

# Dreamhack- Corrupted Disk Image(level1)

## 문제

### Description

[함께실습] [Corrupted Disk Image](#)에서 실습하는 문제입니다.

디스크 이미지가 열리지 않습니다...!

주어진 디스크 이미지를 복원하여 플래그를 구해주세요.

### Info

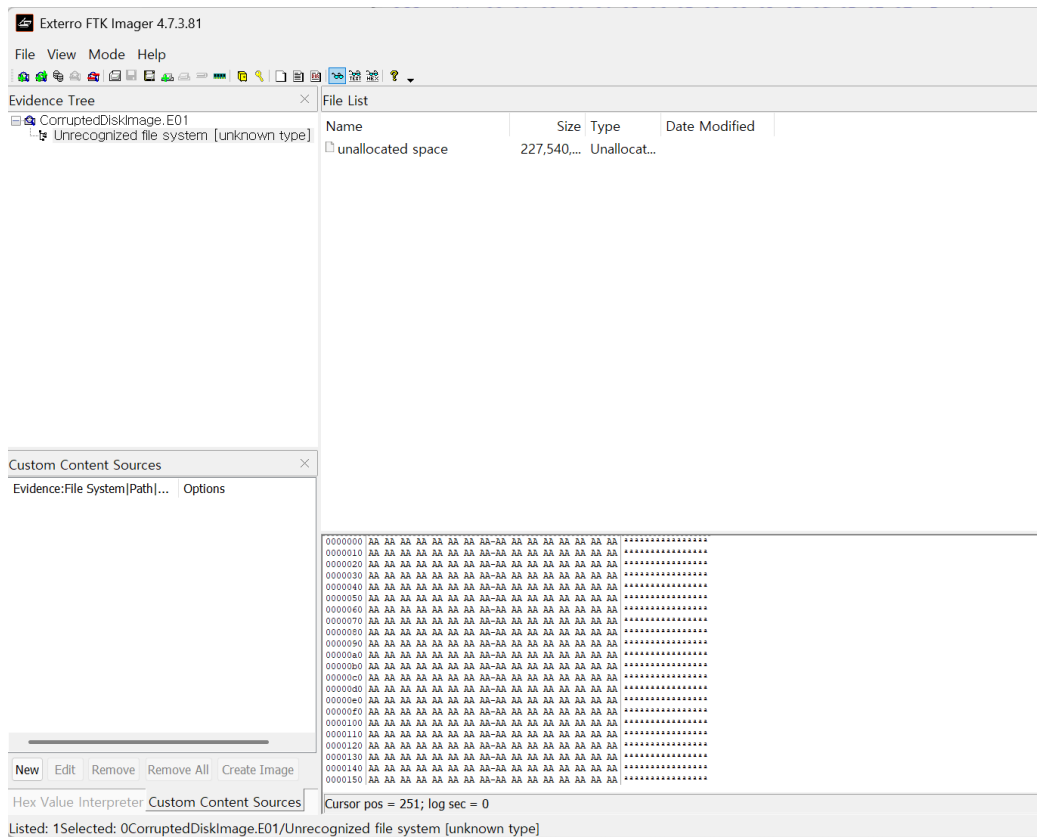
- FLAG: `DH{something}`
- `something` 의 길이는 32자입니다.

## 풀이

1. 문제 파악  
제공된

디스크 이미지 파일이 손상되어 열리지 않음 → 파일 시스템 구조나 일부 데이터를 복원하기 → 파티션 복구 필요

2. 문제 풀이



E01파일을 FTK를 통해 확인해보니 깨진 파일을 발견.

비워져 있는 섹터 부분에 원래의 데이터 정보를 삽입해줘야한다.

CorruptedDiskImage.E01																	unallocated space
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0D8FFD10	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD20	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD30	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD40	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD50	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD60	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD70	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD80	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFD90	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDA0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDB0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDC0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDD0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDE0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFDF0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	????????????????
0D8FFE00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	er.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	*!.....
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	...ú3ÄZD4.  ûhÄ.
0D8FFE60	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.E^...f.>..N
0D8FFE70	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A»*UÍ.r...û
0D8FFE80	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u.-Ä..u.éÝ..fì
0D8FFE90	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'HŠ...<ö..í.
0D8FFEA0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸfÄ.ZX.rá;...uÜè
0D8FFEB0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ü¹. +è
0D8FFEC0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ŽÄÿ...è
0D8FFED0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èw1.,»í.f#Au-
0D8FFEE0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu\$.ù..r..
0D8FFF00	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..fSfSf
0D8FFF10	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h..fa..í.3Ä¿
0D8FFF20	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..²ö.üó*ép...f`
0D8FFF30	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f;..f.....fh...
0D8FFF40	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..'BŠ..
0D8FFF50	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<óí.fY[ZfYfY.
0D8FFF60	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ŽÄÿ
0D8FFF70	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u4..faÄ;ö..è...
0D8FFF80	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ü.è...öëÿ<ð-<.t.
0D8FFF90	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	'.»...í.èöÄ..A di
0D8FFFA0	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
0D8FFFB0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR
0D8FFFC0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..
0D8FFFD0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+
0D8FFFE0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..
0D8FFFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0D8FFFF0	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	AA	.....Š.S.¿...U*

HxD를 통해 복구 시도하였다. 섹터 맨 뒷부분에서 NTFS 파일 시스템 확인하여 비워져 있던 섹터 부분에 삽입하여 수정해주었다.

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	00	02	08	00	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	* .....
00000040	F6	00	00	00	01	00	00	00	A5	48	A0	F0	7C	A0	F0	F2	ö.....¥H ø  øð
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	...ú3ÄŽÐ4.  ûhA.
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»²UÍ.r..û
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*ü.÷Ä..u.éÝ..fi
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'HŠ...<ó..í.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÝfÄ.žX.rá;...uÜē
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ü¹. +ē
000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ŽÄÿ...è
000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+ēwi,.»í.f#Äu-
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.3Äž
00000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	...²ð.úó²ép...f`.
00000120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f;.f.....fh...
00000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..'BŠ..
00000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<óí.fÿ{ZfYfY.
00000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ŽÄÿ
00000160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u4..faÄ;ð.è..
00000170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	;ú.è..ðēÿ<ð-<.t.
00000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	`.»..í.èðÄ..A di
00000190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
000001A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR
000001B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..
000001C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+
000001D0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	AA	.....Š.\$..ç....U²

Exterro FTK Imager 4.7.3.81  
File View Mode Help  
Evidence Tree  
CorruptedDiskImage.E01  
unallocated space  
TEST [NTFS]  
[orphan]  
[root]  
(unallocated space)

File List  

Name	Size	Type	Date Modified
\$AttrDef	2,560 (3 ...)	Regular F...	2024-03-31 오후 11:00
\$BadClus	-	Regular F...	2024-03-31 오후 11:00
\$Bitmap	6,944 (7 ...)	Regular F...	2024-03-31 오후 11:00
\$Boot	8,192 (8 ...)	Regular F...	2024-03-31 오후 11:00
\$I30	4,096 (4 ...)	NTFS Ind...	2024-03-31 오후 11:00
\$LogFile	4,325,37...	Regular F...	2024-03-31 오후 11:00
\$MFT	262,144 (...)	Regular F...	2024-03-31 오후 11:00
\$MFTMirr	4,096 (4 ...)	Regular F...	2024-03-31 오후 11:00
\$Secure	56 (1 KB)	Regular F...	2024-03-31 오후 11:00
\$TXF_DATA	56 (1 KB)	NTFS Lo...	2024-03-31 오후 11:00
\$UpCase	131,072 (...)	Regular F...	2024-03-31 오후 11:00
\$Volume	0 (0 KB)	Regular F...	2024-03-31 오후 11:00
DO_NOT_READ_THIS.png	25,899 (25,899 B)	Regular F...	2024-03-31 오후 11:00
keyFile	512 (1 KB)	Regular F...	2024-03-31 오후 11:00

Custom Content Sources  
Evidence:File System|Path|... Options  
New Edit Remove Remove All Create Image  
Hex Value Interpreter Custom Content Sources  
Listed: 16Selected: 1unallocated space/TEST [NTFS]/root/DO\_NOT\_READ\_THIS.png

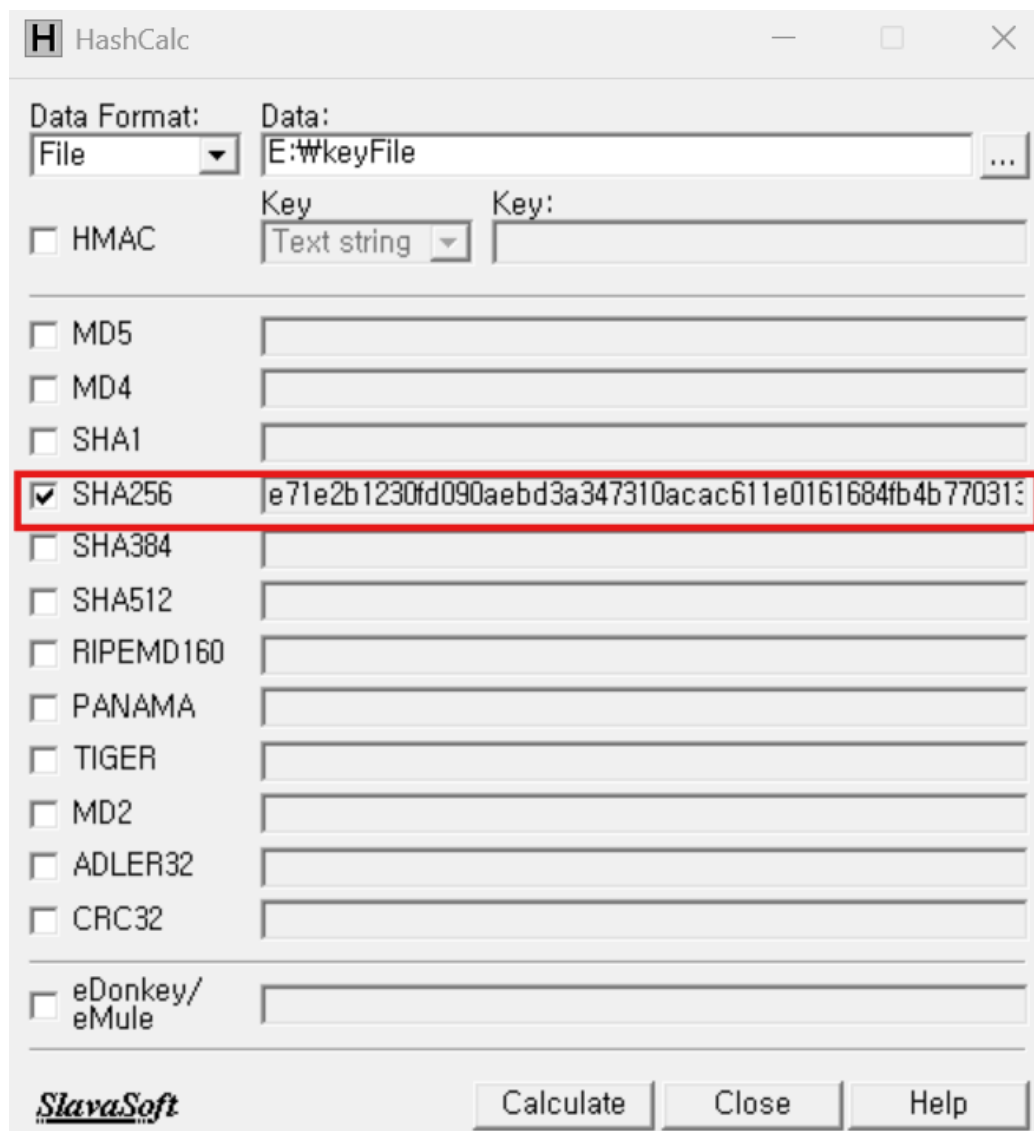
Flag is  
DH{ sha-256 (keyFile) }  
HA HA HA HA

수정한 뒤 재 오픈을 해보니 FTK에서 정상적으로 오픈되는 것을 확인할 수 있었다.

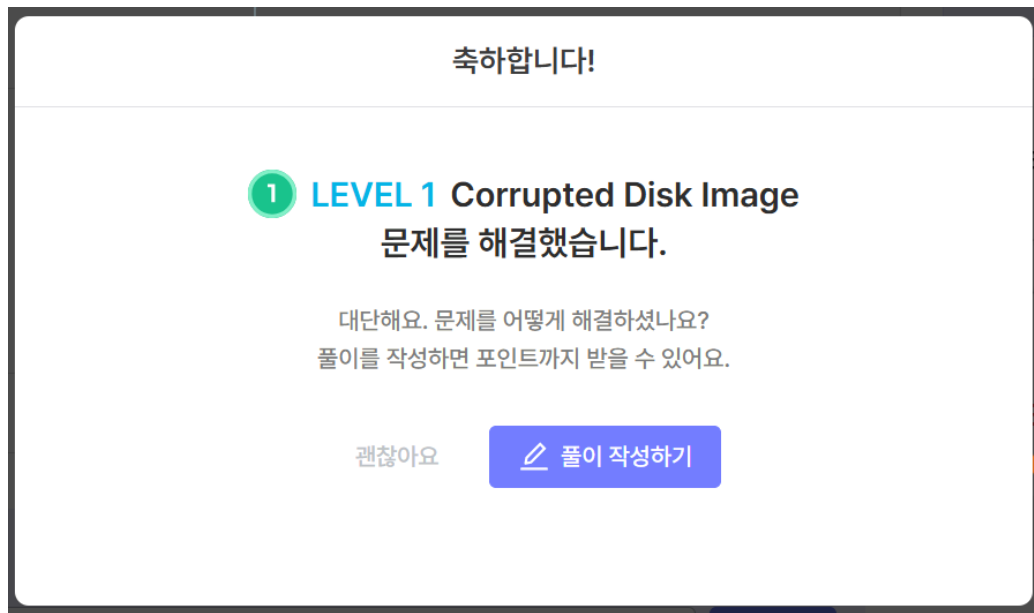
png파일에서 → 플래그 형식 = DH{sha-256(keyFile)} 발견



keyFile의 SHA-256값이 플래그인 것 같아 추출하여 HashCalc로 확인해준다.



DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}



참고 자료

<https://naro-security.tistory.com/18>