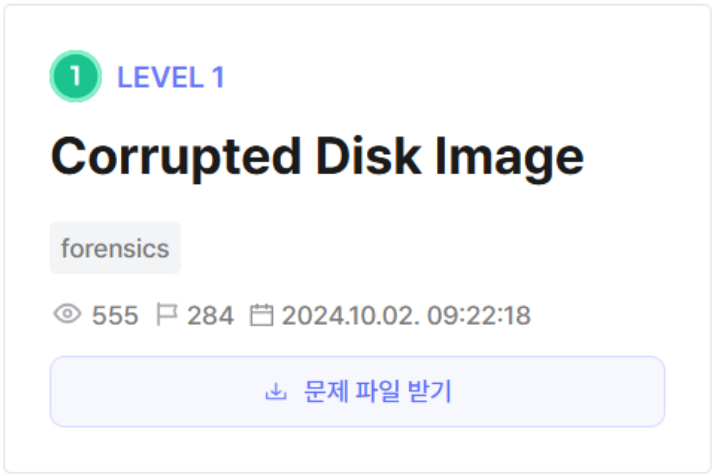
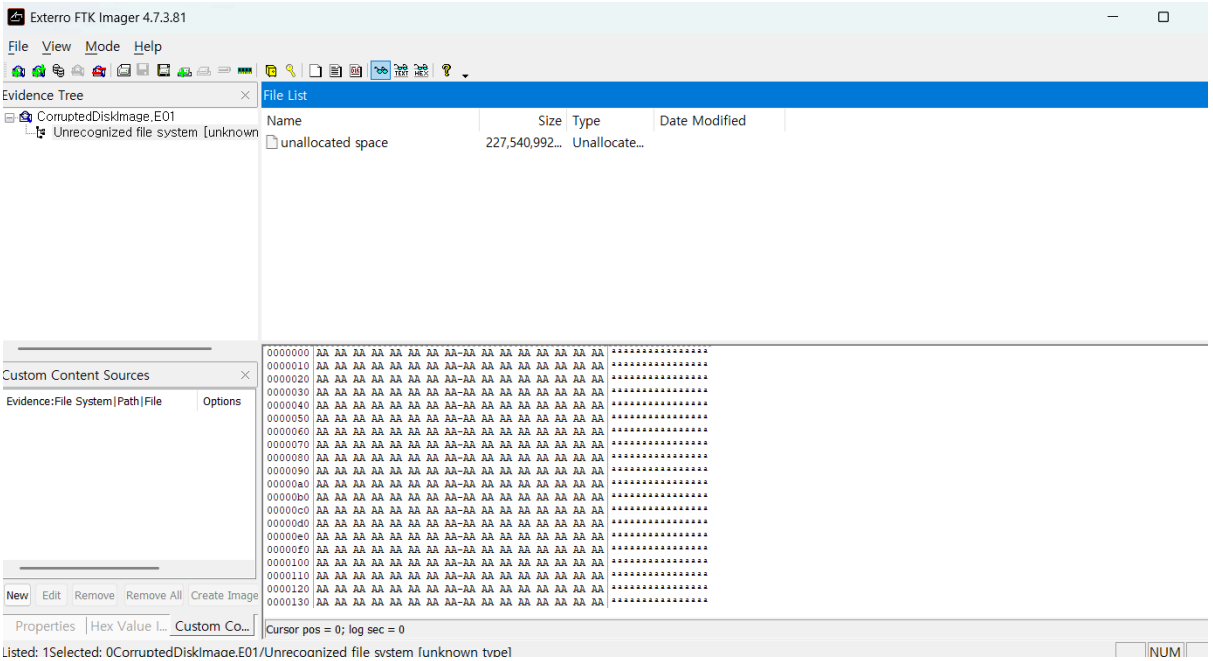
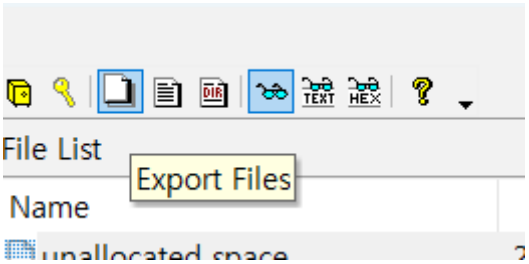
Dreamhack-Corrupted Disk Image





주어진 파일을 ftk imager로 열면 다음과 같이 파일이 손상되어 있다는 것을 확인할 수가 있다.

이 파일을



을 해서

unallocated.space.copy를 만들어주고, unallocated.space.copy를 HxD로 연다.

우리는 이 파일을 복구해야하기 때문에 파일의 복사본을 먼저 찾아야 한다.

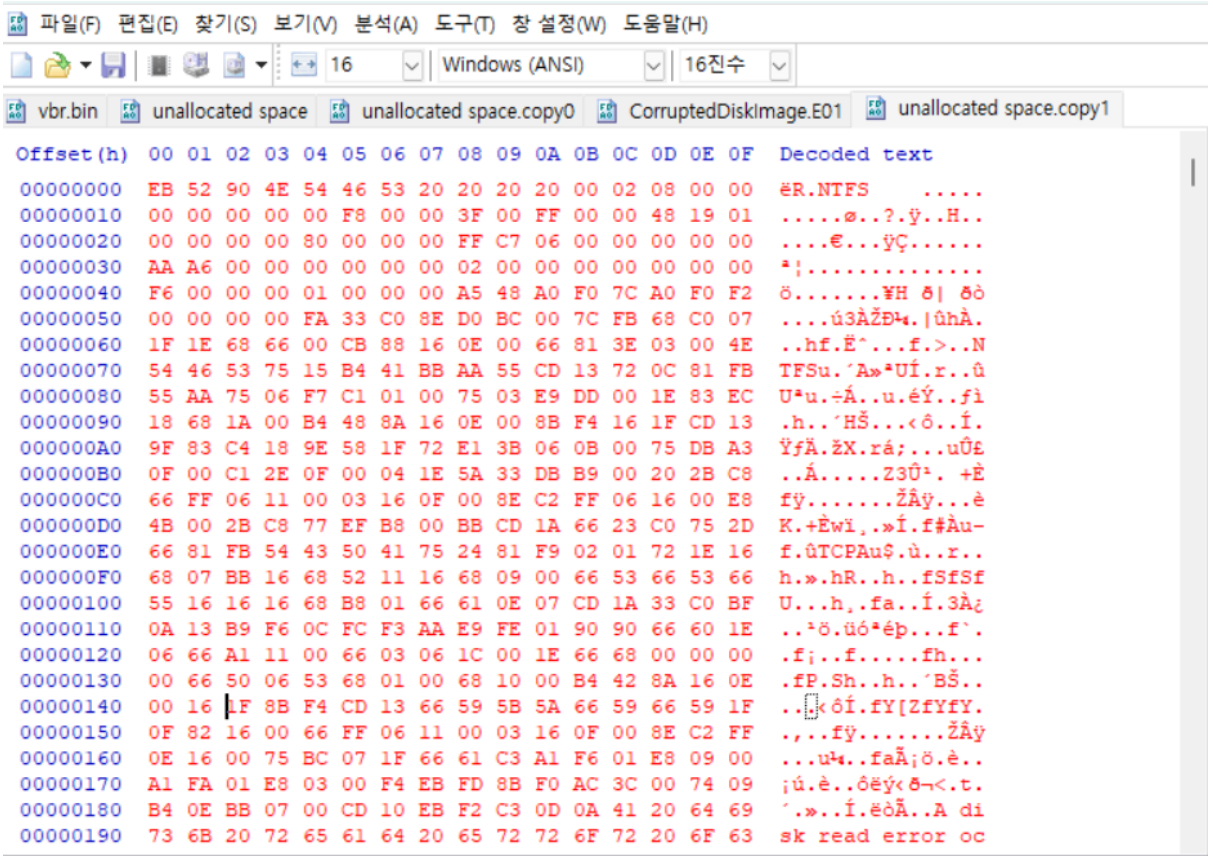
파일의 맨 마지막을 내려보면

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
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..
0D8FFEF0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.».hR..h..fSfSf
0D8FFF00	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h¸.fa..Í.3À¿
0D8FFF10	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..¹ö.üóªéþ...f`.
0D8FFF20	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f¡..f.....fh...
0D8FFF30	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..´BŠ..
0D8FFF40	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...‹ôÍ.fY[ZfYfY.
0D8FFF50	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	.‚..fÿ.......ŽÂÿ
0D8FFF60	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u¼..faÃ¡ö.è..
0D8FFF70	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ú.è..ôëý‹ð¬<.t.
0D8FFF80	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	´.»..Í.ëòÃ..A di
0D8FFF90	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
0D8FFFA0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR

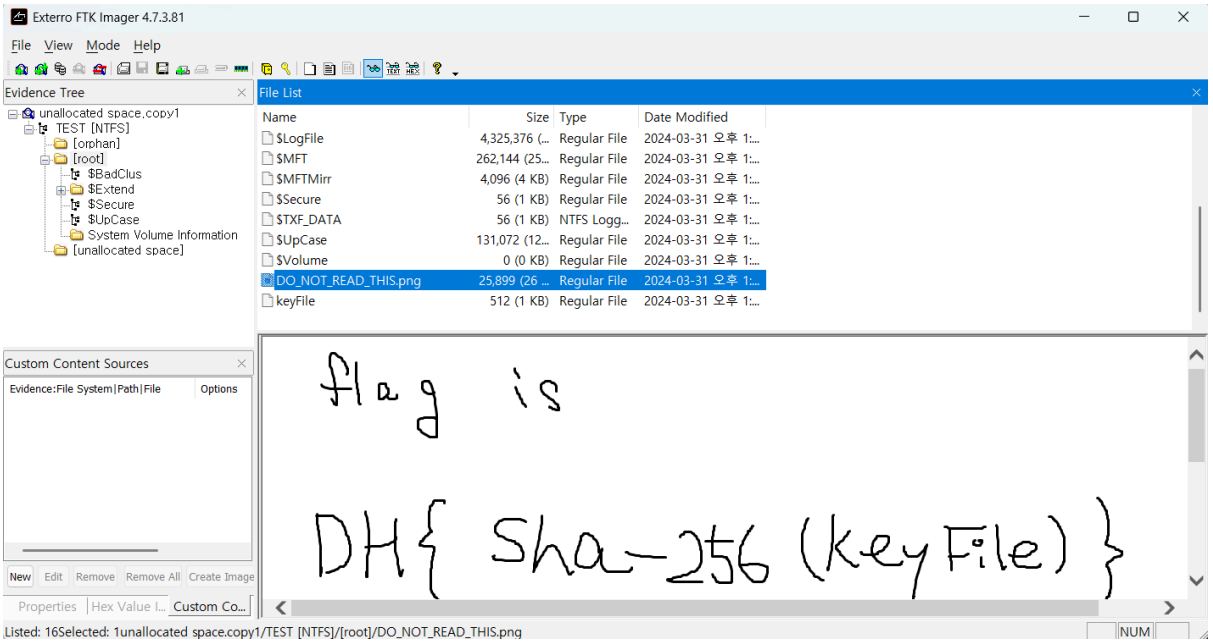
맨 마지막 부분을 보면 NTFS라고 적혀있는 것을 볼 수 있고, 파일의 파일의 0xD8FFe00 위치를 보면 EB 52 90 4E 54 46 53을 확인할 수 있는데, 이는 NTFS 파일 시스템의 VBR 시그니처임을 확인할 수 있다.

=> NTFS 파일은 VBR의 복사본을 볼륨 끝에 저장하므로 이것은 복구용 VBR 이라는 것을 알수가 있다!!

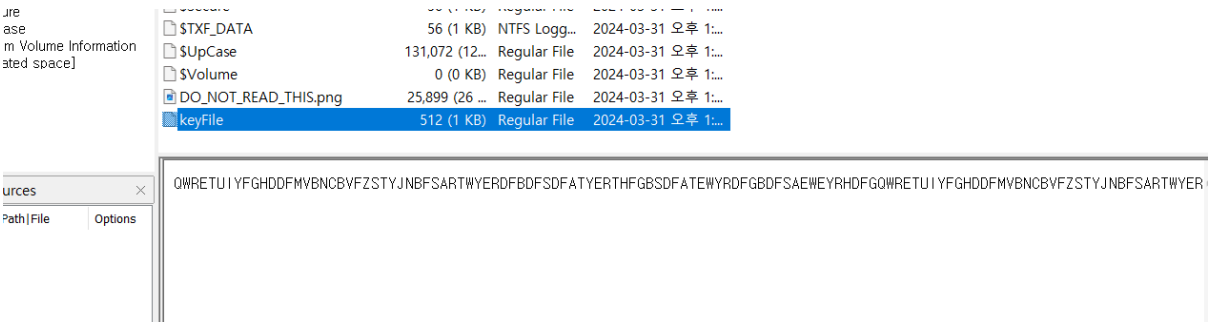
파일을 복구하기 위해서 이 복사본을 컨트롤 씨+ 컨트롤 비 를 이용해서 맨 앞에 데이터에 덮어준다.



이걸 저장하고 ftk imager로 열어준 다음 파일을 열어보면



이렇게 파일이 복구된 것을 볼수가 있다.



플래그는 키 파일에 있는 내용을 sha-256 으로 암호화 하라는 것 같다.

이걸 암호화 시켜주면

이렇게 플래그 값이 나온다.

FLAG:
DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}