Write-up: Corrupted Disk Image (level1)

https://dreamhack.io/wargame/challenges/1189

1. Challenge Info

- **Challenge Name:** Corrupted Disk Image
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

  주어진 디스크의 이미지를 복원하여 플래그를 완성하라.

> 플래그 형식: **DH{something}**
>
> - something의 길이: 32자

2. Problem Description

> “디스크 이미지가 열리지 않습니다...!
> 주어진 디스크 이미지를 복원하여 플래그를 구해주세요.”

- 제공된 디스크 이미지: `CorruptedDiskImage.E01`

---

3. Provided Files

- `CorruptedDiskImage.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

---

4. Tools Used

Tool	Version
FTK Imager	v4.7.8.31
HxD	v2.5.0.0
Windows PowerShell	v5.1.26100.4202

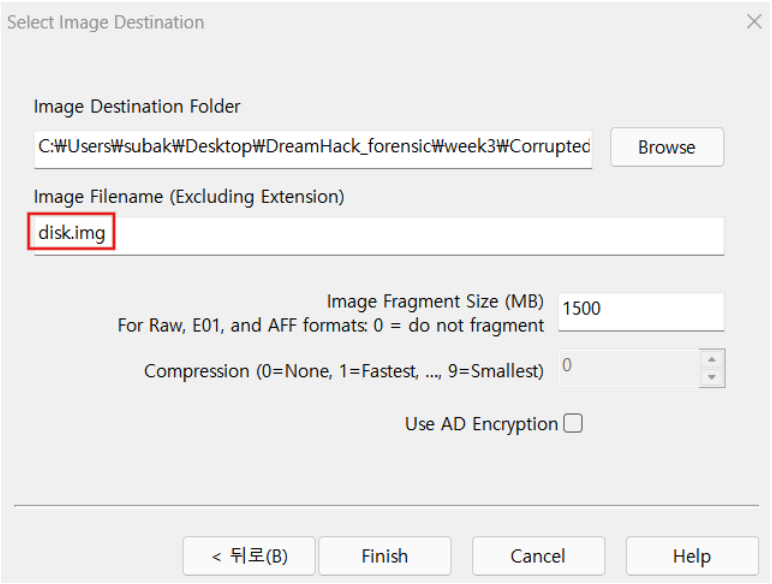
---

5. Analysis Steps

5.1 디스크 이미지 마운트

- **도구:** FTK Imager
- 제공된 `CorruptedDiskImage.E01` 파일을 FTK Imager로 열기
  - Unrecognized file system 표시

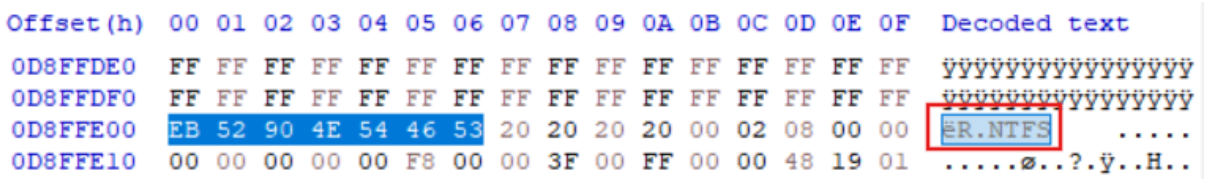
- Export Disk Image → Raw(dd) 선택 → `disk.img` 로 저장



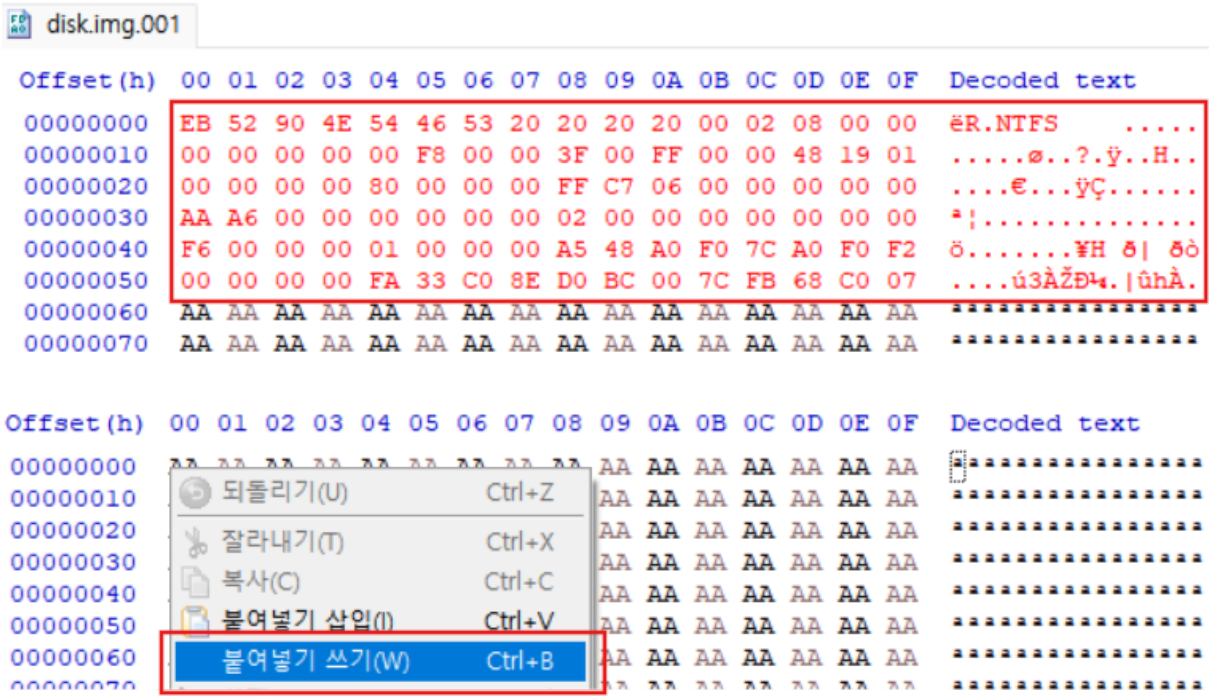
5.2 VBR 시그니처 확인 및 복사

- **도구:** HxD
- 저장한 `disk.img` 파일을 HxD로 열어 NTFS VBR 시그니처를 찾아 덮어써 손상된 VBR을 복구

- VBR 시그니처 확인
  - 문자열 검색에서 NTFS 입력하여 VBR 영역 찾기
  - `EB 52 90 4E 54 46 53` 값이 VBR 시그니처임을 확인



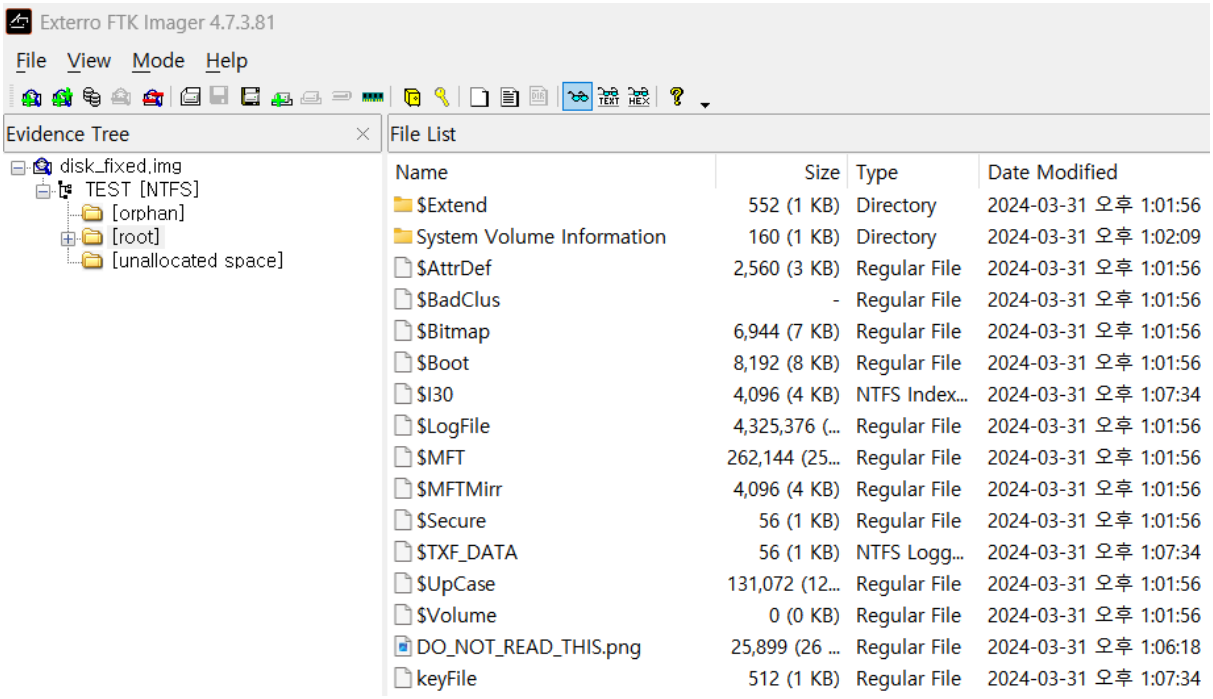
- VBR 시그니처 복사 및 덮어쓰기
  - 시그니처가 있는 영역(`EB 52 90 4E 54 46 53` 이후의 VBR 전체)을 복사하여 손상된 앞 부분에 덮어씀



- 덮어쓴 이미지 다른 이름으로 저장
  - VBR 덮어쓰기가 완료되면, 다른 이름으로 저장을 선택하여 `disk_fixed.img`로 저장

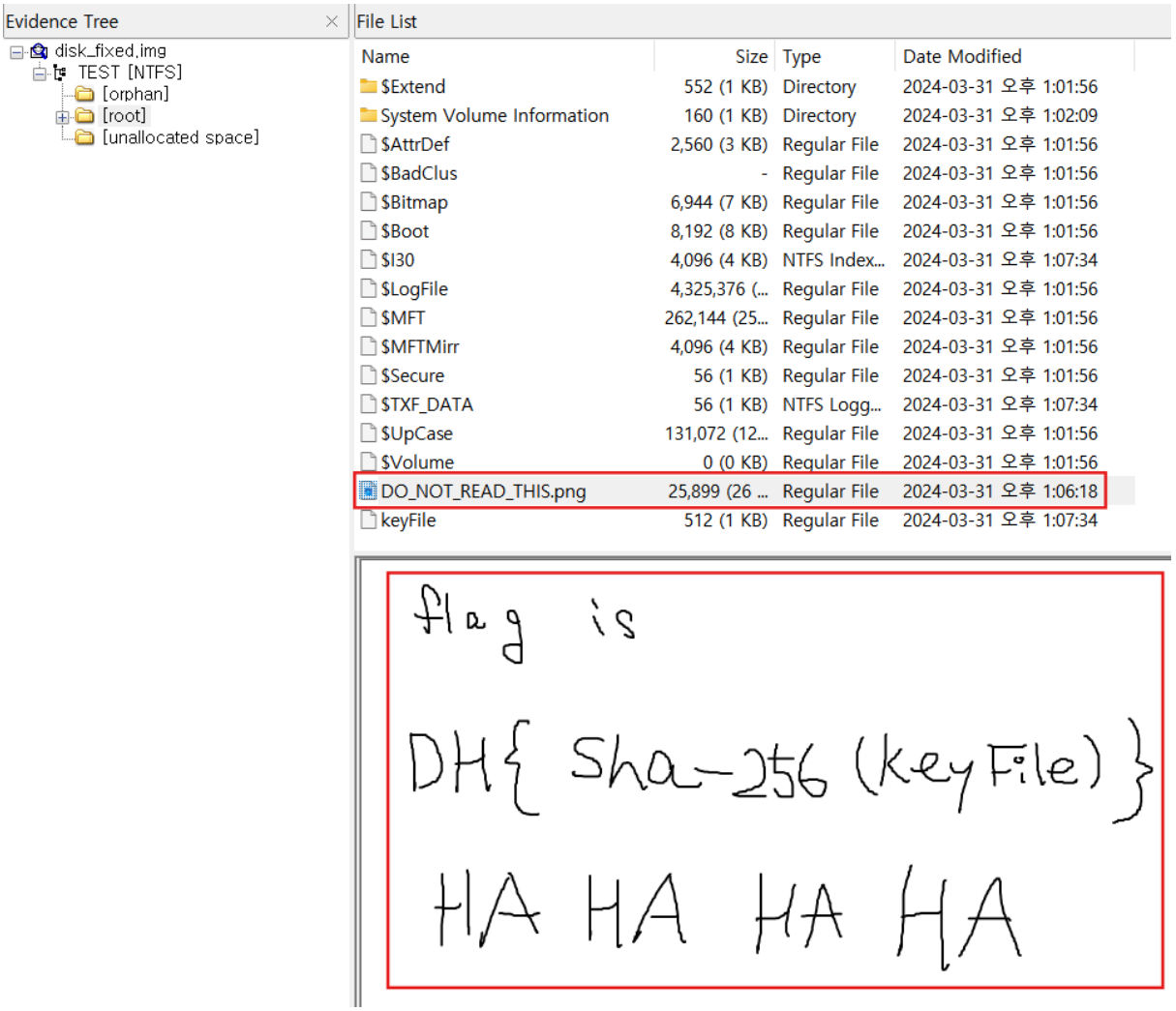
5.3 FTK Imager로 복구 확인

- **도구:** FTK Imager
- 저장한 `disk_fixed.img`를 FTK Imager로 열어 VBR 복구 결과 확인
    - 정상적으로 NTFS 파티션 및 파일 구조가 인식되는지 확인하여 복구 여부 검증

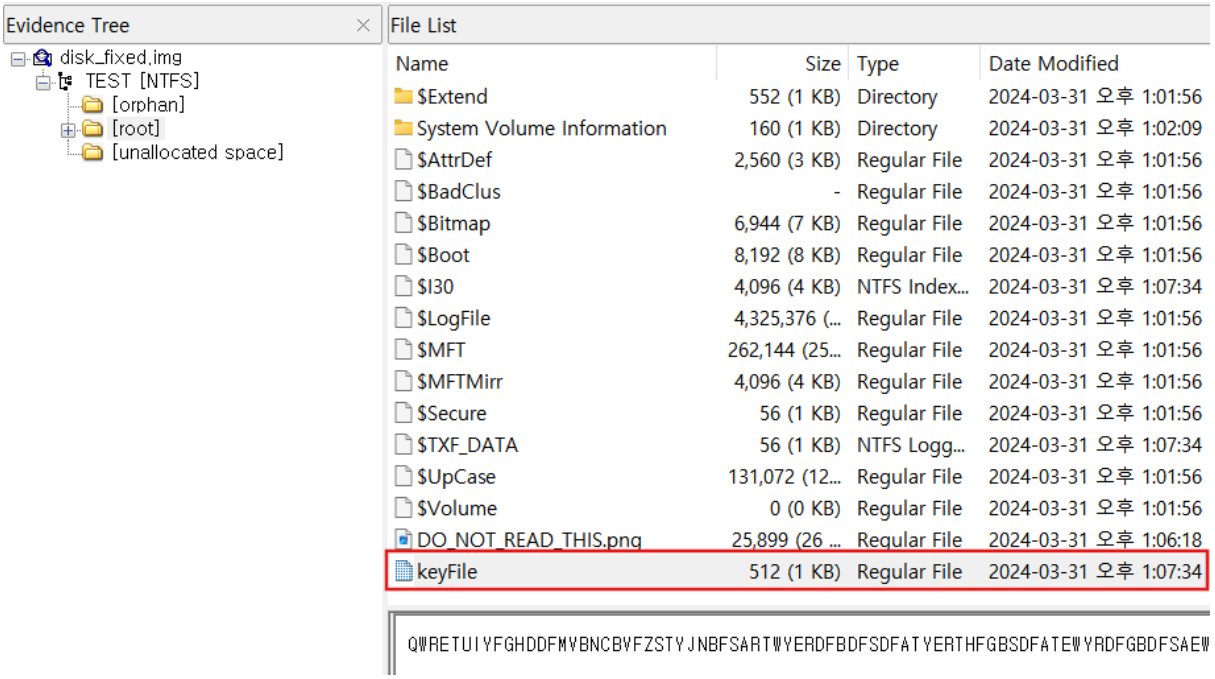


5.4 플래그 확인 및 해시 계산

- **도구:** FTK Imager
- **경로:** `C:\DO_NOT_READ_THIS.png`
  - `DO_NOT_READ_THIS.png` 파일 확인
  - 이미지를 열어보면 플래그가 다음과 같이 작성되어 있음



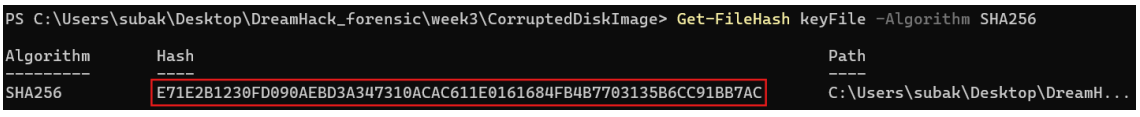
- **도구:** Windows PowerShell
- `C:\keyFile` 파일을 FTK Imager를 이용해 추출



- 추출한 `KeyFile`에 대해 PowerShell에서 SHA-256 해시 확인
- **명령어:**

```
Get-FileHash keyFile -Algorithm SHA256
```

- **KeyFile의 SHA256 해시:**
  `E71E2B1230FD090AEBD3A347310ACAC611E0161684FB4B7703135B6CC91BB7AC`



5.5 최종 정보 정리

something: `E71E2B1230FD090AEBD3A347310ACAC611E0161684FB4B7703135B6CC91BB7AC`

- 플래그 제출 시 대문자로 제출하면 실패
  - 소문자로 변경하여 제출

6. Flag

DH{e71e2b1230fd090aebd3a347310acac611e0161684fb4b7703135b6cc91bb7ac}