# **Dreamhack-Corrupted Disk Image** (level1)



🥟 [함께실습] Corrupted Disk Image에서 실습하는 문제입니다.

디스크 이미지가 열리지 않습니다...!

주어진 디스크 이미지를 복원하여 플래그를 구해주세요.

## 사용 툴 - FTK Imager, HxD

#### 1. 파일 시스템 복구

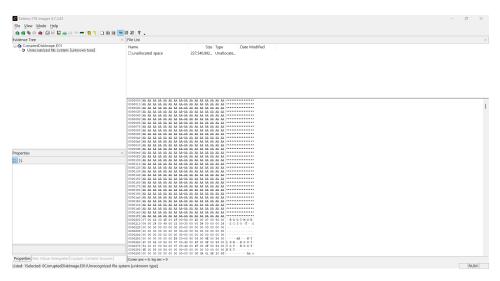
#### 1) Unrecognized file system

- 파일 시스템 손상 또는 구조적 문제가 있어 FTK Imager에서 정상적으로 인식하지 못하는 경 우 발생
- 해당 손상 유형은 Raw(dd) 이미지로 복구를 진행하여야 한다.
- 만약 최초 확인된 이미지가 E01이라면, Raw(dd)로 이미지를 새롭게 생성 후, 복구 진행이 필 요하다.

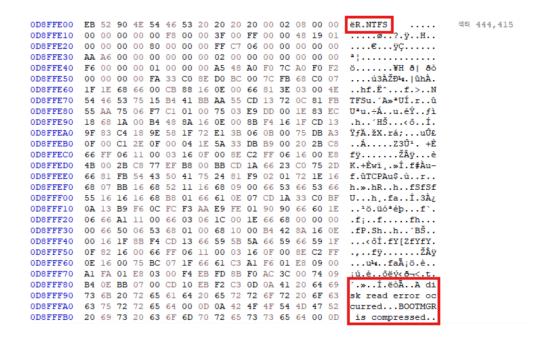
#### 2) Recovered

- 손상 또는 삭제된 파티션을 FTK Imager가 복구했음을 의미함
- 완전한 복구는 아니나, 파티션 자체에 접근은 가능한 상태로, 해당 케이스는 완전 복구 없이, Encase, Autopsy 등에 이미지 로드 시, 직접적으로 내부 파일까지 확인이 가능하여 분석 자 체에는 문제가 없는 상태 (즉 E01 등 확장자 그대로 로드해서 분석이 가능)
- 섹터 (512byte)
  - 。 데이터는 물리적으로 섹터라는 공간에 저장
  - 。 하드디스크의 물리적인 최소 단위
  - 응용 프로그램이 생산한 데이터 집합인 파일은 모두 이 섹터 공간에서 읽기 쓰기 삭제 등의 작업이 이루어짐

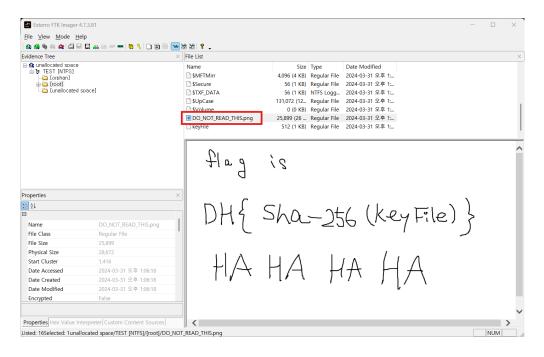
#### 2. FTK Imager 를 통해 unallocated space 파일 추출

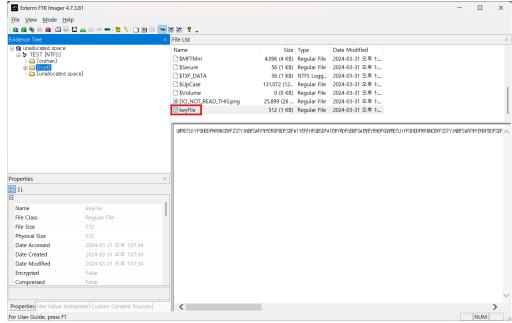


- 3. HxD 디스크 이미지 열기를 통해 파일 구조 파악
  - 분석 내용
    - 헤더 부분이 손상되어 있는 것을 확인할 수 있었음
    - NTFS 의 경우 헤더 복사본이 파티션 섹터 마지막에 존재 → NTFS 파일 시스템인 것을 확인할 수 있었음
    - 。 해당 부분을 헤더 부분에 덮어쓰기



4. 복구한 파일을 FTK Imager 를 통해 분석한 결과 다음과 같은 플래그를 확인할 수 있었음





# [SHA256] 테스트 페이지

### <암호화 예제>

암호문:

QWRETUIYFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFSDFATYERT 🔺 HFGBSDFATEWYRDFGBDFSAEWEYRHDFGQWRETUIYFGHDDFMVBNCBVF ZSTYJNBFSARTWYERDFBDFSDFATYERTHFGBSDFATEWYRDFGBDFSAE 평문: WEYRHDFGQWRETU!YFGHDDFMVBNCBVFZSTYJNBFSARTWYERDFBDFS DFATYERTHFGBSDFATEWYRDFGBDFSAEWEYRHDFGQWRETU I YFGHDDF MVBNCBVFZSTYJNBFSARTWYERDFBDFSDFATYERTHFGBSDFATEWYRD <u>FGRDESAEWEYRHDEGOWRETHLYEGHDDEMVRNCRVEZSTY.INRESARTWY</u> ▼ 암호화 e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b 6cc91bb7ac



DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}