Dreamhack-Corrupted Disk Image(level1)

[forensics]

Description

디스크 이미지가 열리지 않습니다...!

주어진 디스크 이미지를 복원하여 플래그를 구해주세요. (2024.10.02)

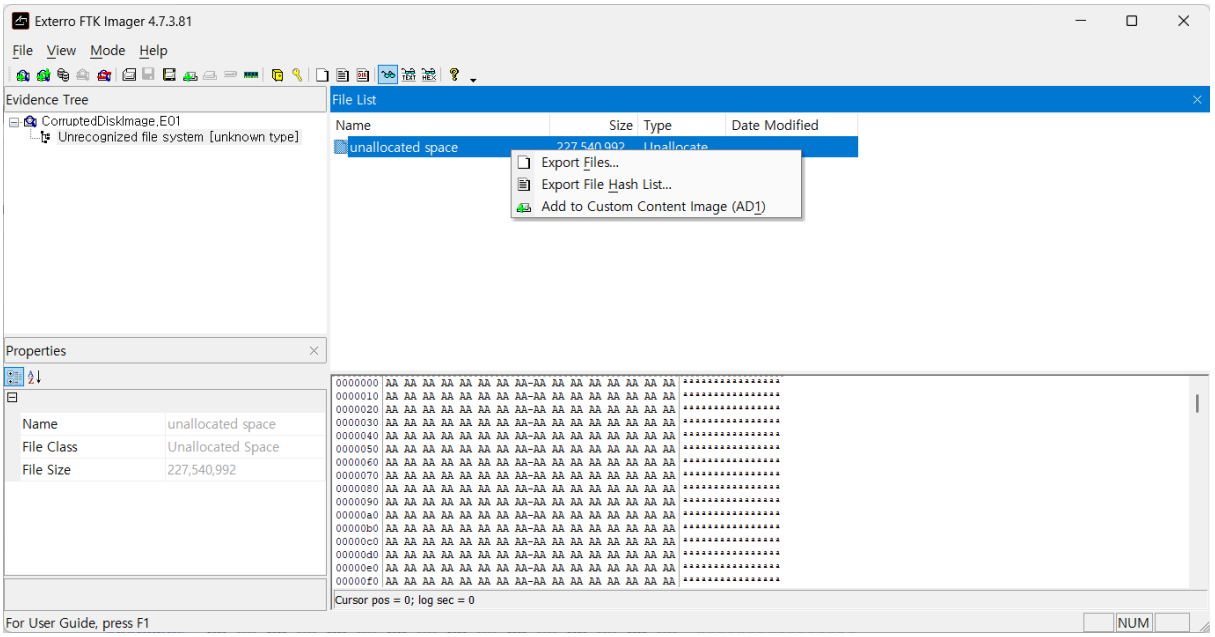
Info

- FLAG: `DH{something}`
- `something`의 길이는 32자입니다.

Write up

- 사용 도구: FTK Imager, HxD

- FTK Imager를 통해 `CorruptedDiskImage.E01` 확인
- `unallocated space` 파일 추출



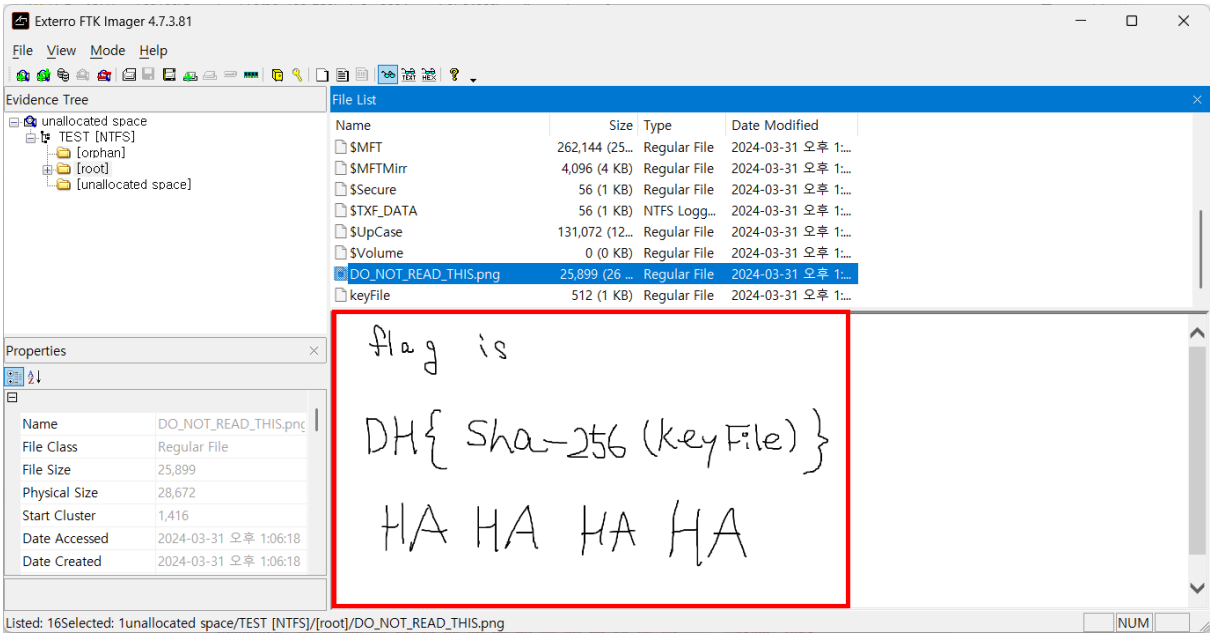
- HxD를 통해 해당 파일의 헥사값 확인
  - HxD에서 `0xD8FFE00` 오프셋에서 NTFS 시그니처(`EB 52 90 4E 54 46 53`) 확인
  - 즉, 해당 위치를 백업 VBR로 추정

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0D8FFDE0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0D8FFDF0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0D8FFE00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS ....
0D8FFE10	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	48	19	01	.....ø..?.ÿ..H..
0D8FFE20	00	00	00	00	80	00	00	00	FF	C7	06	00	00	00	00	00	....€...ÿÇ.....
0D8FFE30	AA	A6	00	00	00	00	00	00	02	00	00	00	00	00	00	00	ª¦..............
0D8FFE40	F6	00	00	00	01	00	00	00	A5	48	A0	F0	7C	A0	F0	F2	ö.......¥H ð| ðò
0D8FFE50	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽÐ¼.|ûhÀ.
0D8FFE60	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N
0D8FFE70	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û
0D8FFE80	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì
0D8FFE90	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.
0D8FFEA0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£
0D8FFEB0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È
0D8FFEC0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.......ŽÂÿ...è
0D8FFED0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwï¸.»Í.f#Àu-
0D8FFEE0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu$.ù..r..

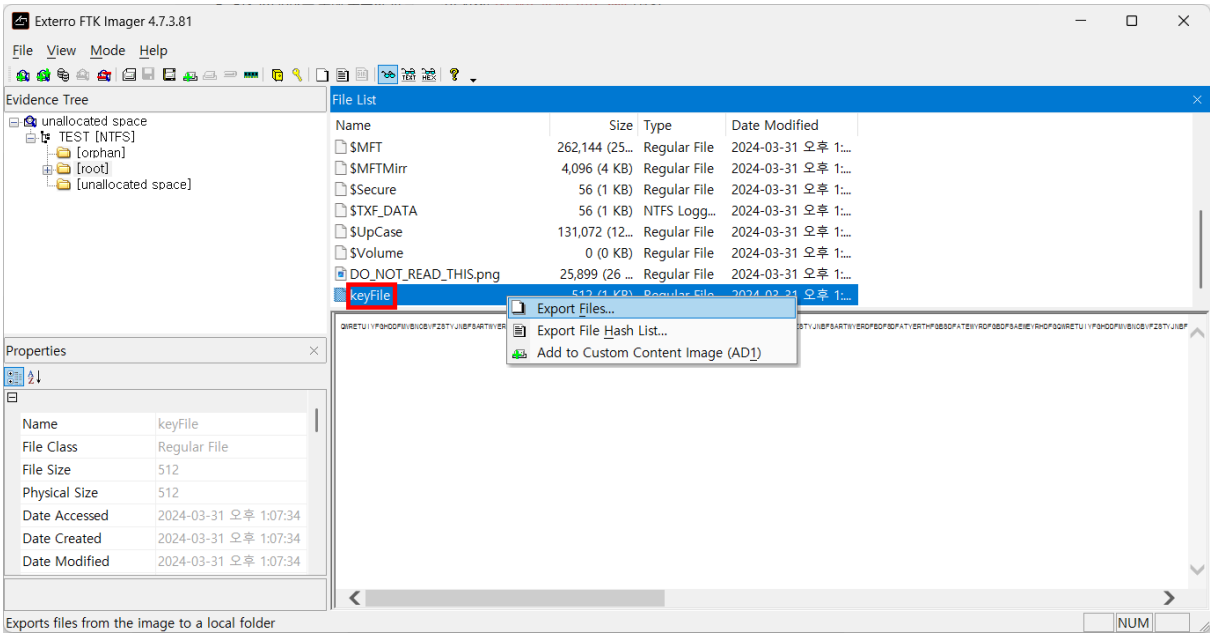
- 해당 백업 VBR을 복사 후 디스크 이미지 시작 부분(`0x0`)에 덮어쓰기 후 저장

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ëR.NTFS    .....
00000010   00 00 00 00 00 F8 00 00 3F 00 FF 00 00 48 19 01  .....ø..?.ÿ..H..
00000020   00 00 00 00 80 00 00 00 FF C7 06 00 00 00 00 00  ....€...ÿÇ......
00000030   AA A6 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ª¦..............
00000040   F6 00 00 00 01 00 00 00 A5 48 A0 F0 7C A0 F0 F2  ö.......¥H ð| ðò
00000050   00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3ÀŽÐ¼.|ûhÀ.
00000060   1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ë^...f.>..N
00000070   54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu.´A»ªUÍ.r..û
00000080   55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  Uªu.÷Á..u.éÝ..ƒì
00000090   18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  .h..´HŠ...‹ô..Í.
000000A0   9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  ŸƒÄ.žX.rá;...uÛ£
000000B0   0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  ..Á.....Z3Û¹. +È
000000C0   66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8  fÿ.......ŽÂÿ...è
000000D0   4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D  K.+Èwï¸.»Í.f#Àu-
000000E0   66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  f.ûTCPAu$.ù..r..
000000F0   68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66  h.».hR..h..fSfSf
00000100   55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF  U...h¸.fa..Í.3À¿
```

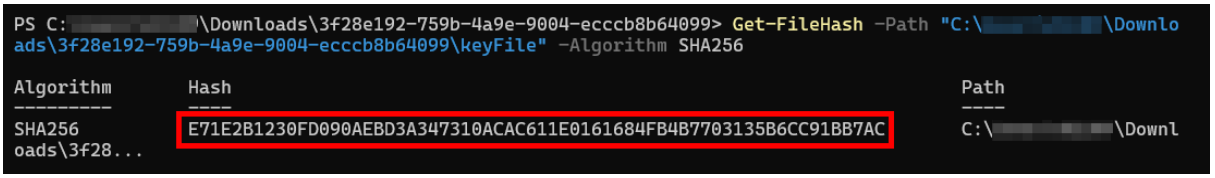
- FTK Imager를 통해 복구한 파일을 열어 사진(`DO_NOT_READ_THIS.png`)확인
  - **DH{sha-256(keyFile)}**



- FTK Imager를 통해 `C:\keyFile` 추출



- `Get-FileHash -Path "C:\keyFile" -Algorithm SHA256` 명령어를 통해 SHA256 해시값 추출



- 대문자 안됨 → 왜? 소문자 변환
- something: **e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac**
- FLAG 형식으로는, DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}

FLAG

DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}