File system

발 표 자 문 승 재

목 차

Ⅰ 파일 시스템 분석의 의의

Ⅱ 파일 시스템

Ⅲ 파티션 복구 실습

파일 시스템 분석의 의의

슬랙 공간 분석

- RAM Slack
- Drive Slack
- File system Slack

시간 정보 분석

$FILE_NAME

$STANDARD_
INFORMATION

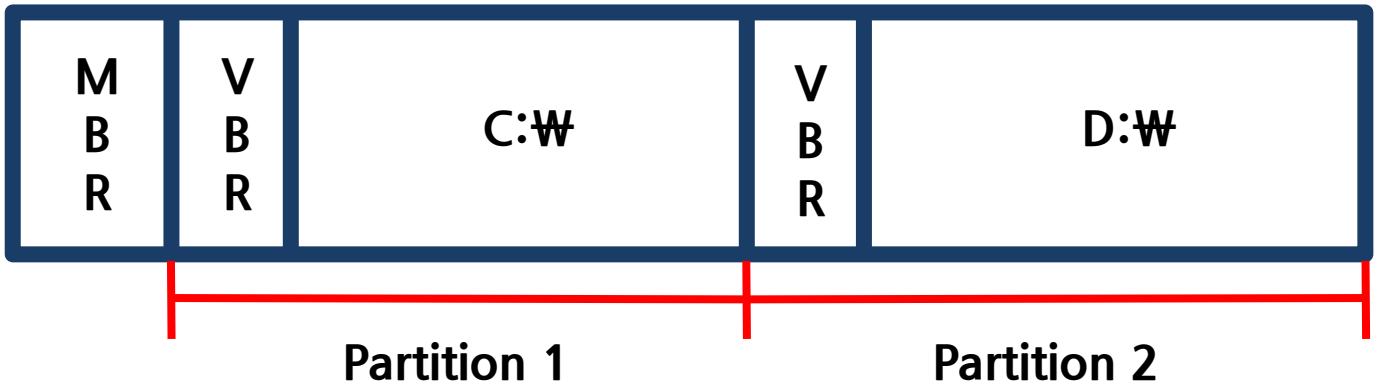
시그니처 분석

$FILE_NAME

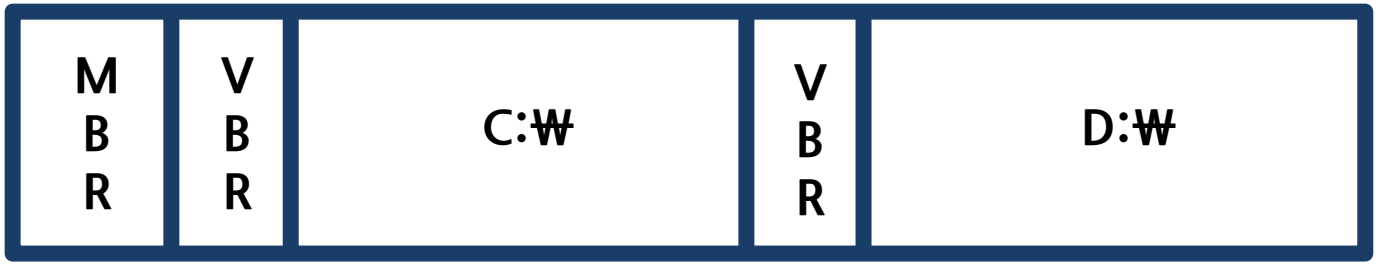
로그 정보 분석

$LogFile

파일 시스템 구조

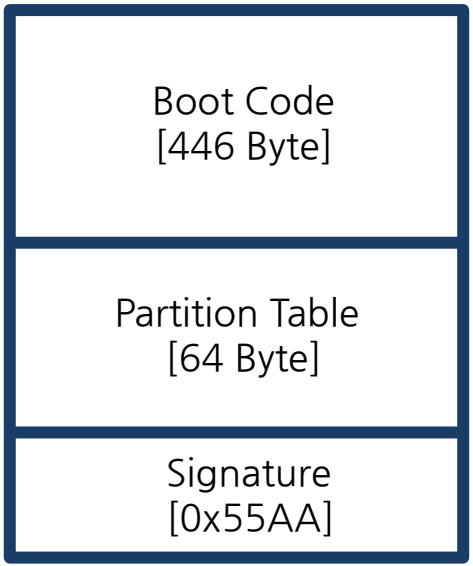


파일 시스템 구조 - MBR



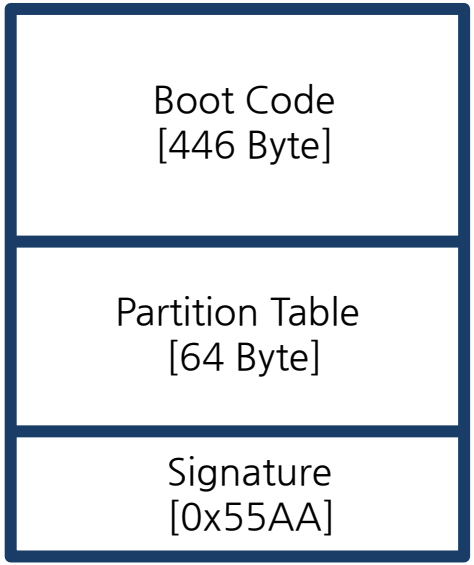
MBR

- Master Boot Recoder의 약자
- 하드디스크의 첫번째 섹터에 위치
- 부트 코드, 파티션테이블의 정보, MBR 시그니처



MBR 구조

파일 시스템 구조 - MBR

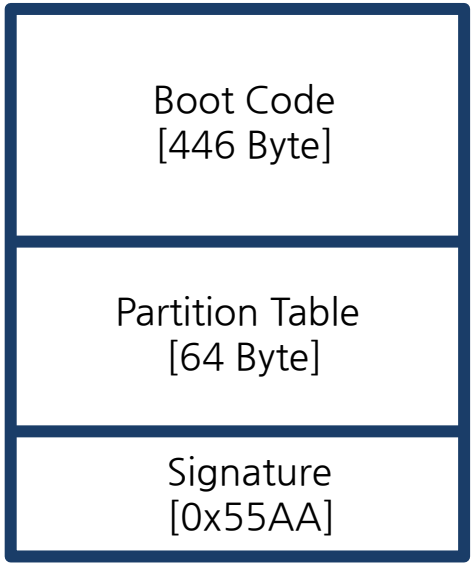


MBR 구조

하드 디스크 3 | 하드 디스크 3

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000000000	EB	06	00	00	00	00	00	00	33	C0	FA	8E	D0	BC	00	7C	ë.....3ÀúŽÐ¼.|
0000000010	FB	8E	D8	8B	F4	8E	C0	BF	26	7E	06	57	BF	00	7E	B9	ûŽØ‹ôŽÀ¿&~.W¿.~¹
0000000020	00	02	FC	F3	A4	CB	BE	02	7E	AD	8B	C8	66	AD	BB	00	..üó¤Ë¾.~.‹Èf.».
0000000030	80	83	F9	00	75	2E	BE	BE	7F	AC	3C	80	74	1B	83	C6	€ƒù.u.¾¾.¬<€t.ƒÆ
0000000040	0F	81	FE	FE	7F	75	F2	BE	44	7F	E8	33	00	BE	92	7F	..þþ.uò¾D.è3.¾'.
0000000050	E8	2D	00	33	C0	CD	16	CD	19	83	C6	07	66	AD	B9	01	è-.3ÀÍ.Í.ƒÆ.f.¹.
0000000060	00	BB	00	7C	32	F6	E8	24	00	BE	62	7F	72	DC	8B	F3	.».|2öè$.¾b.rÜ‹ó
0000000070	81	C6	FE	01	AD	BE	7F	7F	3D	55	AA	75	CD	06	53	CB	.Æþ..¾..=UªuÍ.SË
0000000080	B4	0E	FC	AC	3C	00	74	04	CD	10	EB	F7	C3	66	60	1E	´.ü¬<.t.Í.ë÷Ãf`.
0000000090	06	66	50	53	51	52	8B	EC	B4	41	BB	AA	55	8A	56	00	.fPSQR‹ì´A»ªUŠV.
00000000A0	CD	13	72	39	81	FB	55	AA	75	33	F6	C1	01	74	2E	66	Í.r9.ûUªu3öÁ.t.f
00000000B0	33	C0	66	50	66	8B	46	06	66	50	8B	46	0A	50	8B	46	3ÀfPf‹F.fP‹F.P‹F
00000000C0	04	50	66	B8	10	00	01	00	66	50	16	1F	8B	F4	8B	56	.Pf¸.....fP..‹ô‹V
00000000D0	00	B8	00	42	02	E6	CD	13	83	C4	10	EB	50	B4	08	8A	.¸.B.æÍ.ƒÄ.ëP´.Š
00000000E0	56	00	33	FF	8E	C7	CD	13	72	43	66	83	E1	3F	FE	C6	V.3ÿŽÇÍ.rCfƒá?þÆ
00000000F0	8A	DE	66	8B	46	06	66	33	D2	66	F7	F1	42	52	8A	CB	ŠÞf‹F.f3Òf÷ñBRŠË
0000000100	66	33	D2	66	F7	F1	8A	F2	59	66	3D	FF	03	00	00	77	f3Òf÷ñŠòYf=ÿ...w
0000000110	1B	86	E0	C0	E0	06	03	C8	8E	46	0A	8B	5E	04	8B	46	.†àÀà..ÈŽF.‹^.‹F
0000000120	00	8A	D0	80	C4	02	B0	01	CD	13	EB	01	F9	5A	59	5B	.ŠÐ€Ä.°.Í.ë.ùZY[
0000000130	66	58	72	0B	81	C3	00	02	66	40	49	0F	85	52	FF	07	fXr..Ã..f@I.…Rÿ.
0000000140	1F	66	61	C3	0D	0A	42	4F	4F	54	20	20	20	70	61	72	.faÃ..BOOT par
0000000150	74	69	74	69	6F	6E	20	6E	6F	74	20	66	6F	75	6E	64	tition not found
0000000160	21	00	0D	0A	45	72	72	6F	72	20	6C	6F	61	64	69	6E	!...Error loadin
0000000170	67	20	62	6F	6F	74	20	73	65	63	74	6F	72	21	00	0D	g boot sector!..
0000000180	0A	42	61	64	20	62	6F	6F	74	20	73	65	63	74	6F	72	.Bad boot sector
0000000190	21	00	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65	!...Press any ke
00000001A0	79	2E	2E	2E	0D	0A	00	00	00	00	00	00	00	00	00	00	y..............
00000001B0	65	6D	00	00	00	63	7B	9A	8F	09	00	00	00	00	80	20	em...c{š.....€
00000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	50	70	74	00	00	!..þÿÿ.....Ppt..
00000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	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	..............Uª

파일 시스템 구조 - MBR



MBR 구조

하드 디스크 3 | 하드 디스크 3 | 하드 디스크 3 | 하드 디스크 3

Offset(h)	00	01	02	03	04
0000000000	EB	06	00	00	00
0000000010	FB	8E	D8	8B	F4
0000000020	00	02	FC	F3	A4
0000000030	80	83	F9	00	75
0000000040	0F	81	FE	FE	7F
0000000050	E8	2D	00	33	C0
0000000060	00	BB	00	7C	32
0000000070	81	C6	FE	01	AD
0000000080	B4	0E	FC	AC	3C
0000000090	06	66	50	53	51
00000000A0	CD	13	72	39	81
00000000B0	33	C0	66	50	66
00000000C0	04	50	66	B8	10
00000000D0	00	B8	00	42	02
00000000E0	56	00	33	FF	8E
00000000F0	8A	DE	66	8B	46
0000000100	66	33	D2	66	F7
0000000110	1B	86	E0	C0	E0
0000000120	00	8A	D0	80	C4
0000000130	66	58	72	0B	81
0000000140	1F	66	61	C3	0D
0000000150	74	69	74	69	6F
0000000160	21	00	0D	0A	45
0000000170	67	20	62	6F	6F
0000000180	0A	42	61	64	20
0000000190	21	00	0D	0A	50
00000001A0	79	2E	2E	2E	0D
00000001B0	65	6D	00	00	00
00000001C0	21	00	07	FE	FF
00000001D0	00	00	00	00	00
00000001E0	00	00	00	00	00
00000001F0	00	00	00	00	00

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000000000	EB	06	00	00	00	00	00	00	33	C0	FA	8E	D0	BC	00	7C
0000000010	FB	8E	D8	8B	F4	8E	C0	BF	26	7E	06	57	BF	00	7E	B9
0000000020	00	02	FC	F3	A4	CB	BE	02	7E	AD	8B	C8	66	AD	BB	00
0000000030	80	83	F9	00	75	2E	BE	BE	7F	AC	3C	80	74	1B	83	C6
0000000040	0F	81	FE	FE	7F	75	F2	BE	44	7F	E8	33	00	BE	92	7F
0000000050	E8	2D	00	33	C0	CD	16	CD	19	83	C6	07	66	AD	B9	01
0000000060	00	BB	00	7C	32	F6	E8	24	00	BE	62	7F	72	DC	8B	F3
0000000070	81	C6	FE	01	AD	BE	7F	7F	3D	55	AA	75	CD	06	53	CB
0000000080	B4	0E	FC	AC	3C	00	74	04	CD	10	EB	F7	C3	66	60	1E
0000000090	06	66	50	53	51	52	8B	EC	B4	41	BB	AA	55	8A	56	00
00000000A0	CD	13	72	39	81	FB	55	AA	75	33	F6	C1	01	74	2E	66
00000000B0	33	C0	66	50	66	8B	46	06	66	50	8B	46	0A	50	8B	46
00000000C0	04	50	66	B8	10	00	01	00	66	50	16	1F	8B	F4	8B	56
00000000D0	00	B8	00	42	02	E6	CD	13	83	C4	10	EB	50	B4	08	8A
00000000E0	56	00	33	FF	8E	C7	CD	13	72	43	66	83	E1	3F	FE	C6
00000000F0	8A	DE	66	8B	46	06	66	33	D2	66	F7	F1	42	52	8A	CB
0000000100	66	33	D2	66	F7	F1	8A	F2	59	66	3D	FF	03	00	00	77
0000000110	1B	86	E0	C0	E0	06	03	C8	8E	46	0A	8B	5E	04	8B	46
0000000120	00	8A	D0	80	C4	02	B0	01	CD	13	EB	01	F9	5A	59	5B
0000000130	66	58	72	0B	81	C3	00	02	66	40	49	0F	85	52	FF	07
0000000140	1F	66	61	C3	0D	0A	42	4F	4F	54	20	20	20	70	61	72
0000000150	74	69	74	69	6F	6E	20	6E	6F	74	20	66	6F	75	6E	64
0000000160	21	00	0D	0A	45	72	72	6F	72	20	6C	6F	61	64	69	6E
0000000170	67	20	62	6F	6F	74	20	73	65	63	74	6F	72	21	00	0D
0000000180	0A	42	61	64	20	62	6F	6F	74	20	73	65	63	74	6F	72
0000000190	21	00	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65
00000001A0	79	2E	2E	2E	0D	0A	00	00	00	00	00	00	00	00	00	00
00000001B0	65	6D	00	00	00	63	7B	9A	8F	09	00	00	00	00	80	20
00000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	A8	3C	3A	00	FE
00000001D0	FF	FF	07	FE	FF	FF	00	B0	3C	3A	00	A8	33	3A	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

파일 시스템 구조 - MBR

하드 디스크 3 | 하드 디스크 3

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000000000	EB	06	00	00	00	00	00	00	33	C0	FA	8E	D0	BC	00	7C	ë.......3ÀúŽÐ¼.|
0000000010	FB	8E	D8	8B	F4	8E	C0	BF	26	7E	06	57	BF	00	7E	B9	ûŽØ‹ôŽÀ¿&~.W¿.~¹
0000000020	00	02	FC	F3	A4	CB	BE	02	7E	AD	8B	C8	66	AD	BB	00	..üó¤Ë¾.~.‹Èf.».
0000000030	80	83	F9	00	75	2E	BE	BE	7F	AC	3C	80	74	1B	83	C6	€ƒù.u.¾¾.¬<€t.ƒÆ
0000000040	0F	81	FE	FE	7F	75	F2	BE	44	7F	E8	33	00	BE	92	7F	..þþ.uò¾D.è3.¾'.
0000000050	E8	2D	00	33	C0	CD	16	CD	19	83	C6	07	66	AD	B9	01	è-.3ÀÍ.Í.ƒÆ.f.¹.
0000000060	00	BB	00	7C	32	F6	E8	24	00	BE	62	7F	72	DC	8B	F3	.».|2öè$.¾b.rÜ‹ó
0000000070	81	C6	FE	01	AD	BE	7F	7F	3D	55	AA	75	CD	06	53	CB	.Æþ..¾..=UªuÍ.SË
0000000080	B4	0E	FC	AC	3C	00	74	04	CD	10	EB	F7	C3	66	60	1E	´.ü¬<.t.Í.ë÷Ãf`.
0000000090	06	66	50	53	51	52	8B	EC	B4	41	BB	AA	55	8A	56	00	.fPSQR‹ì´A»ªUŠV.
00000000A0	CD	13	72	39	81	FB	55	AA	75	33	F6	C1	01	74	2E	66	Í.r9.ûUªu3öÁ.t.f
00000000B0	33	C0	66	50	66	8B	46	06	66	50	8B	46	0A	50	8B	46	3ÀfPf‹F.fP‹F.P‹F
00000000C0	04	50	66	B8	10	00	01	00	66	50	16	1F	8B	F4	8B	56	.Pf¸....fP..‹ô‹V
00000000D0	00	B8	00	42	02	E6	CD	13	83	C4	10	EB	50	B4	08	8A	.¸.B.æÍ.ƒÄ.ëP´.Š
00000000E0	56	00	33	FF	8E	C7	CD	13	72	43	66	83	E1	3F	FE	C6	V.3ÿŽÇÍ.rCfƒá?þÆ
00000000F0	8A	DE	66	8B	46	06	66	33	D2	66	F7	F1	42	52	8A	CB	ŠÞf‹F.f3Òf÷ñBRŠË
0000000100	66	33	D2	66	F7	F1	8A	F2	59	66	3D	FF	03	00	00	77	f3Òf÷ñŠòYf=ÿ...w
0000000110	1B	86	E0	C0	E0	06	03	C8	8E	46	0A	8B	5E	04	8B	46	.†àÀà..ÈŽF.‹^.‹F
0000000120	00	8A	D0	80	C4	02	B0	01	CD	13	EB	01	F9	5A	59	5B	.ŠÐ€Ä.°.Í.ë.ùZY[
0000000130	66	58	72	0B	81	C3	00	02	66	40	49	0F	85	52	FF	07	fXr..Ã..f@I.…Rÿ.
0000000140	1F	66	61	C3	0D	0A	42	4F	4F	54	20	20	20	70	61	72	.faÃ..BOOT par
0000000150	74	69	74	69	6F	6E	20	6E	6F	74	20	66	6F	75	6E	64	tition not found
0000000160	21	00	0D	0A	45	72	72	6F	72	20	6C	6F	61	64	69	6E	!...Error loadin
0000000170	67	20	62	6F	6F	74	20	73	65	63	74	6F	72	21	00	0D	g boot sector!..
0000000180	0A	42	61	64	20	62	6F	6F	74	20	73	65	63	74	6F	72	.Bad boot sector
0000000190	21	00	0D	0A	50	72	65	73	73	20	61	6E	79	20	6B	65	!...Press any ke
00000001A0	79	2E	2E	2E	0D	0A	00	00	00	00	00	00	00	00	00	00	y..............
00000001B0	65	6D	00	00	00	63	7B	9A	8F	09	00	00	00	00	80	20	em...c{š......€
00000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	A8	3C	3A	00	FE	!..þÿÿ.....¨<:.þ
00000001D0	FF	FF	07	FE	FF	FF	00	B0	3C	3A	00	A8	33	3A	00	00	ÿÿ.þÿÿ.°<:.¨3:..
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	..............Uª

Bootable Flag

Starting CHS Addr

Partition Type

Ending CHS Addr

Starting LBA Addr

Size in Sector

파일 시스템 구조 - MBR

Bootable Flag

부팅이 가능한 파티션에는 0x80, 아닌 경우 0x00설정

Starting CHS Addr

CHS주소지정방식으로 표시할 때 파티션의 시작 번지 표현

Partition Type

파일시스템 타입을 표시
NTFS파일시스템은 0x07로 표시

Ending CHS Addr

CHS 주소지정방식으로 표시할 때 파티션의 끝 번지 표현

Starting LBA Addr

LBA주소지정방식으로 표시할 때 파티션의 시작 번지를 표현

Size in Sector

해당 파티션에서 사용하는 LBA의 총 섹터의 개수를 표시

파일 시스템 구조 - MBR

Bootable Flag

부팅이 가능한 파티션에는 0x80, 아닌 경우 0x00설정

Ending CHS Addr

CHS 주소지정방식으로 표시할 때 파티션의 끝 번지 표현

CHS

00000001B0	65	6D	00	00	00	63	7B	9A	8F	09	00	00	00	00	80	20
00000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	A8	3C	3A	00	FE
00000001D0	FF	FF	07	FE	FF	FF	00	B0	3C	3A	00	A8	33	3A	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

시작

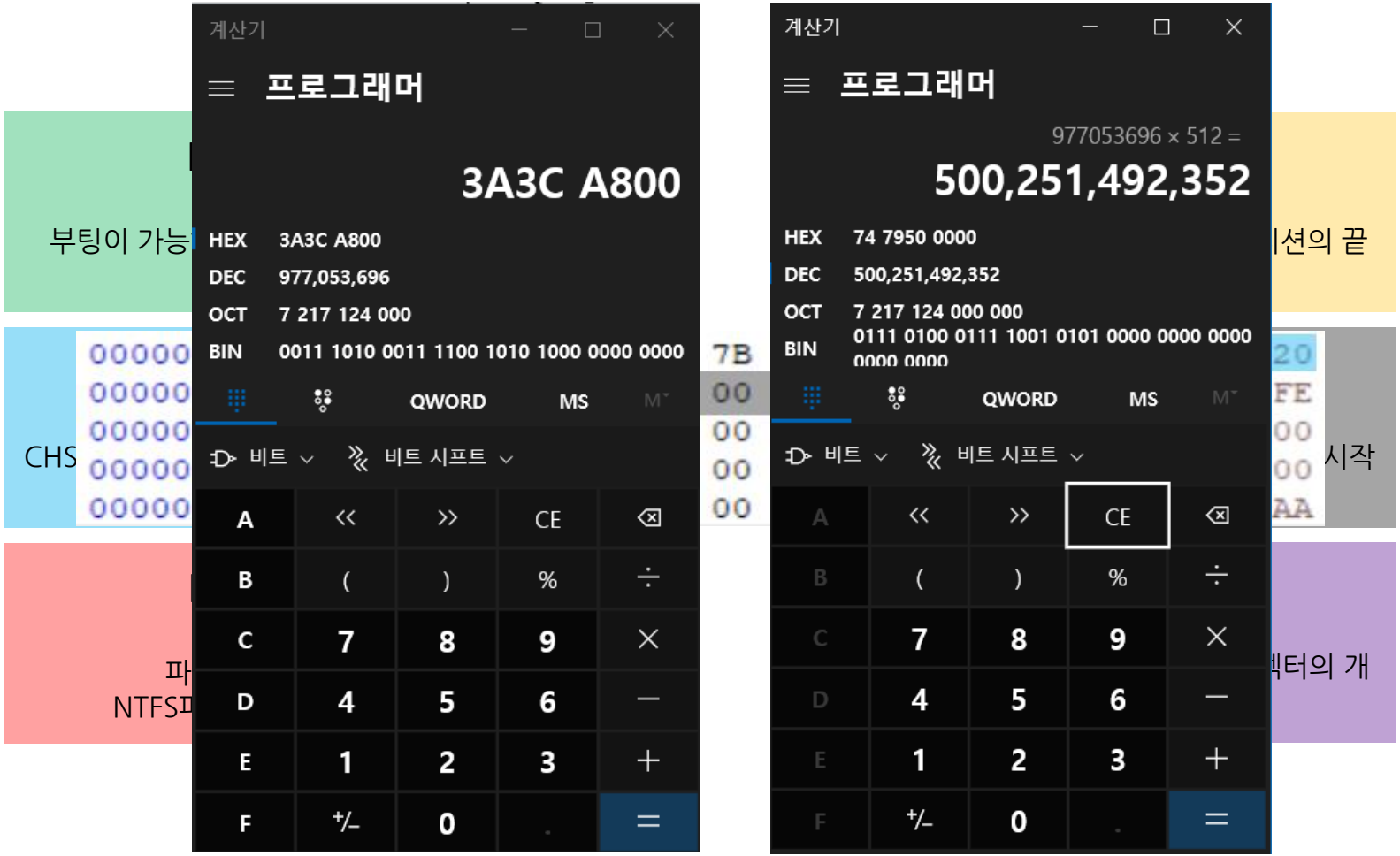
Partition Type

파일시스템 타입을 표시
NTFS파일시스템은 0x07로 표시

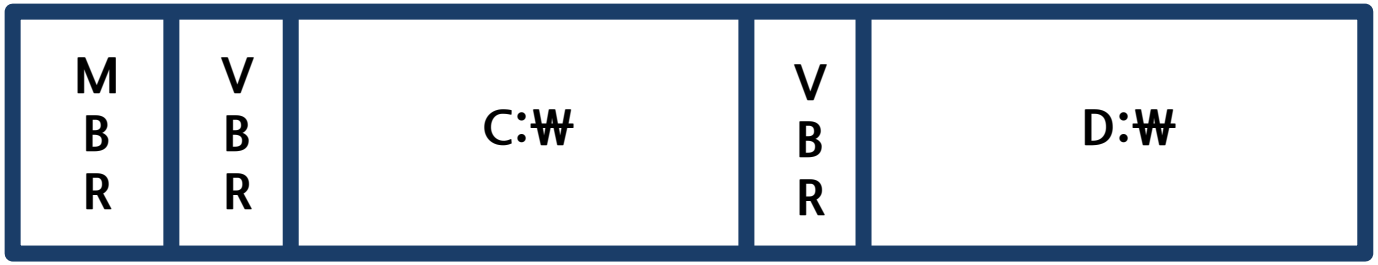
Size in Sector

해당 파티션에서 사용하는 LBA의 총 섹터의 개수를 표시

파일 시스템 구조 - MBR


부팅이 가능
션의 끝
CHS
시작
파
NTFS
터의 개
계산기
프로그래머
3A3C A800
HEX 3A3C A800
DEC 977,053,696
OCT 7 217 124 000
BIN 0011 1010 0011 1100 1010 1000 0000 0000
QWORD
MS
비트
비트 시프트
계산기
프로그래머
977053696 × 512 =
500,251,492,352
HEX 74 7950 0000
DEC 500,251,492,352
OCT 7 217 124 000 000
BIN 0111 0100 0111 1001 0101 0000 0000 0000
0000 0000
QWORD
MS
비트
비트 시프트

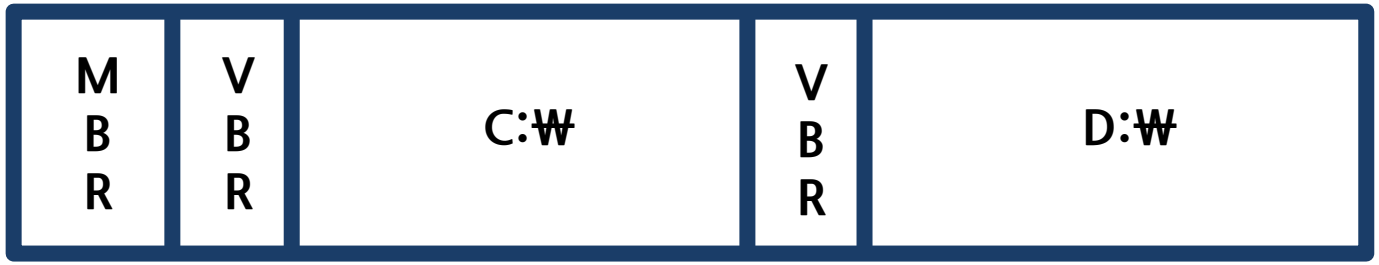
파일 시스템 구조 - VBR



VBR

- Volume Boot Record의 약자
- 부트 섹터와 섹터의 크기, 볼륨의 총 섹터, 클러스터의 크기 등의 정보를 저장하는 부분이다.

파일 시스템 구조 - MFT

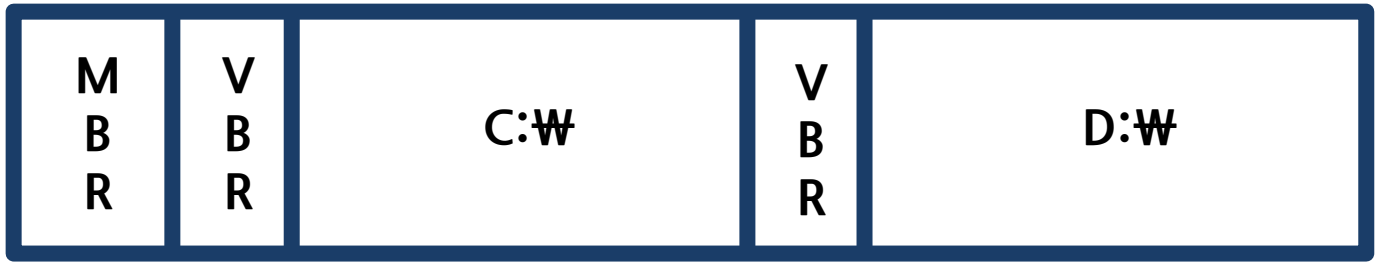


NTFS 파일시스템 구조

MFT

- 디렉토리나 파일 등을 관리하기 위해 존재하는 MFT Entry영역
- 여러 개의 MFT Entry가 존재한다.

파일 시스템 구조 - DATA



NTFS 파일시스템 구조

DATA

- 파일의 실제 내용이 저장되는 영역
- 내용만 저장한다.

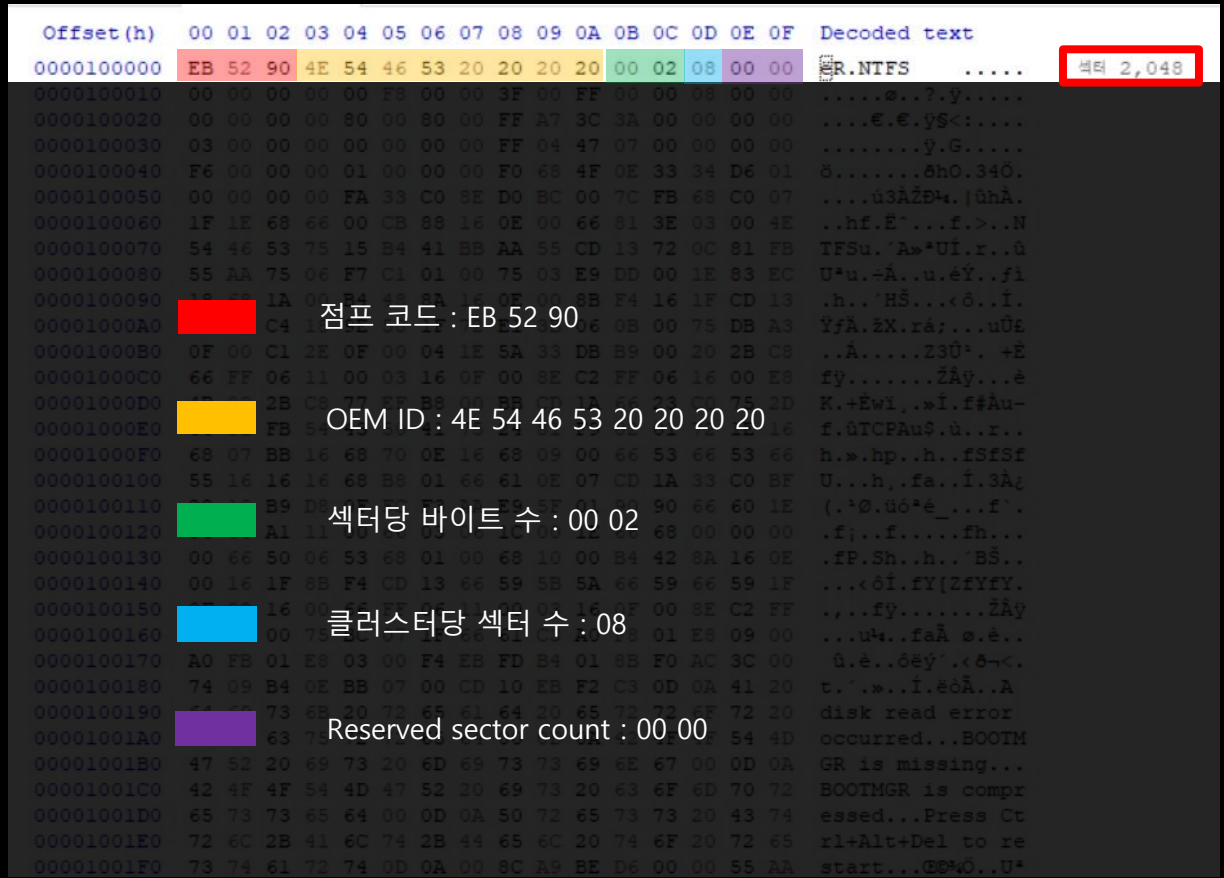
파일 시스템 구조 - VBR

하드 디스크 3 | 하드 디스크 3

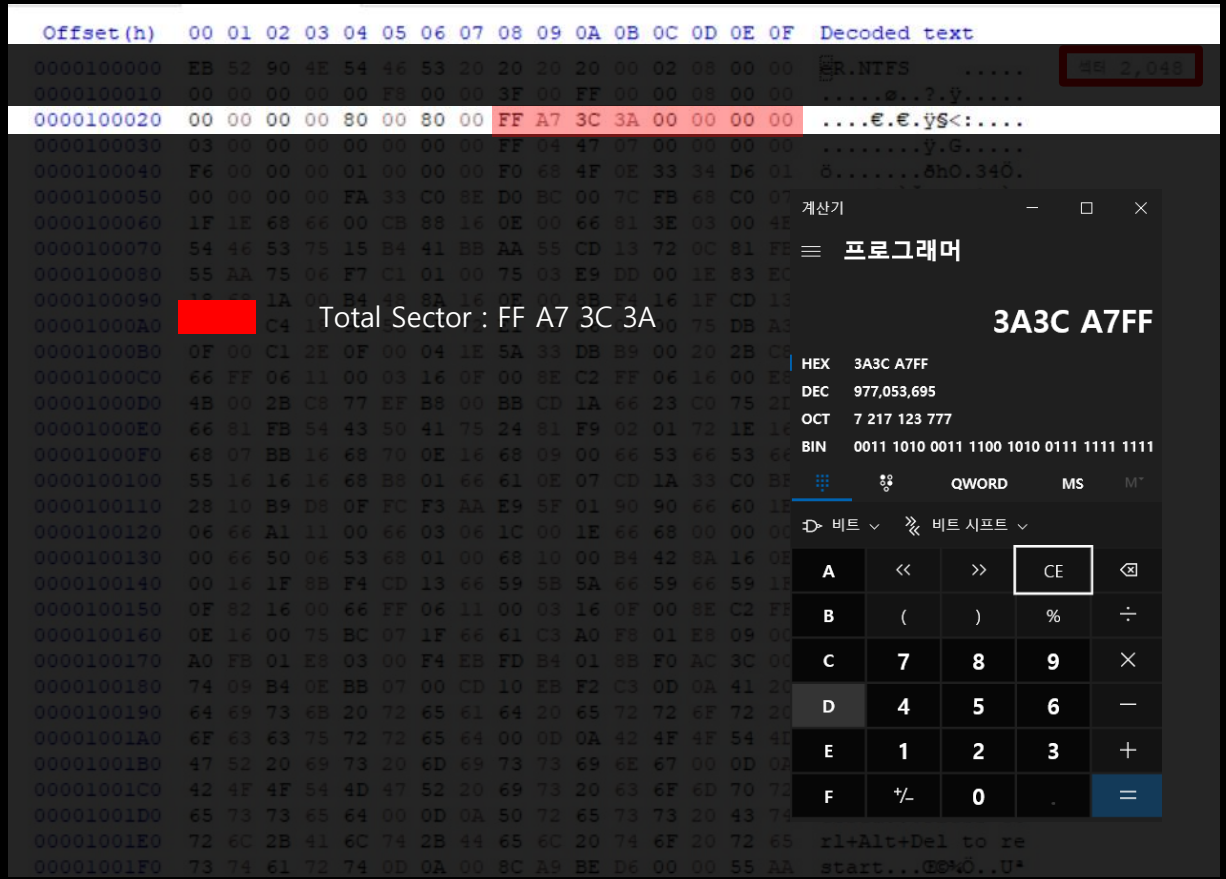
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
0000100010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	.....ø..?.ÿ.....
0000100020	00	00	00	00	80	00	80	00	FF	A7	3C	3A	00	00	00	00	....€.€.ÿ§<:....
0000100030	03	00	00	00	00	00	00	00	FF	04	47	07	00	00	00	00	........ÿ.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	07	....ú3ÀŽÐ¼.|ûhÀ.
0000100060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N
0000100070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û
0000100080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì
0000100090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.
00001000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£
00001000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È
00001000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.......ŽÂÿ...è
00001000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwï¸.»Í.f#Àu-
00001000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu$.ù..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..Í.3À¿
0000100110	28	10	B9	D8	0F	FC	F3	AA	E9	5F	01	90	90	66	60	1E	(.¹Ø.üóªé_...f`.
0000100120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f¡..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	...‹ôÍ.fY[ZfYfY.
0000100150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	.‚..fÿ.......ŽÂÿ
0000100160	0E	16	00	75	BC	07	1F	66	61	C3	A0	F8	01	E8	09	00	...u¼..faÃ ø.è..
0000100170	A0	FB	01	E8	03	00	F4	EB	FD	B4	01	8B	F0	AC	3C	00	û.è..ôëý´.‹ð¬<.
0000100180	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	t.´.»..Í.ëòÃ..A
0000100190	64	69	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	disk read error
00001001A0	6F	63	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	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...Œ©¾Ö..Uª

섹터 2,048

파일 시스템 구조 - VBR

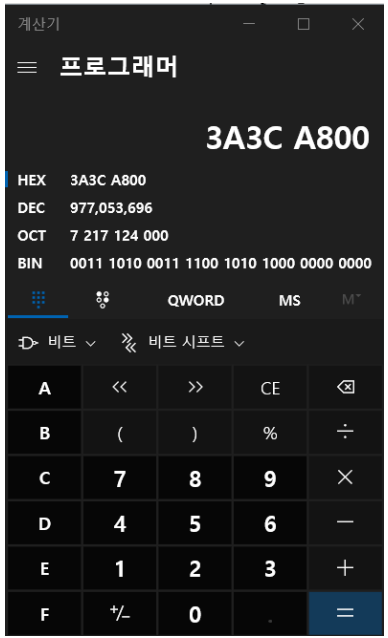

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0000100000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 ëR.NTFS .....
섹터 2,048
점프 코드 : EB 52 90
OEM ID : 4E 54 46 53 20 20 20 20
섹터당 바이트 수 : 00 02
클러스터당 섹터 수 : 08
Reserved sector count : 00 00

파일 시스템 구조 - VBR

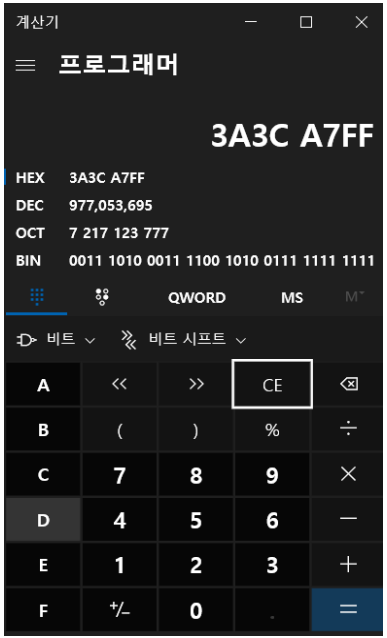

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0000100020 00 00 00 00 80 00 80 00 FF A7 3C 3A 00 00 00 00
Total Sector : FF A7 3C 3A
계산기
프로그래머
3A3C A7FF
HEX 3A3C A7FF
DEC 977,053,695
OCT 7 217 123 777
BIN 0011 1010 0011 1100 1010 0111 1111 1111
QWORD
MS
비트
비트 시프트
A
B
C
D
E
F
CE
7
8
9
4
5
6
1
2
3
0

파일 시스템 구조 - MBR, VBR

MBR에서 파티션 1의 Total sector

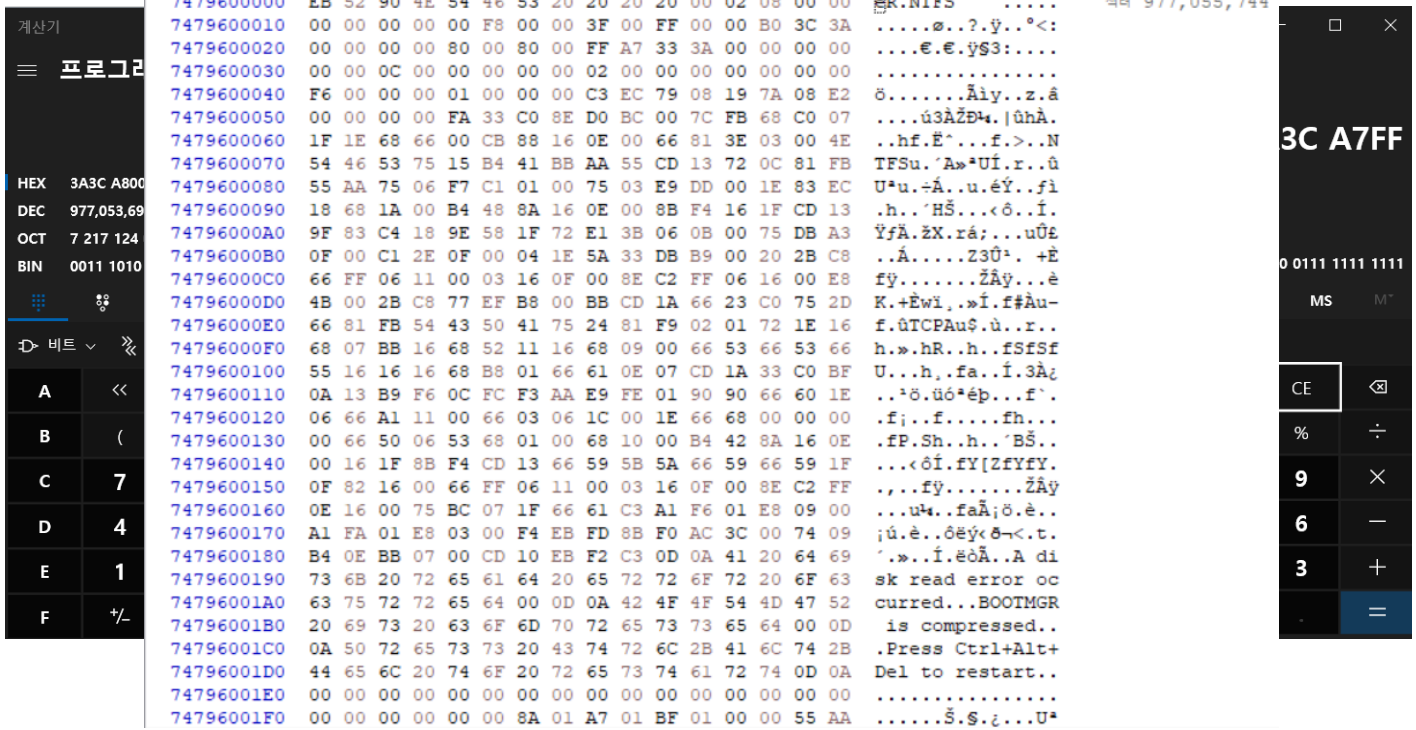


VBR의 Total sector



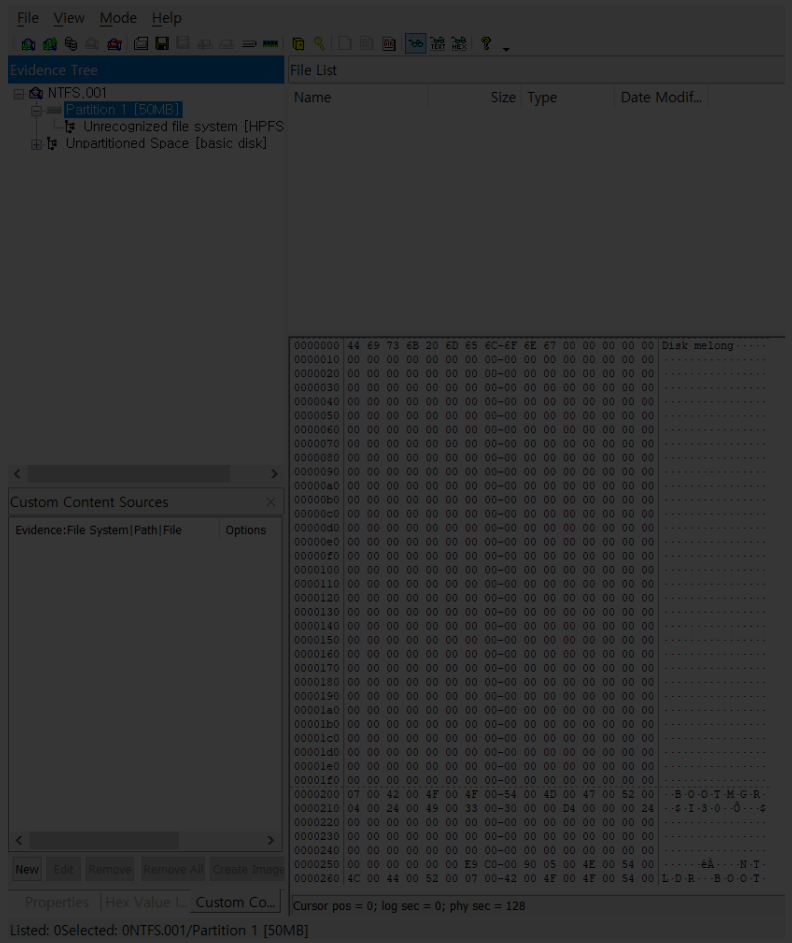
파일 시스템 구조 - MBR, VBR

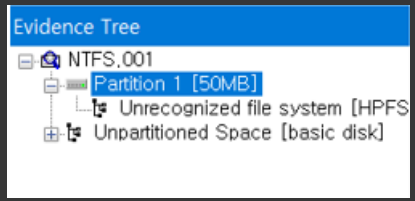
MBR에서 파티션 1의 Total sector VBR의 Total sector

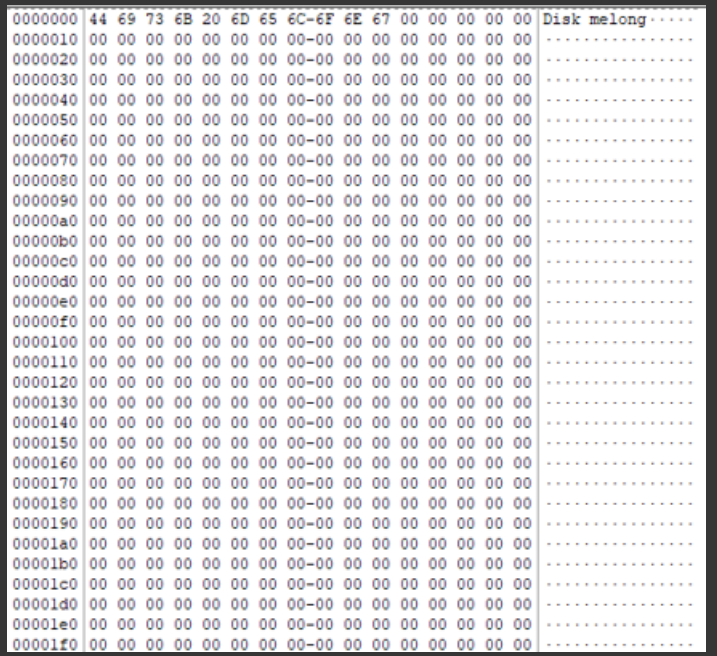


파티션 복구 실습

파티션 복구 실습


File View Mode Help
Evidence Tree
NTFS.001
Partition 1 [50MB]
Unrecognized file system [HPFS
Unpartitioned Space [basic disk]
File List
Name
Size
Type
Date Modif...
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value I...
Custom Co...
Cursor pos = 0; log sec = 0; phy sec = 128
Listed: 0Selected: 0NTFS.001/Partition 1 [50MB]


Evidence Tree
NTFS.001
Partition 1 [50MB]
Unrecognized file system [HPFS
Unpartitioned Space [basic disk]


0000000 44 69 73 6B 20 6D 65 6C-6F 6E 67 00 00 00 00 00 Disk melong
0000010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00001f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

파티션 복구 실습

NTFS.001

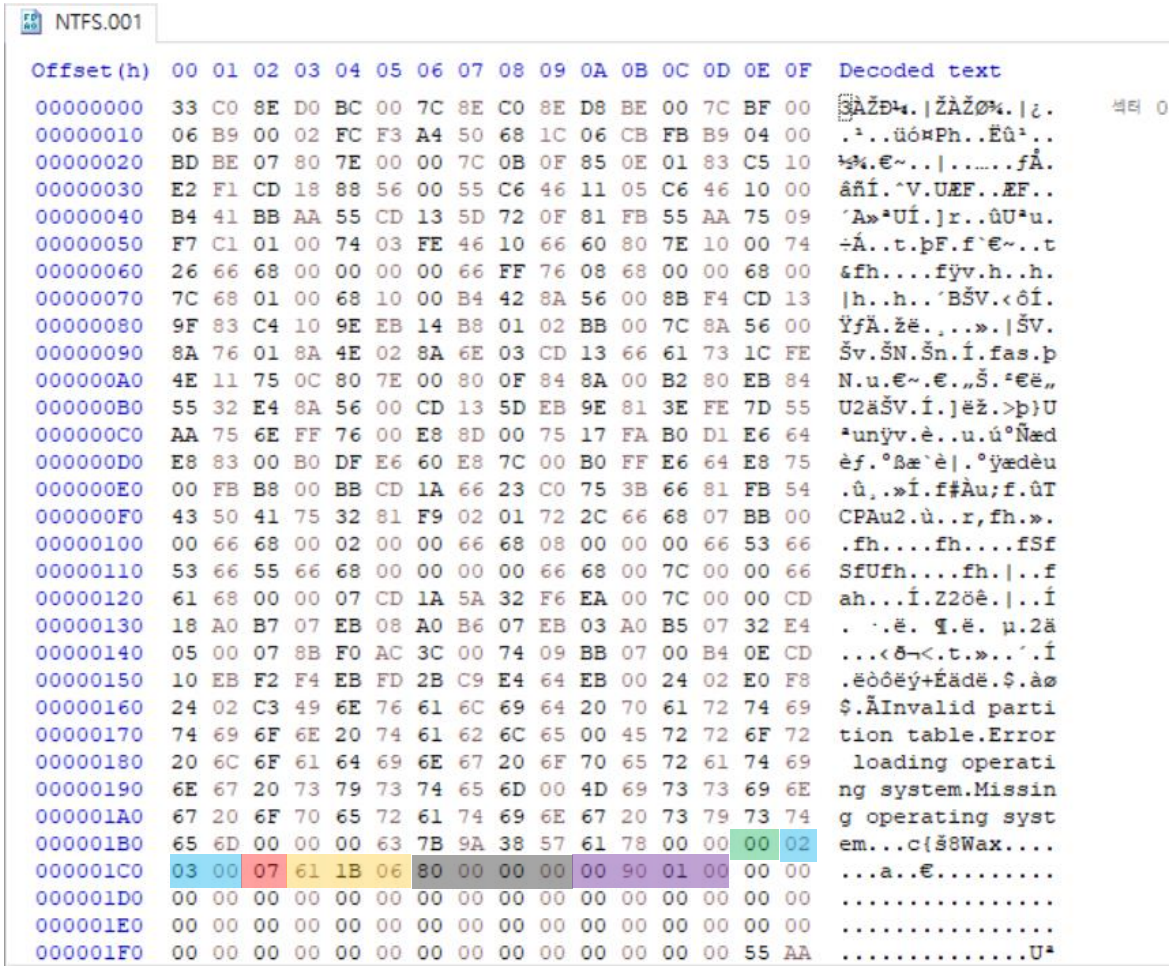
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00	3ÀŽÐ¼.|ŽÀŽØ¾.|¿.
00000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00	.¹..üó¤Ph..ËÛ¹..
00000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10	½¾.€~..|.....ƒÅ.
00000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00	âñÍ.ˆV.UÆF..ÆF..
00000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09	´A»ªUÍ.]r..ûUªu.
00000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74	÷Á..t.þF.f`€~..t
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh....fÿv.h..h.
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	|h..h..´BŠV.‹ôÍ.
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸƒÄ.žë.¸..».|ŠV.
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE	Šv.ŠN.Šn.Í.fas.þ
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84	N.u.€~.€.„Š.²€ë„
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55	U2äŠV.Í.]ëž.>þ}U
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64	ªunÿv.è..u.ú°Ñæd
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75	èƒ.°ßæ`è|.°ÿædèu
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54	.û¸.»Í.f#Àu;f.ûT
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00	CPAu2.ù..r,fh.».
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66	.fh....fh....fSf
00000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66	SfUfh....fh.|..f
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD	ah...Í.Z2öê.|..Í
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4	. ·.ë. ¶.ë. µ.2ä
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD	...‹ð¬<.t.»..´.Í
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8	.ëòôëý+Éädë.$.àø
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	$.ÃInvalid parti
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	tion table.Error
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	38	57	61	78	00	00	00	02	em...c{š8Wax....
000001C0	03	00	07	61	1B	06	80	00	00	00	00	90	01	00	00	00	...a..€.........
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	..............Uª

섹터 0

- Bootable Flag
- Starting CHS Addr
- Partition Type
- Ending CHS Addr
- Starting LBA Addr
- Size in Sector

파티션 복구 실습

NTFS.001



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00	3ÀŽÐ¼.|ŽÀŽØ¾.|¿. 섹터 0
00000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00	.¹..üó¤Ph..Ëû¹..
00000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10	½¾.€~..|.....ƒÅ.
00000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00	âñÍ.ˆV.UÆF..ÆF..
00000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09	´A»ªUÍ.]r..ûUªu.
00000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74	÷Á..t.þF.f`€~..t
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh....fÿv.h..h.
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	|h..h..´BŠV.‹ôÍ.
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸƒÄ.žë.¸...».|ŠV.
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE	Šv.ŠN.Šn.Í.fas.þ
000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84	N.u.€~.€.„Š.²€ë„
000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55	U2äŠV.Í.]ëž.>þ}U
000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64	ªunÿv.è..u.ú°Ñæd
000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75	èƒ.°ßæ`è|.°ÿædèu
000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54	.û¸.»Í.f#Àu;f.ûT
000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00	CPAu2.ù..r,fh.».
00000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66	.fh....fh....fSf
00000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66	SfUfh....fh.|..f
00000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD	ah...Í.Z2öê.|..Í
00000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4	. ·.ë. ¶.ë. µ.2ä
00000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD	...‹ð¬<.t.»..´.Í
00000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8	.ëòôëý+Éädë.$.àø
00000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	$.ÃInvalid parti
00000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	tion table.Error
00000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	loading operati
00000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	ng system.Missin
000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
000001B0	65	6D	00	00	00	63	7B	9A	38	57	61	78	00	00	00	02	em...c{š8Wax....
000001C0	03	00	07	61	1B	06	80	00	00	00	00	90	01	00	00	00	...a..€.........
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	..............Uª

Bootable Flag

0x00이므로 부팅 가능 파티션이 아님

Partition Type

0x07이므로 NTFS파일시스템

Starting LBA Addr

0x80이므로 10진수로 128

시작 섹터는 128섹터

Size in Sector

0x19000이므로 10진수로 102400

이 파티션의 섹터의 개수는 102400개

파티션 복구 실습

NTFS.001

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00010000	44	69	73	6B	20	6D	65	6C	6F	6E	67	00	00	00	00	00	Disk melong.....
00010010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000100F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00010190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000101A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000101B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000101C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000101D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000101E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

섹터 128

Disk melong.....

파티션 복구 실습

Starting LBA Addr

0x80이므로 10진수로 128

시작 섹터는 128섹터

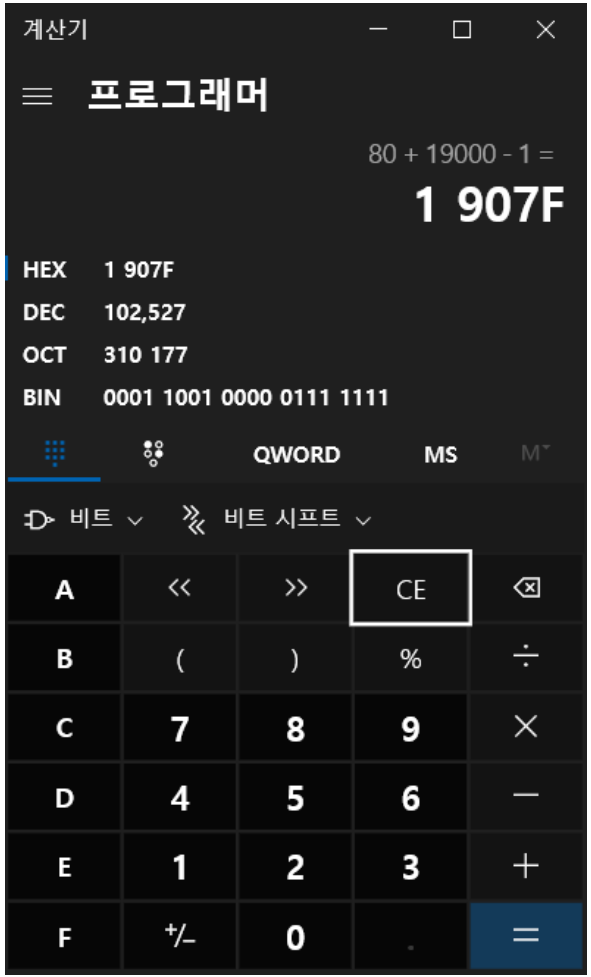
Size in Sector

0x19000이므로 10진수로 102400

이 파티션의 섹터의 개수는 102400개

VBR 백업 위치

[첫번째 파티션 시작 위치 섹터 + 첫번째 파티션 총 섹터개수 -1]



파티션 복구 실습

NTFS.001

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0320FE00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
0320FE10	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00	.....ø..?.ÿ.€...
0320FE20	00	00	00	00	80	00	00	00	FF	8F	01	00	00	00	00	00	....€...ÿ.....
0320FE30	AA	10	00	00	00	00	00	00	02	00	00	00	00	00	00	00	ª.....
0320FE40	F6	00	00	00	01	00	00	00	07	69	A1	9E	8F	A1	9E	96	ö.....i¡ž.¡ž–
0320FE50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽÐ¼.|ûhÀ.
0320FE60	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N
0320FE70	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û
0320FE80	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì
0320FE90	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.
0320FEA0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£
0320FEB0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È
0320FEC0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.......ŽÂÿ...è
0320FED0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwï¸.»Í.f#Àu-
0320FEE0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu$.ù..r..
0320FEF0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..fSfSf
0320FF00	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h¸.fa..Í.3À¿
0320FF10	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..¹ö.üó ªéþ...f`.
0320FF20	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f¡..f.....fh...
0320FF30	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..´BŠ..
0320FF40	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...‹ôÍ.fY[ZfYfY.
0320FF50	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	.‚..fÿ.......ŽÂÿ
0320FF60	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u¼..faÃ¡ö.è..
0320FF70	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ú.è..ôëý‹ð¬<.t.
0320FF80	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	´.»..Í.ëòÃ..A di
0320FF90	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
0320FFA0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR
0320FFB0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..
0320FFC0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+
0320FFD0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..
0320FFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

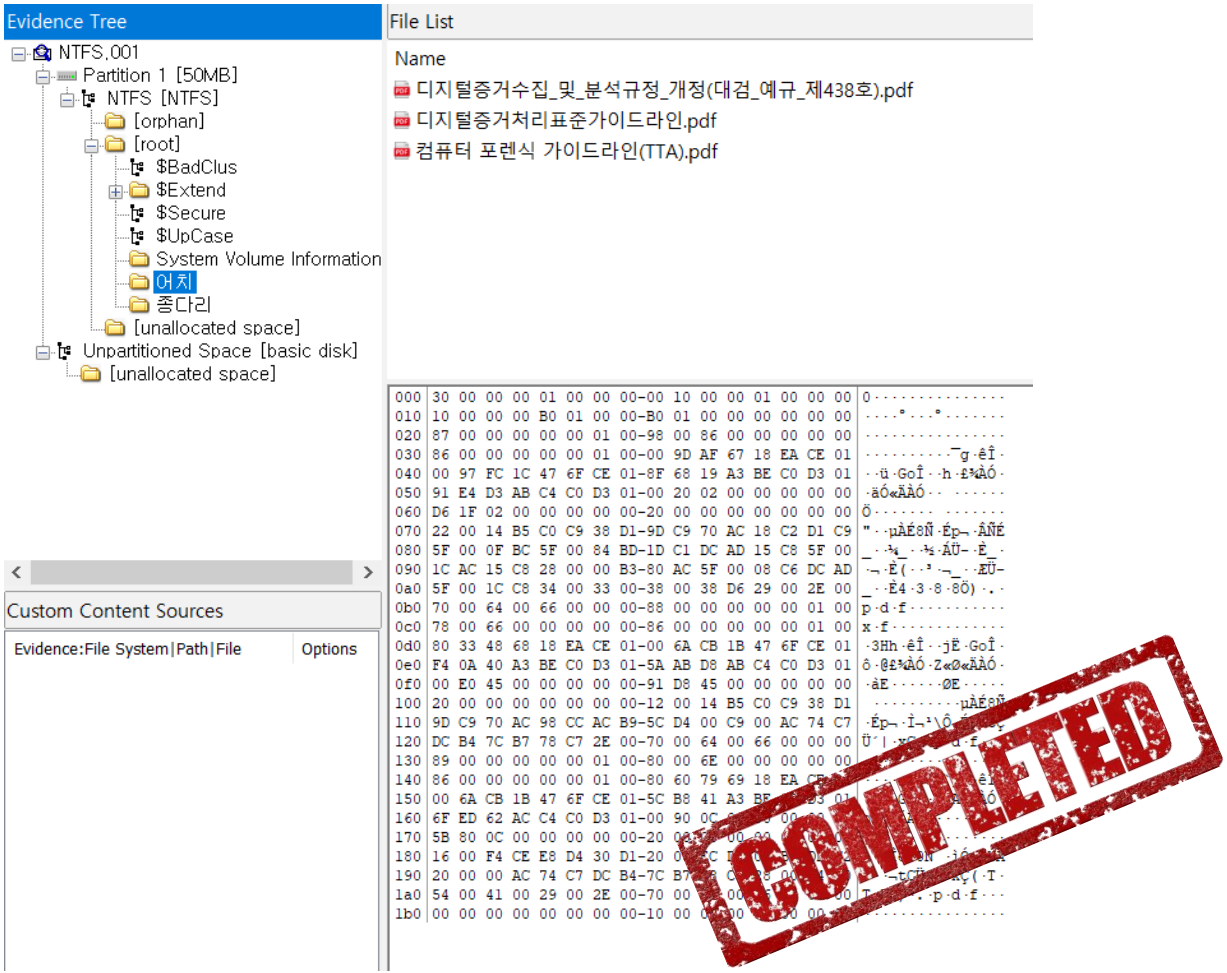
섹터 102,527

파티션 복구 실습

NTFS.001

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
0000FFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
0000FFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00010000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS	섹터 128
00010010	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00	.....ø..?.ÿ.€...	
00010020	00	00	00	00	80	00	00	00	FF	8F	01	00	00	00	00	00	....€...ÿ.....	
00010030	AA	10	00	00	00	00	00	00	02	00	00	00	00	00	00	00	ª.....	
00010040	F6	00	00	00	01	00	00	00	07	69	A1	9E	8F	A1	9E	96	ö.....i¡ž.¡ž–	
00010050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽÐ¼.|ûhÀ.	
00010060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ëˆ...f.>..N	
00010070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û	
00010080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì	
00010090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.	
000100A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£	
000100B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È	
000100C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.......ŽÂÿ...è	
000100D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwï¸.»Í.f#Àu-	
000100E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu$.ù..r..	
000100F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..fSfSf	
00010100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h¸.fa..Í.3À¿	
00010110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..¹ö.üóªéþ...f`.	
00010120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f¡..f.....fh...	
00010130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..´BŠ..	
00010140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...‹ôÍ.fY[ZfYfY.	
00010150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	.‚..fÿ.......ŽÂÿ	
00010160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u¼..faÃ¡ö.è..	
00010170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ú.è..ôëý‹ð¬<.t.	
00010180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	´.»..Í.ëòÃ..A di	
00010190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc	
000101A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR	
000101B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..	
000101C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+	
000101D0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..	
000101E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000101F0	00	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	.....Š.§.¿...U	
00010200	07	00	42	00	4F	00	4F	00	54	00	4D	00	47	00	52	00	.B.O.O.T.M.G.R.	섹터 129

파티션 복구 실습


Evidence Tree
NTFS.001
Partition 1 [50MB]
NTFS [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Secure
$UpCase
System Volume Information
어치
종다리
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name
디지털증거수집_및_분석규정_개정(대검_예규_제438호).pdf
디지털증거처리표준가이드라인.pdf
컴퓨터 포렌식 가이드라인(TTA).pdf
Custom Content Sources
Evidence:File System|Path|File
Options
COMPLETED

Q & A