[FFFFAAAATTT] Write-Up

작성자	박혜미
분석 일자	2024.05.10
작성 일자	2024.05.10
분석 대상	FFFFAAAATTTT.001
문서 버전	2.0
작성자 E-mail	parkm0708@naver.com

0. 목차

1. 문제

URL	https://dreamhack.io/wargame/challenges/303
문제 내용	FIXFIXFIX! FFFAAATTT! (문제파일 다운로드에서 받지 마시고, 아래의 링크를 통해서 문제파일을 다운받으시기 바랍니다.)
문제 파일	https://drive.google.com/file/d/17ESNJryAYuHa3M5GiBIb9r2JNhXLqKBa/view?usp=sharing
문제 유형	디스크 포렌식
난이도	1 / 5

2. 분석 도구

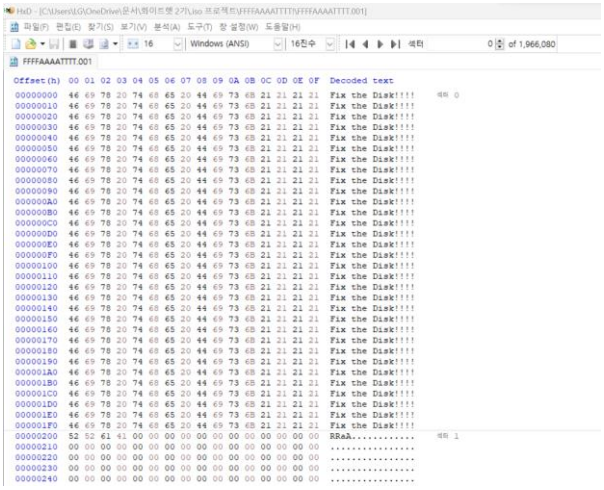
도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/hxd/	2.5
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7.1.2

3. 환경

OS
Windows 11 Home

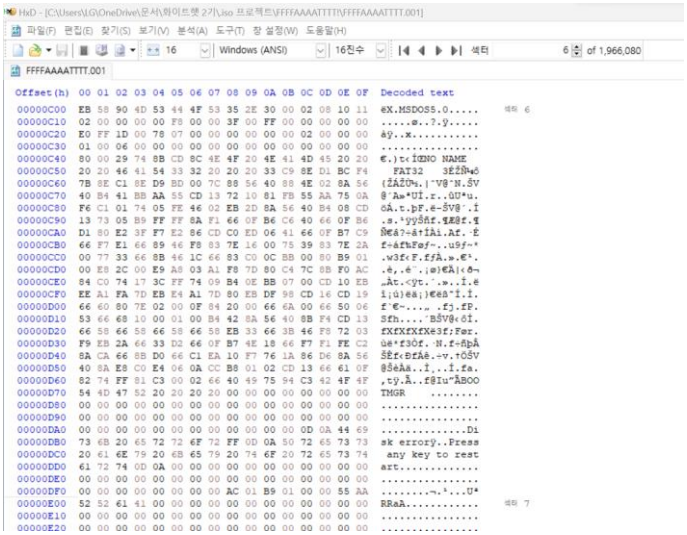
4. Write-Up

파일명	FFFFAAAATTTT.001
용량	960MB
SHA256	b19ed349dfcde9c3ce665053937acf7570b8262d4a78668389b8083604312278
Timestamp	2024-05-10 15:21:55



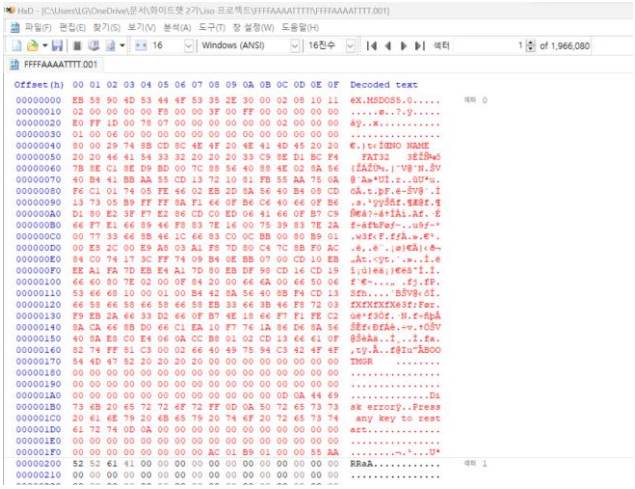
[그림 1] FFFFAAAATTTT.001의 파일 구조

문제명을 확인해 보니 FAT32 와 관련된 문제일 것 같다. 해당 문제 파일을 HxD 로 열어보니 파일이 손상된 것을 확인할 수 있다.



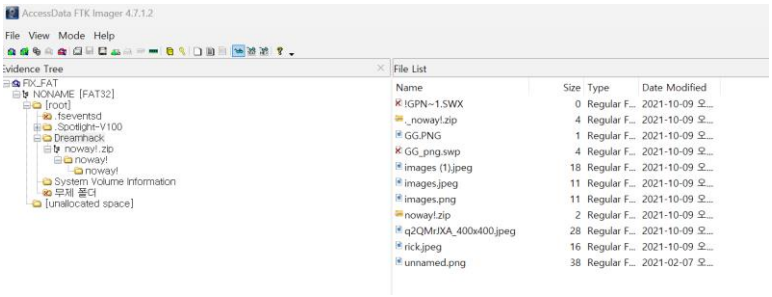
[그림 2] 섹터 6

시스템 이미지의 복원을 위해 **섹터 6 으로 이동하여 백업 BR** 을 확인한다.



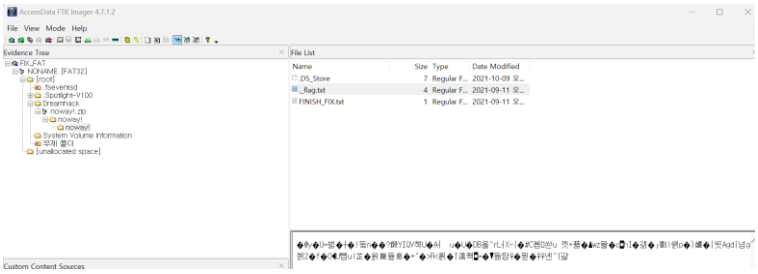
[그림 3] 손상된 파일 복구

섹터 6 에 있는 BR 를 복사하여 복원해야 하는 섹터 0 에 삽입하고 [FIX_FAT]라는 파일명으로 저장한다.



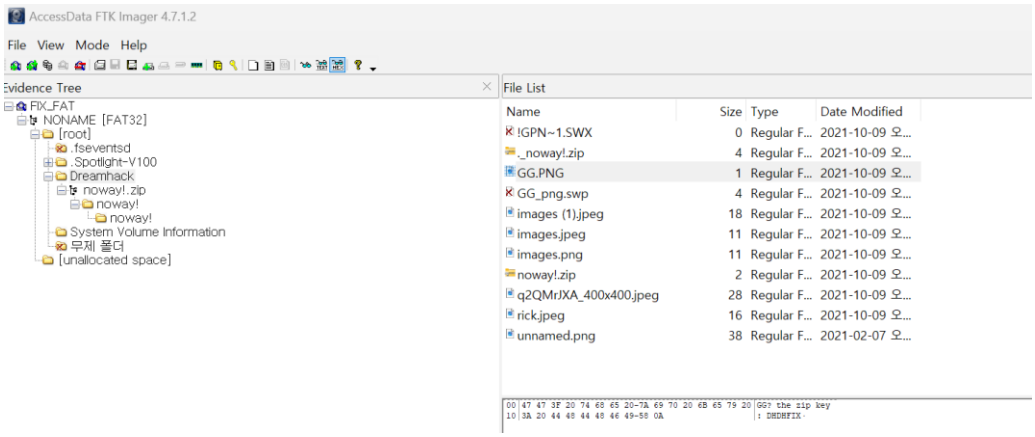
[그림 4] FTK Imager로 확인

FTK Imager 를 사용하여 복원한 [FIX_FAT]을 열어보니 [Dreamhack]이라는 디렉토리를 확인할 수 있다.



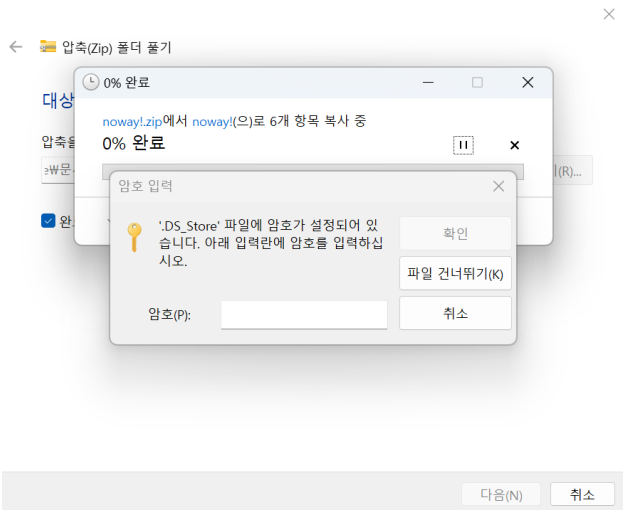
[그림 5] flag.txt

[Dreamhack] 안에 [noway!]라는 디렉토리를 확인해 보니 안에 flag 가 있을 법한 [flag.txt] 파일이 존재한다. 하지만 [그림 5]와 같이 아직 내용을 확인할 수 없다.



[그림 6] GG.PNG에 숨겨진 키 값

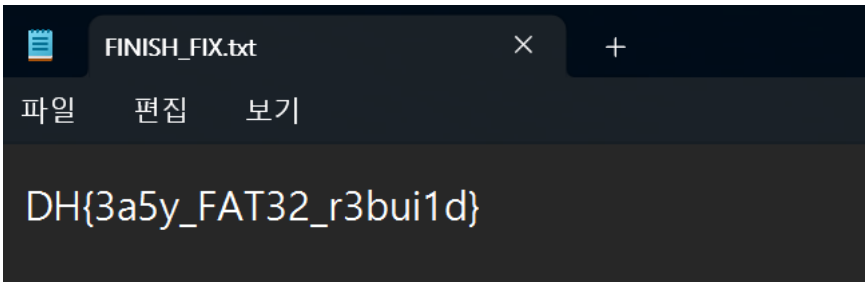
[Dreamhack] 디렉토리 안에 있는 파일을 확인해보니 [GG_PNG.swp]가 한 번 삭제된 것을 확인할 수 있었다. [GG.PNG] 파일을 HEX 값으로 확인해 보니 [GG? the zip key : DHDHFIX]이라는 압축 폴더 키 값을 얻을 수 있다.



[그림 7] 잠겨있는 noway!.zip

Dreamhack 디렉토리를 Export 하여 [noway!] 디렉토리를 압축 해제하려 하니 암호가 걸려 있다. 암호란에 [GG.PNG] 파일에서 얻었던 [DHDHFIX] 값을 입력하니 압축이 해제되었다.

5. Flag



[그림 8] flag 획득

[FINISH_FIX.txt] 파일을 열어 보니 **DH{3a5y_FAT32_r3bui1d}** 라는 flag 값을 획득했다.

6. 별도 첨부

7. Reference

- [URL]