FFFFAAAATTT

Description

> FIXFIXFIX! FFFAAATTT!

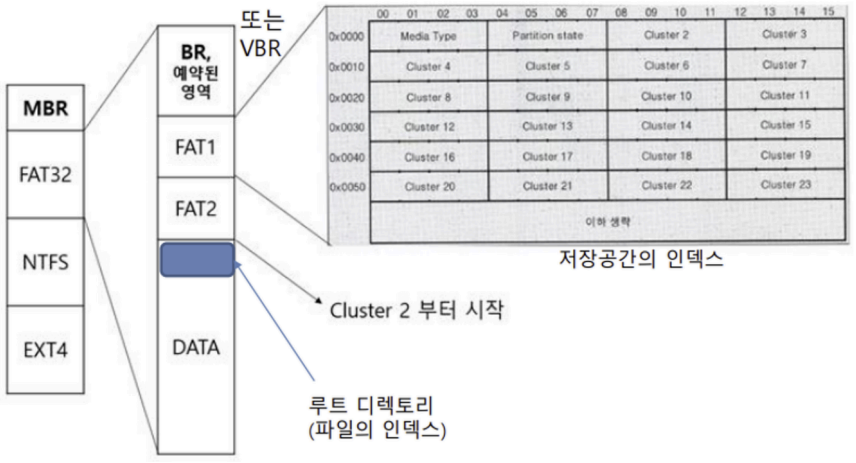
사용한 도구

HxD, FTK Imager

Background

FAT (File Allocation System)

- SD 카드에서 많이 사용하는 파일 시스템
- FAT 16, FAT 32
- 디렉토리 엔트리, FAT 존재
  - 디렉토리 엔트리 : 각 파일과 디렉토리를 데이터 구조체에 할당할 때 사용되는 구조체
  - 파일명, 크기, 파일 내용 시작 주소, 다른 메타데이터가 디렉토리 엔트리에 포함됨
- 암호화 및 압축이 불가능하다
- 예약 영역
  - 파일 시스템 참조 모델 데이터를 포함하는 영역
  - FAT 12, FAT 16 파일 시스템 경우 해당 영역의 크기는 보통 1개의 섹터 크기지만 어떤 경우에는 부트 섹터에서 해당 영역의 크기를 정하기도 함
- FAT 영역
  - 주 FAT 구조체와 부(백업) FAT 구조체를 포함하는 영역
  - 예약된 영역 바로 다음 섹터부터 시작
  - 해당 영역 크기는 FAT 구조체 수와 크기에 따라 달라짐
- 데이터 영역
  - 파일과 디렉토리 내용을 저장하는 클러스터를 포함하는 영역



FAT32는 BR, FAT1, FAT2, DATA 크게 이렇게 4가지로 나누어져 있다.

이 중 디스크가 부팅되기 위해서는 BR 영역이 정해진 구조대로 존재해야한다.

- 망가지면 백업부분을 덮어쓰기하여 복구가 가능하다 (VBR 문제와 유사)
- **보통 FAT32 시스템 이미지의 백업 BR는 섹터 6번에 위치한다.**

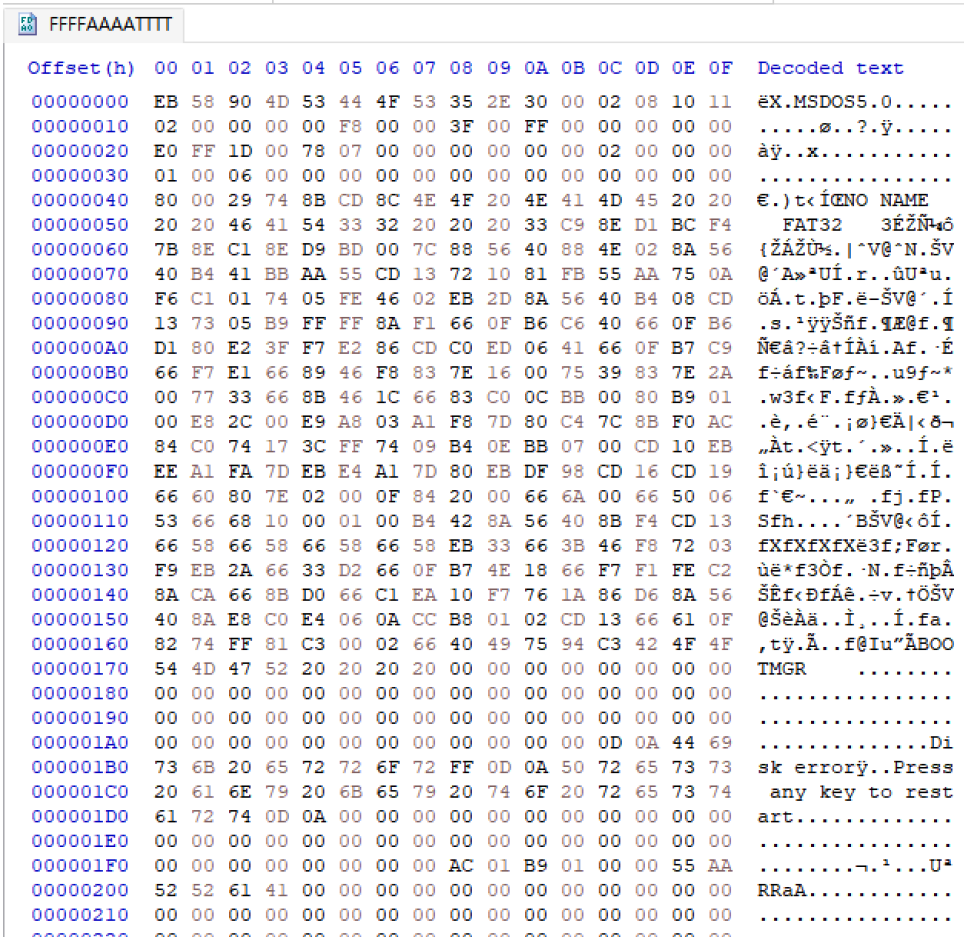
1. HxD 로 주어진 파일 열기

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000BD0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000BE0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000BF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
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.
00000D10   53 66 68 10 00 01 00 B4 42 8A 56 40 8B F4 CD 13  Sfh....´BŠV@‹ôÍ.
00000D20   66 58 66 58 66 58 66 58 EB 33 66 3B 46 F8 72 03  fXfXfXfXë3f;Før.
00000D30   F9 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE C2  ùë*f3Òf.·N.f÷ñþÂ
00000D40   8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A 56  ŠÊf‹ÐfÁê.÷v.†ÖŠV
00000D50   40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61 0F  @ŠèÀä..Ì¸..Í.fa.
00000D60   82 74 FF 81 C3 00 02 66 40 49 75 94 C3 42 4F 4F  ‚tÿ.Ã..f@Iu”ÃBOO
00000D70   54 4D 47 52 20 20 20 20 00 00 00 00 00 00 00 00  TMGR    ........
```

FAT32라고 적힌 것으로 보아 FAT 파일 시스템을 사용한다는 걸 확인할 수 있다.

2. 복구용 BR 섹터 덮어쓰기

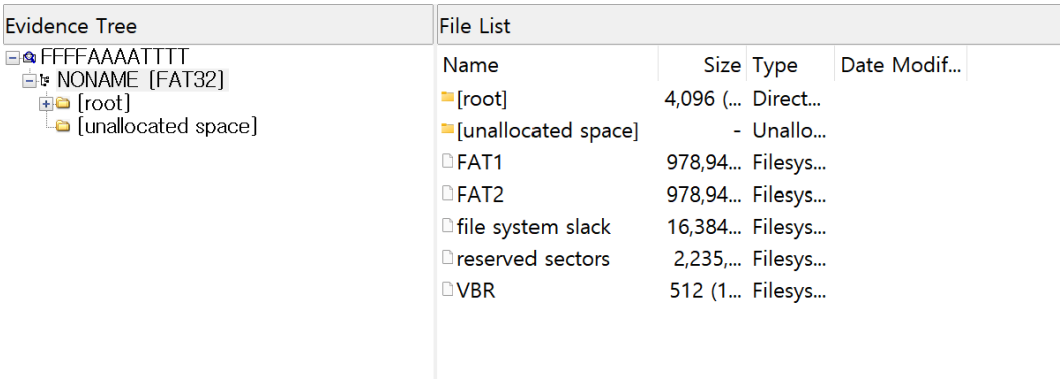
복구를 위해 섹터6부분(offset 00000C00~)을 섹터0 영역에 덮어쓴 뒤 저장해주었다.



FFFFAAAATTTT

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.|^V@^N.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	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
00000200	52	52	61	41	00	00	00	00	00	00	00	00	00	00	00	00	RRaA............
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

3. 복구한 파일 FTK Imager로 확인



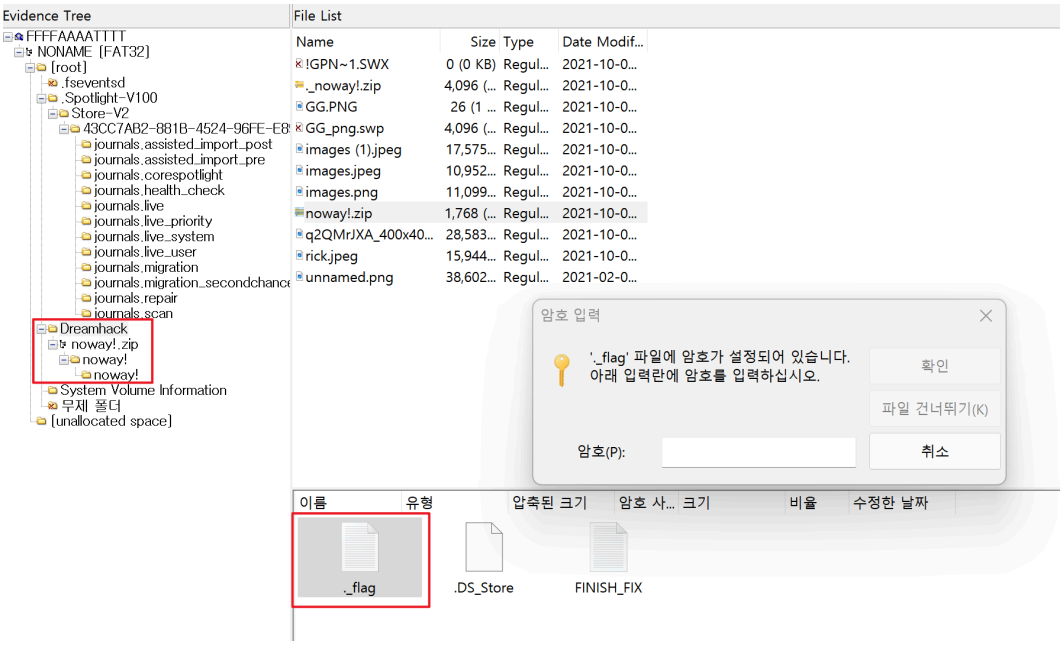
Evidence Tree

- FFFFAAAATTTT
  - NONAME [FAT32]
    - [root]
    - [unallocated space]

File List

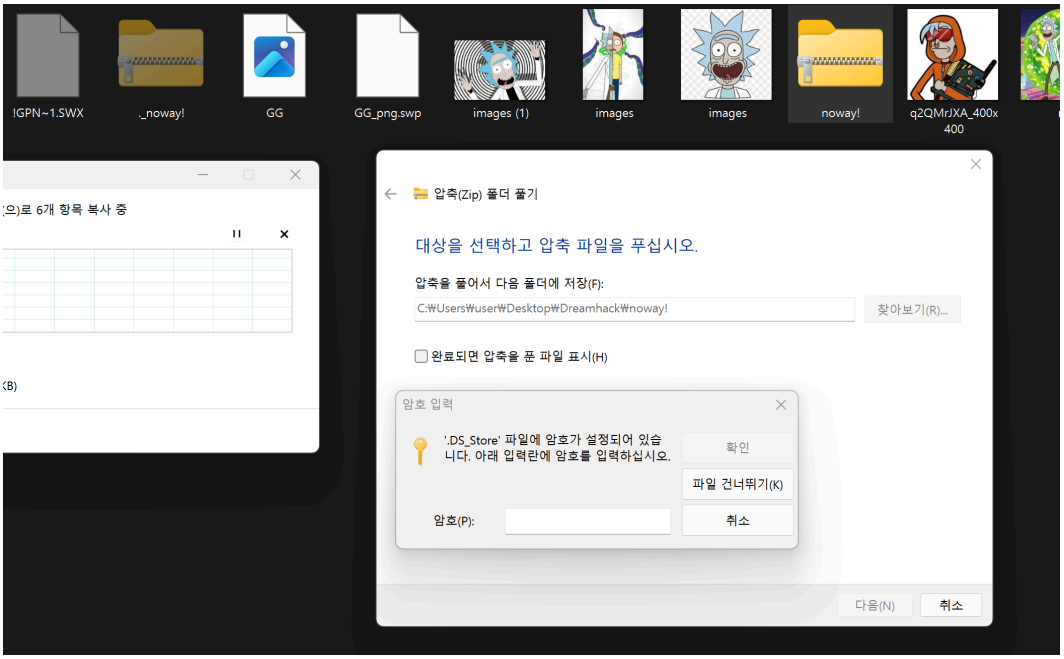
Name	Size	Type	Date Modif...
[root]	4,096 (...	Direct...	
[unallocated space]	-	Unallo...	
FAT1	978,94...	Filesys...	
FAT2	978,94...	Filesys...	
file system slack	16,384...	Filesys...	
reserved sectors	2,235,...	Filesys...	
VBR	512 (1...	Filesys...	

FTK Imager로 열었을 때 정상적으로 파일 내용물이 복구된 걸 확인할 수 있다.



Dreamhack 폴더 속 _noway!.zip 폴더 속 flag와 관련된 파일을 확인할 수 있으나 암호가 설정되어 있다.

분석을 위해 Dreamhack 폴더를 추출하였다.



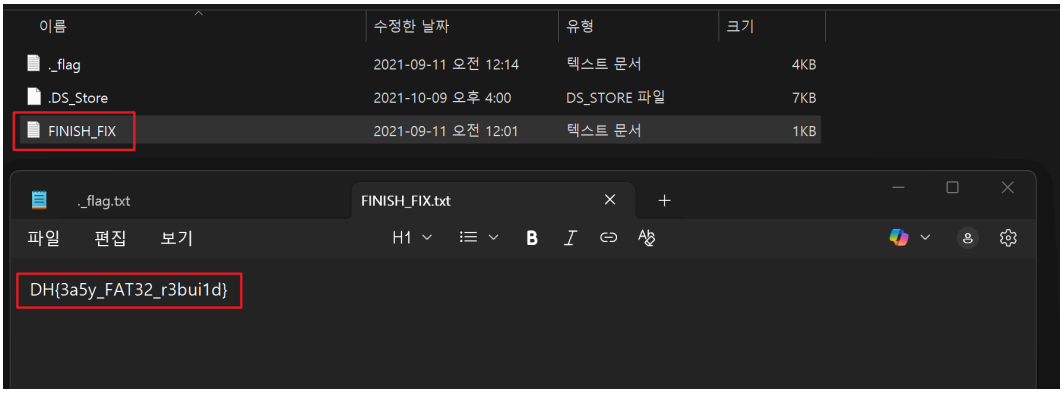
압축해제를 위해서도 암호가 필요하단걸 알 수 있었다.

하나씩 HxD로 열어보다가 GG를 열었을 때 암호를 풀 수 있는 key를 알 수 있었다.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   47 47 3F 20 74 68 65 20 7A 69 70 20 6B 65 79 20  GG? the zip key
00000010   3A 20 44 48 44 48 46 49 58 0A                    : DHDHFIX.
```

DHDHFIX 로 암호를 풀어 성공적으로 압축해제를 할 수 있었다.

`"C:\Users\user\Desktop\Dreamhack\noway!\noway!\noway!\FINISH_FIX.txt"` 에서 flag를 찾을 수 있었다.



FLAG

DH{3a5y_FAT32_r3bui1d}