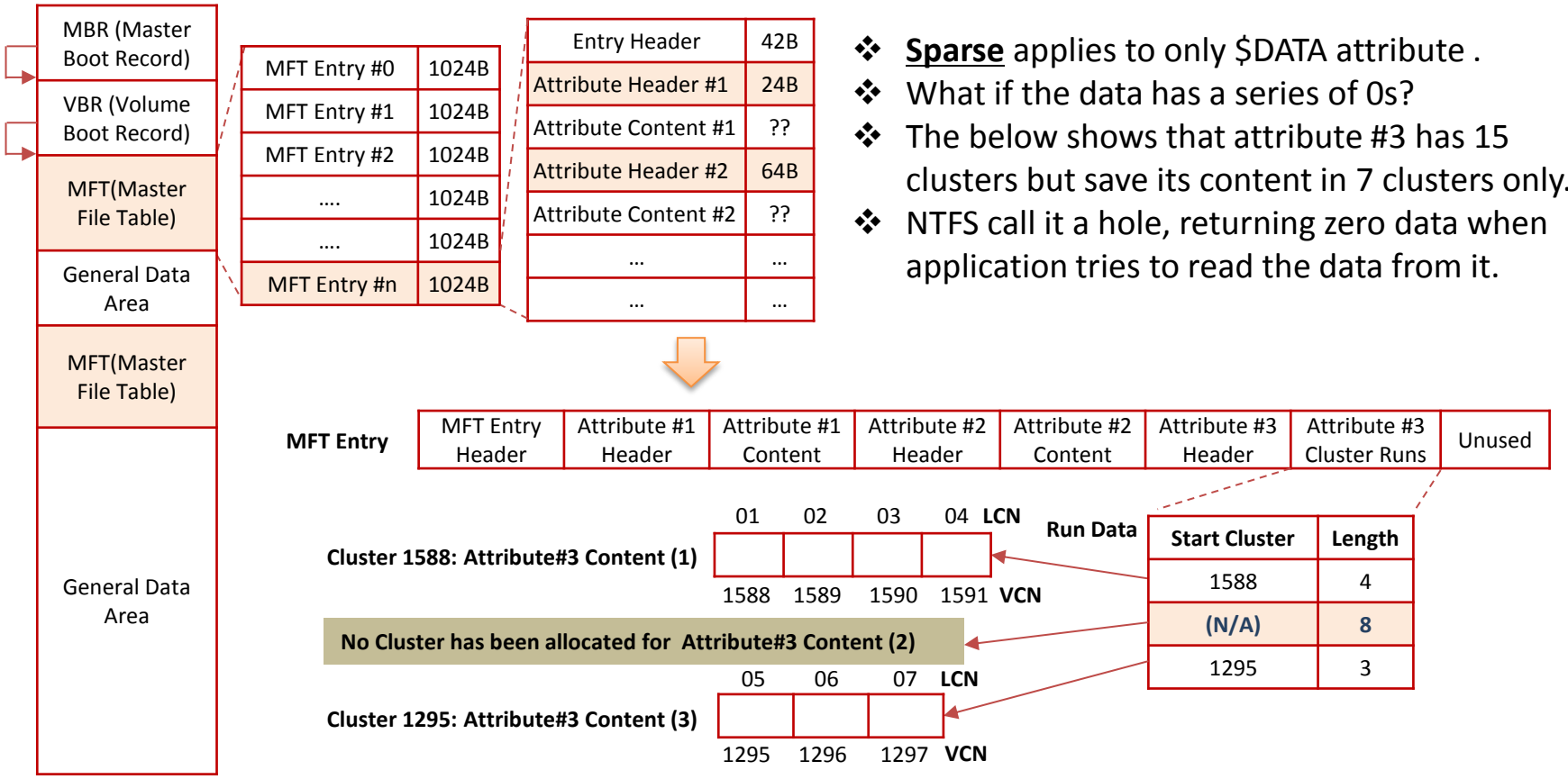
- MFT (Master File Table) Entry Structure: Cluster Runs, LCN & VCN



- If the size of attributes becomes bigger than a single cluster size, then it use **Cluster Runs**.
- It consists of start cluster and length.
- LCN (Logical Cluster Number) means the address in sequence from the first cluster.
- VCN (Virtual Cluster Number) means the relative address in sequence from the file.
- NTFS uses it with VCN-to-LCN mapping.

[References]
http://

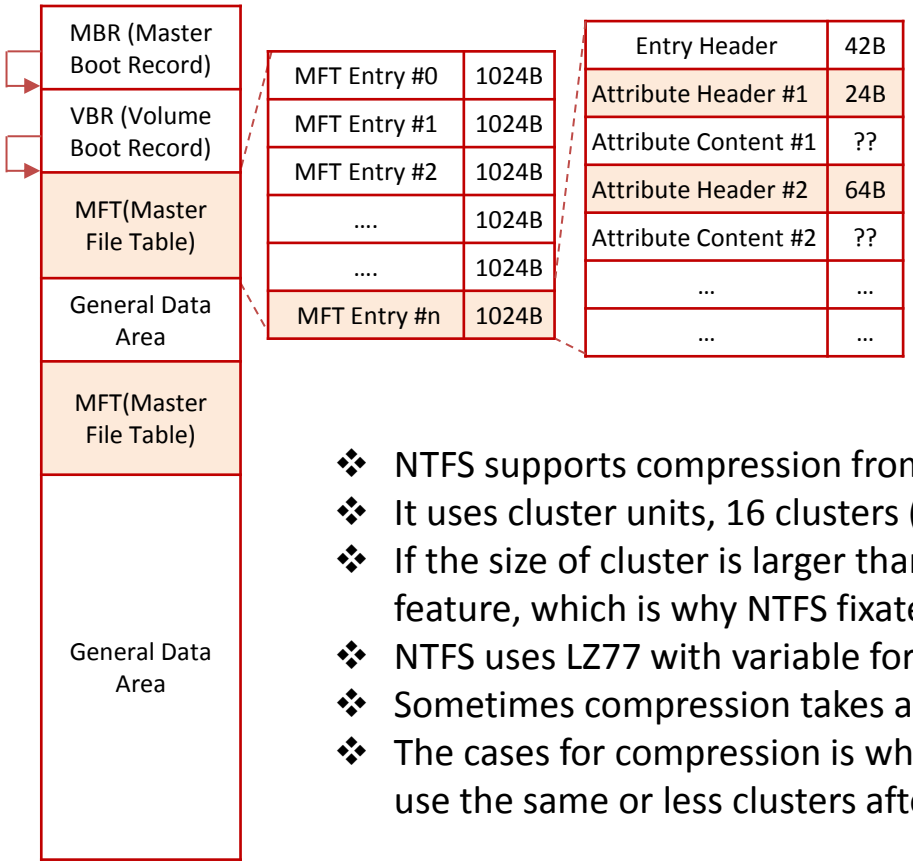
- MFT (Master File Table) Entry Structure: Sparse Attribute



- ❖ **Sparse** applies to only $DATA attribute .
- ❖ What if the data has a series of 0s?
- ❖ The below shows that attribute #3 has 15 clusters but save its content in 7 clusters only.
- ❖ NTFS call it a hole, returning zero data when application tries to read the data from it.

[References]
http://

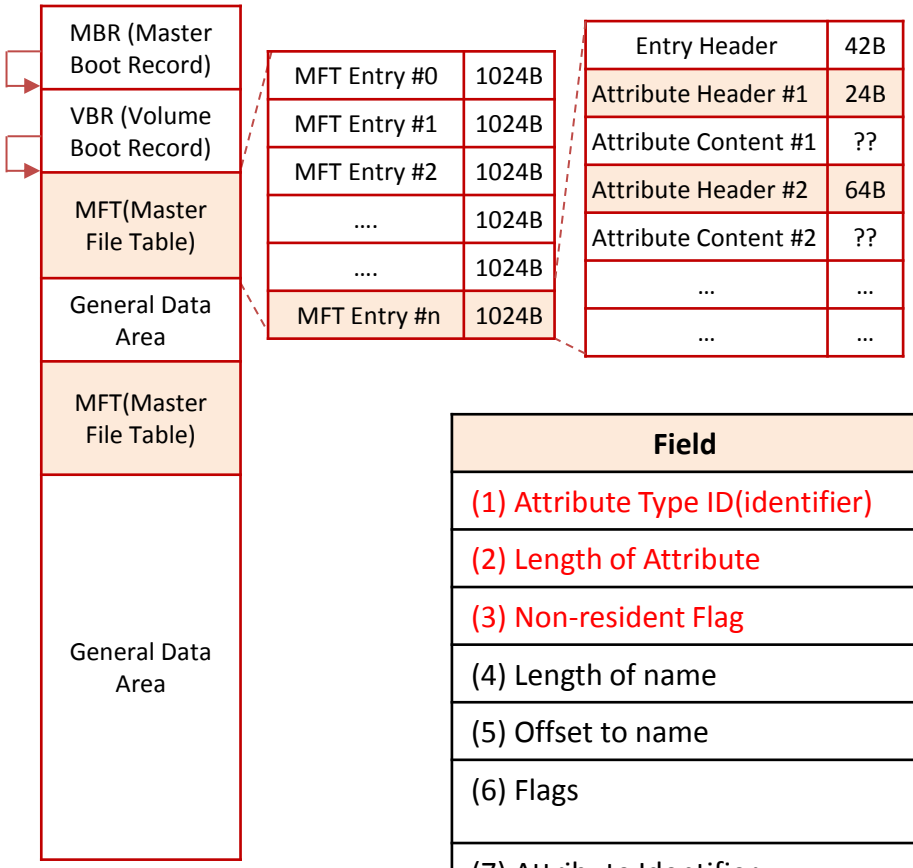
- MFT (Master File Table) Entry Structure: Compression Attribute

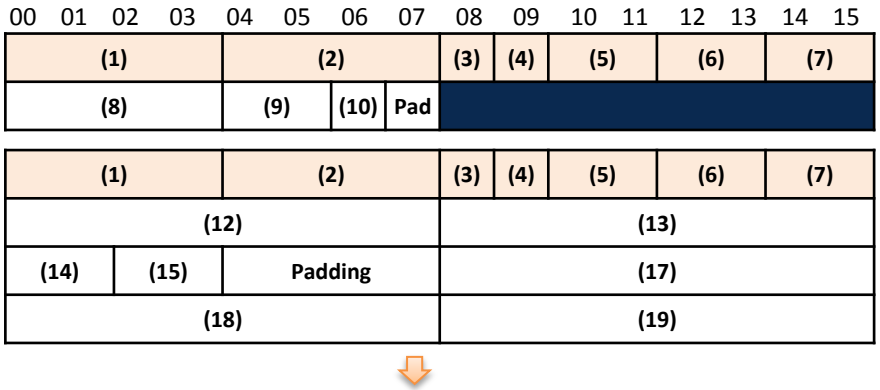


- NTFS supports compression from file system viewpoint.
- It uses cluster units, 16 clusters (usually 64KB) by default.
- If the size of cluster is larger than 4KB, then NTFS does not support compression feature, which is why NTFS fixates it as 4 KB at most.
- NTFS uses LZ77 with variable for compression algorithm.
- Sometimes compression takes advantage of sparse attribute if necessary.
- The cases for compression is when to store all 0s for data (sparse) and when to use the same or less clusters after compression.

[References]
http://

- MFT (Master File Table) Entry Attribute Header (Common)

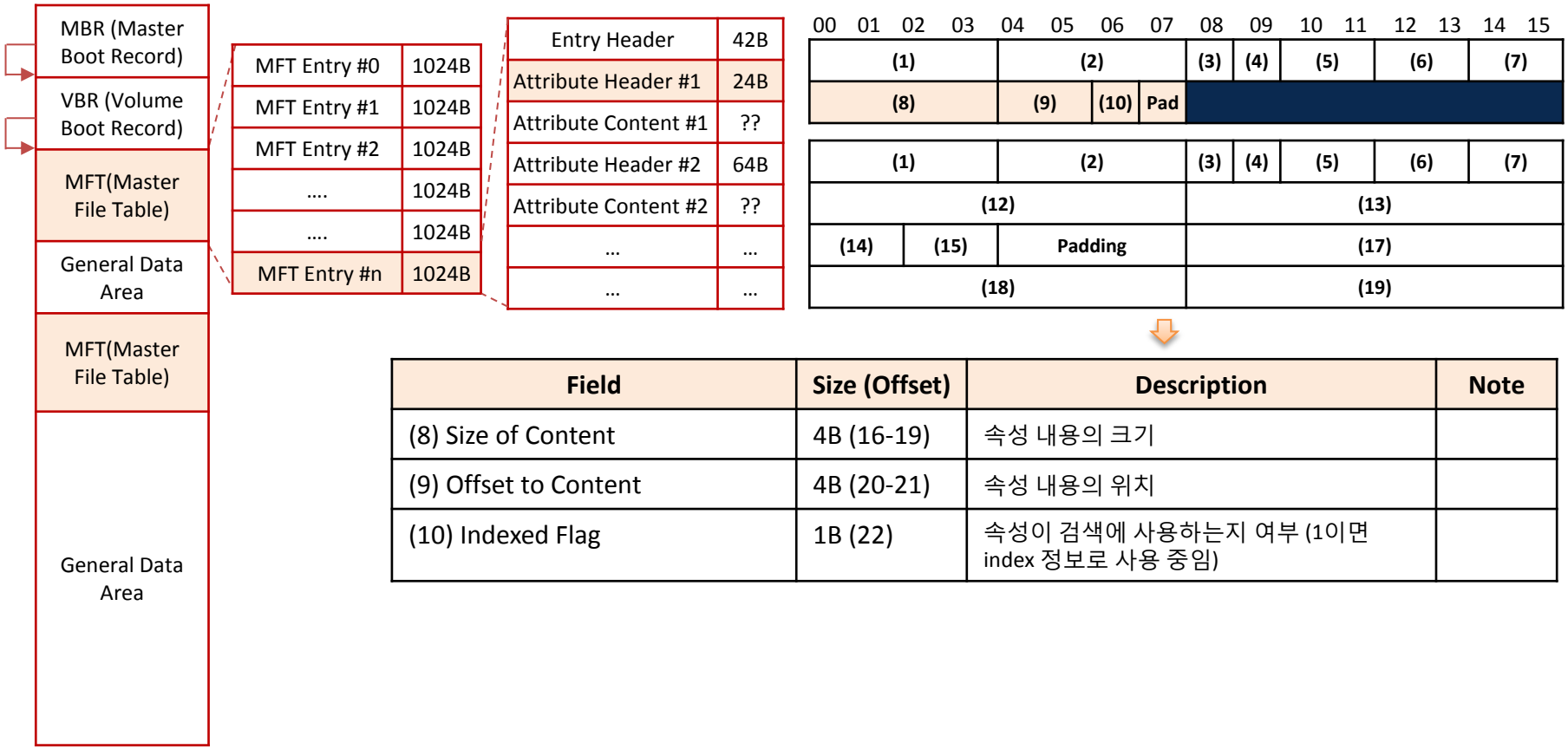




Field	Size (Offset)	Description	Note
(1) Attribute Type ID(identifier)	4B (0-3)	속성 고유의 Type ID	
(2) Length of Attribute	4B (4-7)	속성의 길이 (Header + Content)	
(3) Non-resident Flag	1B (8)	1 (Non-resident), 0 (Resident) 속성	
(4) Length of name	1B (9)	속성 이름의 길이	
(5) Offset to name	2B (10-11)	속성 이름의 저장 위치	
(6) Flags	2B (12-13)	속성의 상태 (0x0001: 압축, 0x4000: 암호화, 0x8000: Sparse)	
(7) Attribute Identifier	2B (14-15)	속성 Type ID과는 별도로 속성 자체 고유값	

[References]
http://

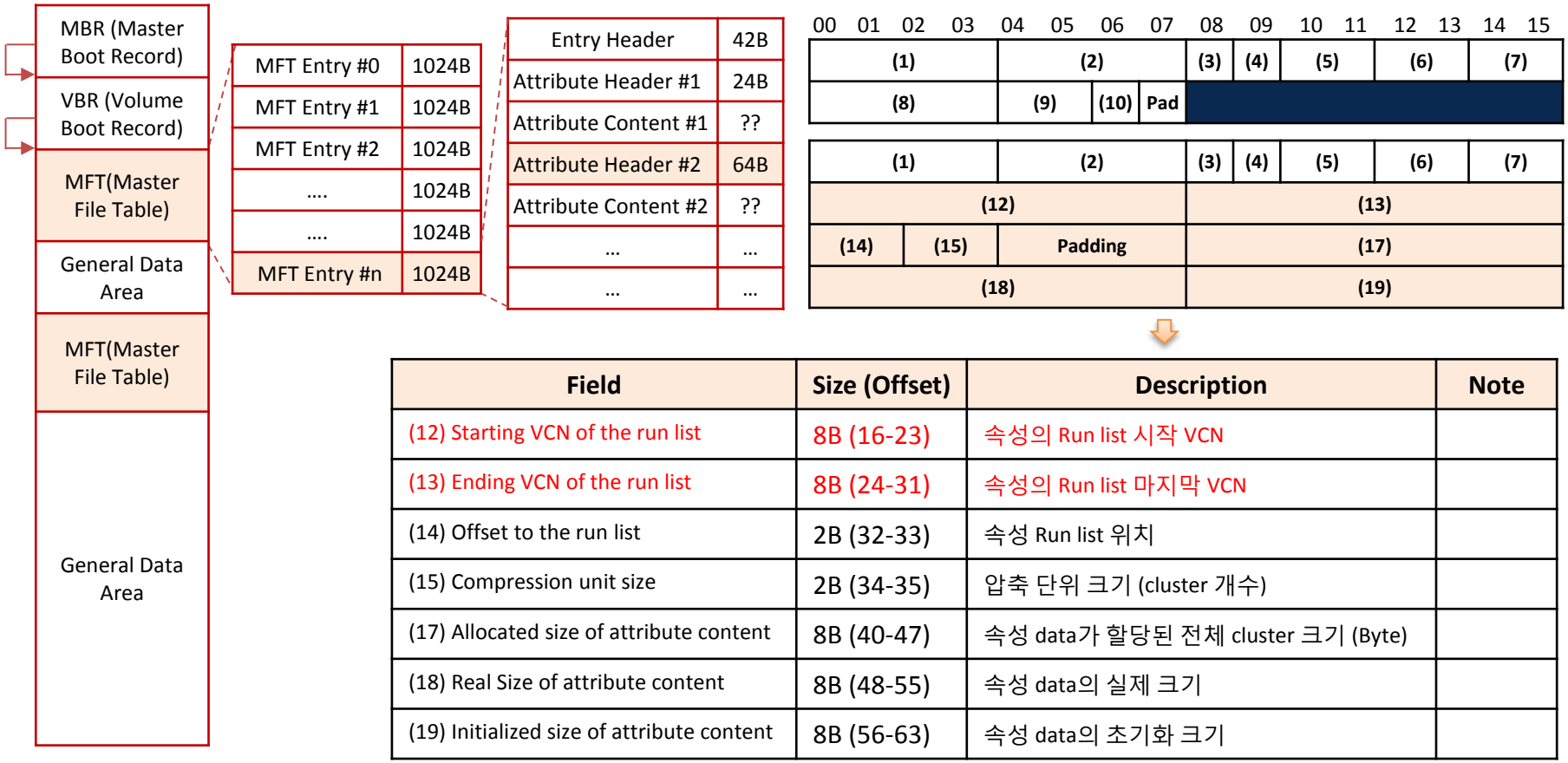
- MFT (Master File Table) Entry Attribute Header (Resident Only)



Field	Size (Offset)	Description	Note
(8) Size of Content	4B (16-19)	속성 내용의 크기	
(9) Offset to Content	4B (20-21)	속성 내용의 위치	
(10) Indexed Flag	1B (22)	속성이 검색에 사용하는지 여부 (1이면 index 정보로 사용 중임)	

[References]
http://

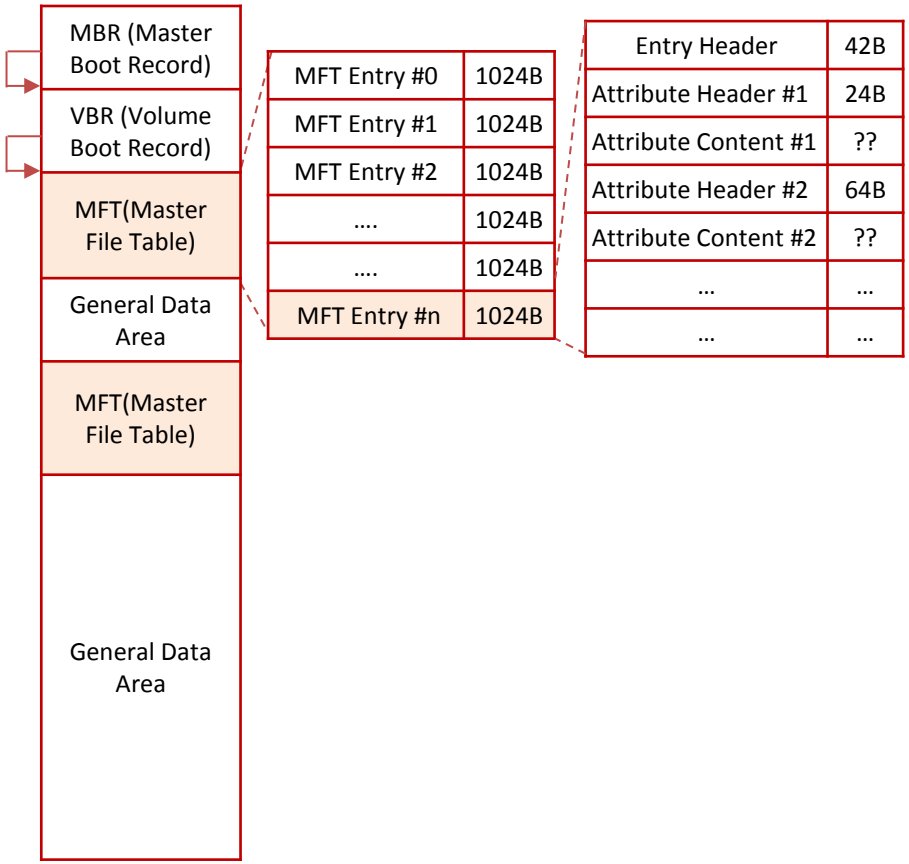
- MFT (Master File Table) Entry Attribute Header (Non-Resident Only)

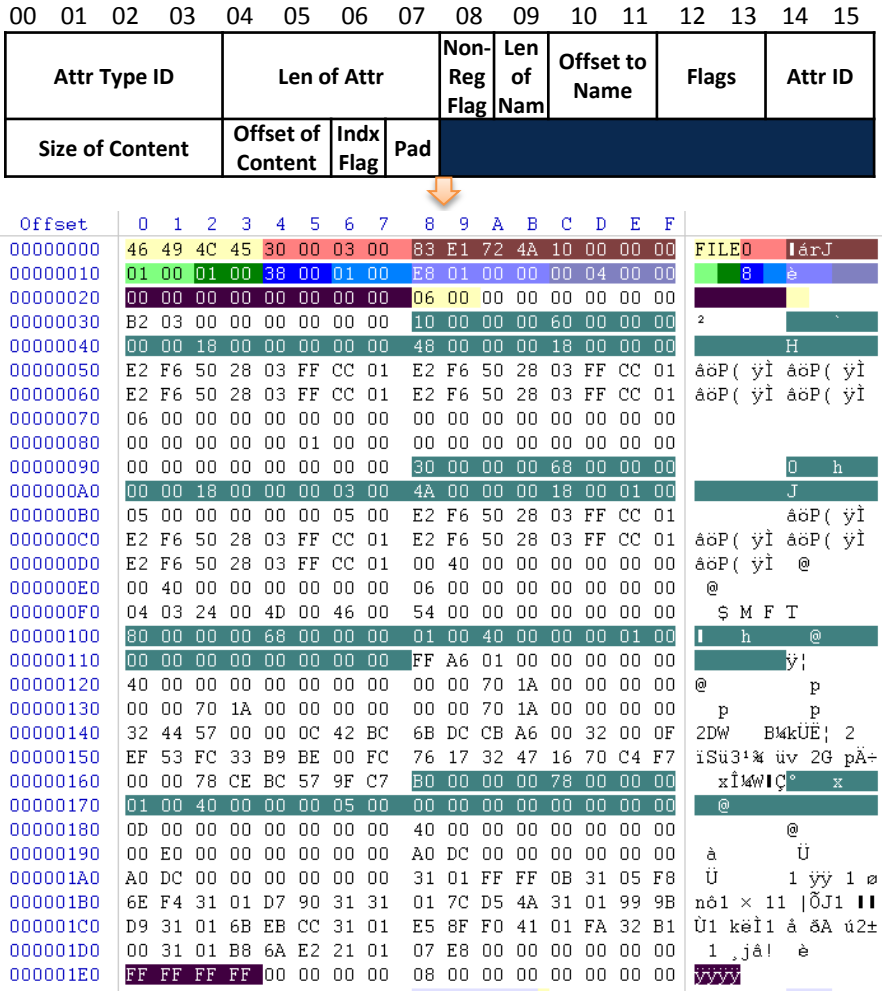


Field	Size (Offset)	Description	Note
(12) Starting VCN of the run list	8B (16-23)	속성의 Run list 시작 VCN	
(13) Ending VCN of the run list	8B (24-31)	속성의 Run list 마지막 VCN	
(14) Offset to the run list	2B (32-33)	속성 Run list 위치	
(15) Compression unit size	2B (34-35)	압축 단위 크기 (cluster 개수)	
(17) Allocated size of attribute content	8B (40-47)	속성 data가 할당된 전체 cluster 크기 (Byte)	
(18) Real Size of attribute content	8B (48-55)	속성 data의 실제 크기	
(19) Initialized size of attribute content	8B (56-63)	속성 data의 초기화 크기	

[References]

- MFT (Master File Table) Entry Attribute: Example for $MFT File





[References]