Dreamhack- Corrupted Disk Image(level1)

문제

Description

[함께실습] Corrupted Disk Image에서 실습하는 문제입니다.

디스크 이미지가 열리지 않습니다...!

주어진 디스크 이미지를 복원하여 플래그를 구해주세요.

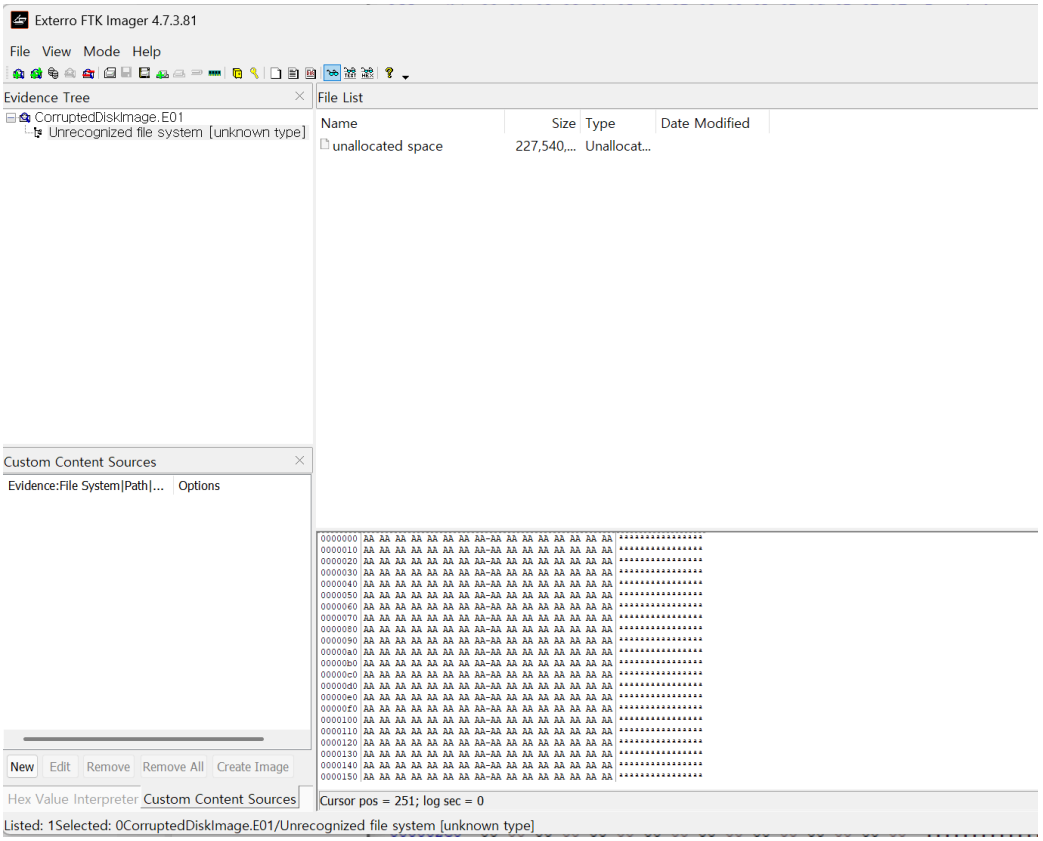
Info

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

풀이

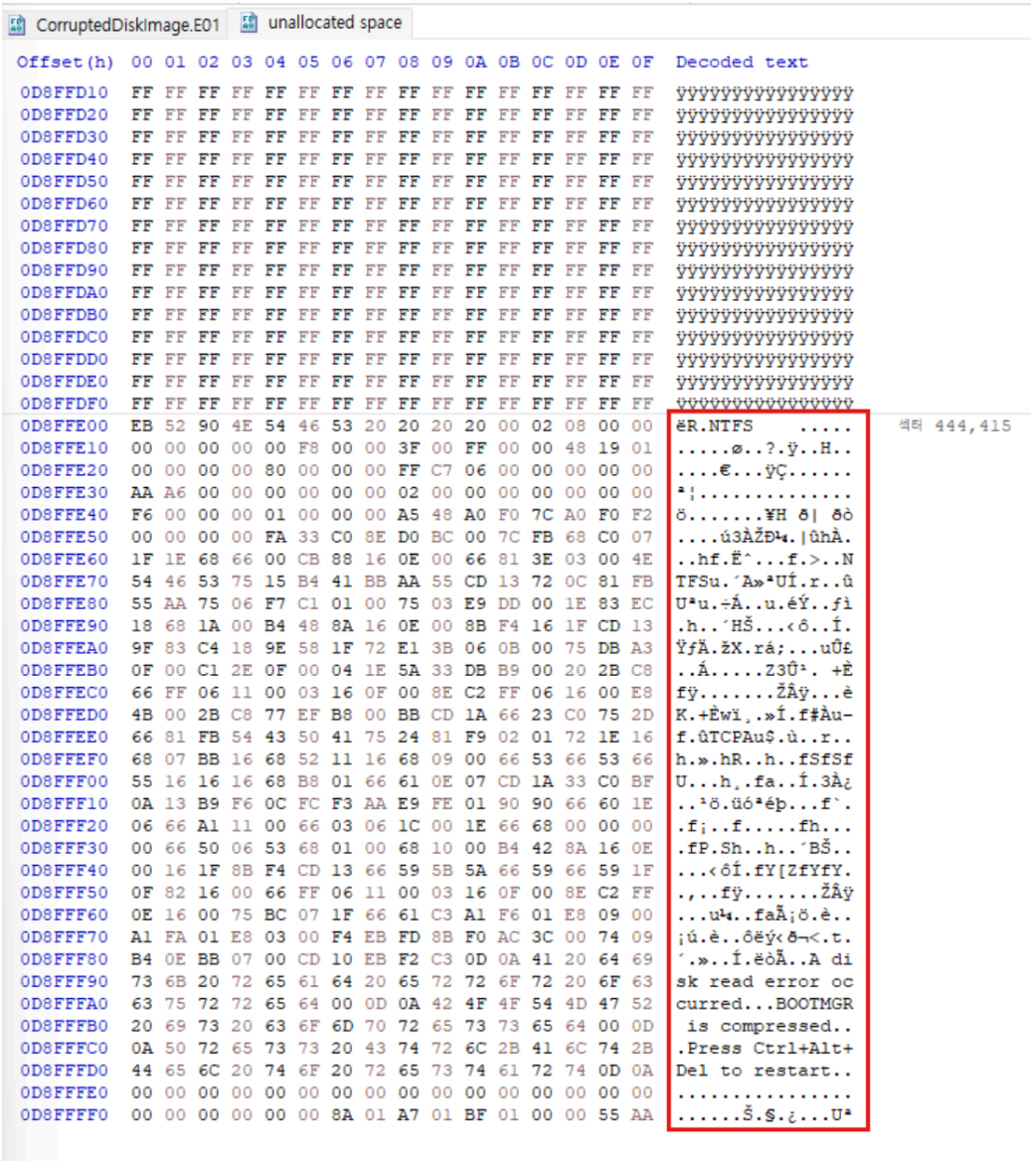
1. 문제 파악
   제공된
   디스크 이미지 파일이 손상되어 열리지 않음 → 파일 시스템 구조나 일부 데이터를 복원하기 → 파티션 복구 필요

2. 문제 풀이

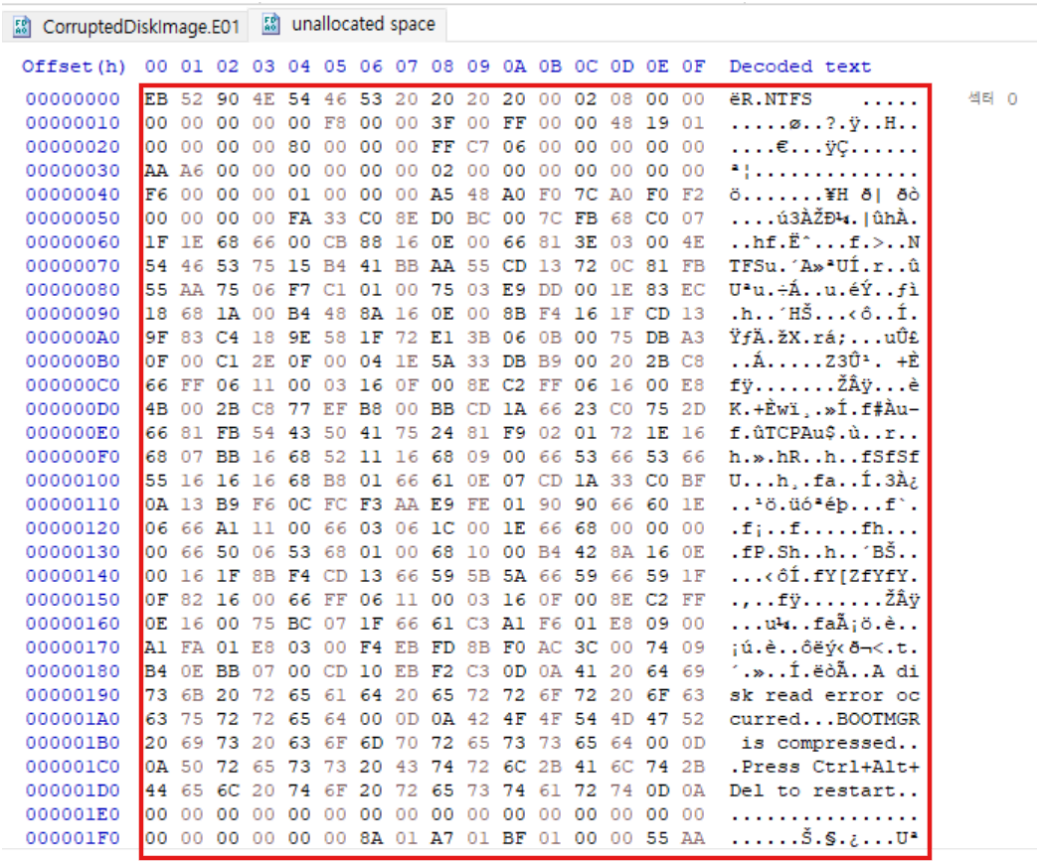


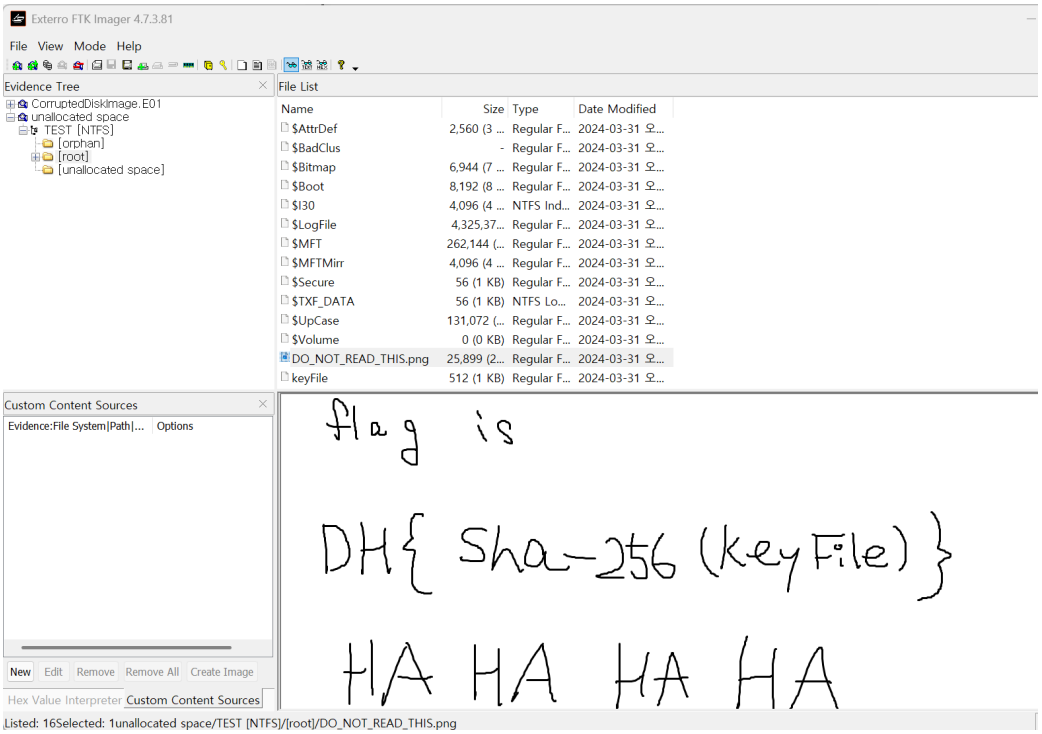
E01파일을 FTK를 통해 확인해보니 깨진 파일을 발견.

비워져 있는 섹터 부분에 원래의 데이터 정보를 삽입해줘야한다.



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

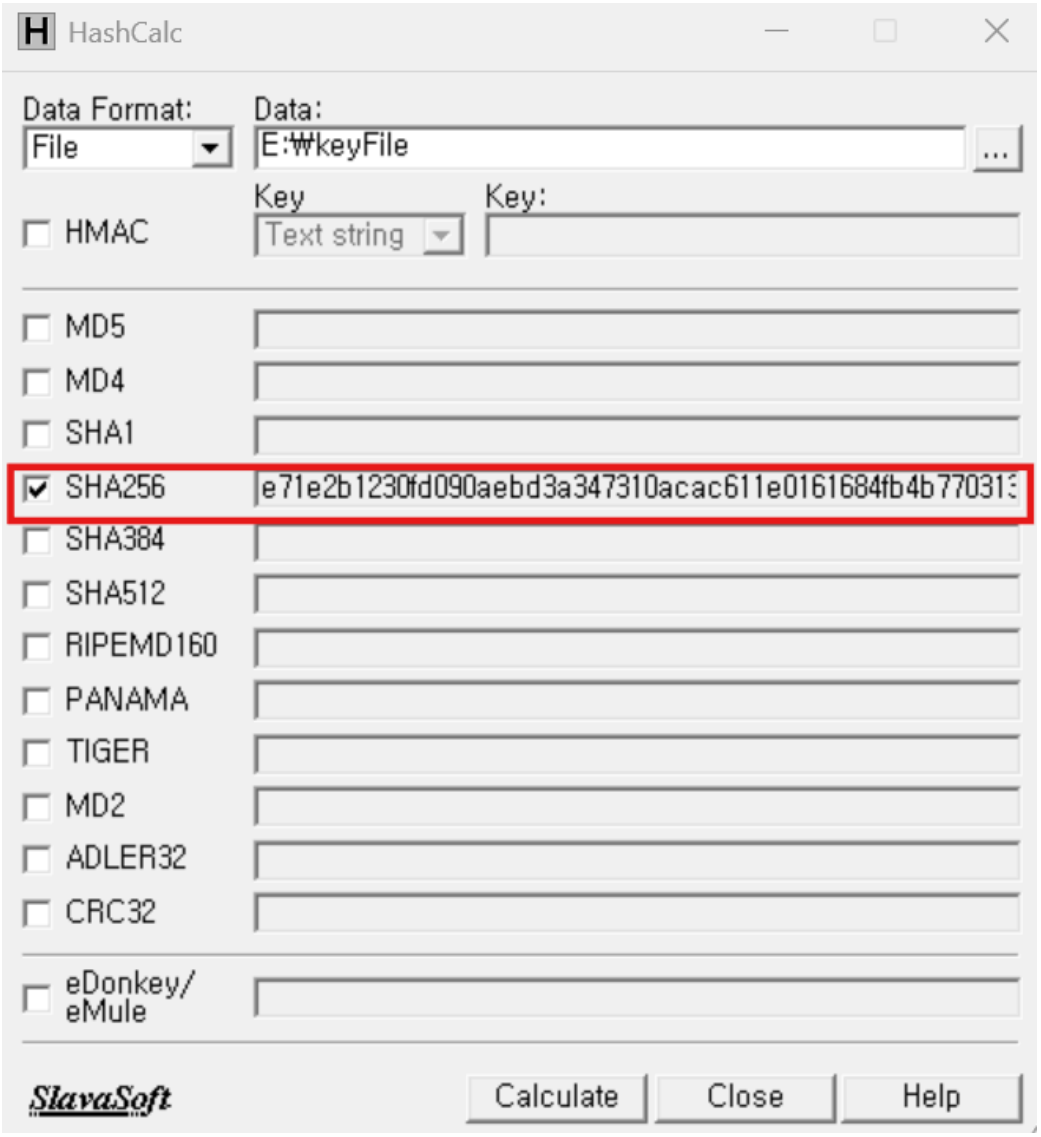




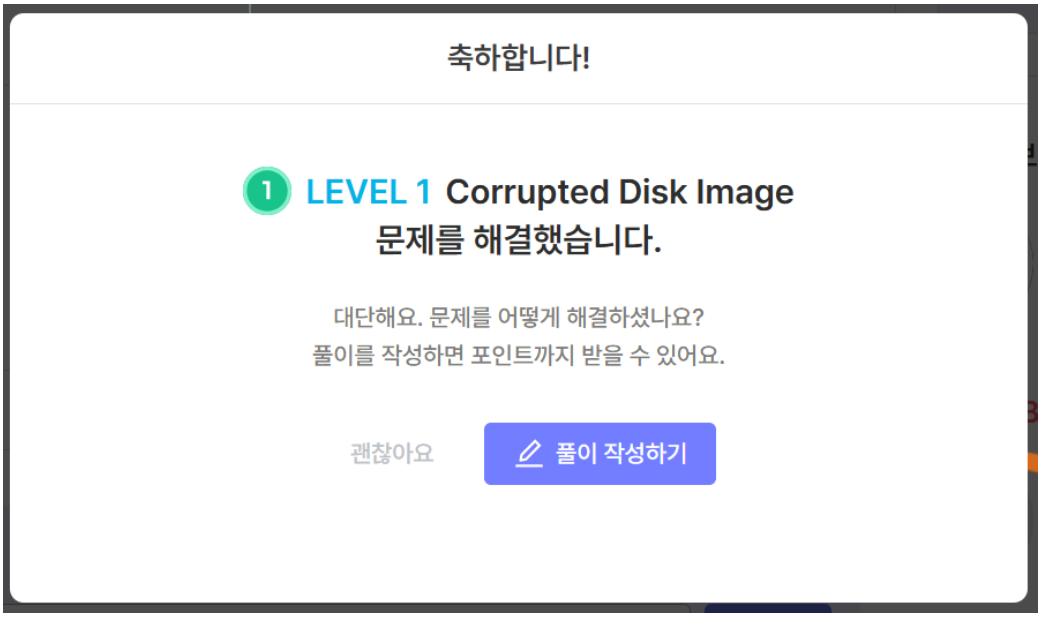
수정한 뒤 재 오픈을 해보니 FTK에서 정상적으로 오픈되는 것을 확인할 수 있었다.

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