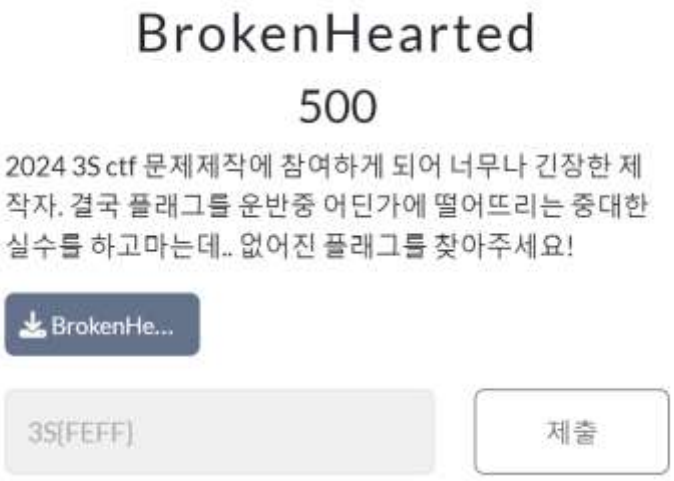
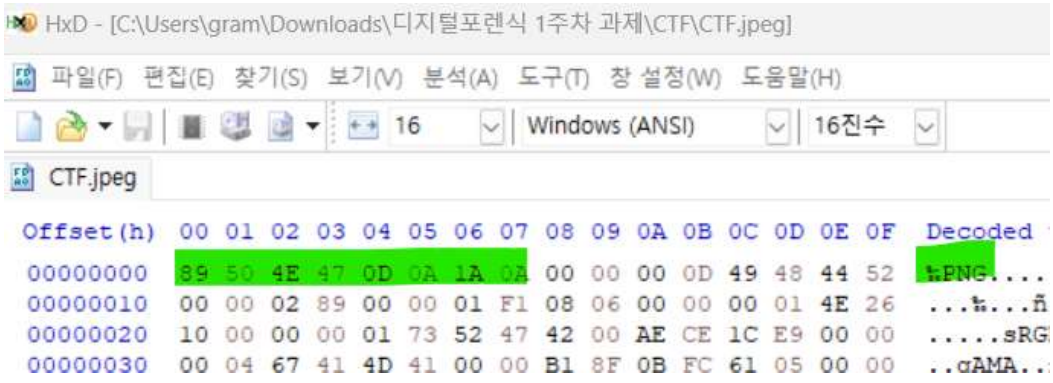
CTF.jpeg (BrokenHearted) Writeup

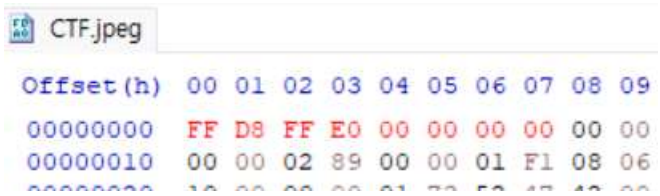


문제는 이렇다.

일단 CTF.jpeg를 헥스 에디터에서 열어보았다.



헤더 시그니처에서 이상한 점을 발견했다. 분명 jpeg 파일인데 헤더 시그니처는 png로 되어있는 것이다.



그래서 이렇게 헥스 에디터로 수동으로 복구해봤는데 파일이 열리지 않았다. 아무래도 수동 복구는 안되는 것 같아 다른 방법을 써보기로 했다.

예전에 이 문제를 3S CTF에서 접한 기억이 나 당시 라이트업을 찾아보았다. 당시에 플래그를 얻어내진 못했지만 이 문제가 파일 카빙을 해야 하는 문제인 것을 밝혀내었던 것 같다.

파일 카빙(File Carving)은 디지털 포렌식에서 사용되는 기술로, 손상되거나 파일 시스템 정보가 손실된 데이터 저장 장치에서 특정 파일이나 데이터를 복구하는 방법을 말한다.

그렇다면 이 문제는 파일 카빙을 통해 손상된 JPEG 파일을 복구해내는 문제라 볼 수 있겠다. 단순히 헥스 에디터에서 시그니처를 수정하는 것으로는 플래그를 얻을 수 없었으므로 다른 도구를 써야 한다.

첫 번째로 써본 것은 foremost이다. foremost는 시그니처 기반으로 파일을 추출하는 도구이기 때문에 헤더 시그니처를 수정해준 다음에 사용했다.

```
yuna@yuna-virtual-machine:~/Desktop$ foremost -t jpg -i CTF.jpeg -o outputnew_fo
lder
Processing: CTF.jpeg
|*|
```

```
------------------------------------------------------------------
File: CTF.jpeg
Start: Tue Mar 25 21:51:40 2025
Length: 223 KB (229365 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

Finish: Tue Mar 25 21:51:40 2025

0 FILES EXTRACTED

------------------------------------------------------------------
```

빠르게 결과가 나오긴 했는데 문제는 무언가 유의미한 값이 나오질 않았다.

그래서 이번에는 다른 도구를 써보기로 했다.

```
yuna@yuna-virtual-machine:~/Desktop$ scalpel -c /etc/scalpel/scalpel.conf -o out
putnew2_folder CTF.jpeg
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/yuna/Desktop/CTF.jpeg"

Image file pass 1/2.
CTF.jpeg: 100.0% |*************************************|  224.0 KB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9"
 --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9"
 --> 0 files
Carving files from image.
Image file pass 2/2.
CTF.jpeg: 100.0% |*************************************|  224.0 KB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 0, elapsed = 0 seconds.
```

Scalpel 또한 foremost와 비슷하게 시그니처를 기반으로 파일을 복원하는 도구이다. 그래서 똑같이 헤더 시그니처를 수정한 파일을 넣어주었다.

```
1
2 Scalpel version 1.60 audit file
3 Started at Tue Mar 25 22:12:41 2025
4 Command line:
5 scalpel -c /etc/scalpel/scalpel.conf -o outputnew2_folder CTF.jpeg
6
7 Output directory: /home/yuna/Desktop/outputnew2_folder
8 Configuration file: /etc/scalpel/scalpel.conf
9
10 Opening target "/home/yuna/Desktop/CTF.jpeg"
11
12 The following files were carved:
13 File              Start                 Chop            Length
  Extracted From
14
15
```

그런데 이렇게 해도 아무것도 추출되지 않는다...