Dreamhack-VBR(level1)

[forensics]

Description

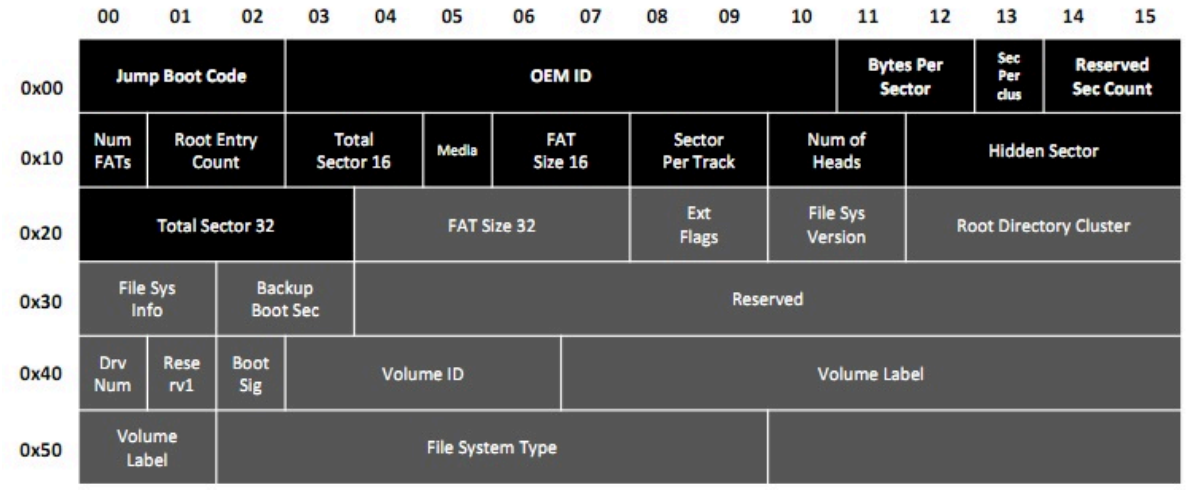
주어진 VBR을 분석하고, 플래그를 계산하시오. (2024.10.02)

Info

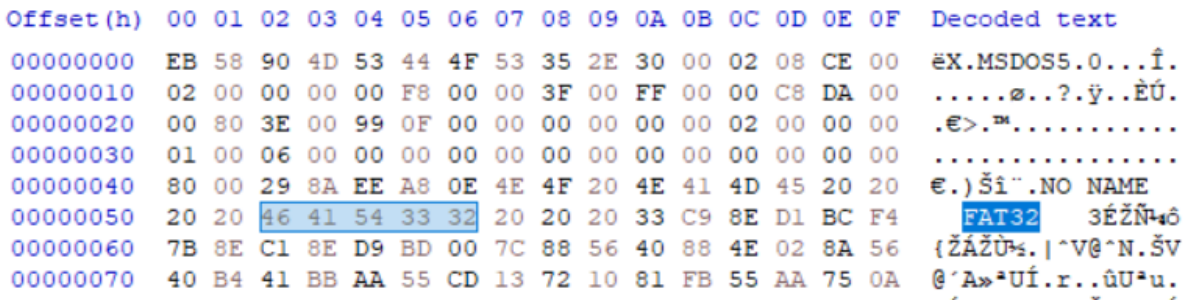
- FLAG = `DH{(A + B + C)}` (단, 더한 값을 십진수로 변환할 것)
  - ◦ A: 파일시스템이 FAT32면 `1`, NTFS면 `2`
  - ◦ B: 해당 볼륨의 크기
  - ◦ C: 볼륨 시리얼 번호
- 예를 들어 파일시스템이 `NTFS`, 볼륨의 크기가 `0x100000`, 그리고 볼륨 시리얼 번호가 `0x12341234` 면, `2 + 0x100000 + 0x12341234 = 0x12441236 = 306450998` (십진수) 이므로 `DH{306450998}` 을 제출하시면 됩니다.

Write up

- 사용 도구: HxD



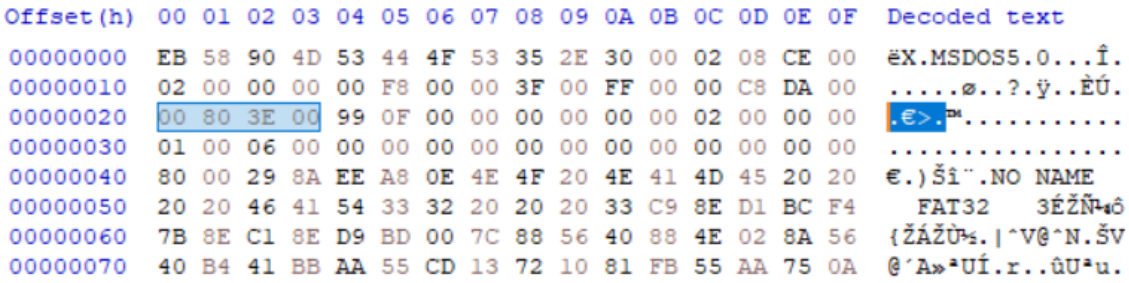
- 파일 시스템 → FAT32 `1`



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.

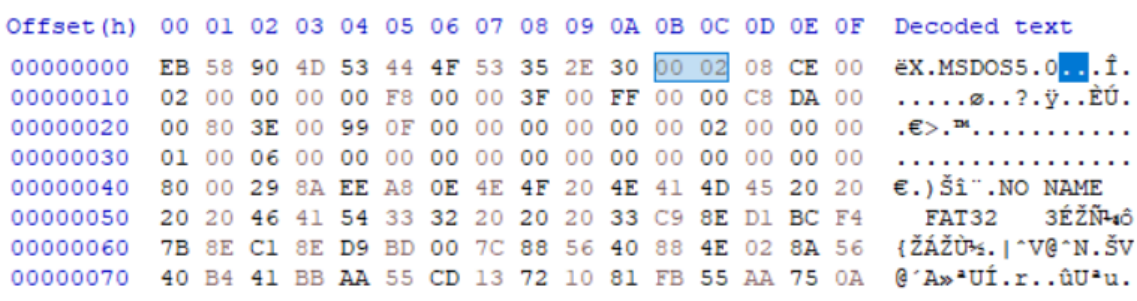
- 볼륨 크기
  - 볼륨 크기 = Total Sectors × Bytes per Sector
  - **7D000000 =** `0x003E8000` x `0x0200`

  - Total Sectors → `00 80 3E 00`
    - 16진수 → `0x003E8000`



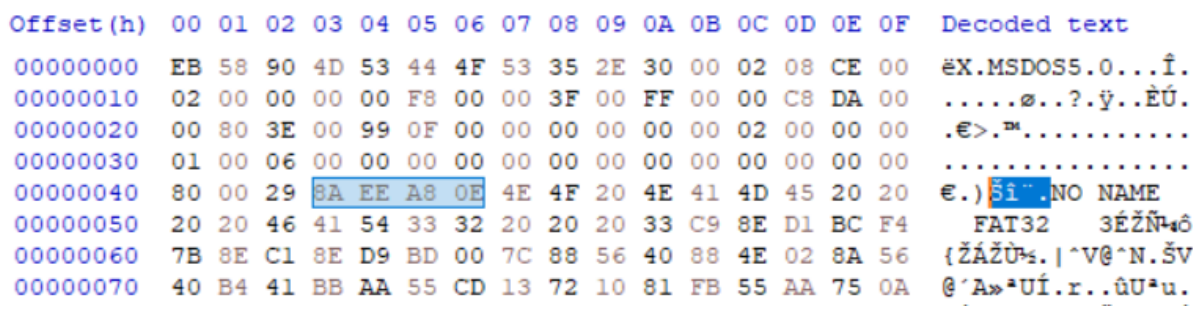
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	CE	00	ëX.MSDOS5.0...Î.
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	C8	DA	00	.....ø..?.ÿ..ÈÚ.
00000020	00	80	3E	00	99	0F	00	00	00	00	00	00	02	00	00	00	.€>.™...........
00000030	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.

  - Bytes per Sector → `00 02`
    - 16진수 → `0x0200`



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.

- 볼륨 시리얼 번호 → `8A EE A8 0E`
  - 16진수 → `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	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.

- A: **1**
- B: **7D000000**
- C: **0x0EA8EE8A**
- A + B + C = 1 + (7D000000 + 0x0EA8EE8A)
- 1 + 8BA8EE8A = 8BA8EE8B(16진수) ⇒ **2343104139**(10진수)
- FLAG 형식으로는, DH{2343104139}

FLAG

DH{2343104139}