<Broken Hearted>

파일을 열어봤다.

힌트를 열어봤다.

Why don't you search for file carving?

파일 카빙?

일단 ctf 사진 파일을 헥사 에디터로 열어봤다.

CTF.jpg

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG........IHDR
00000010	00	00	02	89	00	00	01	F1	08	06	00	00	00	01	4E	26	...‰...ñ......N&
00000020	10	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	.....sRGB.®Î.é..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA..±..üa...
00000040	00	09	70	48	59	73	00	00	16	25	00	00	16	25	01	49	..pHYs...%...%.I
00000050	52	24	F0	00	00	A7	64	49	44	41	54	78	5E	ED	9D	07	R$ð..§dIDATx^i..
00000060	98	14	55	DA	B6	77	3F	D7	35	67	30	47	CC	39	8B	98	˜.UÚ¶w?×5g0GÌ9‹˜
00000070	C5	80	09	73	16	03	98	01	13	66	45	C5	2C	06	CC	59	Å€.s..˜..fEÅ,.ÌY
00000080	14	C5	84	09	CC	11	45	C5	80	22	2A	2A	82	39	A1	62	.Å„.Ì.EÅ€"**‚9¡b

헤더 시그니처에는 문제가 없다.

천천히 살펴보다 보니 문장이 정리되어 있는 것을 발견

```
00037ED0  2E 70 8F 6C F0 9F FF D9 20 4D 61 79 62 65 2E 2E  .p.lðŸÿÙ Maybe..
00037EE0  79 6F 75 20 63 61 6E 20 73 65 61 72 63 68 20 66  you can search f
00037EF0  6F 72 20 4C 53 42 20 53 74 65 67 61 6E 6F 67 72  or LSB Steganogr
00037F00  61 70 68 79 2E 2E 61 6E 64 2E 2E 41 6C 77 61 79  aphy..and..Alway
00037F10  73 20 63 68 65 63 6B 20 74 68 65 20 65 6E 64 20  s check the end
00037F20  63 61 72 65 66 75 6C 6C 79 50 4B 01 02 3F 00 14  carefullyPK..?..
```

이 사진 파일에 다른 파일도 같이 들어있는 것 같다. 그러면 압축 파일인가?

```
00037F50  00 00 00 00 00 00 00 48 69 6E 74 32 2E 70 6E 67  .......Hint2.png
00037FB0  00 00 48 69 6E 74 31 2E 6A 70 67 0A 00 20 00 00  ..Hint1.jpg.. ..
```

압축 파일 헤더가 있는지 확인해보려고 단축키 검색으로 pk를 검색해봤다.

생각보다 많다.

```
00037FD0  EE C7 AF 97 D7 DA 01 80 EB BD 51 44 D7 DA 01 50  îÇ¯—×Ú.€ë½QD×Ú.P
00037FE0  4B 05 06 00 00 00 00 02 00 02 00 B6 00 00 00 A3  K..........¶...£
```

```
00037F20  63 61 72 65 66 75 6C 6C 79 50 4B 01 02 3F 00 14  carefullyPK..?..
```

압축 파일 헤더 시그니처와 푸터 시그니처 각각 2개씩 찾아서 따른 자료로 새롭게 저장해봤다.

HxD - [C:\Users\kimye\OneDrive\바탕 화면\BrokenHearted (1)\CTF.jpg]

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

16 | Windows (ANSI) | 16진수

CTF.jpg

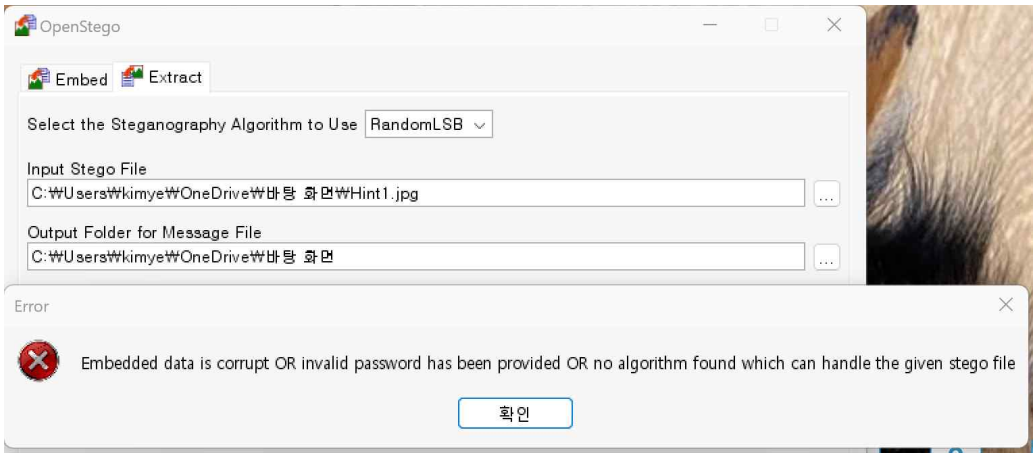
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000A800	74	68	65	72	65	27	73	20	6E	6F	20	68	69	6E	74	20	there's no hint
0000A810	69	6E	20	74	68	69	73	20	70	69	63	74	75	72	65	2E	in this picture.
0000A820	2E	50	4B	03	04	14	00	00	00	08	00	F1	05	F1	58	24	.PK.....ñ.ñX$
0000A830	FF	60	E0	CF	1C	01	00	94	39	1A	00	08	00	00	00	66	ÿ`àÏ...”9.....f
0000A840	6C	61	67	2E	62	6D	70	EC	DC	3B	48	1C	41	1C	07	E0	lag.bmpìÜ;H.A..à
0000A850	F5	4E	44	14	B1	10	42	0C	16	16	0A	01	9B	34	86	C4	õND.±.B.....›4†Ä
0000A860	37	51	EC	02	22	96	A2	9D	88	A5	85	B6	DA	DB	DB	04	7Qì."–¢.ˆ¥…¶ÚÛÛ.
0000A870	1F	58	88	85	85	60	A3	45	0A	05	0B	0B	41	10	04	1B	.Xˆ……`£E....A...
0000A880	23	42	8C	22	22	A2	88	F8	B8	CC	DD	E9	29	1A	C1	24	#BŒ""¢ˆø¸ÌÝé).Á$
0000A890	A6	89	DF	B7	37	33	CB	7F	77	6F	B7	FC	31	3B	EC	A7	¦‰ß·73Ë.wo·ül;ì§
0000A8A0	CF	AF	3E	BE	89	92	DE	87	F6	36	B4	77	F1	28	FA	1A	Ï¯>¾‰’Þ‡ö6´wñ(ú.
0000A8B0	8B	A2	AC	E8	75	AA	FE	ED	43	38	7E	4F	E2	BF	71	75	‹¢¬èuªþíC8~Oâ¿qu
0000A8C0	75	DD	C2	96	1E	13	A9	EE	A6	7C	DD	A5	C7	CC	E9	C9	uÝÂ–..©î¦|Ý¥ÇÌéÉ
0000A8D0	2D	FC	42	4B	77	B7	27	DF	5C	93	A9	A7	F6	32	C7	1F	–üBKw·'ß\“©§ö2Ç.
0000A8E0	D6	93	DB	F5	AD	6F	9F	21	33	DC	1D	93	C3	DD	EB	32	Ö“Ûõ.oŸ!3Ü.“ÃÝë2
0000A8F0	D7	DC	7F	9E	E4	2E	00	00	00	00	00	00	00	00	00	00	×Ü.žä..........
0000A900	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000A910	00	00	00	00	00	00	00	00	00	F0	22	5D	DD	48	00	00	.........ð"]ÝH..
0000A920	F0	6F	3C	16	B7	D2	75	79	0C	00	00	00	00	1E	CE	9B	ðo<.·Òuy......Î›
0000A930	25	00	00	78	0E	67	67	67	47	47	47	FB	FB	FB	BB	BB	%..x.gggGGGûûû»»
0000A940	BB	3F	52	76	76	76	BE	A7	84	9D	50	3F	39	39	B9	BC	»?Rvvv¾§„.P?99¹¼
0000A950	BC	4C	00	00	F0	7C	42	06	3B	38	38	D8	DC	DC	5C	5D	¼L..ð|B.;88ØÜÜ\]
0000A960	5D	5D	58	58	98	9D	9D	9D	9A	9A	9A	98	98	18	1F	1F	]]XX˜...šššš˜˜...
0000A970	1F	1B	1B	1B	19	19	F9	92	32	3A	3A	1A	EA	73	73	73	......ù’2::.êsss
0000A980	CB	CB	CB	1B	1B	1B	21	AA	1D	1F	1F	5F	5C	5C	24	00	ËËË...!ª..._\\$.
0000A990	00	F8	53	21	4D	ED	ED	ED	AD	AC	AC	4C	4F	4F	0F	0D	.øS!Mííí.¬¬LOO..
0000A9A0	0D	F5	F6	F6	76	74	74	B4	B4	B4	34	37	37	37	34	34	.õöövtt´´´477744
0000A9B0	D4	D7	D7	D7	D5	D5	D5	D4	D4	54	57	57	57	55	55	D5	Ô×××ÕÕÕÔÔTWWWUUÕ
0000A9C0	D6	D6	86	7A	5B	5B	5B	77	77	F7	C0	C0	40	48	68	F3	ÖÖ†z[[[ww÷ÀÀ@Hhó
0000A9D0	F3	F3	EB	EB	EB	87	87	87	09	00	00	7E	D3	E9	E9	E9	óóëëë‡‡‡...~Óééé
0000A9E0	D6	D6	D6	E2	E2	62	98	FE	EA	EB	EB	6B	6D	6D	AD	AC	ÖÖÖââb˜þêëëkmm.¬
0000A9F0	AC	2C	2D	2D	2D	2A	2A	CA	CF	CF	CF	C9	C9	C9	CE	CE	¬,---**ÊÏÏÏÉÉÉÎÎ

바탕화면에 이런 파일이 생성됐다.

확장자를 7z로 바꾸어 주니 압축 파일이 나타났다.

열어보니 2개의 사진이 나왔다.

사진을 open stego로 분석해보려고 했는데 오류가 떠서 안된다.



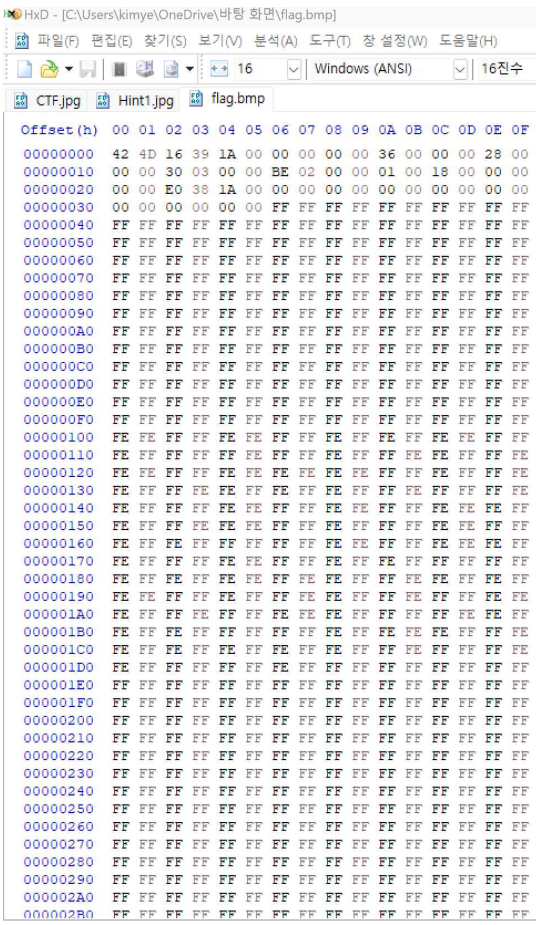
그래서 헥사 에디터로 열어봤다.

이런 문장이 담겨 있다.

```
0000F050  9C 3D 2E 70 8F 6C F0 9F FF D9 20 4D 61 79 62 65  œ=.p.lðŸÿÙ 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

001A3910  FF FF FF FF FF FF 20 4C 6F 6F 6B 20 61 74 20 74  ÿÿÿÿÿÿ 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 전체적으로 똑같은 게 반복되는 게 규칙이 있을 것 같다.



계속 FF이다가 중간에 FF와 FE가 교차 되는 부분이 있다.

```
00000100  FE FE FF FF FE FE FF FF FE FF FE FF FE FE FF FF  þþÿÿþþÿÿþÿþÿþþÿÿ
00000110  FE FF FF FF FF FE FF FF FE FF FF FE FE FF FF FE  þÿÿÿÿþÿÿþÿÿþþÿÿþ
00000120  FE FE FF FF FE FE FE FE FE FE FF FF FE FF FF FE  þþÿÿþþþþþþÿÿþÿÿþ
00000130  FE FF FF FE FE FF FE FF FE FF FF FE FF FF FF FE  þÿÿþþÿþÿþÿÿþÿÿÿþ
00000140  FE FF FF FF FE FE FF FF FE FE FF FF FE FE FE FF  þÿÿÿþþÿÿþþÿÿþþþÿ
00000150  FE FF FF FE FE FE FF FF FE FF FF FF FE FE FF FF  þÿÿþþþÿÿþÿÿÿþþÿÿ
00000160  FE FF FE FF FF FF FF FF FE FE FF FF FE FE FE FF  þÿþÿÿÿÿÿþþÿÿþþþÿ
00000170  FE FF FF FF FE FE FF FF FE FF FE FF FF FF FF FF  þÿÿÿþþÿÿþÿþÿÿÿÿÿ
00000180  FE FF FE FF FE FE FF FE FE FF FF FE FE FF FE FF  þÿþÿþþÿþþÿÿþþÿþÿ
00000190  FE FE FF FF FE FF FF FE FE FF FF FE FF FF FE FE  þþÿÿþÿÿþþÿÿþÿÿþþ
000001A0  FE FF FF FE FF FF FE FE FE FF FF FF FF FE FE FF  þÿÿþÿÿþþþÿÿÿÿþþÿ
000001B0  FE FF FE FF FF FF FF FF FE FF FE FE FE FF FF FE  þÿþÿÿÿÿÿþÿþþþÿÿþ
000001C0  FE FF FE FF FE FF FE FF FE FF FF FE FF FF FF FE  þÿþÿþÿþÿþÿÿþÿÿÿþ
000001D0  FE FF FF FF FF FF FE FF FF FF FF FF FF FF FF FF  þÿÿÿÿÿþÿÿÿÿÿÿÿÿÿ
```

2진수로 치환하면 되는건가?