VBR

Description

주어진 VBR을 분석하고, 플래그를 계산하시오.

FLAG = DH{(A + B + C)} (단, 더한 값을 십진수로 변환할 것)

A: 파일시스템이 FAT32면 1, NTFS면 2
B: 해당 볼륨의 크기
C: 볼륨 시리얼 번호
예를 들어 파일시스템이 NTFS, 볼륨의 크기가 0x100000, 그리고 볼륨 시리얼 번호가 0x

사용한 도구

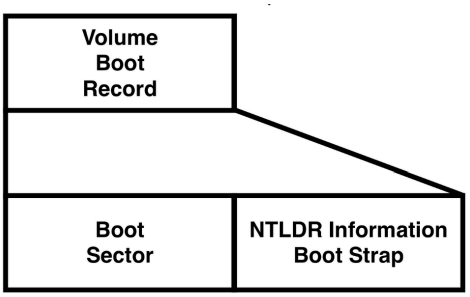
H x D

Background

디스크 포렌식

VBR

- 컴퓨터 부팅 과정에서 사용되는 데이터로 볼륨의 가장 첫 섹터에 저장되는 데이터
- 하나 이상의 섹터로 구성되어있다.
- Boot Sector와 NTLDR Information Boot Strap 영역으로 나뉜다.



VBR 구조

Boot Sector

- 운영 체제가 컴퓨터를 부팅할 때 필요한 정보를 담고 있다.
- BIOS Parameter Block (BPB) (빨간색), Bootstrap Code (초록색), Signature (파란색)으로 나뉜다.

Boot Sector

BIOS Parameter Block (BPB)

- 파일 시스템의 기본적인 정보를 담고 있으며, 드라이브의 구조, 파일 시스템의 크기, 섹터 크기 등을 정의하고, 시스템이 올바르게 액세스 할 수 있게 하는 중요한 메타데이터를 제공한다.

Boot Code

- 부트 코드는 시스템이 부팅될 때 실행되는 코드로, 볼륨을 읽고 부팅 프로세스를 시작하는 데 필요한 지침을 포함한다.

Signature

- Boot Sector의 끝에 위치하며, '0x55 AA'의 2Byte 값으로 구성되어 파일 시스템의 무결성을 검증하고 올바른 볼륨임을 확인하는 데 사용된다.

NTLDR Information Boot Strap

- 시스템의 부팅 과정에서 핵심적인 초기 단계를 담당
- 운영 체제의 커널을 메모리로 로드하고 실행하는 과정을 관리
- NTLDR는 부팅 가능한 디스크, 드라이브 구성, 부팅 메뉴 설정 등을 처리하여 Windows의 부팅 프로세스를 시작하고 진행하는 데 중요한 역할을 수행한다. 특징으로는 BOOTMGR(Boot Manager), $I30으로 시작된다.

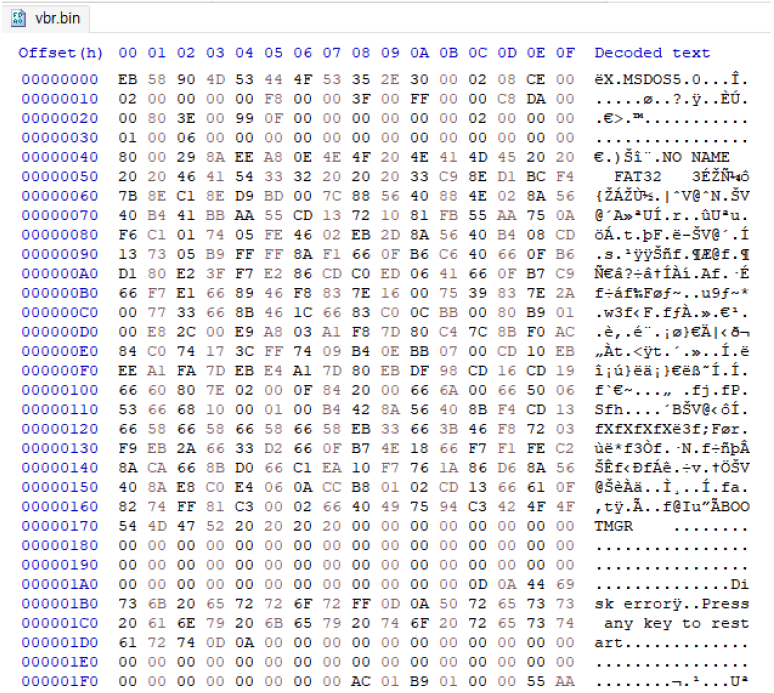
FAT32

- 파일이 저장되는 위치가 기록됨

NTFS

- MFT라는 별도 구조를 두고 MFT에 모든 파일의 메타데이터를 기록

1. 다운로드 받은 vbr.bin 파일을 HxD로 분석



vbr.bin

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 08 CE 00  ëX.MSDOS5.0...Î.
00000010   02 00 00 00 00 F8 00 00 3F 00 FF 00 00 C8 DA 00  .....ø..?.ÿ..ÈÚ.
00000020   00 80 3E 00 99 0F 00 00 00 00 00 00 02 00 00 00  .€>.™...........
00000030   01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040   80 00 29 8A EE A8 0E 4E 4F 20 4E 41 4D 45 20 20  €.)Šî¨.NO NAME
00000050   20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4    FAT32   3ÉŽÑ¼ô
00000060   7B 8E C1 8E D9 BD 00 7C 88 56 40 88 4E 02 8A 56  {ŽÁŽÙ½.|ˆV@ˆN.ŠV
00000070   40 B4 41 BB AA 55 CD 13 72 10 81 FB 55 AA 75 0A  @´A»ªUÍ.r..ûUªu.
00000080   F6 C1 01 74 05 FE 46 02 EB 2D 8A 56 40 B4 08 CD  öÁ.t.þF.ë-ŠV@´.Í
00000090   13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F B6  .s.¹ÿÿŠñf.¶Æ@f.¶
000000A0   D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7 C9  Ñ€â?÷â†ÍÀí.Af.·É
000000B0   66 F7 E1 66 89 46 F8 83 7E 16 00 75 39 83 7E 2A  f÷áf‰Føƒ~..u9ƒ~*
000000C0   00 77 33 66 8B 46 1C 66 83 C0 0C BB 00 80 B9 01  .w3f‹F.fƒÀ.».€¹.
000000D0   00 E8 2C 00 E9 A8 03 A1 F8 7D 80 C4 7C 8B F0 AC  .è,.é¨.¡ø}€Ä|‹ð¬
000000E0   84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB  „Àt.<ÿt.´.».Í.ë
000000F0   EE A1 FA 7D EB E4 A1 7D 80 EB DF 98 CD 16 CD 19  î¡ú}ëä¡}€ëß˜Í.Í.
00000100   66 60 80 7E 02 00 0F 84 20 00 66 6A 00 66 50 06  f`€~...„ .fj.fP.
00000110   53 66 68 10 00 01 00 B4 42 8A 56 40 8B F4 CD 13  Sfh....´BŠV@‹ôÍ.
00000120   66 58 66 58 66 58 66 58 EB 33 66 3B 46 F8 72 03  fXfXfXfXë3f;Før.
00000130   F9 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE C2  ùë*f3Òf.·N.f÷ñþÂ
00000140   8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A 56  ŠÊf‹ÐfÁê.÷v.†ÖŠV
00000150   40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61 0F  @ŠèÀä..Ì¸..Í.fa.
00000160   82 74 FF 81 C3 00 02 66 40 49 75 94 C3 42 4F 4F  ‚tÿ.Ã..f@Iu”ÃBOO
00000170   54 4D 47 52 20 20 20 20 00 00 00 00 00 00 00 00  TMGR    ........
00000180   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0   00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 44 69  ..............Di
000001B0   73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73  sk errorÿ..Press
000001C0   20 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74   any key to rest
000001D0   61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00  art.............
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 AC 01 B9 01 00 00 55 AA  ........¬.¹...Uª
```

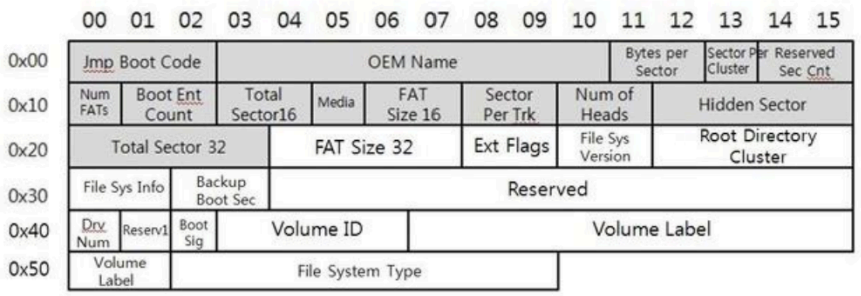
분석 해야할 것

1. 파일 시스템이 FAT32인지 NTFS인지

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	CE	00	ëX.MSDOS5.0...Î.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	C8	DA	00	.....ø..?.ÿ..ÈÚ.
00000020	00	80	3E	00	99	0F	00	00	00	00	00	00	02	00	00	00	.€>.™...........
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	80	00	29	8A	EE	A8	0E	4E	4F	20	4E	41	4D	45	20	20	€.)Šî¨.NO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ¼ô
00000060	7B	8E	C1	8E	D9	BD	00	7C	88	56	40	88	4E	02	8A	56	{ŽÁŽÙ½.|ˆV@ˆN.ŠV
00000070	40	B4	41	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	@´A»ªUÍ.r..ûUªu.
00000080	F6	C1	01	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	öÁ.t.þF.ë-ŠV@´.Í
00000090	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	.s.¹ÿÿŠñf.¶Æ@f.¶
000000A0	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	Ñ€â?÷â†ÍÀí.Af.·É
000000B0	66	F7	E1	66	89	46	F8	83	7E	16	00	75	39	83	7E	2A	f÷áf‰Føƒ~..u9ƒ~*
000000C0	00	77	33	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	.w3f‹F.fƒÀ.».€¹.
000000D0	00	E8	2C	00	E9	A8	03	A1	F8	7D	80	C4	7C	8B	F0	AC	.è,.é¨.¡ø}€Ä|‹ð¬
000000E0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	„Àt.<ÿt.´.».Í.ë
000000F0	EE	A1	FA	7D	EB	E4	A1	7D	80	EB	DF	98	CD	16	CD	19	î¡ú}ëä¡}€ëß˜Í.Í.
00000100	66	60	80	7E	02	00	0F	84	20	00	66	6A	00	66	50	06	f`€~...„ .fj.fP.
00000110	53	66	68	10	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	Sfh....´BŠV@‹ôÍ.
00000120	66	58	66	58	66	58	66	58	EB	33	66	3B	46	F8	72	03	fXfXfXfXë3f;Før.
00000130	F9	EB	2A	66	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	ùë*f3Òf.·N.f÷ñþÂ
00000140	8A	CA	66	8B	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	ŠÊf‹ÐfÁê.÷v.†ÖŠV
00000150	40	8A	E8	C0	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	@ŠèÀä..Ì¸..Í.fa.
00000160	82	74	FF	81	C3	00	02	66	40	49	75	94	C3	42	4F	4F	‚tÿ.Ã..f@Iu”ÃBOO
00000170	54	4D	47	52	20	20	20	20	00	00	00	00	00	00	00	00	TMGR ....
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	0D	0A	44	.............Di
000001B0	73	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	sk errorÿ..Press
000001C0	20	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	any key to rest
000001D0	61	72	74	0D	0A	00	00	00	00	00	00	00	00	00	00	00	art.............
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	AC	01	B9	01	00	00	55	AA	........¬.¹...Uª

FAT32라고 나와있으므로 1

2. 해당 볼륨의 크기



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	CE	00	ëX.MSDOS5.0...Î.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	C8	DA	00	.....ø..?.ÿ..ÈÚ.
00000020	00	80	3E	00	99	0F	00	00	00	00	00	00	02	00	00	00	.€>.™...........
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	80	00	29	8A	EE	A8	0E	4E	4F	20	4E	41	4D	45	20	20	€.)Šî¨.NO NAME
00000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ¼ô

볼륨의 크기 : Total Sector*Bytes Per Sector

Total Sector 32 : 0x003E8000 (리틀엔디안 형식) → 4096000 (10진수)

Bytes Per Sector : 0x200 → 512bytes

- 볼륨의 크기 = 4096000*512 = 2,097,152,000bytes

3. 볼륨 시리얼 번호

   0x0EA8EE8A → 245652138

FLAG

A+B+C = 2,343,104,139

DH{2343104139}