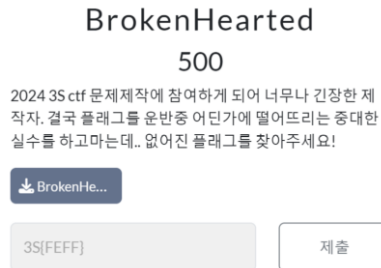


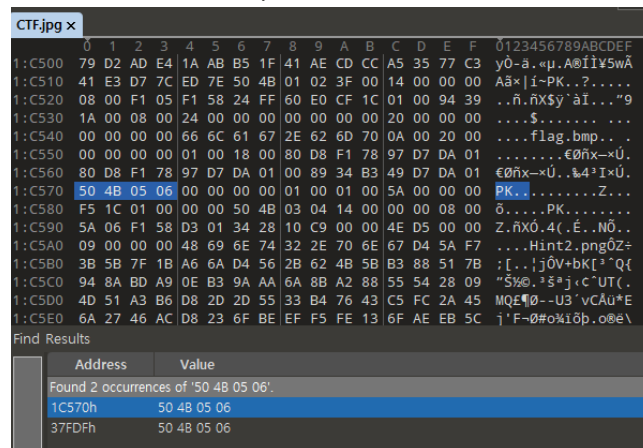
3S CTF

Forensic-BrokenHearted

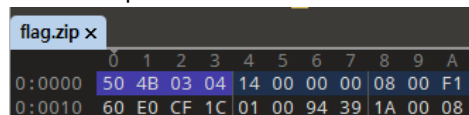
SWING 32 기 한재희



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.

flag.zip	flag.bmp x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1A:3890	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:38F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:3900	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyyyyyy
1A:3910	FF	FF	FF	FF	FF	FF	20	4C	6F	6F	6B	20	61	74	20	74		yyyyyy Look at t
1A:3920	68	65	20	64	69	66	66	65	72	65	6E	74	20	48	65	78		he different Hex
1A:3930	20	76	61	6C	75	65	73	20	6F	6E	20	6C	69	6E	65	73		values on lines
1A:3940	20	30	30	30	30	30	31	30	30	20	74	6F	20	30	30	30		00000100 to 000
1A:3950	30	35	30	30	30	2E	20	54	68	65	20	66	6C	61	67	20		05000. The flag
1A:3960	62	65	67	69	6E	73	20	77	69	74	68	20	46	45	20	61		begins with FE a
1A:3970	6E	64	20	63	6F	6E	73	69	73	74	73	20	6F	66	20	61		nd consists of a
1A:3980	20	74	6F	74	61	6C	20	6F	66	20	32	31	36	20	62	79		total of 216 by
1A:3990	74	65	73	2E														tes._

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 쯤

ED0	35	06	2C	45	87	CC	58	25	B1	66	05	D3	9F	AF	9C	3D	5..E+IX%+f.ÖY~e=
ED0	2E	70	8F	6C	F0	9F	FF	D9	20	4D	61	79	62	65	2E	2E	.p.läYyÜ Maybe..
EE0	79	6F	75	20	63	61	6E	20	73	65	61	72	63	68	20	66	you can search f
EF0	6F	72	20	4C	53	42	20	53	74	65	67	61	6E	6F	67	72	or LSB Steganogr
F00	61	70	68	79	2E	2E	61	6E	64	2E	2E	41	6C	77	61	79	aphy..and..Alway
F10	73	20	63	68	65	63	6B	20	74	68	65	20	65	6E	64	20	s check the end
F20	63	61	72	65	66	75	6C	6C	79	50	4B	01	02	3F	00	14	carefullyPK..?..
F30	00	00	00	08	00	5A	06	F1	58	D3	01	34	28	10	C9	00Z.ñX0.4(.É.
F40	00	4E	D5	00	00	09	00	24	00	00	00	00	00	00	00	20	.NÖ....\$......

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

00:00F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyy
00:0100	FE	FE	FF	FF	FE	FE	FF	FF	FE	FE	FF	FE	FE	FF	FF	FF	FF	byyybyyybyb
00:0110	FE	FF	FF	FF	FF	FE	FF	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0120	FE	FE	FF	FF	FE	FE	FF	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0130	FE	FF	FF	FF	FE	FF	FF	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0140	FE	FF	FF	FF	FE	FE	FF	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0150	FE	FF	FF	FE	FE	FE	FF	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0160	FE	FF	FE	FF	FF	FF	FF	FF	FE	FE	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0170	FE	FF	FF	FF	FE	FE	FF	FF	FE	FF	FE	FE	FF	FF	FF	FF	FE	byyybyyybyb
00:0180	FE	FF	FE	FF	FF	FE	FF	FF	FE	FF	FE	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:0190	FE	FE	FF	FF	FE	FF	FF	FE	FE	FF	FE	FE	FF	FF	FF	FE	FE	byyybyyybyy
00:01A0	FE	FF	FF	FE	FF	FF	FE	FF	FE	FF	FF	FE	FF	FF	FF	FF	FE	byyybyyybyy
00:01B0	FE	FF	FE	FF	FF	FF	FF	FF	FE	FF	FE	FE	FF	FF	FF	FE	FE	byyybyyybyb
00:01C0	FE	FF	FE	FF	FE	FF	FF	FF	FE	FF	FF	FE	FF	FF	FF	FE	FE	byyybyyybyy
00:01D0	FE	FF	FF	FF	FF	FF	FF	FF	FE	FF	FF	FF	FF	FF	FF	FF	FE	byyybyyybyy
00:01E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	yyyyyyyyyyyy

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 바뀌어서 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}