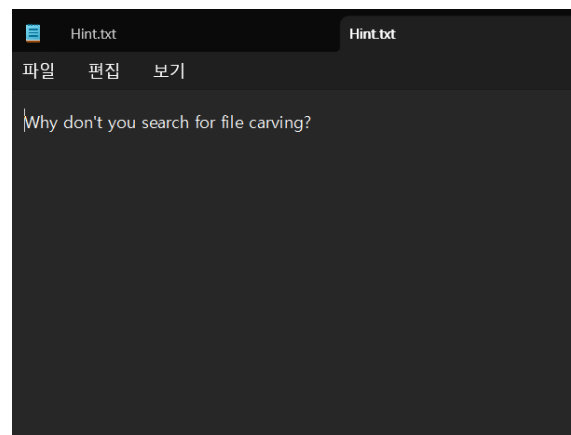


## 2024 3S CTF - BrokenHearted (포렌식) Writeup

32기 김효주

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

Welcome To  
3S CTF!  

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.

```

HxD - [C:\Users\김효주\Downloads\BrokenHearted (2)\CTF.jpg]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)
16 Windows (ANSI) 10진수
CTF.jpg

Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 Decoded text
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00000016 00 00 02 89 00 00 01 F1 08 06 00 00 00 01 4E 26 ...%.ñ.....N&
00000032 10 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 .....sRGB.®í.é...
00000048 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..üa...
00000064 00 09 70 48 59 73 00 00 16 25 00 00 16 25 01 49 ..pHYs...%...%.I
00000080 52 24 F0 00 00 A7 64 49 44 41 54 78 5E ED 9D 07 R$ð...$dIDATx^i...
00000096 98 14 55 DA B6 77 3F D7 35 67 30 47 CC 39 8B 98 ~.UÚqW?×5g0Gİ9<~
00000112 C5 80 09 73 16 03 98 01 13 66 45 C5 2C 06 CC 59 Å€.s...~..fEÄ, .İY
00000128 14 C5 84 09 CC 11 45 C5 80 22 2A 2A 82 39 A1 62 .Ä,,.İ.EÄ€"**,9;b
00000144 0E EB AA 9B CE FF DF AF F3 96 67 AA 7B 66 7A 66 .ë²>İÿB-ó-g²{fzf
00000160 3A 54 77 3F F7 75 9D AB 67 BA AB 2B 9C AA AE F3 :Tw?÷u.«g°«+œ²@ó
00000176 D4 9B CE 5F 82 10 42 08 21 84 10 29 24 12 85 10 Ô>İ_,.B.!..$....
00000192 42 08 21 44 0E 12 89 42 08 21 84 10 22 07 89 44 B.!D..%B.!...".%D
00000208 21 84 10 42 08 91 83 44 A2 10 42 08 21 84 C8 41 !,,.B.`fDc.B.!..EÄ
00000224 22 51 08 21 84 10 42 E4 20 91 28 84 10 42 08 21 "Q.!..Bä `(.B.!
00000240 72 90 48 14 42 08 21 84 10 39 48 24 0A 21 84 10 r.H.B.!..9H$.!...
00000256 42 88 1C 24 12 85 10 42 08 21 44 0E 12 89 42 08 B^.$....B.!D..%B.
00000272 21 84 10 22 07 89 44 21 84 10 42 08 91 83 44 A2 !..".%D!..B.`fDc
00000288 10 42 08 21 84 C8 41 22 51 08 21 84 10 42 E4 20 .B.!..EÄ"Q.!..Bä
00000304 91 28 84 10 42 08 21 72 90 48 14 42 08 21 84 10 `(.B.!r.H.B.!...
00000320 39 48 24 0A 21 84 10 42 88 1C 24 12 85 10 42 08 9H$.!..B^.$....B.
00000336 21 44 0E 12 89 42 08 21 84 10 22 07 89 44 21 84 !D..%B.!...".%D!..
00000352 10 42 08 91 83 44 A2 10 42 08 21 84 C8 41 22 51 .B.`fDc.B.!..EÄ"Q
00000368 08 21 84 10 42 E4 20 91 28 84 10 42 08 21 72 90 .!..Bä `(.B.!r.
00000384 48 14 42 08 21 84 10 39 48 24 0A 21 84 10 42 88 H.B.!..9H$.!..B^
00000400 1C 24 12 85 10 42 08 21 44 0E 12 89 42 08 21 84 .$....B.!D..%B.!..

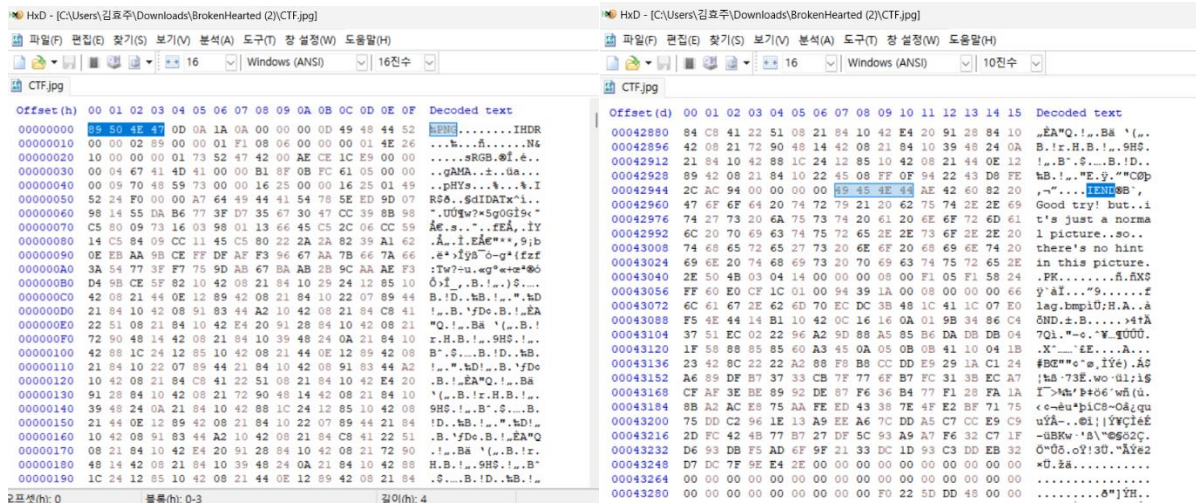
```

여기에서 내가 찾아야 하는 것은 파일 시그니처, 그 중에서도 헤더와 푸터 시그니처를 찾아야 한다.

(푸터 시그니처는 png랑 jpg 파일만 갖고 있다고 함)

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

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



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

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

(이때 IEND 청크는 이미지의 맨 뒤에 위치하는 청크로 PNG 파일의 끝임을 나타냄 -> PNG 파일 이구나 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 시그니처가 뭔지 안 보임 저번에 png랑 jpg랑 시그니처가 같다고 하였던 것 같은데 확실치 않음)

(jpeg는 jpg랑 또 시그니처가 다르더라)

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

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

```
0  ,~"....IENDØB` ,
3  Good try! but..i
1  t's just a norma
0  l picture..so..
3  there's no hint
3  in this picture.
4  .PK.....ñ.ñX$
```

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

그래서 강 뭐라도 하자 싶어서 다른 파일 형식 시그니처가 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 시그니처들을 검색하다 zip 파일 시그니처가 있다는 걸 확인했다!!!!!!

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



HxD - [C:\Users\김호주\Downloads\BrokenHearted (2)\CTF.jpg]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 10진수

CTF.jpg

Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 Decoded text

00167504 14 4C 3E 22 81 59 43 F2 2E 11 9D 4D B9 5C F3 4A .Lp^Yc0...M,\oJ  
00167520 54 05 7D 41 5E 49 26 90 41 90 6B 5E 92 11 90 57 T,1A^I4.A.k^'.W  
00167536 76 69 1A 39 83 47 E2 A4 59 3E 0C 51 FE 7F B8 55 vi.9fgWZ>.Qp..U  
00167552 F5 ED 73 43 5F 8D 05 8E D7 7A B9 0B CA 74 F0 B7 01ac...Zu+Et6-  
00167568 D0 C3 CB FD CC FC A0 6D CB 39 C1 D1 96 BF 44 C6 DkYfu mE5d-DE  
00167584 58 46 71 20 63 F8 61 96 61 91 96 DC 29 CB D0 C8 XFq^caa-a~0(EBE  
00167600 F5 21 DC 08 6E C4 5A 4B 96 EF FC FF 00 50 4B 03 010.nAZK-iuy.Q.  
00167616 0E 14 00 00 00 00 00 23 06 F1 58 DE 79 0B 50 45 .,....#.AXPy.FE  
00167632 F0 00 00 A8 F0 00 00 09 00 00 00 48 69 4E 74 31 0..e8....Hint1  
00167648 2E 6A 70 67 94 58 55 54 1C 0B 12 6E 34 B8 07 77 .jpy^XT.k.e4..w  
00167664 27 48 70 77 1B 9C 04 97 C1 82 DB 0E 2E 21 81 20 'Hpw.e.-d,0A.!.  
00167680 C1 D0 82 BB 0E 7E 71 77 24 D8 E0 01 06 0F AY..i-qu^0A...  
00167696 B9 CB EE 39 2B AF 5B FD D6 D5 A7 FE AF FE B2 AF 'E19+^y00sp^~  
00167712 EB EF D5 BF BF 03 7A 8A CA 8A 00 02 02 02 A0 ei0L.x^SE5....  
00167728 F4 F2 00 7F 6F 00 72 00 2A 32 0A 2A 32 2A 2A 00...o.r.^..2\*\*  
00167744 0A EA AB 57 AB 68 18 78 18 18 E8 E8 18 44 3B B8 .hW^h.x..e8.D8.  
00167760 58 78 24 44 A4 A4 24 44 C4 C4 E4 54 4C 34 E4 14 XsDhwSDAAATL4A.  
00167776 0C 94 C4 C4 B4 1C B4 0C CC 2C 6C 6F D8 C8 68 38 .^A^..i,1o0Eh8  
00167792 B9 39 59 B9 59 D9 5F 69 04 E1 D5 AB 57 18 'y1^XKxy1.a0W.  
00167808 68 18 84 18 18 84 AC E4 C4 84 AC FF B7 FC FD 17 h....nA8-q^0y.  
00167824 80 8F 6E 48 85 78 8E 04 40 F0 20 E2 23 20 E1 23 e..H.x2.S. A# A#  
00167840 FC 3D 08 50 00 00 22 D2 3F D1 FE 57 10 90 90 51 u~.P..^078p...Q  
00167856 10 51 5F BD 28 C9 11 FE A5 04 FE 57 89 F8 A2 45 .Q.h(E.pW.pWu8E  
00167872 FD 7B 1D C0 42 7A 51 E2 21 E1 BD BC F2 66 9F 19 y(L.A0o0A1A0wEY.  
00167888 3C 8D 15 0E 87 A4 39 D7 3F BC 10 B8 6D EC 33 94 <....+m5^7E..n1^~  
00167904 B0 BA 7B 71 98 F8 38 C8 BC 7B DB 97 E3 D1 14 A7 \*(q^m8E+(0~aL.s  
00167920 F1 F0 81 14 8D 04 16 30 07 D0 A4 91 E0 3D 8E 0B h8...^..0.Bh^a2.  
00167936 DA 2E D5 69 4A ED 26 82 2C 44 48 72 AC D8 25 CE 0.0id1.,dHc-0h1  
00167952 FE C9 FD 42 2E 69 5C 8D FB 9D 0D 0F 79 F2 51 04 p8y8.i1.d^Y.y000  
00167968 CE 78 8D 5A FE CB AA 45 49 9A 3D D4 DE 7E 8F 18 fx.2pE^E18=08-...

특수 편집기

데이터 변환기

16진수 (8바이트) 01010000

Int8 인출 80

UInt8 인출 80

Int16 인출 19280

UInt16 인출 19280

Int32 인출 215888

UInt32 인출 215888

Int64 인출 67324752

UInt64 인출 67324752

LEB128 인출 -48

ULEB128 인출 80

AnsiChar / char8\_t P

WideChar / char16\_t P

UTF-8 code point P (U+0050)

Single (float32) 1.5433557799794E-36

Double (float64) 유효하지 않음

CLETIME 유효하지 않음

FILETIME 유효하지 않음

바이트 순서 (Byte Order)

☒ 리틀 엔디언 ☐ 빅 엔디언

☐ 16진수 형식으로 변환 (중수)

체크섬 검색 (3개의 검색 결과)

오브젝트 43041 6E 20 74 68 69 73 20 70 69 63 74 75 72 65 2E 2E 50 4B 03 04 14 00 00 00 08 01 F5 01 5... n this picture.PK.....f.fX\$y  
116102 00 00 01 00 01 00 5A 00 00 00 F5 1C 01 00 00 00 50 4B 03 04 14 00 00 00 08 01 5A 06 F1 ... Z.0..PK.....Z.fX0.  
167613 CB D0 C8 F5 21 DC 08 6E C4 5A 4B 96 EF FC FF 00 50 4B 03 04 14 00 00 00 08 00 23 06 F1 ... EdE0U.nAZK-iuy.QK.....#fXpy

오브젝트(d): 167613 블록(d): 167613-167616 길이(d): 4 영역쓰기

HxD - [C:\Users\김호주\Downloads\BrokenHearted (2)\CTF.jpg]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

16 Windows (ANSI) 10진수

CTF.jpg

Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 Decoded text

00115872 AD DC 15 94 56 D0 1D 28 0E 1C BA 81 D4 26 6D 30 .Ü."Vð.(..°.Ô&m0  
00115888 24 60 9E 7F BB 37 75 13 9D 9C 0F 1E 9C C9 7D 00 \$`z.»7u..æ..æÊ).  
00115904 00 00 00 00 00 00 00 00 00 00 00 00 D8 84 2E A5 DC .....0.....ÿÜ  
00115920 E5 4C B6 78 4D 31 04 FF F0 D9 74 F6 1F BD 5C 7A ãLqxmL.yðÜtö.¼\z  
00115936 FA AA 92 95 62 6E D1 AF 86 BE 97 95 7F EF DB 75 ú^'·bnN~+¼-.iÜu  
00115952 BA B6 5D 48 6E D6 E8 E7 98 AB DE D1 16 9D 8E 72 °qJHnOèç~«pN..Žr  
00115968 79 D2 AD E4 1A AB B5 1F 41 AE CD CC A5 35 77 C3 yO.ä.«µ.A0Íi¥5wÃ  
00115984 41 E3 D7 7C ED 7E 50 4B 01 02 3F 00 14 00 00 00 Aä~|i~PK..?.....  
00116000 08 00 F1 05 F1 58 24 FF 60 E0 CF 1C 01 00 94 39 ..ñ.fX\$y^aI...^9  
00116016 1A 00 08 00 24 00 00 00 00 00 00 00 20 00 00 00 ....\$......  
00116032 00 00 00 00 66 6C 61 67 2E 62 6D 70 0A 00 20 00 ....flag.bmp...  
00116048 00 00 00 00 01 00 18 00 80 D8 F1 78 97 D7 DA 01 .....€0ñx~xÚ.  
00116064 80 D8 F1 78 97 D7 DA 01 00 89 34 B3 49 D7 DA 01 €0ñx~xÚ...¼^I×Ú.  
00116080 50 4B 05 06 00 00 00 00 01 00 01 00 5A 00 00 00 PK.....Z...  
00116096 F5 1C 01 00 00 00 50 4B 03 04 14 00 00 00 08 00 0..PK.....  
00116112 5A 06 F1 58 D3 01 34 28 10 C9 00 00 4E D5 00 00 Z.fX0.4(.Ê..N0..  
00116128 09 00 00 00 48 69 6E 74 32 2E 70 6E 67 D4 5A F7 ...Hint2.pngÔZ÷  
00116144 3B 5B 7F 1B A6 6A D4 56 2B 62 4B 5B B3 88 51 7B ;[...!jÔV+bK[~^Q{  
00116160 94 8A BD A9 0E B3 9A AA 6A 8B A2 88 55 54 28 09 "Š~0.~š^j<^~UT(.  
00116176 4D 51 A3 B6 D8 2D 2D 55 33 B4 76 43 C5 FC 2A 45 MQE90--U3^vCÄü^E  
00116192 6A 27 46 AC D8 23 6F BE EF F5 FE 13 6F AE EB 5C j'F~0#~o^i0p.o0ë\  
00116208 79 CE F9 E1 F3 C3 33 EE FB 7E EE 73 DE D8 58 19 yIüáóÃ3iü~isE0X.  
00116224 B3 33 B3 03 69 68 68 D8 4C 4D 6E D9 D1 D0 5C A8 ^3'.ihh0LMnÜNÜ\^  
00116240 A0 5E 0A 4C 0C D4 27 4E 38 83 0B D4 3F DA 00 3B ^..L.Ô^N8f.Ô?Ü.;  
00116256 63 03 9A EA 41 21 22 F5 E6 A2 D7 4D CB 9B 34 34 c.šêA!"0æc~ME>44  
00116272 5F 52 58 4E 3D F8 A9 F7 97 FC 4C EF 06 D0 D0 F0 RXN=æ0--üI.f.f0A

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

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

(근데 헤더는 3개 나오는데 푸터는 2개 나오네.... 뭘까)

그렇게 찾다가 첫 번째 푸터 시그니처 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

```
.5 35 77 C3 yO.ä.«µ.A@II¥5wA D7 DA 01 €Øñx-×Ú..%4³I×Ú.
4 00 00 00 Aã×|í~PK..?..... 00 00 00 PK.....Z...
1 00 94 39 ..ñ.ñX$ÿ`àĭ..."9 00 08 00 ð.....PK.....
0 00 00 00 .....$. .... D5 00 00 Z.ñXÓ.4(.É..NÕ..
A 00 20 00 ....flag.bmp... D4 5A F7 ....Hint2.pngôZ÷
7 D7 DA 01 .....€Øñx-×Ú. 88 51 7B ;[...!jÔV+bK[³^Q{
9 D7 DA 01 €Øñx-×Ú..%4³I×Ú. 54 28 09 "Š¼@.³š²j<c^UT(.
A 00 00 00 PK.....Z... FC 2A 45 MQ£ŧØ--U3´vCÅü*E
0 00 08 00 ð.....PK..... AE EB 5C j'F-Ø#o%ĩõp.o@ë\
E D5 00 00 Z.ñXÓ.4(.É..NÕ.. D8 58 19 yîùáóÃ3îû~îsßØX.
```

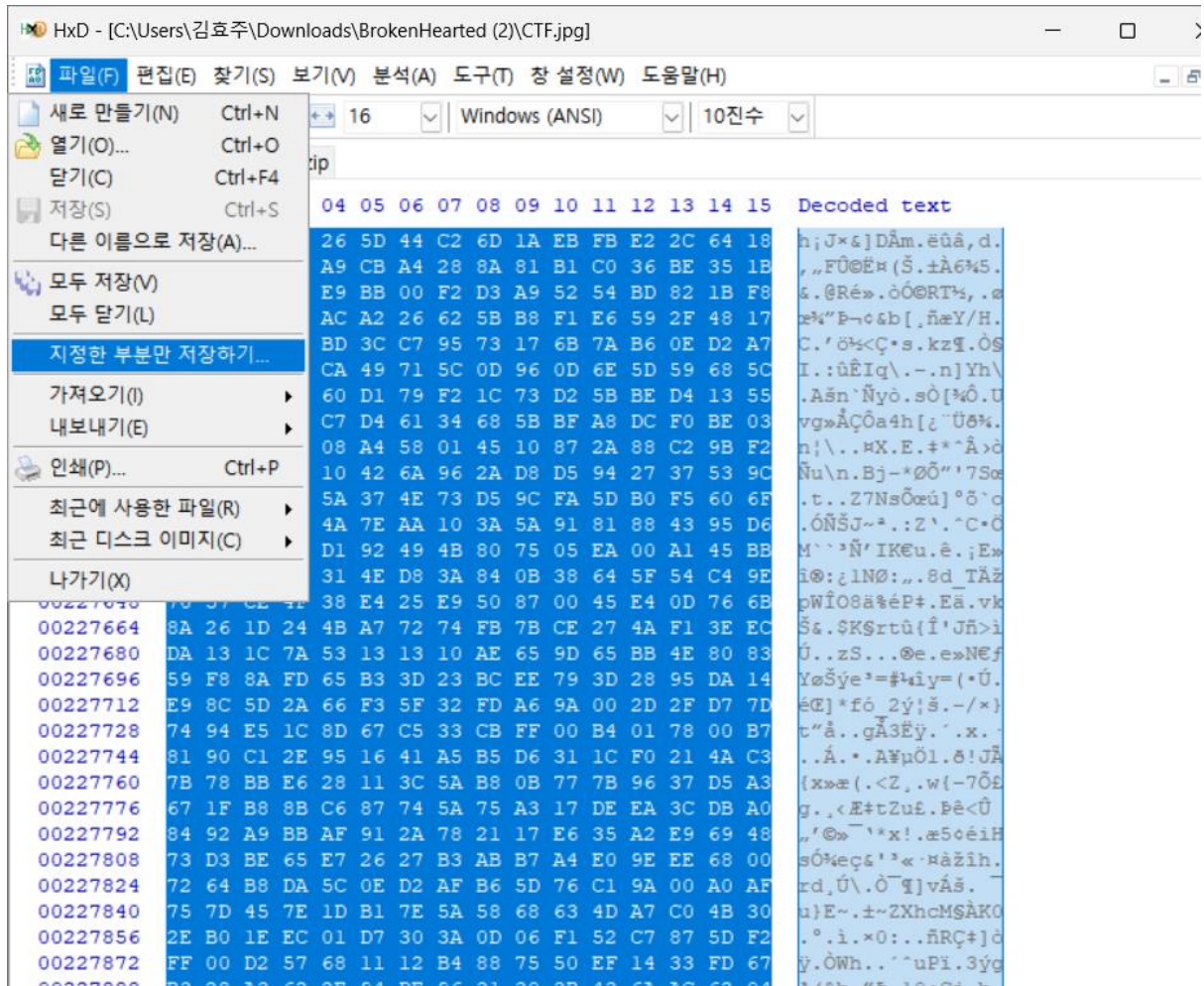
근데 그 zip파일을 어떻게 푸는? 건지 어떻게 찾아내는지?를 모르겠어서 엄청나게 구글링을 했다.

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

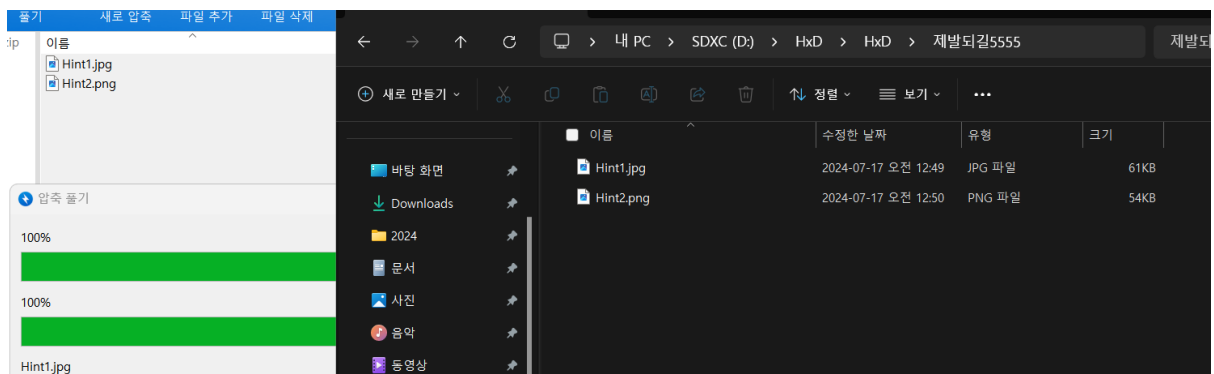
근데 다른 문제도 실패하고 강 하루 뒤에 다시 돌아옴. 피같은 노력 끝에 시력을 포기하고... 방법을 찾아냄!!!!!!!!!!!!!!

zip 파일 추출하는 법

1. zip 파일 헤더 시그니처 찾아내기
2. 거기서부터 끝까지 선택하기
3. 선택한 채로 파일 눌러서 지정한 부분만 저장하기 누르기
4. 이름 적고 .zip 꼭 붙이기 (안 붙이면 안 열림)



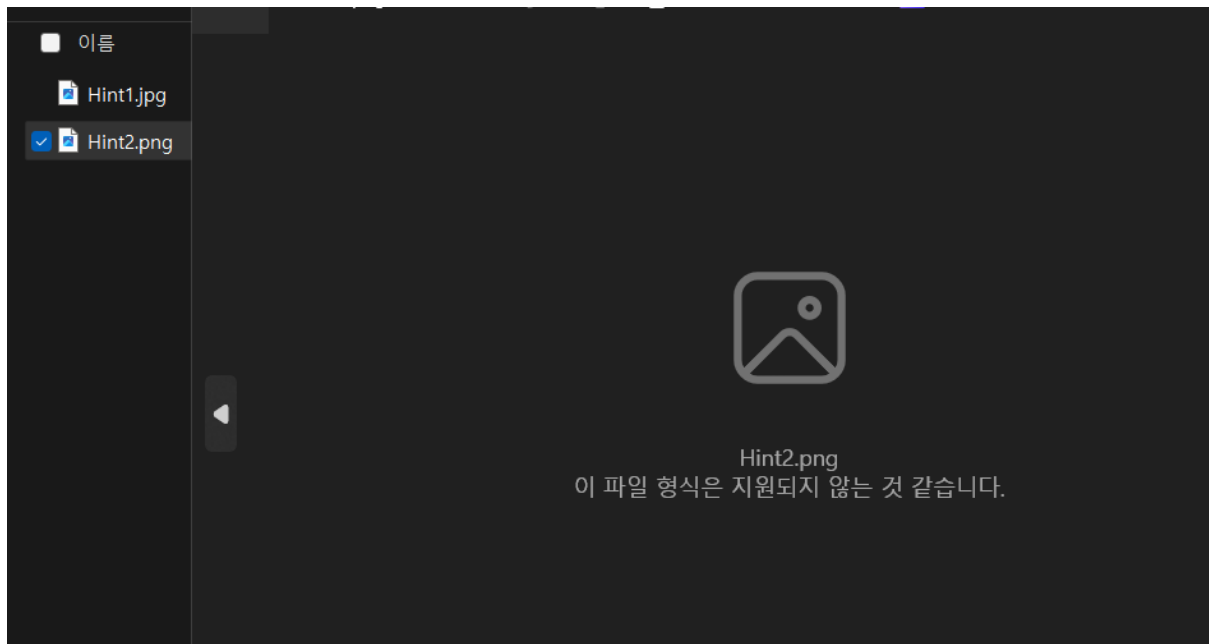
이렇게 해서 생성된 zip 파일을 압축 풀면



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 ㄱㄱ겠쥬 ㄱㄱ아야만 됨



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

```
0000D500 C3 46 AA 31 C6 18 63 8C A9 1C 36 52 8D 31 C6 18  AF=1E.c@.6R.1E.
0000D510 63 4C C5 C8 B2 FF 0F 11 45 4C 17 6D 3C 48 B4 00  cLAE=y..EL.m<H'.
0000D520 00 00 00 49 45 4E 44 AE 42 60 82 57 68 61 74 20  ...IEND@B',What
0000D530 79 6F 75 20 73 68 6F 75 6C 64 20 64 6F 20 69 73  you should do is
0000D540 20 63 6F 6D 62 69 6E 69 6E 67 20 4C 53 42      combining LSB
```

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.....



```

0000F030 6A 7D A6 17 22 B7 A7 8F 43 7E A0 72 E9 00 3B EC j}!."$.C~ ré.;i
0000F040 CA 18 35 06 2C 45 87 CC 58 25 B1 66 05 D3 9F AF È.5.,E+ix%+f.ÓY
0000F050 9C 3D 2E 70 8F 6C F0 9F FF D9 20 4D 61 79 62 69 æ=.p.lôÿÿÙ Maybe
0000F060 2E 2E 79 6F 75 20 63 61 6E 20 73 65 61 72 63 68 ..you can search
0000F070 20 66 6F 72 20 4C 53 42 20 53 74 65 67 61 6E 6F for LSB Stegano
0000F080 67 72 61 70 68 79 2E 2E 61 6E 64 2E 2E 41 6C 77 graphy..and..Alw
0000F090 61 79 73 20 63 68 65 63 6B 20 74 68 65 20 65 6E ays check the en
0000F0A0 64 20 63 61 72 65 66 75 6C 6C 79 d carefully

```

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

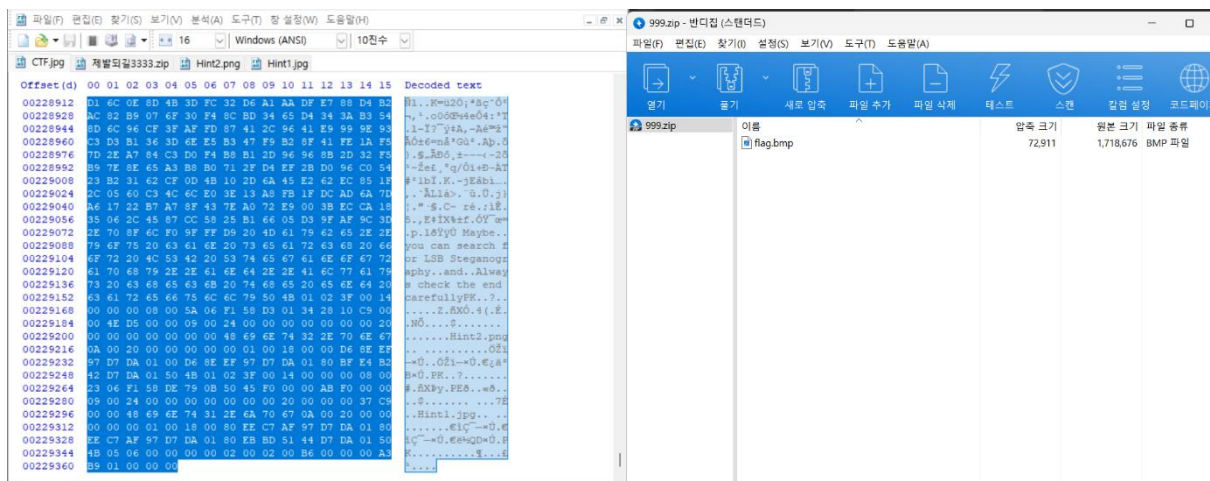
진짜 별 실수를 다 하네요 hint 파일 켜고 zip를 찾으니까 당연히 안되죠...

암튼 중간중간 이상한 실수 많이 하고,...

뭔 손상된 파일이라고 그러고..

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

암튼 그래서 결국 찾아냈다 나의 flag파일.....



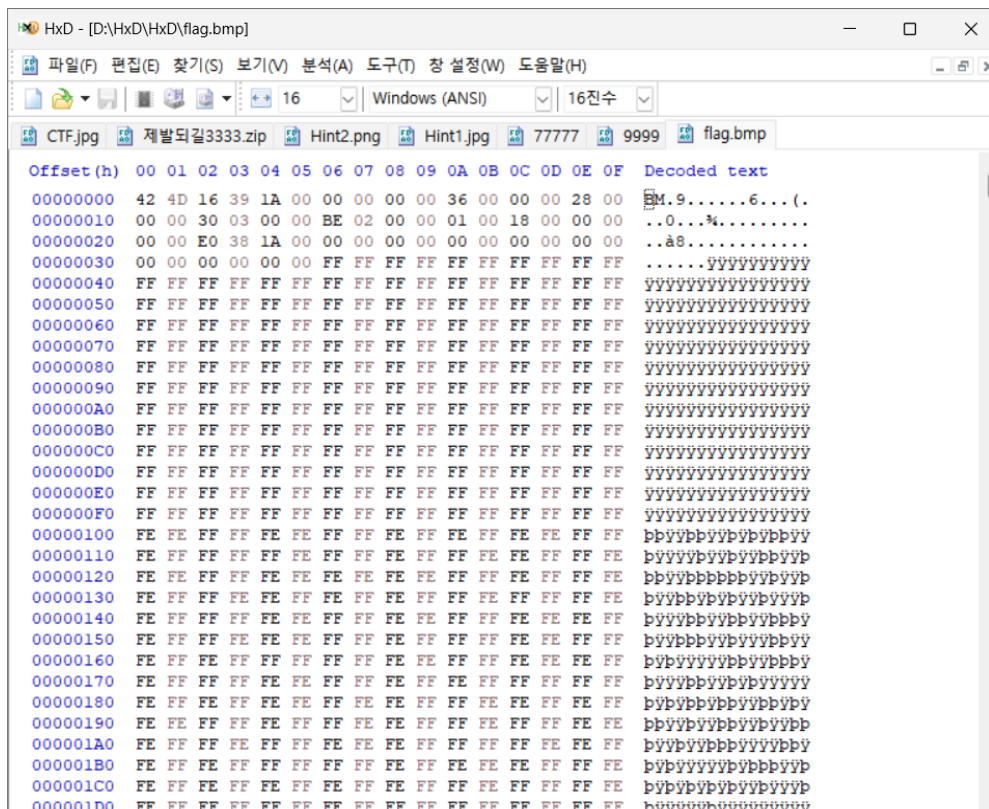
(영 근데 저거 복붙하다 발견한 건데 첫 번째로 깐 zip 안에 있던 힌트 문구 CTF.jpg 안에도 있었네? 당연한 거긴 한데....)

하.... 거의 다 왔다 (아마)

이제 HxD를 사용해서 까보자!!!



...문제가 생김 이게뭐죠?



001A38C0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	FFFFFFFFFFFFFFFF
001A38D0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	FFFFFFFFFFFFFFFF
001A38E0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	FFFFFFFFFFFFFFFF
001A38F0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	FFFFFFFFFFFFFFFF
001A3900	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	FFFFFFFFFFFFFFFF
001A3910	FF FF FF FF FF FF 20 4C 6F 6F 6B 20 61 74 20 74	yyyyyy Look at t
001A3920	68 65 20 64 69 66 66 65 72 65 6E 74 20 48 65 78	he different Hex
001A3930	20 76 61 6C 75 65 73 20 6F 6E 20 6C 69 6E 65 73	values on lines
001A3940	20 30 30 30 30 30 31 30 30 20 74 6F 20 30 30 30	00000100 to 000
001A3950	30 35 30 30 30 2E 20 54 68 65 20 66 6C 61 67 20	05000. The flag
001A3960	62 65 67 69 6E 73 20 77 69 74 68 20 46 45 20 61	begins with FE a
001A3970	6E 64 20 63 6F 6E 73 69 73 74 73 20 6F 66 20 61	nd consists of a
001A3980	20 74 6F 74 61 6C 20 6F 66 20 32 31 36 20 62 79	total of 216 by
001A3990	74 65 73 2E	tes.

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

아 이건가보다 근데 너무 범위가 넓은데?

아 이건가보다 근데 너무 범위가 넓은데?

000000F0	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyyyy
00000100	FE FE FF FF FE FE FF FF FE FE FF FE FE FE FF FE	pyybbbyybbybbyy
00000110	FE FF FF FF FF FE FF FF FE FF FF FE FE FF FF FE	pyyvybvybvbybvy
00000120	FE FE FF FF FE FE FE FE FE FF FF FE FF FF FE FE	bpyybbbbbbbpybvy
00000130	FE FF FF FE FE FF FE FF FE FF FE FF FE FF FF FE	pyybbvybvvybvyyy
00000140	FE FF FF FF FE FE FF FF FE FE FF FF FE FE FE FF	pyyvvbpyvbyvbby
00000150	FE FF FF FE FE FE FE FE FE FE FF FE FF FE FF FE	pyybbbybbybbybby

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.

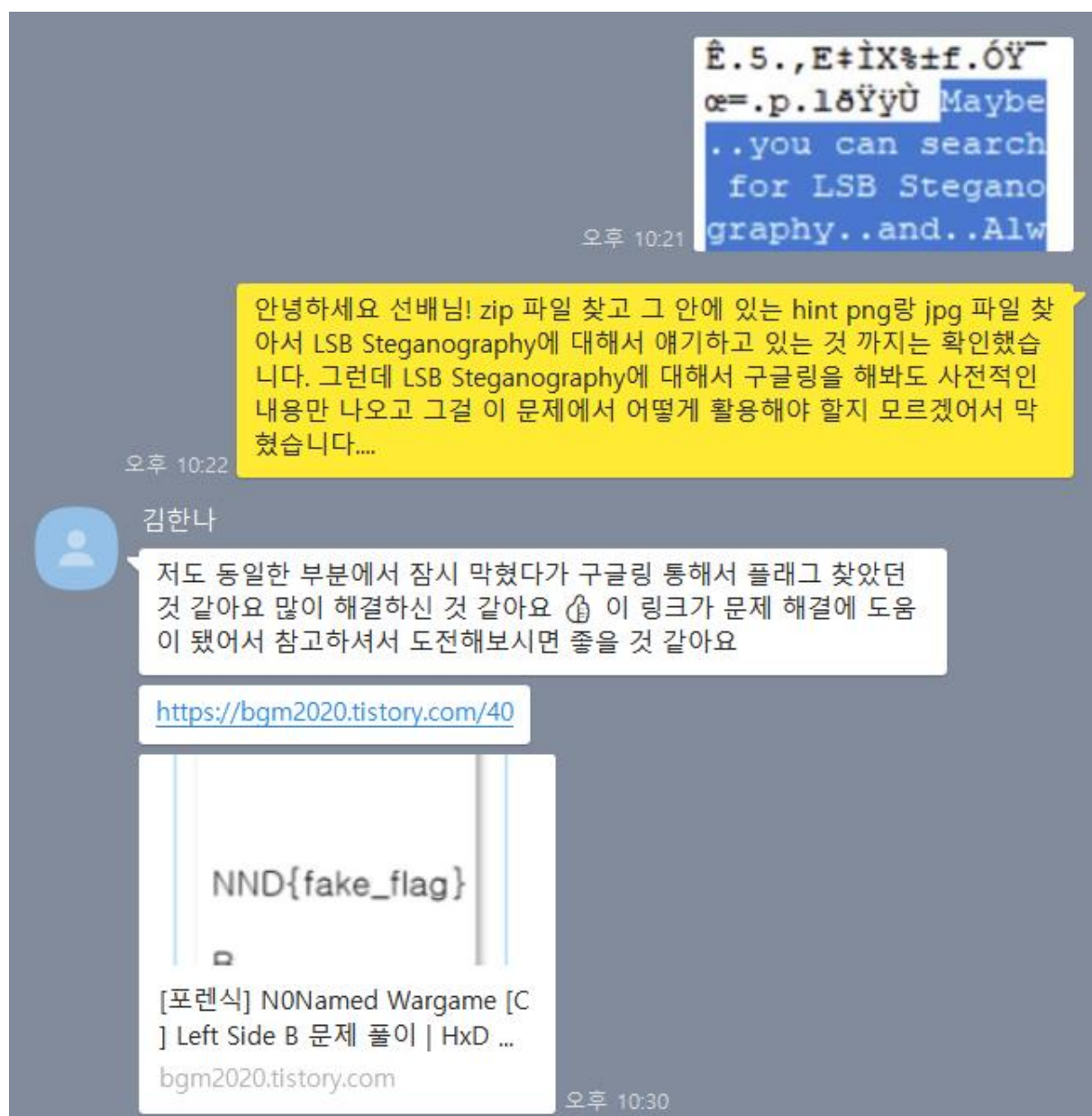
영어 자료만 많고 그것도 논문이나 암호화 방식만 설명한 거라

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....



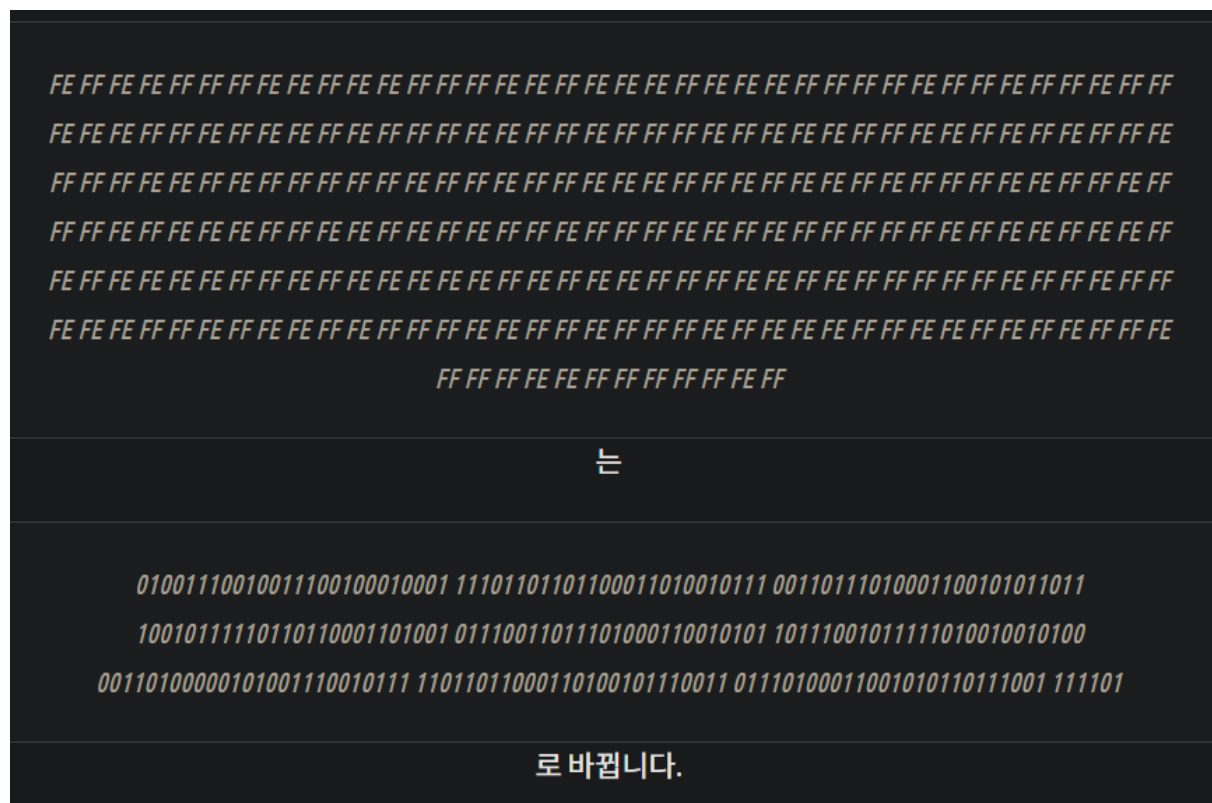
선배님께서!!!!!! 도움이 될만한 링크를 보내주셨다!!!! 다시 감사드립니다.....

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

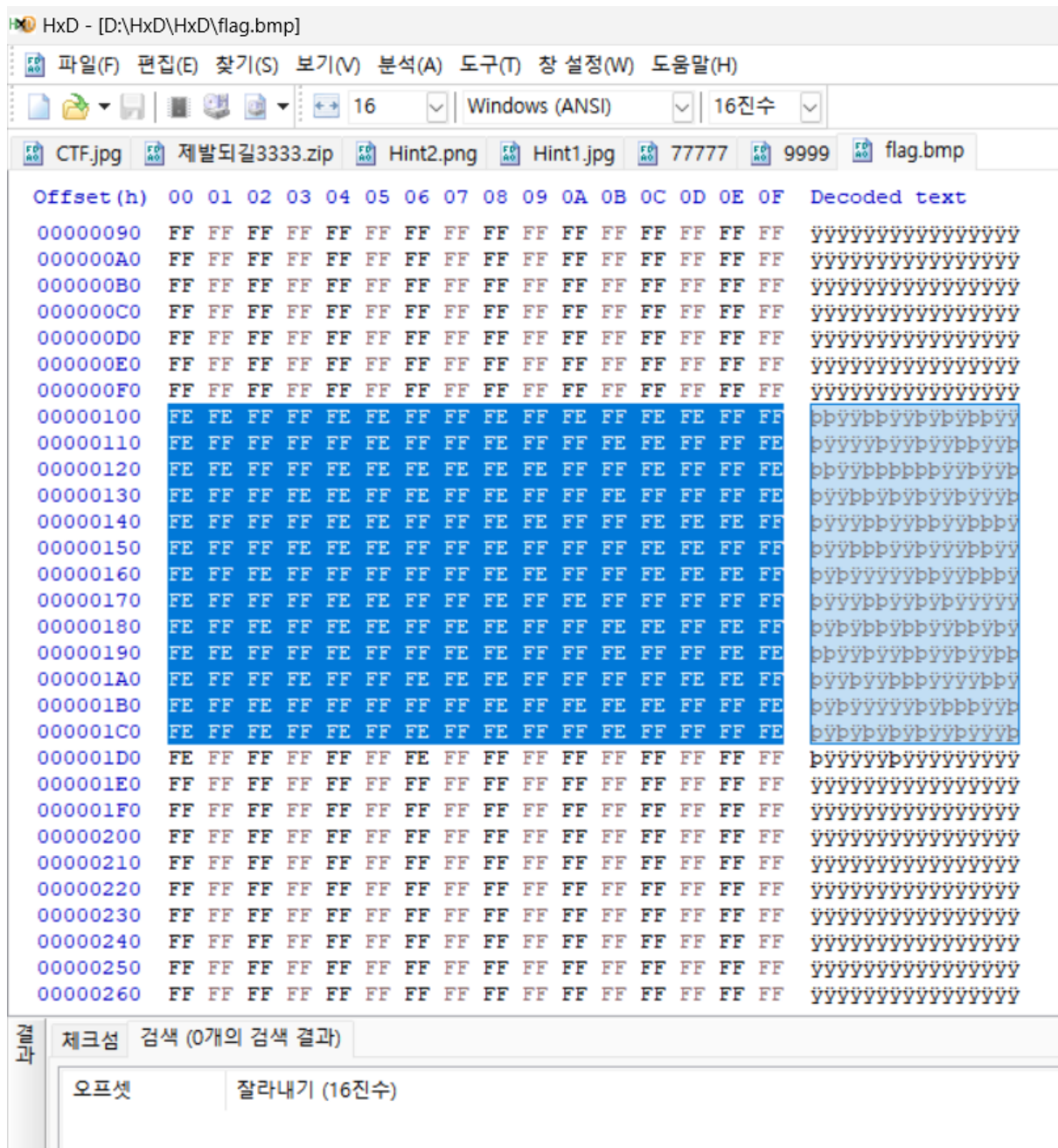


이제 이해했으니까 나도 해보자. 아까 범위가 너무 넓어서 걱정했는데

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 강 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 FF FF FE FF FF FF FE
```

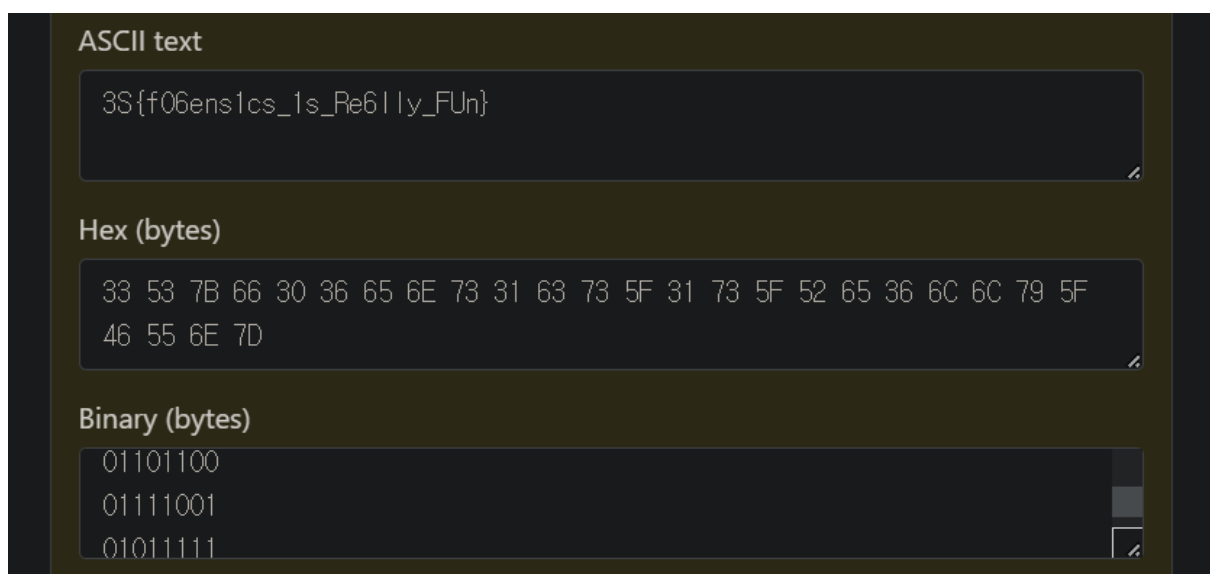
FE FF FF FE FE FF FE FF FE FF FF FE FF FF FF FE  
FE FF FF FF FE FE FF FF FE FE FF FF FE FE FE FF  
FE FF FF FE FE FE FF FF FE FF FF FF FE FE FF FF  
FE FF FE FF FF FF FF FF FE FE FF FF FE FE FE FF  
FE FF FF FF FE FE FF FF FE FF FE FF FF FF FF FF  
FE FF FE FF FE FE FF FE FE FF FF FE FE FF FE FF  
FE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

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..... 이걸 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 톼툼이 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