

# Corrupted Disk Image

## Description

[함께실습] Corrupted Disk Image에서 실습하는 문제입니다.

디스크 이미지가 열리지 않습니다...!

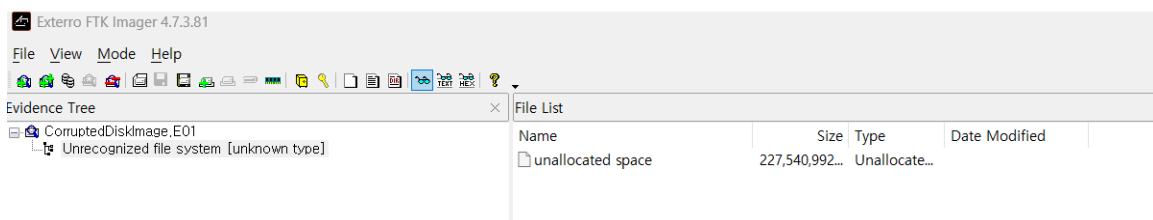
주어진 디스크 이미지를 복원하여 플래그를 구해주세요.

## Info

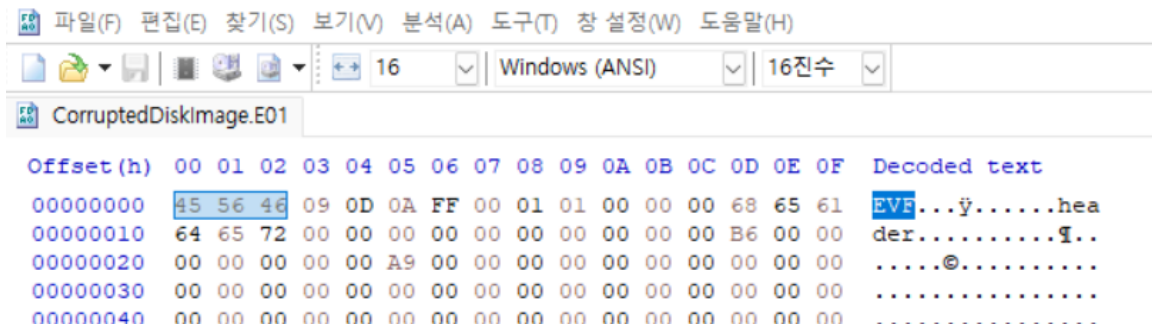
FLAG: `DH{something}something` 의 길이는 32자입니다.

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

1. FTK Imager로 열었을때 디스크 내용을 볼수 없었다.



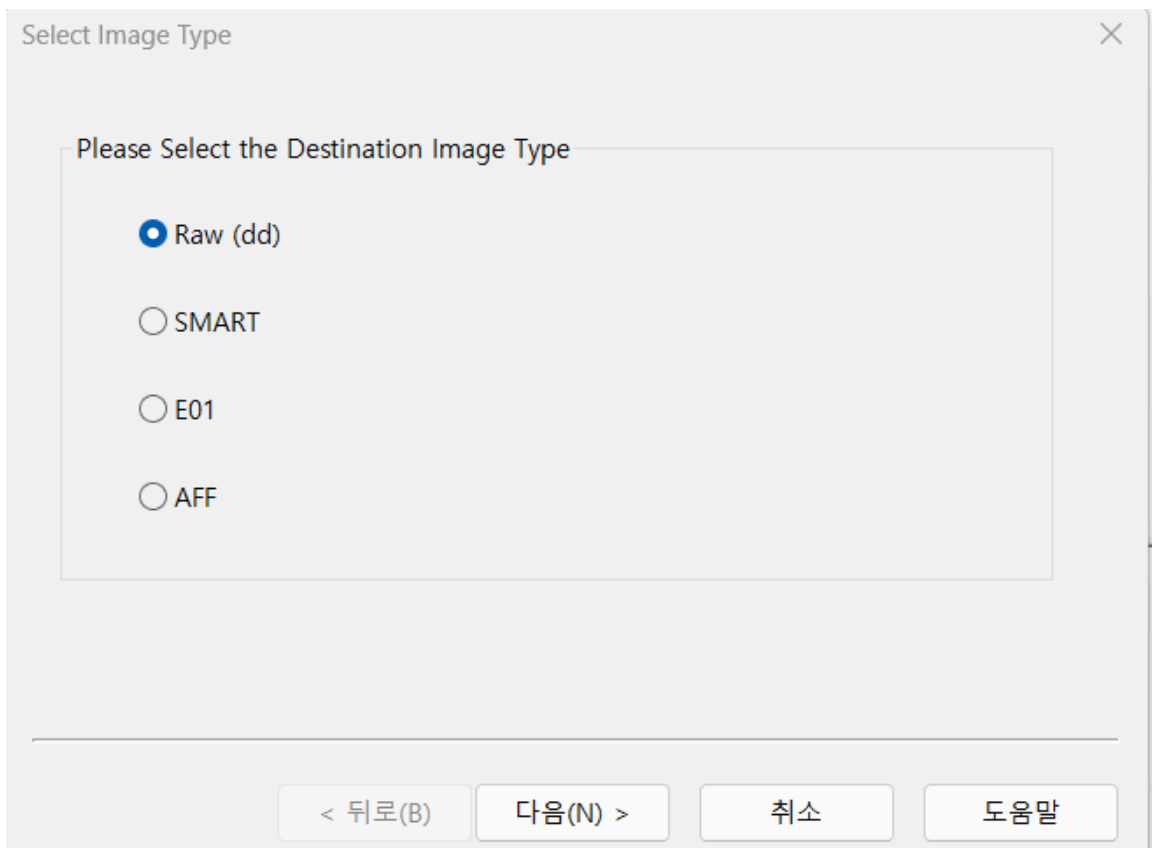
2. HxD 열기



EVF 파일은 Encase에서 사용하는 파일 포맷이다.

하지만 EVF를 사용한다는 것 말고 알 수 있는 것이 없음

### 3. FTK Imager로 E01 파일을 raw로 변환



E01 이미지를 Raw 포맷으로 변경하는 이유는 손상된 파티션의 복구 가능성을 높이기 위함

E01 포맷은 압축된 이미지 방식이지만, 간혹 파티션 손상 시 분석 및 복구에 어려움이 있을 수 있다.

따라서 손상된 파티션의 복구 가능성을 높이기 위해 RAW 포맷으로 재이미징하여 분석을 진행

#### 4. HxD로 복구용 VBR 찾기

```

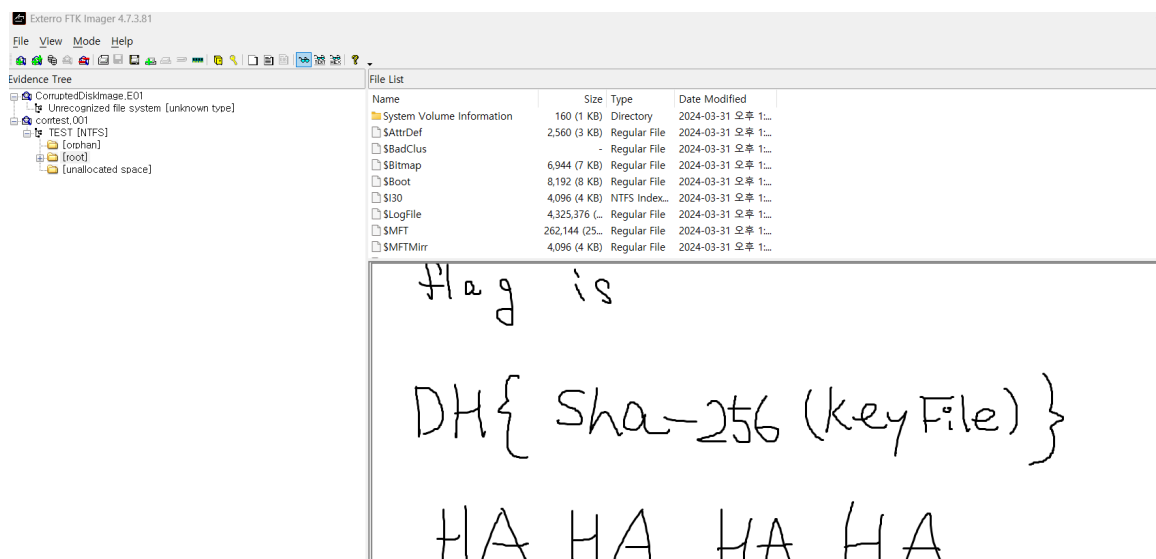
0D8FFE00 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 @R.NTFS .....
0D8FFE10 00 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 48 19 01 .....ø...?.ÿ..H..
0D8FFE20 00 00 00 00 80 00 00 00 FF C7 06 00 00 00 00 00 00 .....€...ÿÇ.....
0D8FFE30 AA A6 00 00 00 00 00 00 02 00 00 00 00 00 00 00 *!|.....
0D8FFE40 F6 00 00 00 01 00 00 00 A5 48 A0 F0 7C A0 F0 F2 ö.....¥H 8| 8ò
0D8FFE50 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 ....ú3ÀŽÐ¼. |ùhÀ.
0D8FFE60 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.Ě^...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.÷Ă..u.éÝ..fì
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 ŸfĂ.žX.rá;...uÔž
0D8FFEB0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 ..Ă.....Z3Ů¹. +È
0D8FFEC0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 fÿ.....ŽĂÿ...è
0D8FFED0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D K.+Èwī,.»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.3Ăž
0D8FFF10 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E ...³ò.üó*ép...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.....ŽĂÿ
0D8FFF60 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 ...u¼...faĂ;ö.è..

```

해당 마지막 섹터 복사해서 섹터0에 붙여넣기

| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text      |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 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 ö  öö    |
| 00000050  | 00 | 00 | 00 | 00 | FA | 33 | C0 | 8E | D0 | BC | 00 | 7C | FB | 68 | C0 | 07 | ....ú3ÄŽĐ+. ûhÄ.  |
| 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 | U²u.÷Á..u.éÝ..fi  |
| 00000090  | 18 | 68 | 1A | 00 | B4 | 48 | 8A | 16 | 0E | 00 | 8B | F4 | 16 | 1F | CD | 13 | .h..'HŠ...<ö..í.  |
| 000000A0  | 9F | 83 | C4 | 18 | 9E | 58 | 1F | 72 | E1 | 3B | 06 | 0B | 00 | 75 | DB | A3 | ŸfÄ.žX.rá;...uŮž  |
| 000000B0  | 0F | 00 | C1 | 2E | 0F | 00 | 04 | 1E | 5A | 33 | DB | B9 | 00 | 20 | 2B | C8 | ..Ä.....Z3Ů². +È  |
| 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.+Èwì,..»í.f#Au- |
| 000000E0  | 66 | 81 | FB | 54 | 43 | 50 | 41 | 75 | 24 | 81 | F9 | 02 | 01 | 72 | 1E | 16 | f.ŮTCPAu\$.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 | ..²ö.üó²ép...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[Zfÿfÿ.  |
| 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 | ...u²..faÄ;ö.è..  |
| 00000170  | A1 | FA | 01 | E8 | 03 | 00 | F4 | EB | FD | 8B | F0 | AC | 3C | 00 | 74 | 09 | ¡ú.è..öëÿ<ö-<.t.  |
| 00000180  | B4 | 0E | BB | 07 | 00 | CD | 10 | EB | F2 | C3 | 0D | 0A | 41 | 20 | 64 | 69 | '.»...í.èöÄ..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 | curréd...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.\$.\$...U² |
| 00000200  | 07 | 00 | 42 | 00 | 4F | 00 | 4F | 00 | 54 | 00 | 4D | 00 | 47 | 00 | 52 | 00 | ..B.O.O.T.M.G.R.  |

## 5. FTK Imager로 확인하기



DH{sha-256 (ket File)

→ 키 파일 확인

## 6. 키 파일

Codeeeeeee   홈페이지   JSON 분석 및 형식 지정 검사   해시▼   인코딩 및 디코딩▼   암호화 및

홈페이지 / 해시 / SHA2 암호화

SHA256 / SHA512 / SHA224 / SHA384 온라인 암호화 도구

암호화할 내용을 입력하세요

QWRETUIYFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFSDFATYERTHFGBSDFATEWYRD  
FGBDFSAEWEYRHDFGQWRETUIYFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFSDFATY  
ERTHFGBSDFATEWYRDFGBDFSAEWEYRHDFGQWRETUIYFGHDDFMVBNCBVFZSTYJNBFS  
ARTWYERDFBDFSDFATYERTHFGBSDFATEWYRDFGBDFSAEWEYRHDFGQWRETUIYFGHDDFM  
VBNCBVFZSTYJNBFSARTWYERDFBDFSDFATYERTHFGBSDFATEWYRDFGBDFSAEWEYRHDF  
GQWRETUIYFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFSDFATYERTHFGBSDFATEWYR  
DFGBDFSAEWEYRHDFGQWRETUIYFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFSDFAT  
YERTHFGBSDFATEWYRDFGBDFSAEWEYRHDFGQWRETUIYFGHDDFMVBNCB

해시 함수

☒ SHA256   ☐ SHA512   ☐ SHA384   ☐ SHA224

암호화

e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac

**1 LEVEL 1 Corrupted Disk Image**  
문제를 해결했습니다.