[Forensic] so easy?

파일을 열어보니 이런 사진 한장이 달랑 있다. 어쩌라는 건지 모르겠다 난 포렌식 해본 적이 없다.

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/cc15f26f-4e98-4d3f-817f-747b5c5618d8/CTF가이드_Forensics.pdf

포렌식 문제를 풀기위한 정보를 잘 정리한 가이드를 찾았다! 감사합니다

배경: 파일 시그니처

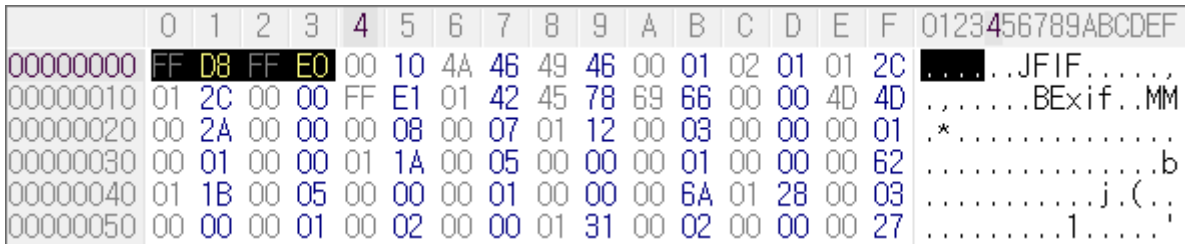
자동등록방지를 위해 보안절차를 거치고 있습니다.

http://forensic-proof.com/archives/300

모든 파일은 파일 포맷별로 고유한 포맷을 가지고 있다. 이러한 포맷의 기본이 되는 내용이 **파일 시그니처**이다.

파일의 가장 처음에 위치하는 특정 바이트들은 파일 포맷을 구분하기 위해 사용한다.

예들들어 jpeg 파일은 “FF D8 FF E0” 혹은 “FF D8 FF E1” 시그너처를 사용한다.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	01	2C	....JFIF.....,
00000010	01	2C	00	00	FF	E1	01	42	45	78	69	66	00	00	4D	4D	.,....BExif..MM
00000020	00	2A	00	00	00	08	00	07	01	12	00	03	00	00	00	01	.*..............
00000030	00	01	00	00	01	1A	00	05	00	00	00	01	00	00	00	62	.............b
00000040	01	1B	00	05	00	00	00	01	00	00	00	6A	01	28	00	03	.........j.(..
00000050	00	00	00	01	00	02	00	00	01	31	00	02	00	00	00	27	.........1....'

제일 앞부분에 jpeg 파일의 시그니처를 확인할 수 있다.

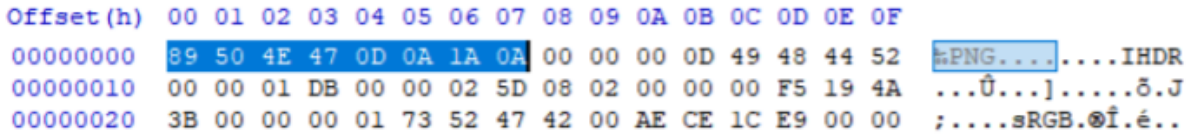
파일 시그니처는 보통 파일의 첫부분 혹은 파일의 마지막에 존재한다.

파일의 처음에 존재하는 시그니처를 **Header 시그니처**, 마지막에 존재하는 시그니처를 **Footer 시그니처**라 부른다.

*파일에는 png와 jpg 파일만 footer 시그니처를 가지고 있다고 적혀있는데 검색해 보니 다른 파일도 푸터 시그니처를 가지고 있는거 같다... (?)

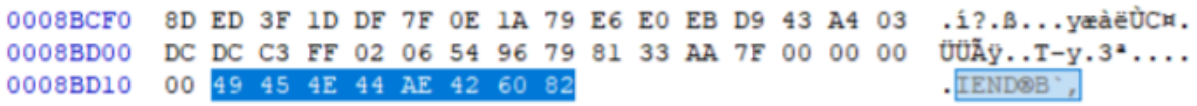
File Type	Header Signature(Hex)	Footer Signature(Hex)
JPEG	FF D8 FF E0 FF D8 FF E8	FF D9
GIF	47 49 46 38 37 61 47 49 46 38 39 61	00 3B
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
PDF	25 50 44 46 2D 31 2E	25 25 45 4F 46
ZIP	50 4B 03 04	50 4B 05 06
ALZ	41 4C 5A 01	43 4C 5A 02
RAR	52 61 72 21 1A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

예를 들어 png 파일을 열어봤을 때,



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG....IHDR
00000010	00	00	01	DB	00	00	02	5D	08	02	00	00	00	F5	19	4A	...Û...]....õ.J
00000020	3B	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	;....sRGB.®Î.é..

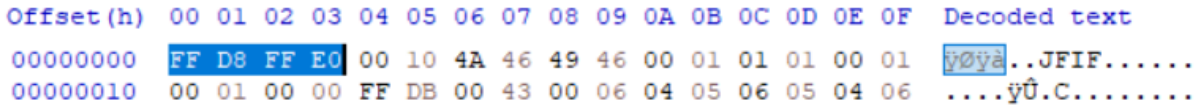
png의 헤더 시그니처인 89 50 4E 47 0D 0A 1A 0A를 확인할 수 있으며



0008BCF0	8D	ED	3F	1D	DF	7F	0E	1A	79	E6	E0	EB	D9	43	A4	03	.í?.ß...yæàëÙC¤.
0008BD00	DC	DC	C3	FF	02	06	54	96	79	81	33	AA	7F	00	00	00	ÜÜÃÿ..T-y.3ª....
0008BD10	00	49	45	4E	44	AE	42	60	82								.IEND®B`,

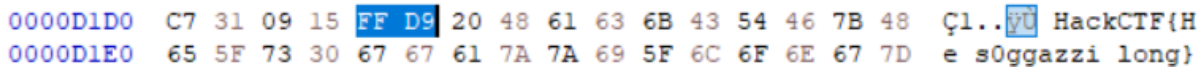
png의 푸터 시그니처인 49 45 4E 44 AE 42 60 82 또한 확인할 수 있다.

문제풀이



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	43	00	06	04	05	06	05	04	06	....ÿÛ.C.....

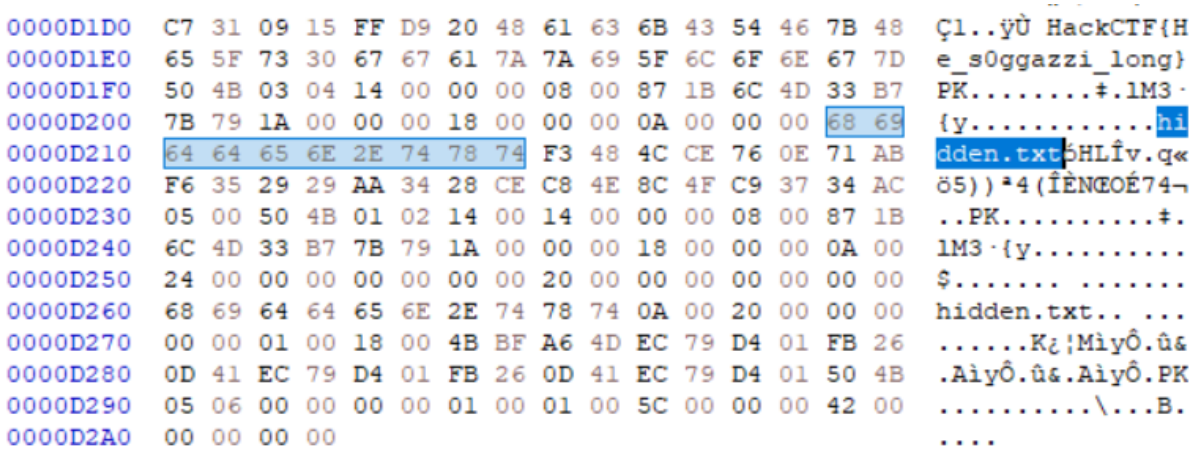
HxD로 열어봤을때 jpg파일의 헤더 시그니처를 확인할 수 있다.



0000D1D0	C7	31	09	15	FF	D9	20	48	61	63	6B	43	54	46	7B	48	Ç1..ÿÙ HackCTF{H
0000D1E0	65	5F	73	30	67	67	61	7A	7A	69	5F	6C	6F	6E	67	7D	e_s0ggazzi_long}

푸터 시그니처도 확인 가능하다.

(저 플래그는 오답뜸.....)



0000D1D0	C7	31	09	15	FF	D9	20	48	61	63	6B	43	54	46	7B	48	Ç1..ÿÙ HackCTF{H
0000D1E0	65	5F	73	30	67	67	61	7A	7A	69	5F	6C	6F	6E	67	7D	e_s0ggazzi_long}
0000D1F0	50	4B	03	04	14	00	00	00	08	00	87	1B	6C	4D	33	B7	PK.....‡.lM3·
0000D200	7B	79	1A	00	00	00	18	00	00	00	0A	00	00	00	68	69	{y.....hi
0000D210	64	64	65	6E	2E	74	78	74	F3	48	4C	CE	76	0E	71	AB	dden.txtóHLÎv.q«
0000D220	F6	35	29	29	AA	34	28	CE	C8	4E	8C	4F	C9	37	34	AC	ö5))ª4(ÎÈNŒOÉ74¬
0000D230	05	00	50	4B	01	02	14	00	14	00	00	00	08	00	87	1B	..PK.....‡.
0000D240	6C	4D	33	B7	7B	79	1A	00	00	00	18	00	00	00	0A	00	lM3·{y.....
0000D250	24	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	$..... .....
0000D260	68	69	64	64	65	6E	2E	74	78	74	0A	00	20	00	00	00	hidden.txt.. ...
0000D270	00	00	01	00	18	00	4B	BF	A6	4D	EC	79	D4	01	FB	26	.....K¿¦MìyÔ.û&
0000D280	0D	41	EC	79	D4	01	FB	26	0D	41	EC	79	D4	01	50	4B	.AìyÔ.û&.AìyÔ.PK
0000D290	05	06	00	00	00	00	01	00	01	00	5C	00	00	00	42	00	.....\...B.
0000D2A0	00	00	00	00													....

그보다 더 아래에 hidden.txt라고 적혀있는 것들이 보인다.

```
0000D1D0  C7 31 09 15 FF D9 20 48 61 63 6B 43 54 46 7B 48  Ç1..ÿÙ HackCTF{H
0000D1E0  65 5F 73 30 67 67 61 7A 7A 69 5F 6C 6F 6E 67 7D  e_s0ggazzi_long}
0000D1F0  50 4B 03 04 14 00 00 00 08 00 87 1B 6C 4D 33 B7  PK..........‡.lM3·
0000D200  7B 79 1A 00 00 00 18 00 00 00 0A 00 00 00 68 69  {y.............hi
0000D210  64 64 65 6E 2E 74 78 74 F3 48 4C CE 76 0E 71 AB  dden.txtóHLÎv.q«
0000D220  F6 35 29 29 AA 34 28 CE C8 4E 8C 4F C9 37 34 AC  ö5))ª4(ÎÈNŒOÉ74¬
0000D230  05 00 50 4B 01 02 14 00 14 00 00 00 08 00 87 1B  ..PK..........‡.
0000D240  6C 4D 33 B7 7B 79 1A 00 00 00 18 00 00 00 0A 00  lM3·{y..........
0000D250  24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00  $.......  .......
0000D260  68 69 64 64 65 6E 2E 74 78 74 0A 00 20 00 00 00  hidden.txt..  ...
0000D270  00 00 01 00 18 00 4B BF A6 4D EC 79 D4 01 FB 26  ......K¿¦MìyÔ.û&
0000D280  0D 41 EC 79 D4 01 FB 26 0D 41 EC 79 D4 01 50 4B  .AìyÔ.û&.AìyÔ.PK
0000D290  05 06 00 00 00 00 01 00 01 00 5C 00 00 00 42 00  ..........\...B.
0000D2A0  00 00 00 00                                      ....
```

zip파일의 헤더 시그니처도 찾을 수 있었다

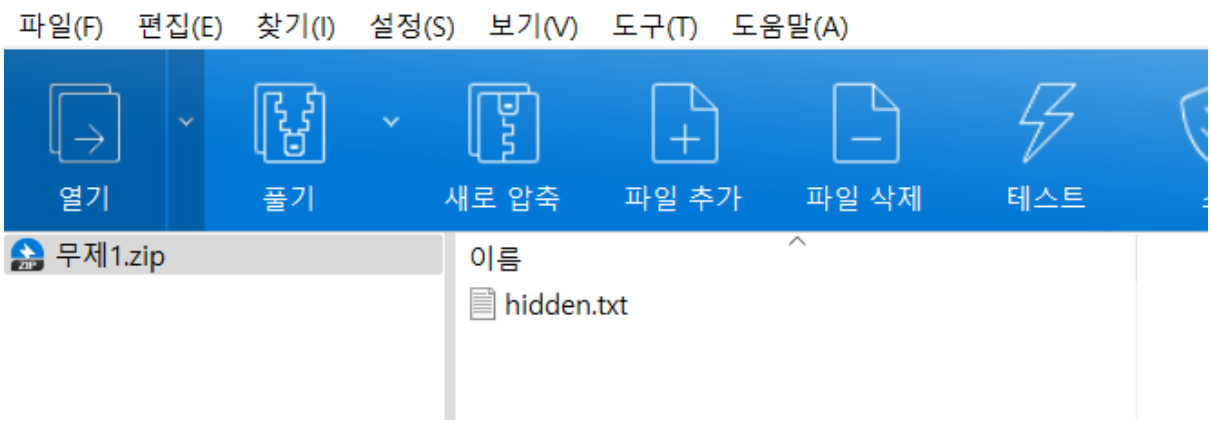
```
0000D1D0  C7 31 09 15 FF D9 20 48 61 63 6B 43 54 46 7B 48  Ç1..ÿÙ HackCTF{H
0000D1E0  65 5F 73 30 67 67 61 7A 7A 69 5F 6C 6F 6E 67 7D  e_s0ggazzi_long}
0000D1F0  50 4B 03 04 14 00 00 00 08 00 87 1B 6C 4D 33 B7  PK........‡.lM3·
0000D200  7B 79 1A 00 00 00 18 00 00 00 0A 00 00 00 68 69  {y.............hi
0000D210  64 64 65 6E 2E 74 78 74 F3 48 4C CE 76 0E 71 AB  dden.txtóHLÎv.q«
0000D220  F6 35 29 29 AA 34 28 CE C8 4E 8C 4F C9 37 34 AC  ö5))ª4(ÎÈNŒOÉ74¬
0000D230  05 00 50 4B 01 02 14 00 14 00 00 00 08 00 87 1B  ..PK..........‡.
0000D240  6C 4D 33 B7 7B 79 1A 00 00 00 18 00 00 00 0A 00  lM3·{y..........
0000D250  24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00  $.......  .......
0000D260  68 69 64 64 65 6E 2E 74 78 74 0A 00 20 00 00 00  hidden.txt..  ...
0000D270  00 00 01 00 18 00 4B BF A6 4D EC 79 D4 01 FB 26  ......K¿¦MìyÔ.û&
0000D280  0D 41 EC 79 D4 01 FB 26 0D 41 EC 79 D4 01 50 4B  .AìyÔ.û&.AìyÔ.PK
0000D290  05 06 00 00 00 00 01 00 01 00 5C 00 00 00 42 00  ..........\...B.
0000D2A0  00 00 00 00                                      ....
```

zip 파일의 푸터 시그니처도 보인다!

qwer.jpg | 무제1.zip

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   50 4B 03 04 14 00 00 00 08 00 87 1B 6C 4D 33 B7  PK........‡.lM3·
00000010   7B 79 1A 00 00 00 18 00 00 00 0A 00 00 00 68 69  {y.............hi
00000020   64 64 65 6E 2E 74 78 74 F3 48 4C CE 76 0E 71 AB  dden.txtóHLÎv.q«
00000030   F6 35 29 29 AA 34 28 CE C8 4E 8C 4F C9 37 34 AC  ö5))ª4(ÎÈNŒOÉ74¬
00000040   05 00 50 4B 01 02 14 00 14 00 00 00 08 00 87 1B  ..PK..........‡.
00000050   6C 4D 33 B7 7B 79 1A 00 00 00 18 00 00 00 0A 00  lM3·{y..........
00000060   24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00  $.......  .......
00000070   68 69 64 64 65 6E 2E 74 78 74 0A 00 20 00 00 00  hidden.txt..  ...
00000080   00 00 01 00 18 00 4B BF A6 4D EC 79 D4 01 FB 26  ......K¿¦MìyÔ.û&
00000090   0D 41 EC 79 D4 01 FB 26 0D 41 EC 79 D4 01 50 4B  .AìyÔ.û&.AìyÔ.PK
000000A0   05 06 00 00 00 00 01 00 01 00 5C 00 00 00 42 00  ..........\...B.
000000B0   00 00 00 00                                      ....
```

헤더부분부터 복사해 새로운 파일로 저장해 zip 파일로 만들어 보았다.



wow! hidden.txt가 나왔다!