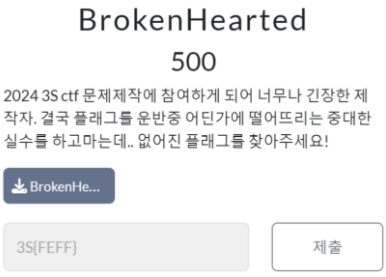
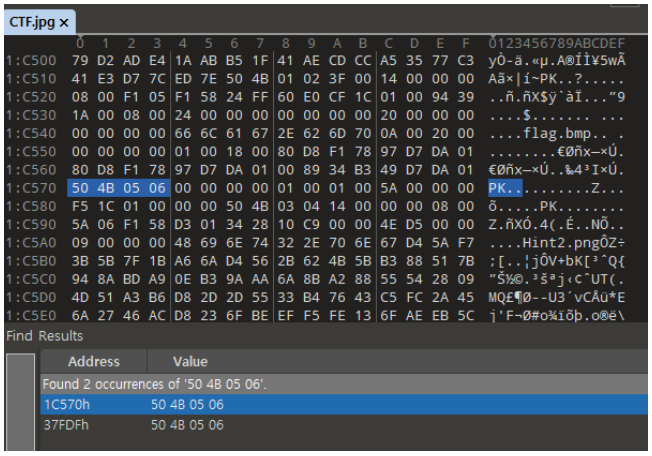
3S CTF
Forensic-BrokenHearted

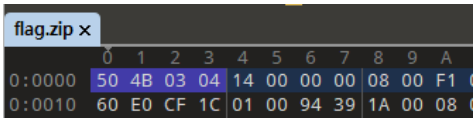
SWING 32 기 한재희



파일을 다운 받으면 이런 이미지가 뜬다.
010 에디터로 열어서 보다가 PNG 시그니처 값은 제대로 있어서 안에 zip 파일이 있는지 확인하려고 zip 시그니처를 검색해봤다.



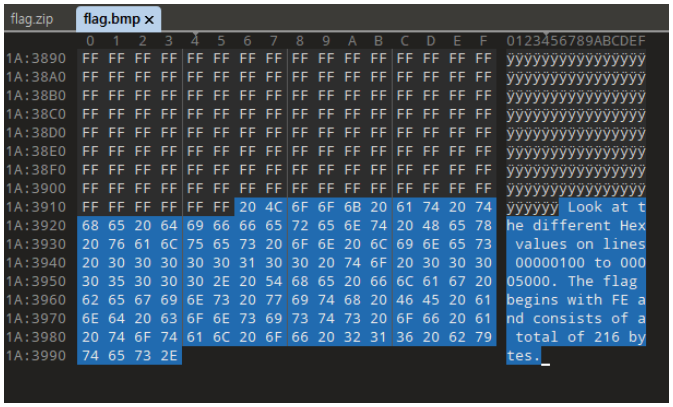
보니까 zip 파일이 존재하는 것 같아서



50 4B 03 04 부터 50 4B 05 06 까지 잘라서 zip 파일로 만들어서 압축을 풀었더니

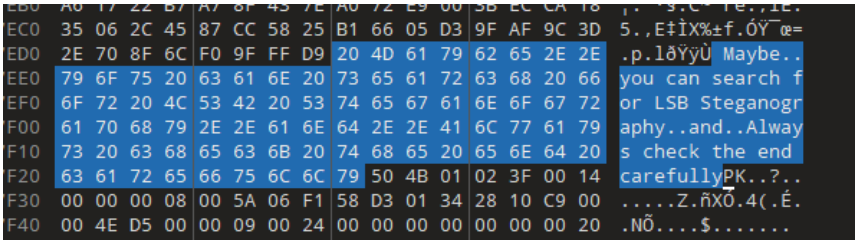
Where is the Flag!!!

이 사진이 나왔다. 다시 이 사진을 010 에디터로 확인했다.



맨 마지막 줄에 flag.bmp 파일의 00000100~00005000 사이 값을 잘 살펴보라는 식으로 나와있었다. Flag 값이 FE 로 시작하고 총 216byte 라는 힌트가 나와있는 사진이었다.

그리고 다시 원본 사진을 보다 마지막 줄 쯤에



스테가노그래피를 사용하라는 거 같은 힌트가 적혀 있었다. 이미지 변조 기법 중에 최하위 버전인 LSB 를 변조한 것 같아 보여서 flag.bmp 파일을 봐줬다.

FE 를 검색해봤더니 딱 이 부분만 FE 가 있어서 아까 216 바이트라고 했으니까 8 바이트씩 27 줄로 만들고 FE 는 0, FF 는 1 로 바꿔서 나타난 2 진수를 아스키코드로 변환해봤다.

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 → 01111101 → }

3S{f06ens1cs_1s_Re6lly_FUn}