

# Dreamhack-VBR (level1)



**[함께실습]** VBR에서 실습하는 문제입니다.

주어진 VBR을 분석하고, 플래그를 계산하시오.

| 사용 툴 - FTK Imager, HxD

## 1. VBR

- Volume Boot Record = Boot Record
- 볼륨의 가장 첫번째 1개의 섹터는 반드시 부트 섹터가 오게 됨
  - VBR의 크기 = 1섹터 → 부트섹터 = VBR
  - VBR 크기 > 1섹터 → 부트섹터 ≠ VBR
- **VBR = 부팅 가능한 파티션의 첫번째 섹터!**

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000007E00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS .....
000007E10	00	00	00	00	00	F8	00	00	3F	00	FF	00	3F	00	00	00	.....ø...?.ý.?....
000007E20	00	00	00	00	80	00	80	00	D8	A6	3F	01	00	00	00	00	.....ë.ë.ø! ?.....
000007E30	00	00	0C	00	00	00	00	00	6D	FA	13	00	00	00	00	00	.....mú.....
000007E40	F6	00	00	00	01	00	00	00	0D	68	14	F4	7F	14	F4	52	ö.....h.ö..óR
000007E50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	B8	C0	07	...ú3ÀZD%. ú.À.
000007E60	8E	D8	E8	16	00	B8	00	0D	8E	C0	33	DB	C6	06	0E	00	Ž0è.....ŽÀ3ÜÆ...
000007E70	10	E8	53	00	68	00	0D	68	6A	02	CB	8A	16	24	00	B4	.èS.h...hj.ÈŠ.\$.'
000007E80	08	CD	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	.í.s.'ýýŠñf.ŕÆ0f
000007E90	0F	B6	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	.ŕÑëá?÷á+íÀi.Af.
000007EA0	B7	C9	66	F7	E1	66	A3	20	00	C3	B4	41	BB	AA	55	8A	.Éf÷áfE .Ã'A»*UŠ
000007EB0	16	24	00	CD	13	72	0F	81	FB	55	AA	75	09	F6	C1	01	\$.í.r...úU²u.óÁ.
000007EC0	74	04	FE	06	14	00	C3	66	60	1E	06	66	A1	10	00	66	t.p...Ãf'..fj..f
000007ED0	03	06	1C	00	66	3B	06	20	00	0F	82	3A	00	1E	66	6A	....f; . . . , : . . fj
000007EE0	00	66	50	06	53	66	68	10	00	01	00	80	3E	14	00	00	.fP.Sfh....ë>...
000007EF0	0F	85	0C	00	E8	B3	FF	80	3E	14	00	00	0F	84	61	00	.....è³yë>.....a.
000007F00	B4	42	8A	16	24	00	16	1F	8B	F4	CD	13	66	58	5B	07	'BŠ.\$...<óÍ.fX[.
000007F10	66	58	66	58	1F	EB	2D	66	33	D2	66	0F	B7	0E	18	00	fXfX.è-f3Óf. ....
000007F20	66	F7	F1	FE	C2	8A	CA	66	8B	D0	66	C1	EA	10	F7	36	f÷ñpÀŠÉf<ĐfÁé.÷6
000007F30	1A	00	86	D6	8A	16	24	00	8A	E8	C0	E4	06	0A	CC	B8	..+ÖŠ.\$.\$èÀä..ì,
000007F40	01	02	CD	13	0F	82	19	00	8C	C0	05	20	00	8E	C0	66	..í.,...ÆÀ. .ŽÀf
000007F50	FF	06	10	00	FF	0E	0E	00	0F	85	6F	FF	07	1F	66	61	ý...ý.....oy..fa
000007F60	C3	A0	F8	01	E8	09	00	A0	FB	01	E8	03	00	FB	EB	FE	Ã ø.è.. ú.è..úép
000007F70	B4	01	8B	F0	AC	3C	00	74	09	B4	0E	BB	07	00	CD	10	'.<ð~<.t.'...»..í.
000007F80	EB	F2	C3	0D	0A	41	20	64	69	73	6B	20	72	65	61	64	è0Ã..A disk read
000007F90	20	65	72	72	6F	72	20	6F	63	63	75	72	72	65	64	00	error occurred.
000007FA0	0D	0A	4E	54	4C	44	52	20	69	73	20	6D	69	73	73	69	..NTLDR is missi
000007FB0	6E	67	00	0D	0A	4E	54	4C	44	52	20	69	73	20	63	6F	ng...NTLDR is co
000007FC0	6D	70	72	65	73	73	65	64	00	0D	0A	50	72	65	73	73	mpressed...Press
000007FD0	20	43	74	72	6C	2B	41	6C	74	2B	44	65	6C	20	74	6F	Ctrl+Alt+Del to
000007FE0	20	72	65	73	74	61	72	74	0D	0A	00	00	00	00	00	00	restart.....
000007FF0	00	00	00	00	00	00	00	00	83	A0	B3	C9	00	00	55	AA	.....f³É..U²

- 노란색 : CPU Jump Command + OEM ID
  - CPU 점프 명령 → 해당 위치로 점프하여 그 이후 코드 실행
  - OEM ID → 파일 시스템 종류
- 빨간색 : BPB (BIOS Parameter Block)
- 보라색 : BPB 확장 영역 → 파티션의 물리주소 레이아웃에 관련된 내용
  - 총 섹터 수, 크기, 트랙 당 섹터 수 등
- 주황색 : 부트스트랩 코드
  - 해당 볼륨 정보, 파일시스템 타입, 부트코드 및 에러메시지 등

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Jump Boot Code			OEM Name								Byte Per Sector		SP	RS	
0x10	FAT개수	Root Directory Entry 개수		Total Sector 16		Media Type	FAT Size16		Sector Per Track		Head 개수		Hidden Sector			
0x20	Total Sector 32				FAT Size 32				EXT Flags		File System Version		Root Directory Cluster			
0x30	File System Information		Boot Record Backup Sector		Reserved											
0x40	Dirve Num	Reser ved1	Boot Sign	Volume ID				Volume Label(1)								
0x50	Volume Label(2)		File System Type													

CF : <https://plummmm.tistory.com/13>

## 2. 다운로드 받은 파일 압축해제 후 HxD 를 통하여 분석 진행

- 파일시스템 : FAT32 = 1
- 해당 볼륨의 크기 : Total Sector X Bytes Per Sector = 003E8000 X 0200 =
- 볼륨 시리얼 번호 : 8A EE A8 0E = 0x0EA8EE8A

```

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 eX.MSDOS5.0...î.
00000010 02 00 00 00 00 F8 00 00 3F 00 FF 00 00 C8 DA 00 .....ø...?.ÿ..ËÚ.
00000020 00 80 3E 00 99 0F 00 00 00 00 00 00 02 00 00 00 .e>..™.....
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 e )Ši" NO NAME
00000050 20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4 FAT32 3ÉŽÑ+ô
00000060 7B 8E C1 8E D9 BD 00 7C 88 56 40 88 4E 02 8A 56 {ZAZU%|^V@^N.ŠV
00000070 40 B4 41 BB AA 55 CD 13 72 10 81 FB 55 AA 75 0A @'A»^Uí.r..ûU^u.
00000080 F6 C1 01 74 05 FE 46 02 EB 2D 8A 56 40 B4 08 CD ôÁ.t.pF.ë-ŠV@'.í
00000090 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F B6 .s.'ÿÿŠñf.Ź@f.Ź
000000A0 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7 C9 Ŋeá?÷â+îîi.Af.·É
000000B0 66 F7 E1 66 89 46 F8 83 7E 16 00 75 39 83 7E 2A f÷áf%Føf~..u9f~*
000000C0 00 77 33 66 8B 46 1C 66 83 C0 0C BB 00 80 B9 01 .w3f<F.fjÀ.».é¹.
000000D0 00 E8 2C 00 E9 A8 03 A1 F8 7D 80 C4 7C 8B F0 AC .è,.é".;ø)ëÄ|<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; }ëëß"í.í.
00000100 66 60 80 7E 02 00 0F 84 20 00 66 6A 00 66 50 06 f'ë~....„ .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 fXfXfXfXfXf3f;Før.
00000130 F9 CA 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE C2 ùë*f3òf.·N.f÷ñpÂ
00000140 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A 56 ŠÊf<ðfÀë.÷v.+ÖŠV
00000150 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61 0F @ŠëÄä..î,..í.fa.
00000160 82 74 FF 81 C3 00 02 66 40 49 75 94 C3 42 4F 4F ,tÿ.Ä..f@Iu"ÄBOO
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.....

```



DH{2343104139}