3S CTF

BrokenHearted:p

```
CTF.png.jpg X
         flag.bmp
                                          0123456789ABCDEF
     2C AC 94 00 00 00 00 49 45 4E 44 AE 42 60 82 20
                                          ,¬"....IEND®B`,
0:A7E0 74 27 73 20 6A 75 73 74 20 61 20 6E 6F 72 6D 61
                                          t's just a norma
0:A7F0 6C 20 70 69 63 74 75 72 65 2E 2E 73 6F 2E 2E 20 1 picture..so..
     74 68 65 72 65 27 73 20 6E 6F 20 68 69 6E 74 20 there's no hint
0:A810 69 6E 20 74 68 69 73 20 70 69 63 74 75 72 65 2E
                                          in this picture.
.PK.....ñ.ñX$
                                         ÿ`àÏ..."9.....f
0:A830 FF 60 E0 CF 1C 01 00 94 39 1A 00 08 00 00 00 66
0:A840 6C 61 67 2E 62 6D 70 EC DC 3B 48 1C
                                41
                                   1C 07 E0
                                          lag.bmpìÜ;H.A..à
0:A860 37 51 EC 02 22 96 A2 9D 88 A5 85 B6 DA DB DB 04
                                          7Qì."-¢.^¥...¶ÚÛÛ.
                                          .X^.....`£E....A...
#BŒ""¢^ø lYé).Á$
     23 42 8C 22 22 A2 88 F8 B8 CC DD E9 29 1A C1 24
0:A890 A6 89 DF B7 37 33 CB 7F 77 6F B7 FC 31 3B EC A7
                                          ¦‰ß·73Ë.wo·ü1;ì§
```

주어진 파일에는 Hint.txt와 CTF.png가 담겨져 있다.

010 Hex Editor을 통해 CTF.png에서 IEND 뒤의 내용을 읽어보았다. 아무래도 png 파일을 이용해 flag를 얻어내는 형태의 문제가 아닌 것 같다는 점을 알게 되었다. CTF.png에서 bmp와 PK에 대한 내용이 나타나있다.



Flag.bmp 형식의 파일을 찾게 되었다. 이때 LSB 스테가노그레피 기법에 대한 힌트가 CTF.png에 주어졌다. 색상 조정을 해봐도 이미지 파일에서 마땅한 플래그를 얻을 수 없어 Hex값을 찾아보기로 했다. Flag.bmp에는 FE로 시작하는 216byte 형태 크기의 플래그를 찾을 수 있다는 문구가 적혀져 있다.

00:0100 bbÿÿbbÿÿbÿbbÿÿb 00:0110 þÿÿÿÿþÿÿþbÿÿþ 00:0120 FE FE FF FF FE FE FE FE FE FE FF FF FE FF FF **þþÿÿþþþþþþÿÿþÿÿþ** 00:0130 FE FF FF FE FF FF FF FF FF FF FF FF FF þÿÿþþÿþÿþÿÿþÿÿÿþ 00:0140 FE FF FF FE FE FF FF FE FE FF þÿÿÿþþÿÿþþþÿ 00:0150 FE FF FF FE FE FE FF FF FE FF FF FF FE þÿÿþþþÿÿþÿÿÿþþÿÿ 00:0160 þÿþÿÿÿÿÿþþÿÿþþþÿ 00:0170 FE FF FF FF FE FF FF FF FF FF FF FF FF þÿÿÿþþÿÿþÿÿÿÿÿ 00:0180 FE FF FE FF FE FE FF FE FE FF FF FE FE FF FE FF þÿþÿþþÿþþÿþþÿþÿ 00:0190 FF FF FE FE FE FE FF FF FE FF FF FE FF FF FE FE þþÿÿþÿÿþþÿÿþþ þÿÿþÿÿþþþÿÿÿÿþþÿ 00:01B0 FE FF FE FF FF FF FF FE FF FE FF FF FF þÿþÿÿÿÿÿþÿþþþÿÿþ 00:01C0 FE FF FE FF FE FF FE FF FE FF FE FF FF FF FE bÿbÿbÿbÿbÿÿbÿÿÿb bÿÿÿÿÿbÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ 00:01F0 FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ

이 CTF 문제에 대해 LSB가 언급된 이유는 bmp파일에서 LSB를 1-2bit 정도 바꿔 사람들이 알 수 없도록 스테가노그래피를 사용한다는 점인데 이를 토대로 FE를 0으로, FF를 1로 생각해 플래그를 해독해보는 방법을 알 수 있게 되었다.

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

많은 데이터를 찾아보다가 FE와 FF가 적절히 섞여있는 216byte 형태의 Hex값을 찾아냈다. 이를 0과 1형태의 이진수를 해독해보면 무엇인가 얻을 수 있겠다고 생각했다. 따라서 ASCII 값으로 변환하는 사이트를 통해 값을 확인했다



3S{f06ens1cs_1s_Re611y_Fun}이라는 플래그를 찾을 수 있게 되었다.