Dreamhack-FFFFAAAATTT(level1)

[forensics]

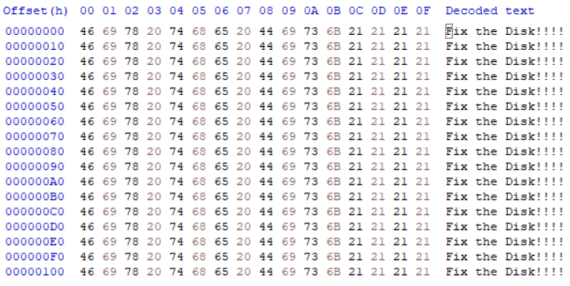
Description

> **FIXFIXFIX! FFFAAATTT!** (2021.10.07)

Write up

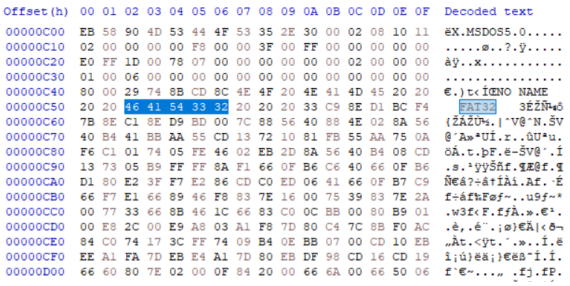
- 사용 도구: HxD, FTK Imager

- HxD를 통해 손상된 FAT 영역 복구
  - FAT 시그니처(`46 41 54 33 32`) 발견
  - 해당 백업 VBR을 복사 후 디스크 이미지 시작 부분(`0x0`)에 덮어쓰기 후 저장



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000010	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000020	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000030	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000040	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000050	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000060	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000070	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000080	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000090	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000A0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000B0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000C0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000D0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000E0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000F0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000100	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!

손상된 파일



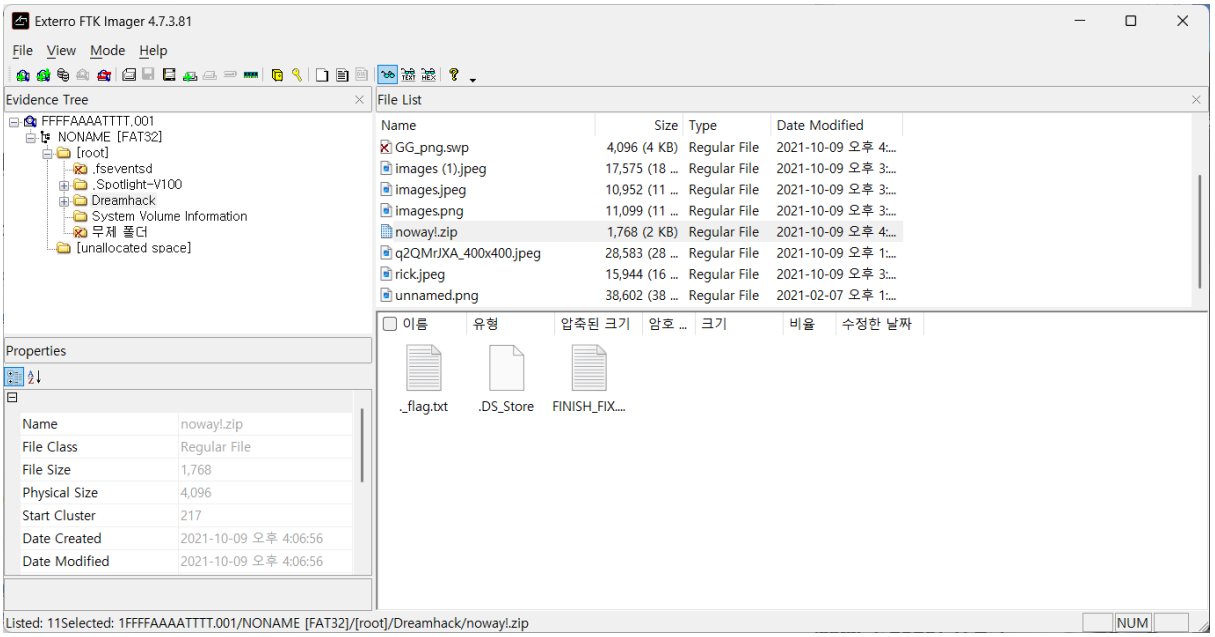
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000C00	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	10	11	ëX.MSDOS5.0.....
00000C10	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00	.....ø..?.ÿ.....
00000C20	E0	FF	1D	00	78	07	00	00	00	00	00	00	02	00	00	00	àÿ..x...........
00000C30	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000C40	80	00	29	74	8B	CD	8C	4E	4F	20	4E	41	4D	45	20	20	€.)t‹ÍŒNO NAME
00000C50	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ¼ô
00000C60	7B	8E	C1	8E	D9	BD	00	7C	88	56	40	88	4E	02	8A	56	{ŽÁŽÙ½.|ˆV@ˆN.ŠV
00000C70	40	B4	41	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	@´A»ªUÍ.r..ûUªu.
00000C80	F6	C1	01	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	öÁ.t.þF.ë-ŠV@´.Í
00000C90	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	.s.¹ÿÿŠñf.¶Æ@f.¶
00000CA0	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	Ñ€â?÷â†ÍÀí.Af.·É
00000CB0	66	F7	E1	66	89	46	F8	83	7E	16	00	75	39	83	7E	2A	f÷áf‰Føƒ~..u9ƒ~*
00000CC0	00	77	33	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	.w3f‹F.fƒÀ.».€¹.
00000CD0	00	E8	2C	00	E9	A8	03	A1	F8	7D	80	C4	7C	8B	F0	AC	.è,.é¨.¡ø}€Ä|‹ð¬
00000CE0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	„Àt.<ÿt.´.».Í.ë
00000CF0	EE	A1	FA	7D	EB	E4	A1	7D	80	EB	DF	98	CD	16	CD	19	î¡ú}ëä¡}€ëß˜Í.Í.
00000D00	66	60	80	7E	02	00	0F	84	20	00	66	6A	00	66	50	06	f`€~.... .fj.fP.

FAT 시그니처

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	10	11	ëX.MSDOS5.0.....
00000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00	.....ø..?.ÿ.....
00000020	E0	FF	1D	00	78	07	00	00	00	00	00	00	02	00	00	00	àÿ..x...........
00000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	80	00	29	74	8B	CD	8C	4E	4F	20	4E	41	4D	45	20	20	€.)t‹ÍŒNO 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.

시작 부분에 FAT 시그니처 덮어쓰기

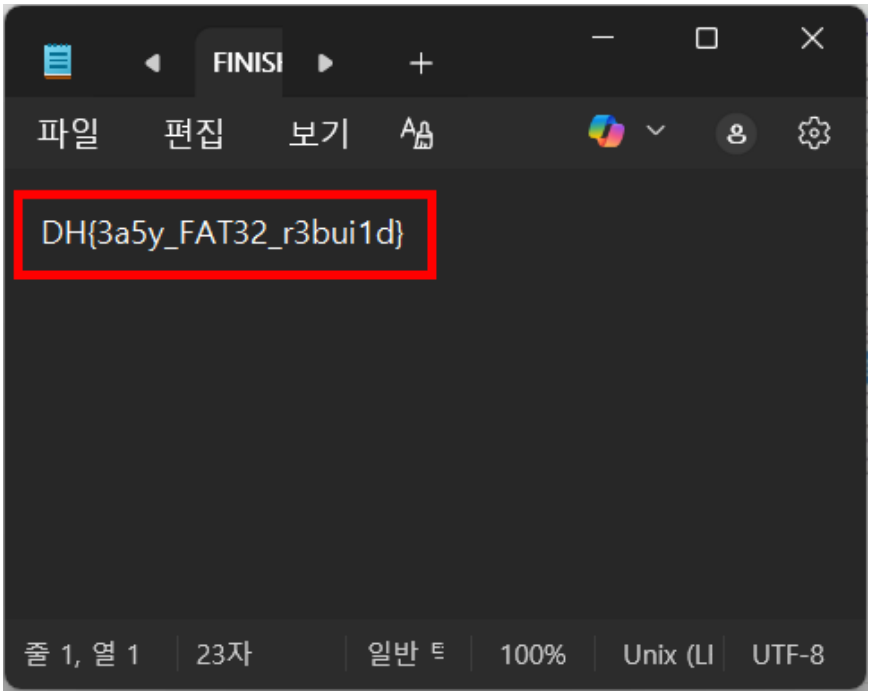
- FTK Imager를 통해 내부 파일 확인
  - C:\Dreamhack\noway!.zip 파일 확인



- noway!.zip 파일에 암호가 걸려있음
  - HxD를 통해 해당 파일의 암호 검색 ⇒ **DHDHFIX**

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
004F1F80   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1F90   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FA0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FB0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FC0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FD0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FE0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F1FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F2000   47 47 3F 20 74 68 65 20 7A 69 70 20 6B 65 79 20  GG? the zip key
004F2010   3A 20 44 48 44 48 46 49 58 0A 00 00 00 00 00 00  : DHDHFIX.......
004F2020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F2030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004F2040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

- FINISH_FIX.txt 내부에서 DH 형태의 FLAG 확인



- FLAG는, DH{3a5y_FAT32_r3bui1d}

FLAG

DH{3a5y_FAT32_r3bui1d}