



BrokenHearted
500

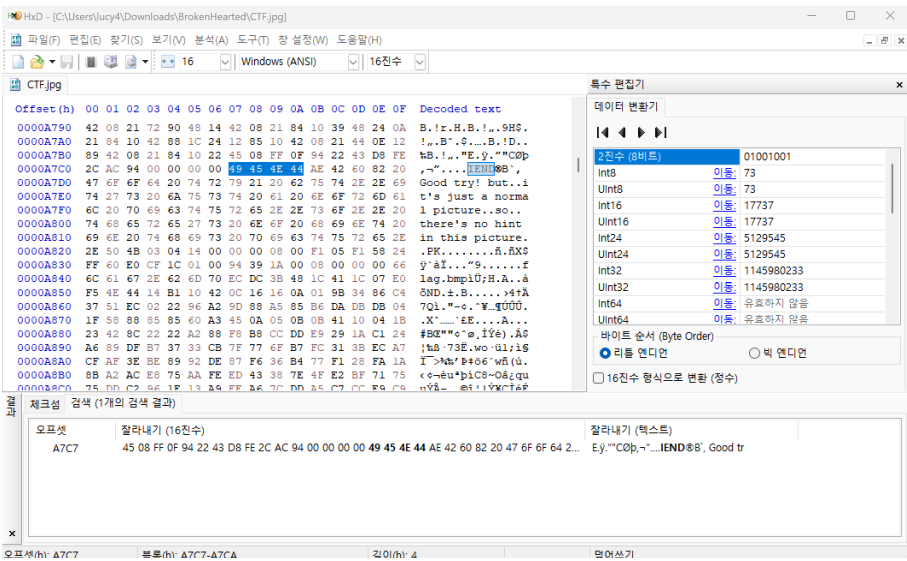
BrokenHe...

3S{FEFF}

제출

파일을 다운 받은 후 압축을 해제하니 다음과 같은 **CTF.jpg** 이미지가 나왔다.

PNG 이미지에 FLAG와 관련된 힌트가 있을까 싶어 HxD 툴을 사용해 열어봤다.

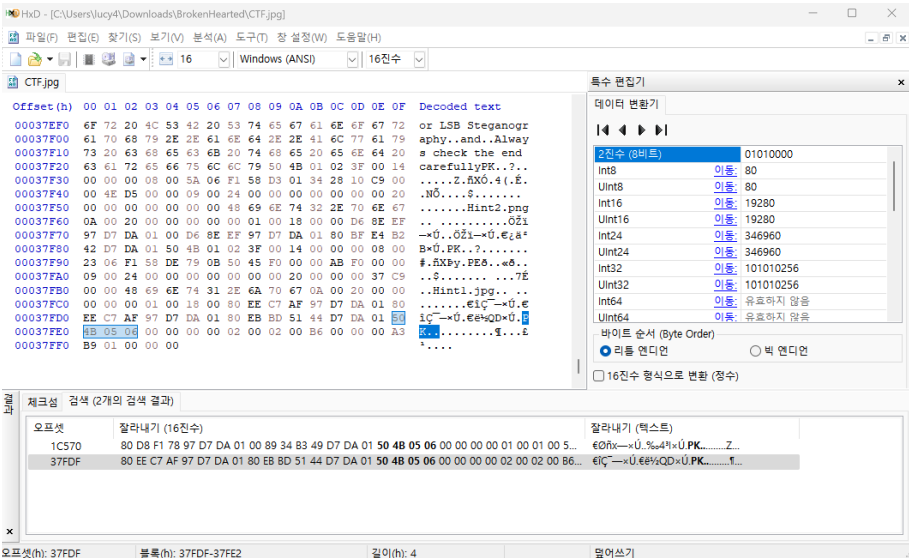
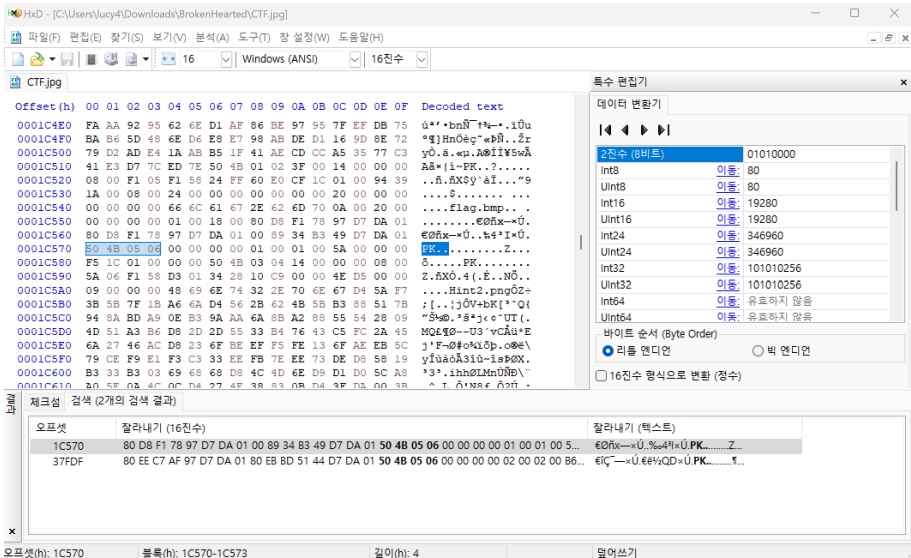


PNG의 헤더 시그니처와 푸터 시그니처가 모두 포함되어 있는 것은 확인이 되었지만, 푸터 시그니처에서 끝나지 않고 뒷 부분에 문장이 이어져 있는 것을 볼 수 있다.

Good try! but..it's just a normal picture..so.. there's no hint in this picture..

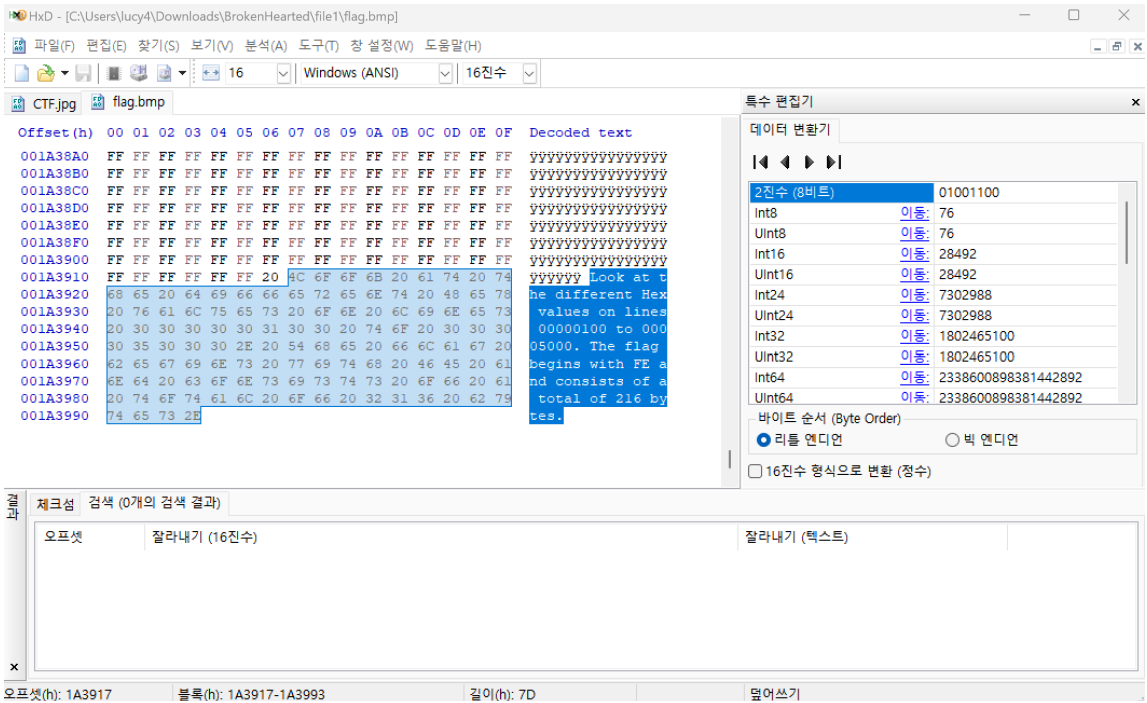
해당 PNG 파일은 평범한 사진이어서 힌트가 없다는 것이다. PNG 파일에 해당되는 값을 살펴본 결과 이 말이 틀린 말은 아니라는 것을 알았다.

이에 해당 문장 뒤에 이어진 값을 살펴보니, ZIP 파일의 헤더 시그니처인 것을 알 수 있었다.



혹시나 싶어 ZIP 파일의 푸터 시그니처를 검색해보니 총 두 개의 ZIP 파일이 존재하는 것을 볼 수 있다.

Where is the Flag!!!



첫 번째의 ZIP 파일 값을 새로운 ZIP 파일로 생성하여 압축을 풀어보니, 다음과 같은 **flag.bmp** 이미지가 나왔다.

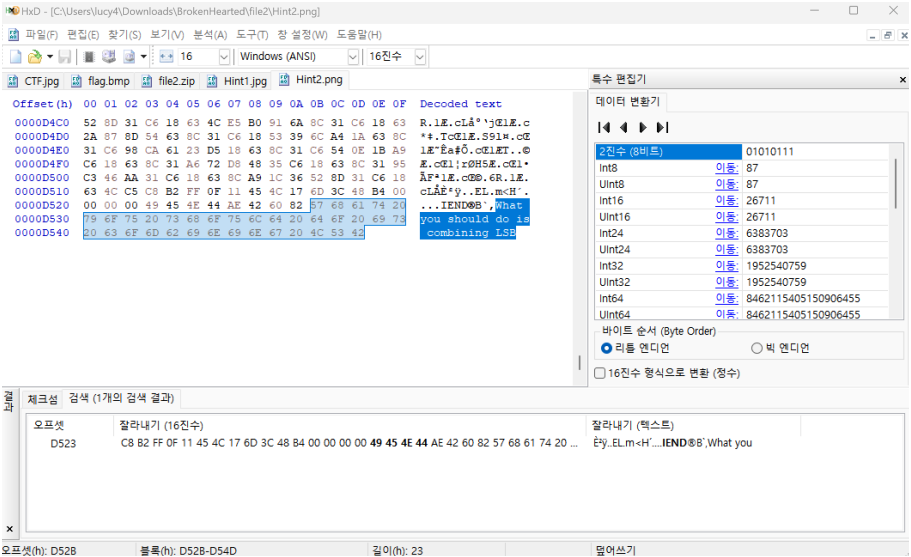
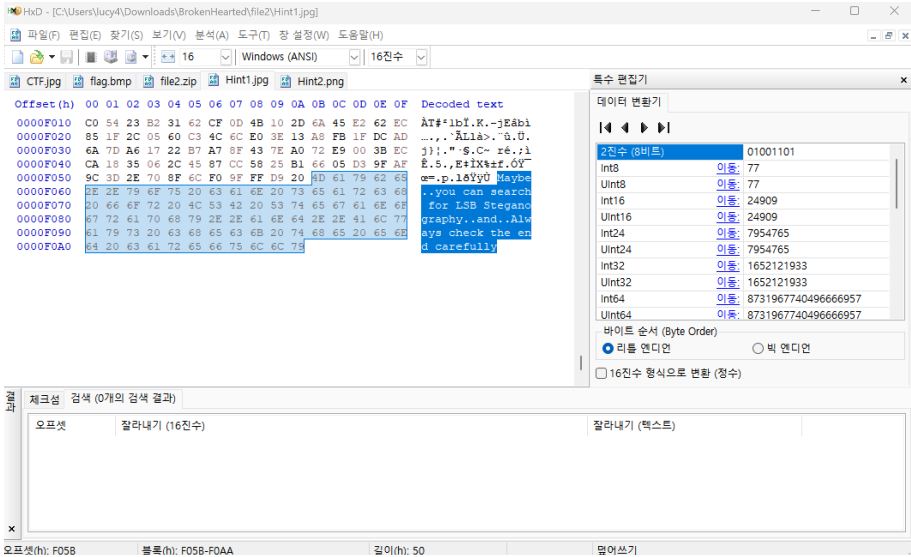
제대로 살펴보니 PNG나 JPEG 파일이 아닌 BMP 파일이었고, 해당 파일도 HxD 툴을 통해 살펴본 결과 맨 마지막에서 힌트가 되는 문장을 발견했다.

Look at the different Hex values on lines 00000100 to 00005000. The flag begins with FE and consists of a total of 216 bytes.

flag.bmp 파일의 00000100 ~ 00005000 사이 값을 통해 찾는 듯 보였다.

FLAG 값은 FE로 시작하며, 총 216 바이트라는 것 또한 알게 되었다.

그러나 해당 정보들로는 FLAG를 구하기에 힘들어, 앞선 ZIP 파일 말고 또 다른 ZIP 파일을 생성해 살펴보았다.



두 번째 ZIP 파일 안에는 `Hint1.jpg`, `Hint2.png` 파일이 들어있다.

해당 파일들 또한 HxD 툴을 통해 살펴본 결과, 마지막에 힌트가 되는 문장들이 숨어있다.

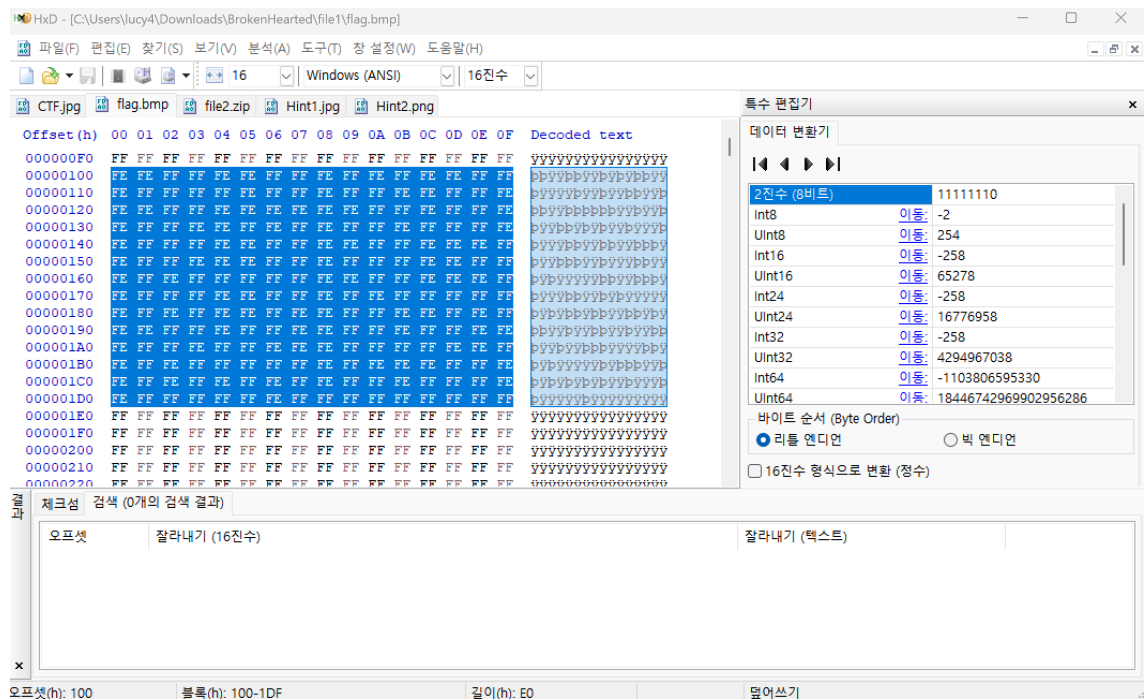
`Maybe..you can search for LSB Steganography..and..Always check the end carefully`

`What you should do is combining LSB`

두 문장 모두 LSB를 이야기하기에, `LSB Steganography` 가 무엇인지 찾아봤다.

이미지를 변조하여 데이터를 숨기는 방법 중에 LSB(최하위 비트)를 변조하는 방법이 가장 일반적이라고 한다.

그렇다면 `flag.bmp` 파일의 마지막에 있던 문장을 참고하여 FLAG 값을 구할 수 있을 것 같아 해당 파일을 살펴봤다.



flag.bmp 파일의 00000100 부분을 살펴보면, 해당 부분부터 000001D0 라인까지 FE와 FF로 이루어진 것을 볼 수 있다.

이를 8바이트씩 총 27줄로 정렬한 후, FE는 0, FF는 1로 치환하여 2진수를 ASCII 코드로 변환하면 되지 않을까 싶어 시도해봤다.

```
FE FE FF FF FE FE FF FF → 00110011 → 3
FE FF FE FF FE FE FF FF → 01010011 → S
FE FF FF FF FF FE FF FF → 01111011 → {
FE FF FF FE FE FF FF FE → 01100110 → f
FE FE FF FF FE FE FE FE → 00110000 → 0
FE FE FF FF FE FF FF FE → 00110110 → 6
FE FF FF FE FE FF FE FF → 01100101 → e
FE FF FF FE FF FF FF FE → 01101110 → n
FE FF FF FF FE FE FF FF → 01110011 → s
FE FE FF FF FE FE FE FF → 00110001 → 1
FE FF FF FE FE FE FF FF → 01100011 → c
FE FF FF FF FE FE FF FF → 01110011 → s
FE FF FE FF FF FF FF FF → 01011111 → _
FE FE FF FF FE FE FE FF → 00110001 → 1
FE FF FF FF FE FE FF FF → 01110011 → s
FE FF FE FF FF FF FF FF → 01011111 → _
FE FF FE FF FE FE FF FE → 01010010 → R
FE FF FF FE FE FF FE FF → 01100101 → e
FE FE FF FF FE FF FF FE → 00110110 → 6
FE FF FF FE FF FF FE FE → 01101100 → l
FE FF FF FE FF FF FE FE → 01101100 → l
FE FF FF FF FF FE FE FF → 01111001 → y
FE FF FE FF FF FF FF FF → 01011111 → _
FE FF FE FE FE FF FF FE → 01000110 → F
FE FF FE FF FE FF FE FF → 01010101 → U
FE FF FF FE FF FF FF FE → 01101110 → n
FE FF FF FF FF FF FE FF → 01111011 → }
```

BrokenHearted

500

2024 3S ctf 문제 제작에 참여하게 되어 너무나 긴장한 제작자. 결국 플래그를 운반중 어딘가에 떨어뜨리는 중대한 실수를 하고마는데.. 없어진 플래그를 찾아주세요!

📄 BrokenHe...

플래그

제출

Correct

3S{f06ens1cs_1s_Re6lly_FUn}