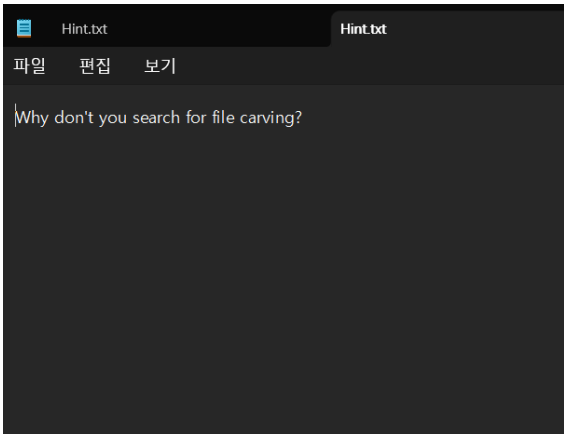
2024 3S CTF - BrokenHearted (포렌식) Writeup

32기 김효주

먼저 문제 파일을 다운받고 압축 파일을 해제하면 아래와 같이 CTF.jpg와 Hint.txt를 확인할 수 있다.

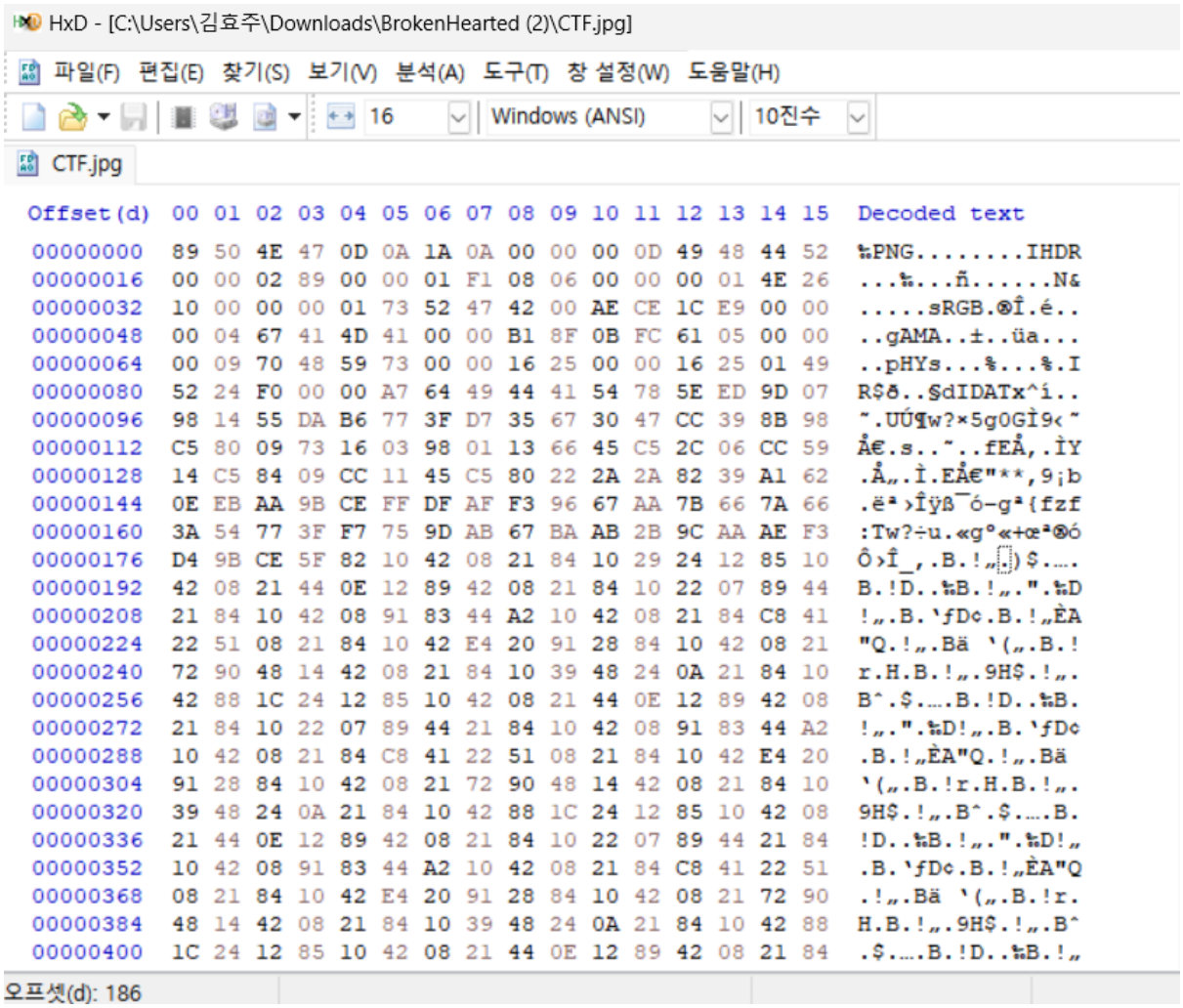


힌트를 보니 파일 카빙을 해서 플래그를 찾아야 하는 것 같다.

여기서 파일 카빙이란 바이너리 데이터를 이용해 디스크의 비할당 영역에서 파일을 복구하는 방식이다.

내가 아는 포렌식 툴 중 회장님이 사용 방법을 알려주신 (내 노트북에 깔려있는) 툴인 HxD를 사용해야겠다.

HxD를 사용해 jpg 파일을 열어보니 다음과 같이 뜨는 것을 확인할 수 있었다.

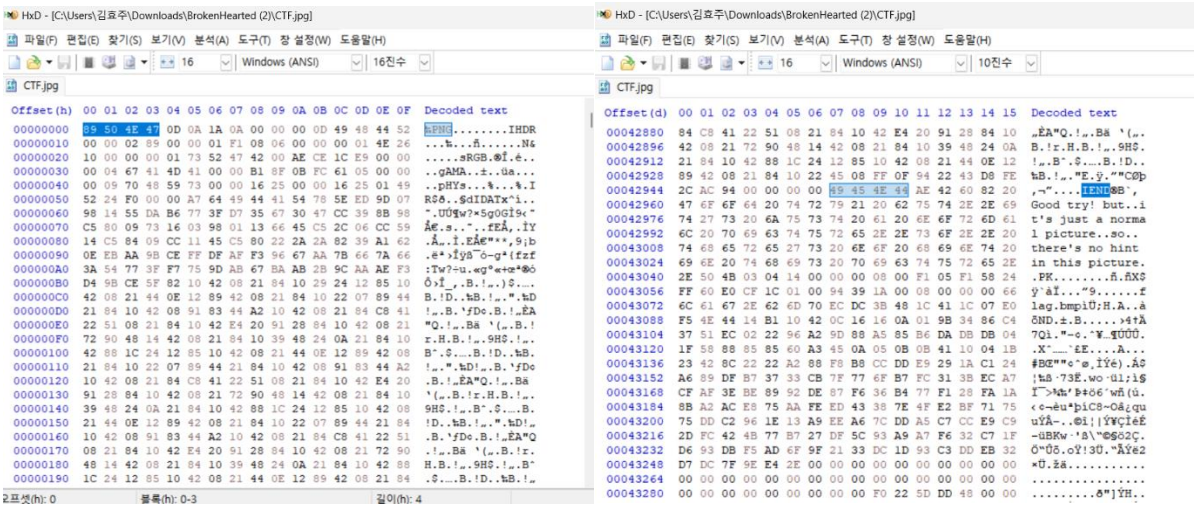


여기에서 내가 찾아야 하는 것은 파일 시그니쳐, 그 중에서도 헤더와 푸터 시그니쳐를 찾아야 한다.

(푸터 시그니쳐는 png랑 jpg 파일만 갖고 있다고 함)

(CTF.jpg 파일을 열어 숨겨진 파일은 없는지, 파일의 시그니쳐가 제대로 작성되어있는지 확인해야 하니까)

먼저 헤더는 맨 처음에 있으니까 쉽게 찾을 수 있었고, png 시그니쳐가 나오니까 검색해서 푸터도 찾았다.



헤더 시그니쳐 : 89 50 4E 47, Decoded text : PNG

푸터 시그니쳐 : 49 45 4E 44, Decoded text : IEND

(이때 IEND 청크는 이미지의 맨 뒤에 위치하는 청크로 PNG 파일의 끝임을 나타냄 -> PNG 파일이구나 알 수 있음)

File Type	Header Signature(Hex)	Footer Signature(Hex)
JPEG	FF D8 FF E0 FF D8 FF E8	FF D9
GIF	47 49 46 38 37 61 47 49 46 38 39 61	00 3B
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
PDF	25 50 44 46 2D 31 2E	25 25 45 4F 46
ZIP	50 4B 03 04	50 4B 05 06
ALZ	41 4C 5A 01	43 4C 5A 02
RAR	52 61 72 21 1A 07	3D 7B 00 40 07 00

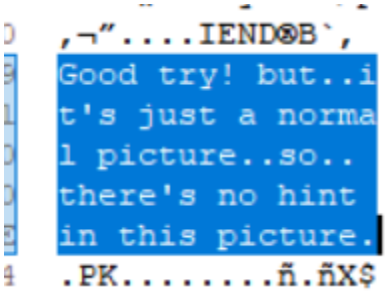
위의 표를 봐도 Decoded tex를 봐도 그냥 보기엔 jpg 파일이지만 HxD로 열어보면 png 파일이라는 걸 알 수 있다.

(근데 jpg는 아무리 찾아도 시그니쳐가 뭔지 안 보임 저번에 png랑 jpg랑 시그니쳐가 같다고 하셨던 것 같은데 확실치 않음)

(jpeg는 jpg랑 또 시그니쳐가 다르더라)

근데 딱히 png 형식이랑 시그니쳐가 다른 것도 아니고... 뭘 더 해야하나 싶다가 푸터 시그니쳐 뒤에 있는 문장을 발견했다.

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



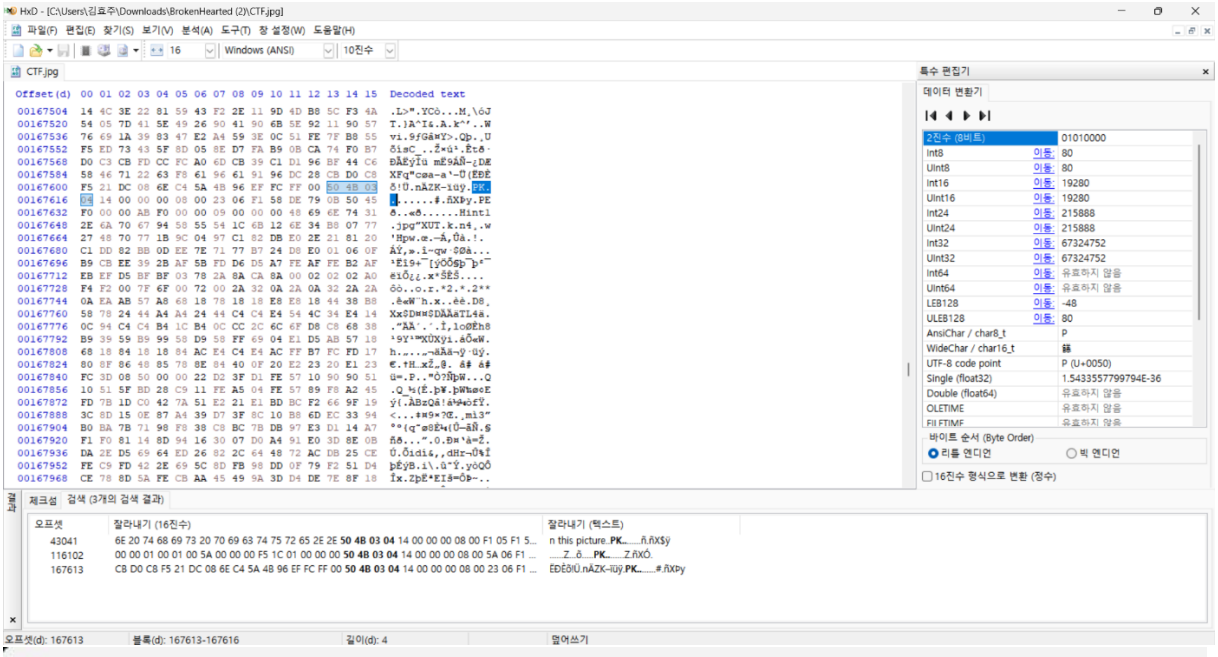
하...우찌하나... 솔직히 여기서 더 못하겠어서 다른 문제로 넘어갔는데 그게 더 안 풀려서 이틀 뒤에 다시 돌아왔다.

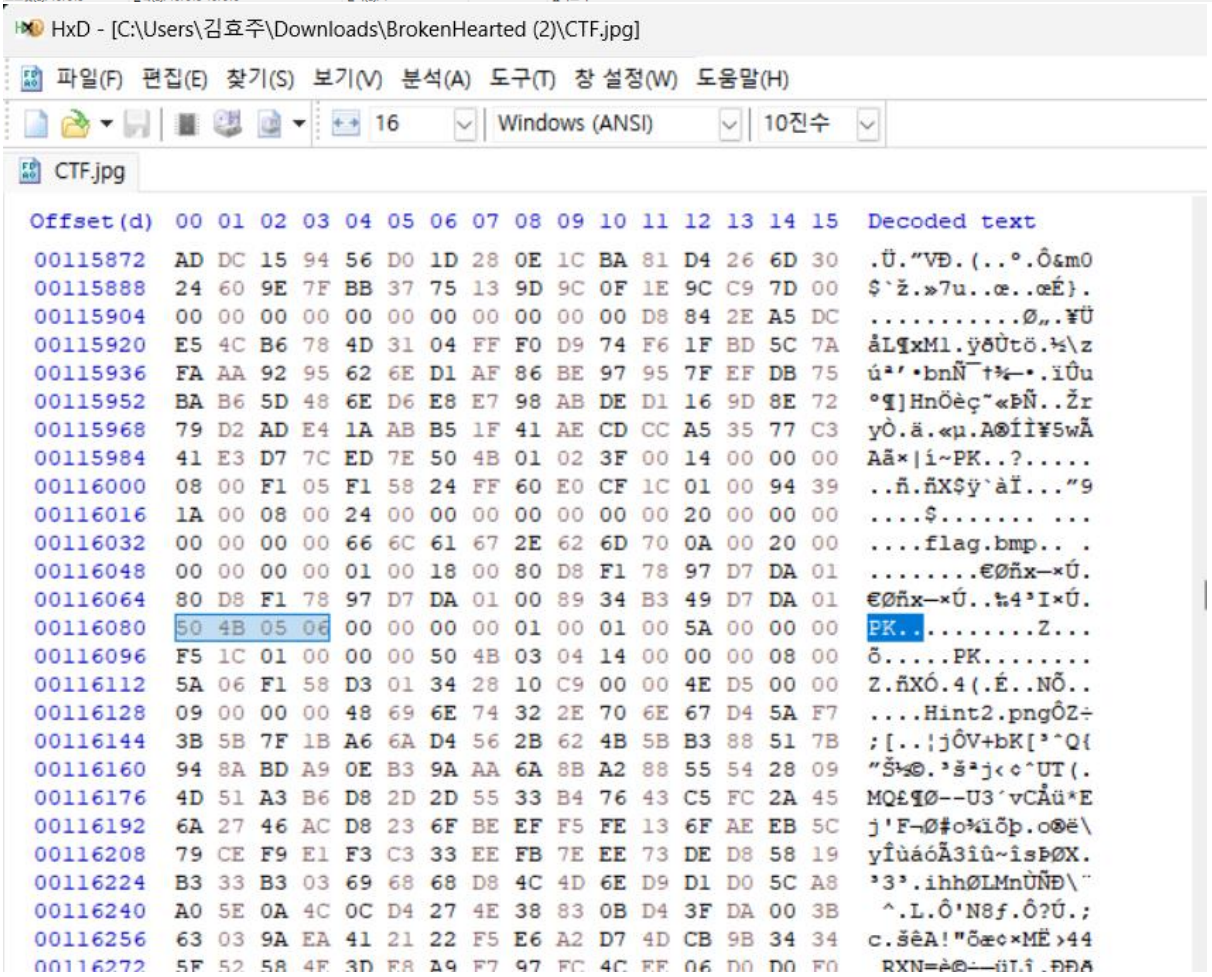
그래서 걍 뭐라도 하자 싶어서 다른 파일 형식 시그니쳐가 있는지 검색해봤다. 뭐 숨겨져 있을 수도 있으니까...

(사실 다른 사람들이 이런 포렌식 문제 풀 때 이렇게 하는 것 같아서 따라해봄)

그렇게 위에 있는 표에 나온 시그니쳐들을 검색하다 zip 파일 시그니쳐가 있다는 걸 확인했다!!!!!!

(여기서 Decoded text에 있는 PK : zip 파일 헤더에 pk라는 문자열이 들어간다고 함, pk 있으면 zip 이구나 생각하기)





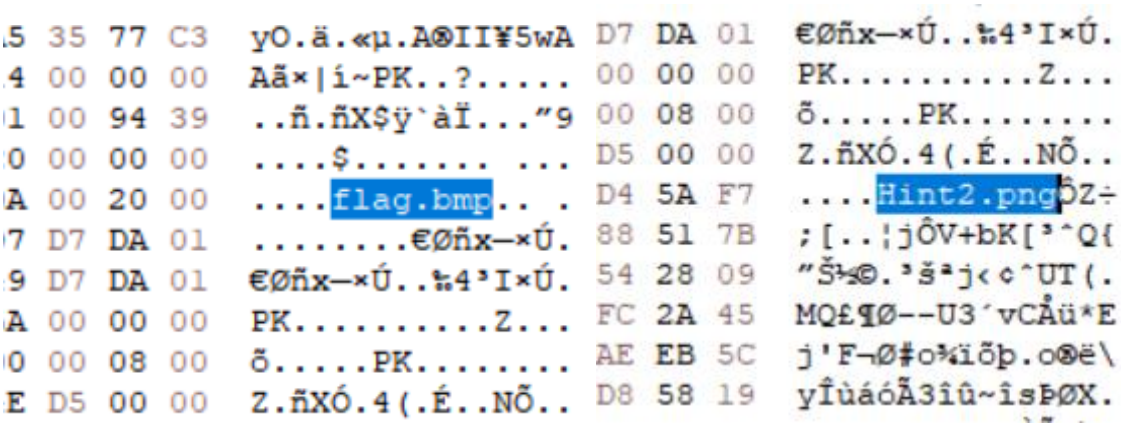
헤더 시그니쳐 : 40 4B 03 04, Decoded text : PK

푸터 시그니쳐 : 40 4B 05 06, Decoded text : PK

(근데 헤더는 3개 나오는데 푸터는 2개 나오네.... 뭘까)

그렇게 찾다가 첫 번째 푸터 시그니쳐 근처에 flag.bmp랑 hint2.png가 있는 걸 발견함

그럼 이 CTF.jpg 안에 있는 zip를 풀면 flag.bmp랑 hint2.png가 있으니 힌트를 보고 플래그를 찾는 것 같음



근데 그 zip파일을 어떻게 푸는? 건지 어떻게 찾아내는지?를 모르겠어서 엄청나게 구글링을 했다.

근데 다 너무 어렵고 이건 아닌 것 같고 그래서 다시 다른 문제 시도....

근데 다른 문제도 실패하고 걍 하루 뒤에 다시 돌아옴. 피같은 노력ㄱ끝에 시력을 포기하고... 방법을 찾아냄!!!!!!!!!!!!!!

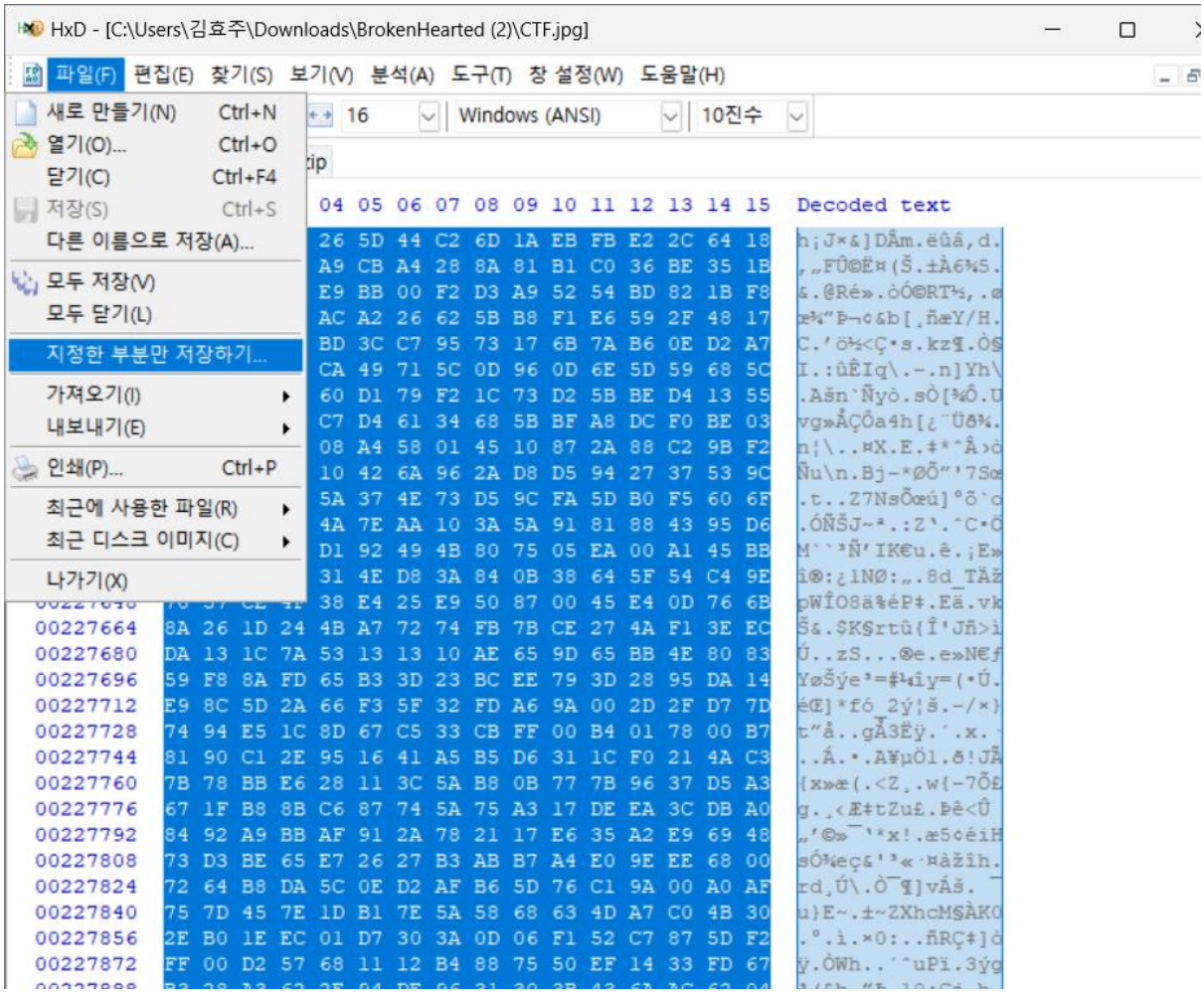
zip 파일 추출하는 법

1. zip 파일 헤더 시그니쳐 찾아내기

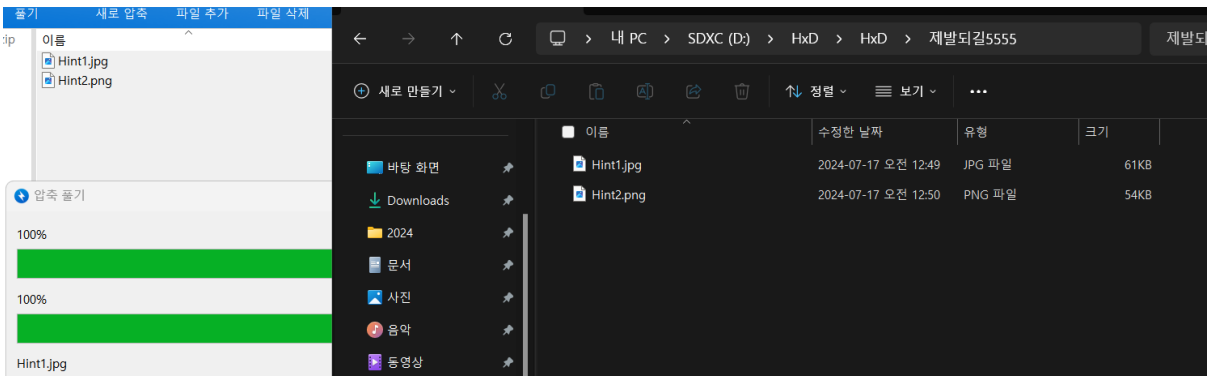
2. 거기서부터 끝까지 선택하기

3. 선택한 채로 파일 눌러서 지정한 부분만 저장하기 누르기

4. 이름 적고 .zip 꼭 붙이기 (안 붙이면 안 열림)



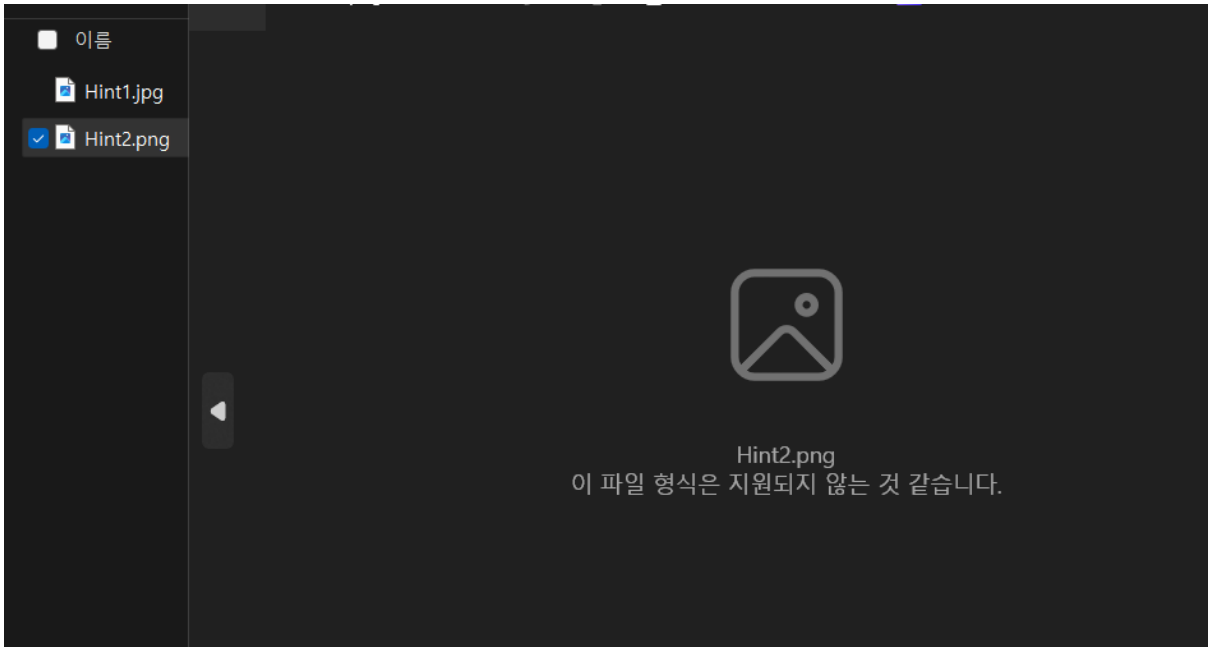
이렇게 해서 생성된 zip 파일을 압축 풀면



이렇게 됨 근데 문제가 생김.....

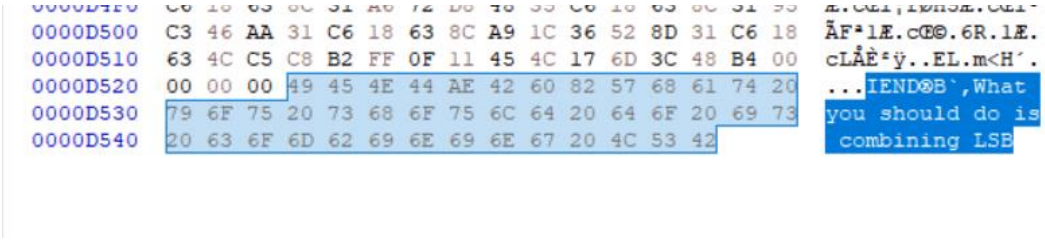
내가 아까 본 건 flag랑 hint2인데 지금 hint1랑 hint2만 있고.... flag.bmp 파일은 없음

그리고 hint2 파일 안 열림...ㅎ HxD로 까보면 ㄱㅊ겠죠 ㄱㅊ아야만 됨



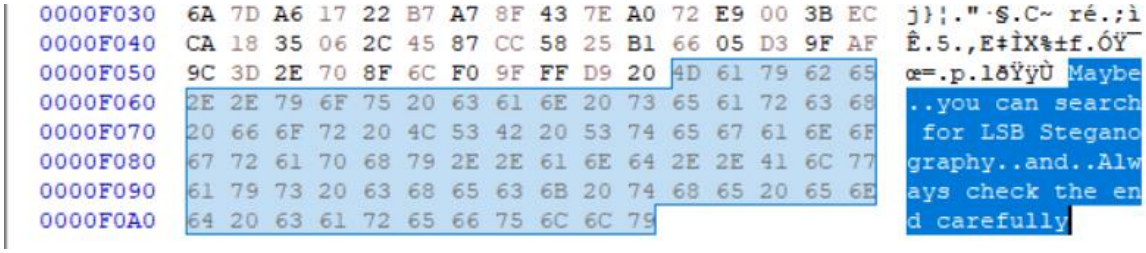
오 HxD로 헤더랑 푸터 시그니쳐 (첨에 했던 것처럼 똑같이) 찾아봤는데 마지막에 힌트를 얻었음

combining LSB 하라네요



혹시 몰라서 hint1도 까봤는데 내가 맨 처음에 봤던 힌트 파일 (문제 다운받으면 볼 수 있는 파일) 이랑 다르네!!!!

당연히 다르겠지 효주야 정신차려라 맨 처음에 봤던 힌트 파일은 txt였다.....



이제 좀 요령 생기는 듯? 언제나 끝을 보기... 맞아요 사실 저 이번엔 푸터 검색 안 하고 바로 마지막 봤어요

그리고 여기도 LSB Steganography를 찾아보라네요

ㅇㅋ 일단 접수하고 먼저 flag.bmp를 찾아봅시다 내가 뭔가 놓친 게 있겠지

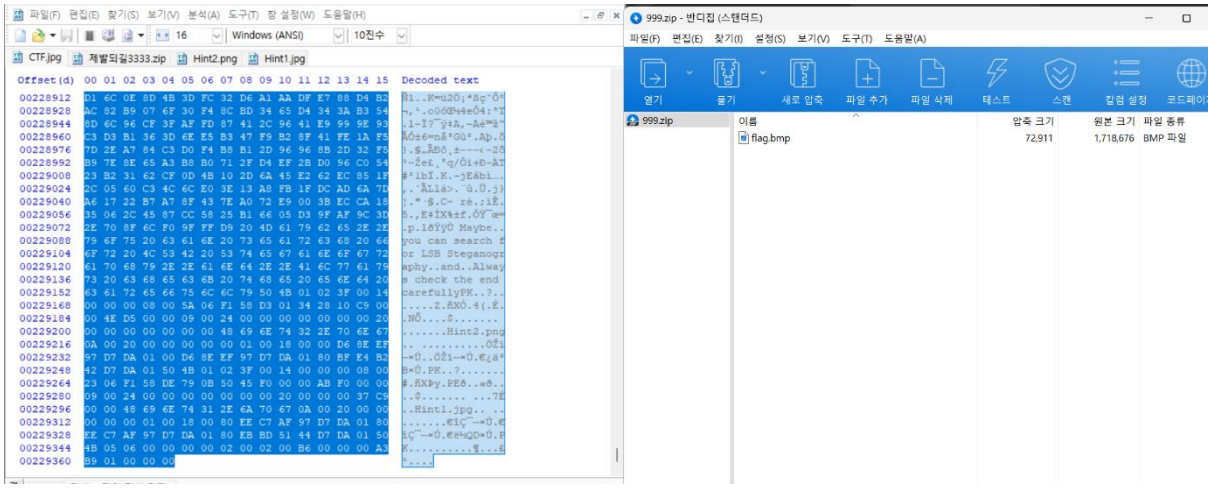
진짜 별 실수를 다 하네요 hint 파일 켜고 zip를 찾으니까 당연히 안되죠....

암튼 중간중간 이상한 실수 많이 하고,...

뭔 손상된 파일이라고 그러고..

해당 부분부터 복사를 하라는데 그것도 못찾아서 쌩으로 복붙하고,.,,

암튼 그래서 결국 찾아냈다 나의 flag파일.....

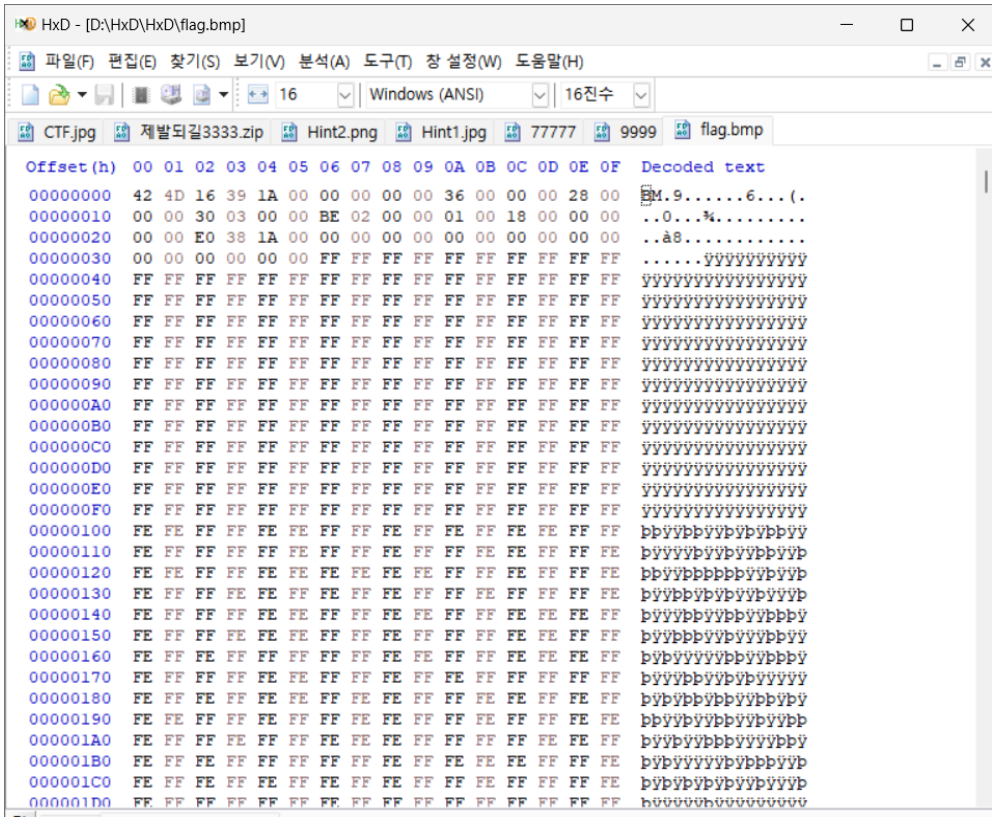


(엥 근데 저거 복붙하다 발견한 건데 첫 번째로 깐 zip 안에 있던 힌트 문구 CTF.jpg 안에도 있었네? 당연한 거긴 한데....)

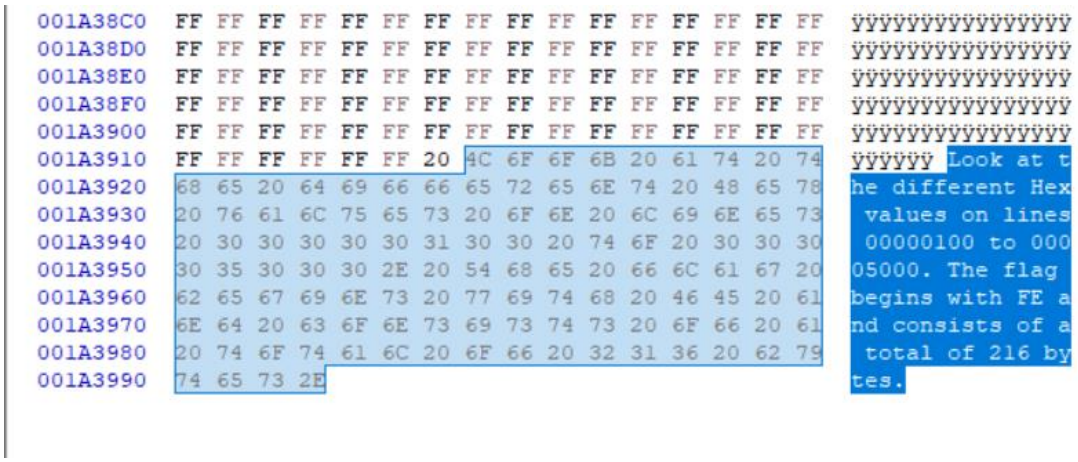
하.... 거의 다 왔다 (아마)

이제 HxD를 사용해서 까보자!!!

...문제가 생김 이게뭐죠?



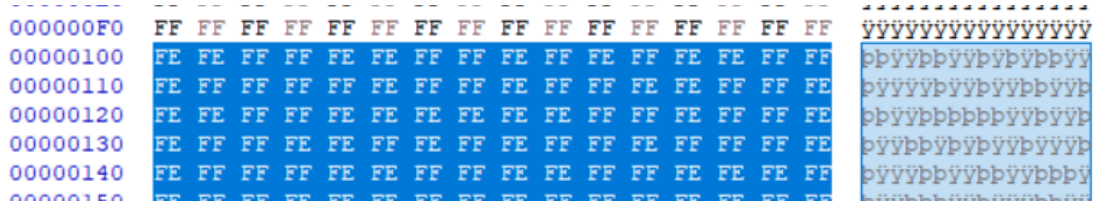
마지막 희망.. 맨 밑으로 내려가 봄



플래그 값은 fe로 시작하고 총 바이트 수는 216이란다 이건 ㅇㅋ

근데 값은 00000100 ~ 00005000 사이라는 것 같은데 무슨 값을 말하는 거지?

아 이건가보다 근데 너무 범위가 넓은데?



그럼 이제 힌트를 사용해보자 아까 LSB teganography를 찾아보라고 했으니까 구글링해보자

LSB steganography is a commonly used technique for hiding secret messages within images. It works by replacing the least significant bits of the cover image with the secret message bits.

아 근데 진짜 다 찾아봤는데 모르겠다....

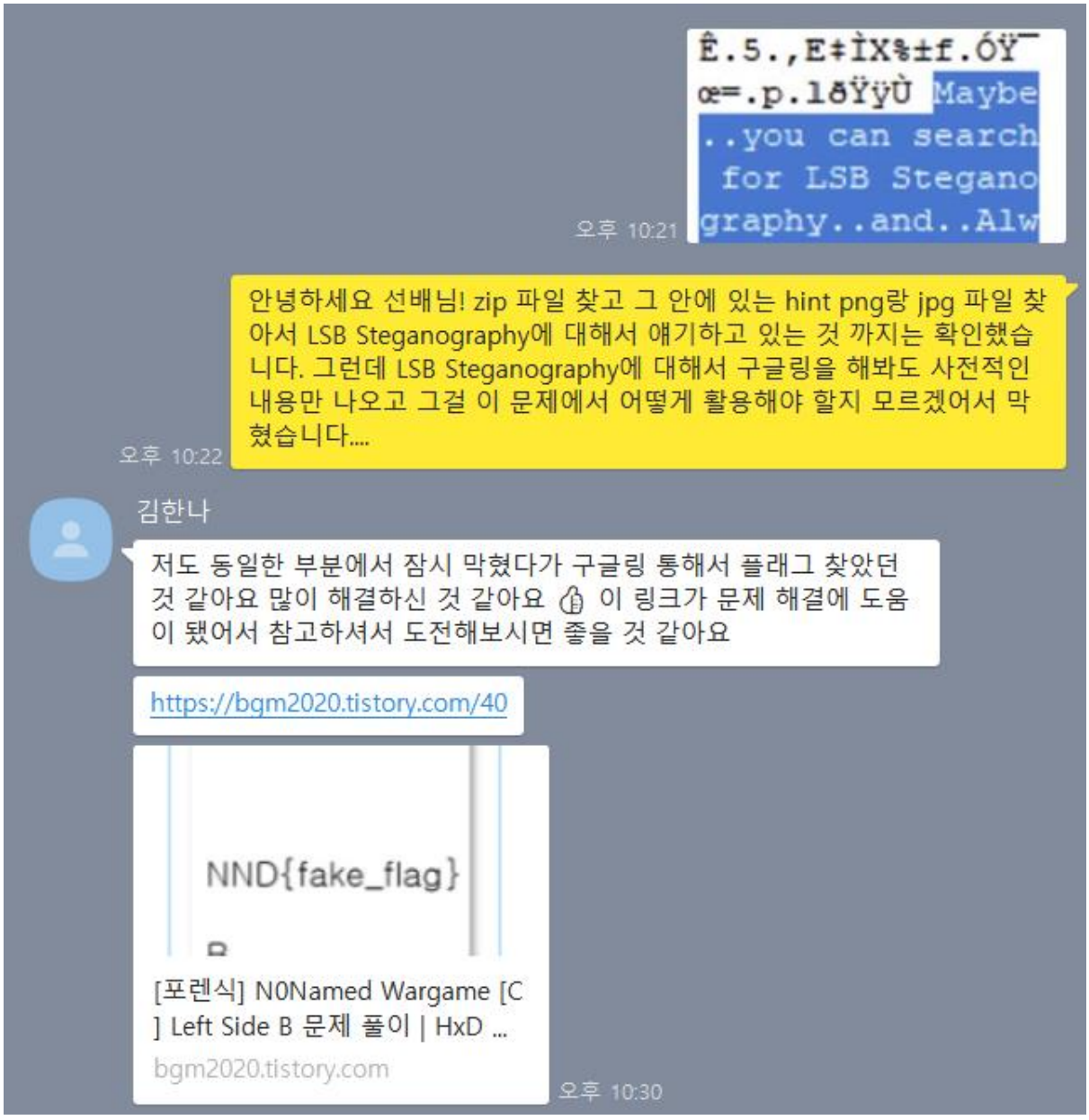
영어 자료만 많고 그것도 논문이나 암호화 방식만 설명한 거라

지금 내가 문제를 푸는 데에 도움이 1도 안됨....

더 이상 못할 것 같은데 근데 이것만 풀면 플래그 얻을 수 있을 것 같은데...

여기서 또 다른 문제 풀다가 진정하고 다시 시도해봄.. 근데 전혀 정말 너무 모르겠어서

3S CTF 문제 풀 때 우리 팀에 이 문제 푼 선배님이 계셨던 걸 기억하고 도움을 요청했다....



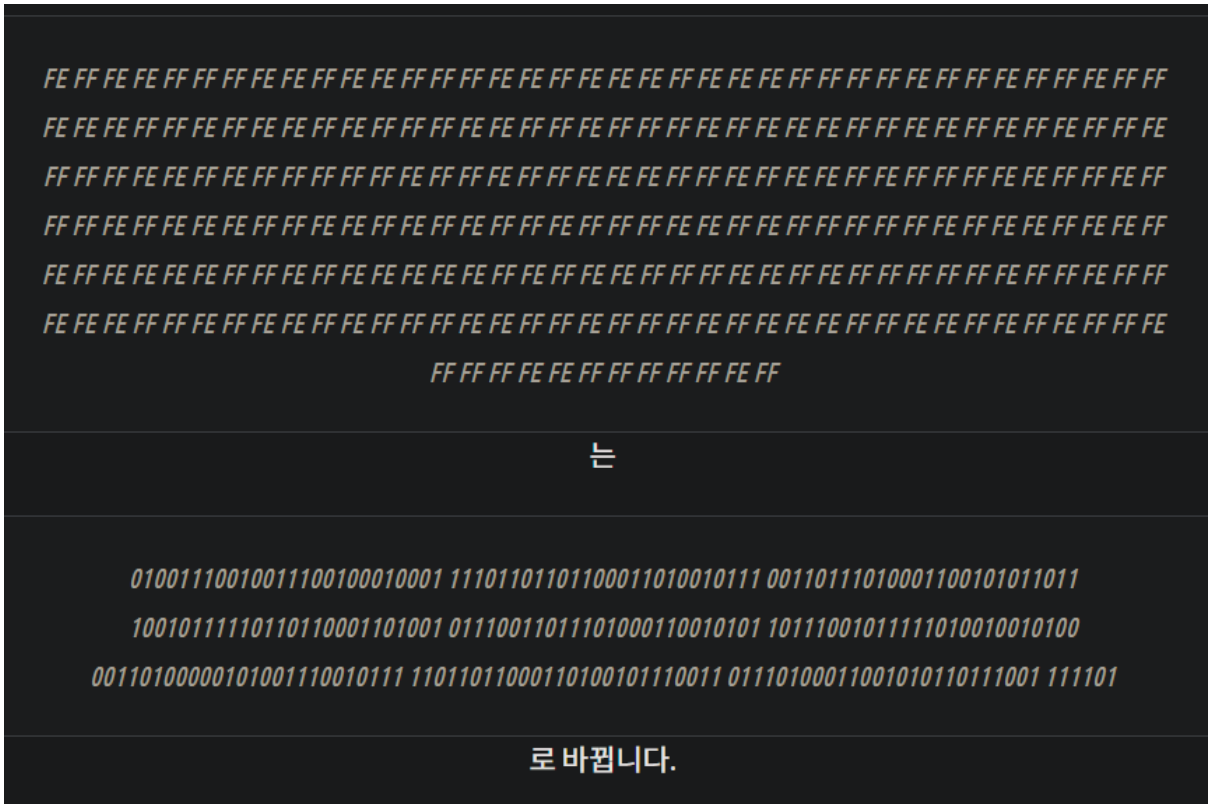
선배님께서!!!!!! 도움이 될만한 링크를 보내주셨다!!!!! 다시 감사드립니다.....

앞으론 구글링도 좀 열심히 잘 해봐야지 내가 할 땐 왜 저런 거 못찾았지

암튼 블로그 보고 이해한 결과 LSB 변조는 최하위 비트를 바꿔서 메시지를 숨기는 방식이다

ff는 1111 1111이고 fe는 1111 1110 -> 최하위 비트만 다름!!!

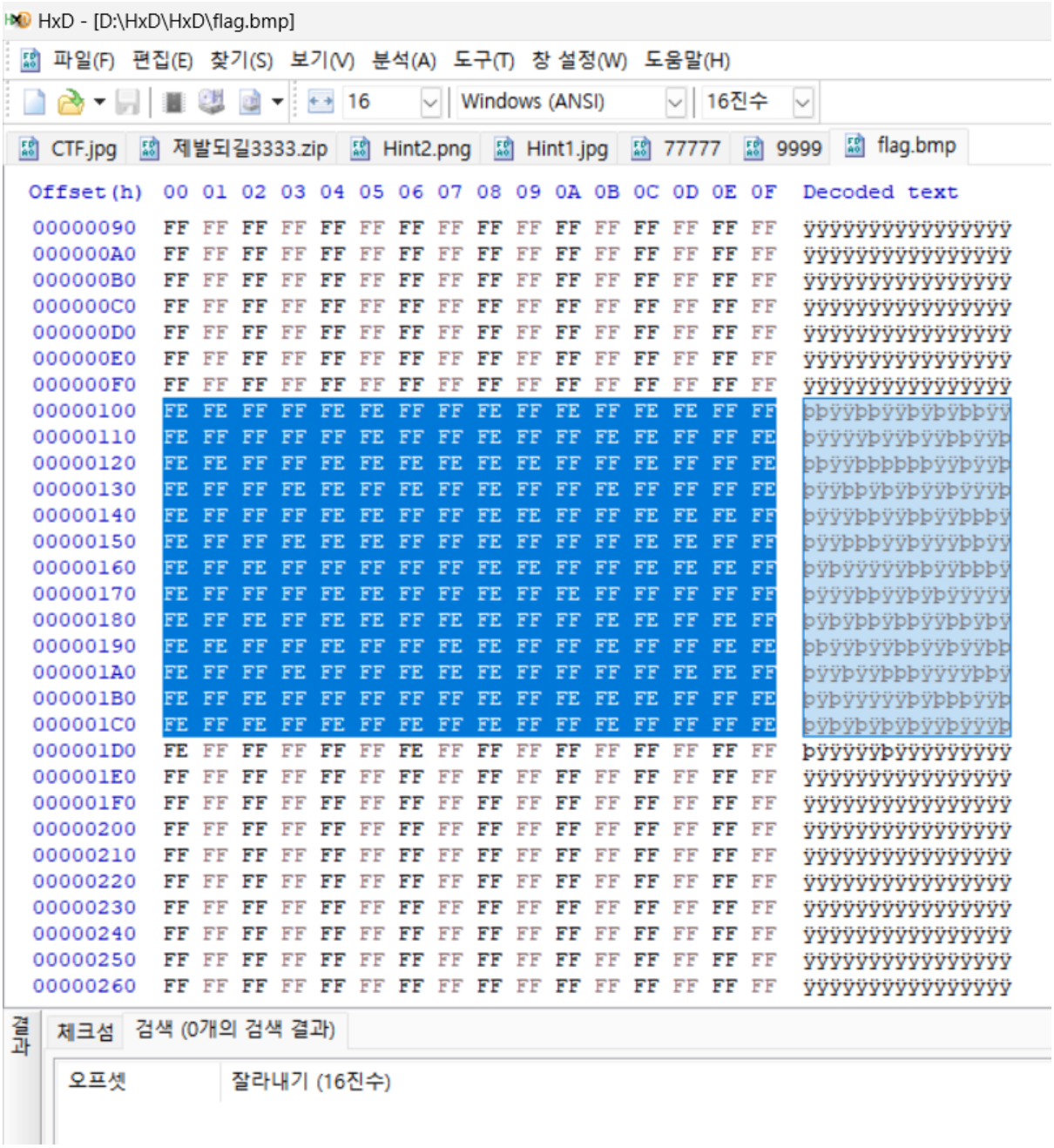
그래서 블로그 주인은 이렇게 바꾸었다고 한다



이제 이해했으니까 나도 해보자. 아까 범위가 너무 넓어서 걱정했는데

fe랑 ff를 찾는 거니까 ff만 계속 있는 부분은 안 해도 된다는 걸 깨달음

그럼 딱 이 부분만 바꾸면 된다는 뜻!!!



ㅇㅋ 해보자 블로그 주인님이 올려주신 파이썬 변환 코드.....가 있지만 너무 날로 먹는 것 같아서 걍 하나하나 함

일단 내가 변환해야 할 코드는

FE FE FF FF FE FE FF FF FE FF FE FF FE FE FF FF

FE FF FF FF FF FE FF FF FE FF FF FE FE FF FF FE

FE FE FF FF FE FE FE FE FE FE FF FF FE FF FF FE

FE FF FF FE FE FF FE FF FE FF FF FE FF FF FF FE

FE FF FF FF FE FE FF FF FE FE FF FF FE FE FE FF

FE FF FF FE FE FE FF FF FE FF FF FF FE FE FF FF

FE FF FE FF FF FF FF FF FE FE FF FF FE FE FE FF

FE FF FF FF FE FE FF FF FE FF FE FF FF FF FF FF

FE FF FE FF FE FE FF FE FE FF FF FE FE FF FE FF

FE FE FF FF FE FF FF FE FE FF FF FE FF FF FE FE

FE FF FF FE FF FF FE FE FE FF FF FF FF FE FE FF

FE FF FE FF FF FF FF FF FE FF FE FE FE FF FF FE

FE FF FE FF FE FF FE FF FE FF FF FE FF FF FF FE

FE FF FF FF FF FF FE FF FF FF FF FF FF FF FF FF

fe는 0으로 ff는 1로 바꾸고 8개씩 끊어서 나누면 이렇게 된다

00110011

01010011

01111011

01100110

00110000

00110110

01100101

01101110

01110011

00110001

01100011

01110011

01011111

00110001

01110011

01011111

01010010

01100101

00110110

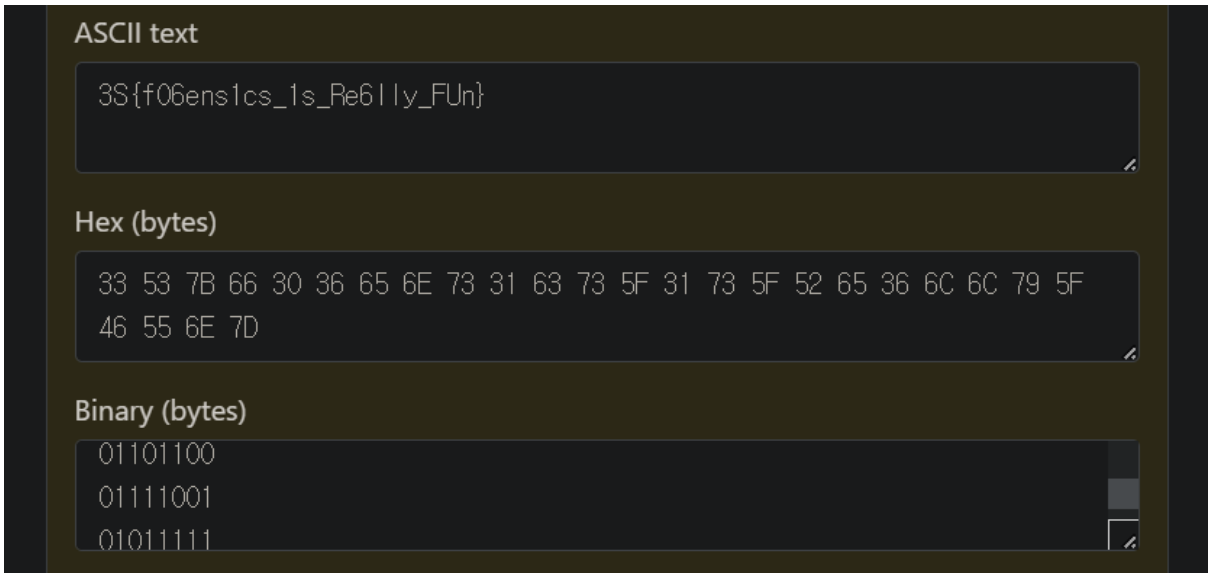
01101100

01101100

01111001

01011111
01000110
01010101
01101110
01111101

이 아스키코드를 변환해주기만 하면 된다..... 이건 변환 사이트가 있어서 변환 사이트를 이용했다



플래그는 3S{f06ens1cs_1s_Re6lly_FUn} !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

난생 처음 3S ctf 대회에 나가면서 정말 많은 걸 느꼈다....

하루종일 문제를 풀 시간이 있으니 적어도 한 문제는 맞출 줄 알았는데

아니 적어도 조금이나마 공부한 웹 문제는 실마리가 잡힐 줄 알았는데

정말 단 한 문제도 못 풀어서 너무 답답하고 나 자신에게도 실망스러웠다....

그래서 일주일 동안에 두 문제는 꼭 풀어보자 하고 라이트업 과제를 시작했는데

일주일 내내 틈틈이 푸는데도 한 문제도 겨우 풀었다

도커도 제대로 실행 안 되고... OSINT나 PDF 문제같은 문제도 못 풀겠고....

일주일 내내 빨리 실력을 키워서 이 문제를 언젠간 풀고 싶다는 생각밖에 못했던 것 같다

지금까지 워게임 공부나 문제 풀이를 별로 하지 못했고

있어도 웹 몇 개, 포렌식 한 두 개였기 때문에 어떻게 시작해야 할지도 모르는 문제도 많았다

이제 부족함을 뼈저리게 느꼈으니.... 꾸준히 공부하고 다른 학회원들이 올린 라이트업도 참고해서

이번 학기 내로 이번 3S 문제를 다 풀어보고 싶다

다행히 2학기 강의는 웹해킹 포렌식 강의인 걸로 알고 있으니

열심히 공부하고 따라가서 다음 CTF는 꼭 대회 기간 내에 문제를 풀 수 있었으면 좋겠다