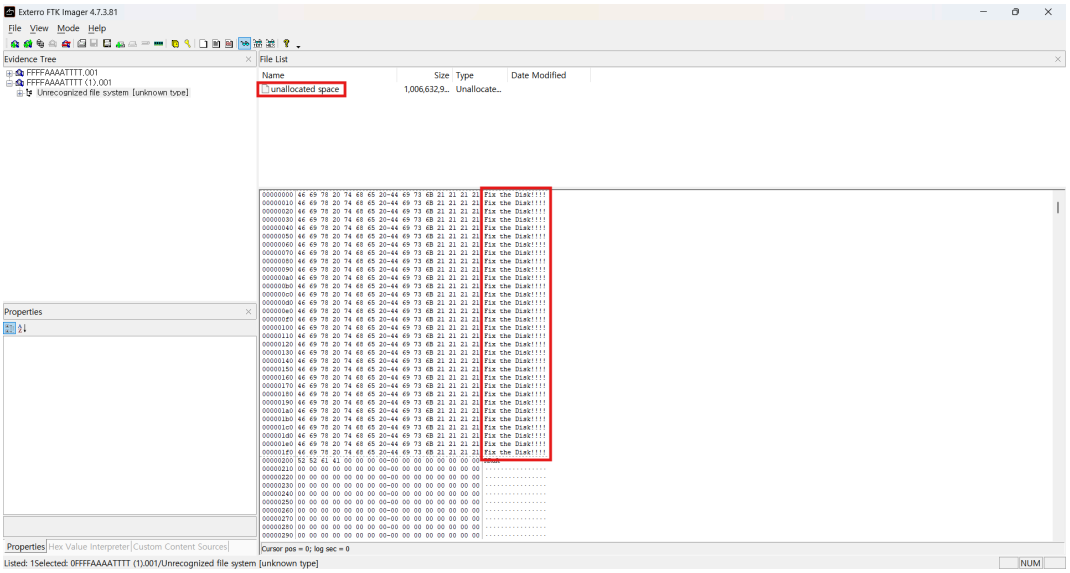
Dreamhack-FFFAAATTT(level1)

👉🏻 **FIXFIXFIX! FFFFAAAATTT!**

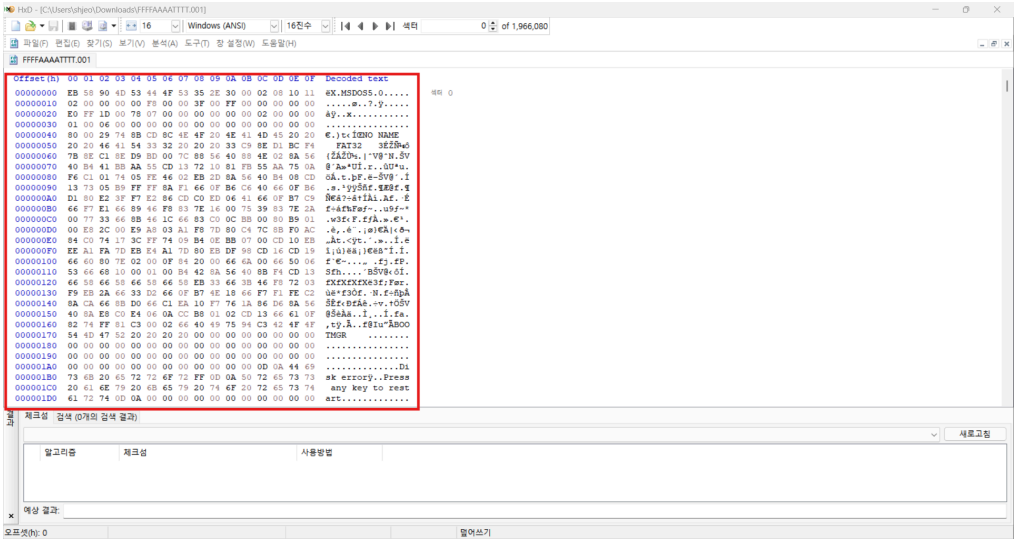
사용 툴 - FTK Imager, HxD

👉🏻 부트레코드란, 컴퓨터 부팅을 시작하는 데 필요한 데이터를 유지 관리하는 데 사용되는 하드 디스크의 저장소 공간 섹션이다. 일반적으로 부팅 레코드는 하드 드라이브의 첫 번째 섹터에 보관되므로 시스템이 응용 프로그램을 시작하는 데 필요한 파일을 쉽게 찾고 읽고 실행할 수 있다. 파일에 액세스하고 부팅을 시작하는 데 필요한 모든 코드는 마스터 부팅 레코드에 포함된다.

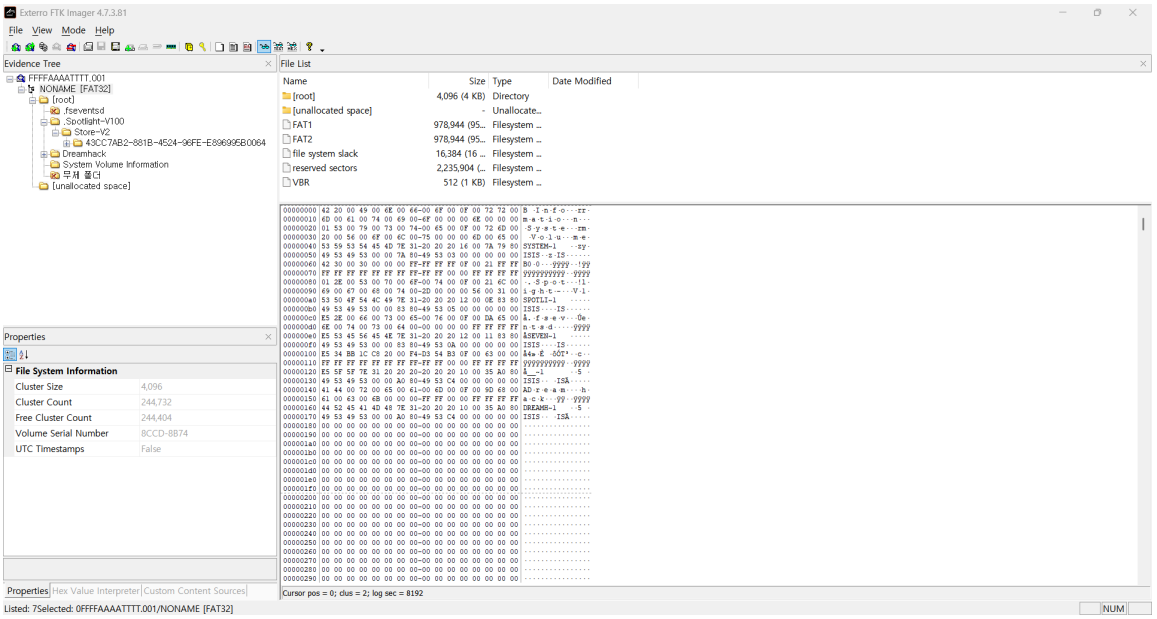
1. 다운로드 받은 파일을 FTK Imager 를 통해 확인한 결과, 다음과 같이 손상되어 있는 것을 확인



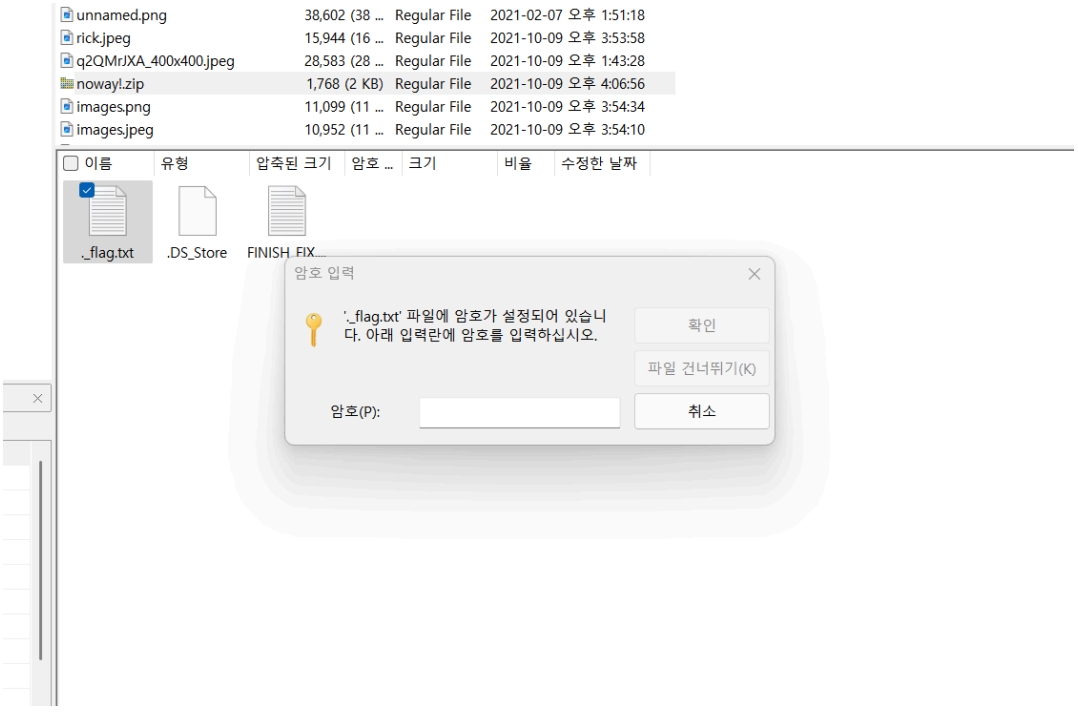
2. HxD 를 통해 디스크 이미지 파일을 열어 복구 진행
    - 분석 내용 : "MSDOS5.0" 아스키 값을 통해 FAT32 이미지의 Boot Record 백업 데이터가 저장되어 있는 것을 확인하여 해당 섹터의 헥스 값을 가장 처음 섹터로 전체 복사



3. 복구한 파일을 FTK Imager 를 통해 확인한 결과, 복구되어 있는 것을 확인



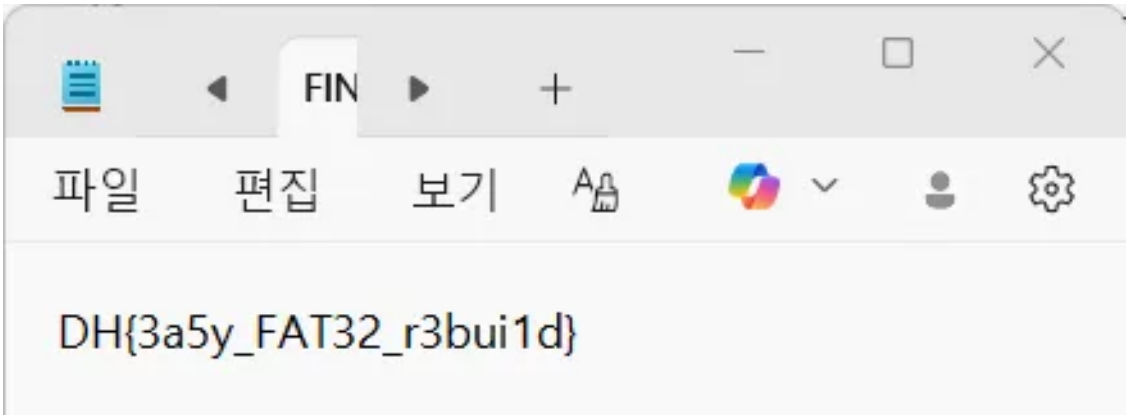
4. flag 와 관련된 파일을 발견했으나, 암호화되어 있음



5. dreamhack 전체 폴더 추출 후 해당 경로 내에 함께 존재되어 있는 이미지들의 헥스 값을 확인함 → 암호 발견 (DHDHFIX)

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   47 47 3F 20 74 68 65 20 7A 69 70 20 6B 65 79 20  GG? the zip key
00000010   3A 20 44 48 44 48 46 49 58 0A                    : DHDHFIX.
```

6. 암호화되어 있는 플래그 파일 (FINISH_FIX.txt) 확인 가능



👉 DH{3a5y_FAT32_r3bui1d}