ascetic_zip

Description

> JPG 파일과 반딧불이가 사고가 나서 큰 충돌이 났다.
> 충돌한 지점을 찾아서 flag를 제출해라.

사용한 도구

HxD

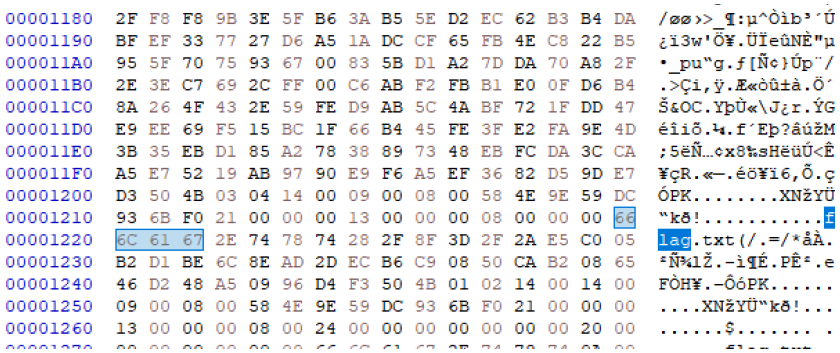
Background

PK Signature

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

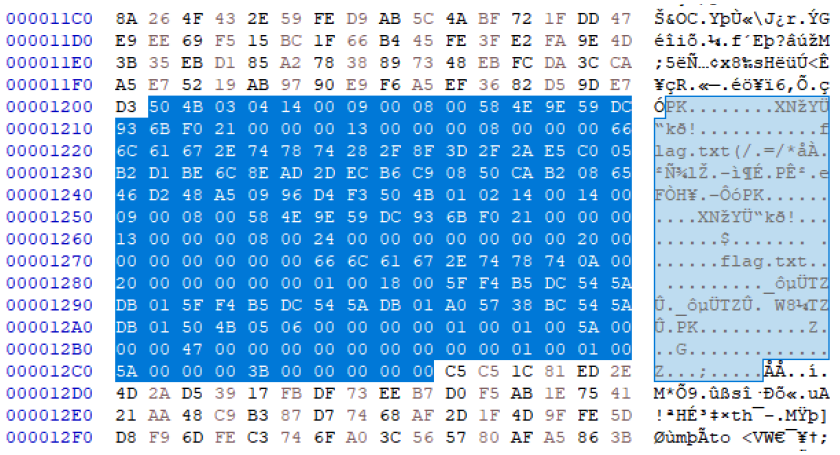
50 49 43 54 00 08 P I C T	IMG	Graphics – ADEX ChromaGraph Graphics Card Bitmap Graphics File
50 4B 03 04 P K	ZIP, DOCX, PPTX, XLSX, JAR, SXC, SXD, SXI, SXW WMZ, XPI,	Archive – Pkzip Archive File Microsoft Office Open XML Format Document Java Archive Package OpenOffice Spreadsheet, Drawing, Presentation Windows Media Compressed Skin File Mozila Browser Archive eXact Packager Models

1. 주어진 flag.jpg 를 HxD로 분석



```
00001180  2F F8 F8 9B 3E 5F B6 3A B5 5E D2 EC 62 B3 B4 DA  /øø›>_¶:µ^Òìb³´Ú
00001190  BF EF 33 77 27 D6 A5 1A DC CF 65 FB 4E C8 22 B5  ¿ï3w'Ö¥.ÜÏeûNÈ"µ
000011A0  95 5F 70 75 93 67 00 83 5B D1 A2 7D DA 70 A8 2F  •_pu"g.ƒ[Ñ¢}Úp¨/
000011B0  2E 3E C7 69 2C FF 00 C6 AB F2 FB B1 E0 0F D6 B4  .>Çi,ÿ.Æ«òû±à.Ö´
000011C0  8A 26 4F 43 2E 59 FE D9 AB 5C 4A BF 72 1F DD 47  Š&OC.YþÙ«\J¿r.ÝG
000011D0  E9 EE 69 F5 15 BC 1F 66 B4 45 FE 3F E2 FA 9E 4D  éîiõ.¼.f´Eþ?âúžM
000011E0  3B 35 EB D1 85 A2 78 38 89 73 48 EB FC DA 3C CA  ;5ëÑ…¢x8‰sHëüÚ<Ê
000011F0  A5 E7 52 19 AB 97 90 E9 F6 A5 EF 36 82 D5 9D E7  ¥çR.«—.éö¥ï6‚Õ.ç
00001200  D3 50 4B 03 04 14 00 09 00 08 00 58 4E 9E 59 DC  ÓPK........XNžYÜ
00001210  93 6B F0 21 00 00 00 13 00 00 00 08 00 00 00 66  "kð!...........f
00001220  6C 61 67 2E 74 78 74 28 2F 8F 3D 2F 2A E5 C0 05  lag.txt(/.=/*åÀ.
00001230  B2 D1 BE 6C 8E AD 2D EC B6 C9 08 50 CA B2 08 65  ²Ñ¾lŽ.-ì¶É.PÊ².e
00001240  46 D2 48 A5 09 96 D4 F3 50 4B 01 02 14 00 14 00  FÒH¥.–ÔóPK......
00001250  09 00 08 00 58 4E 9E 59 DC 93 6B F0 21 00 00 00  ....XNžYÜ"kð!...
00001260  13 00 00 00 08 00 24 00 00 00 00 00 00 00 20 00  ......$....... .
```

flag를 검색해서 주변을 먼저 살펴보았다.

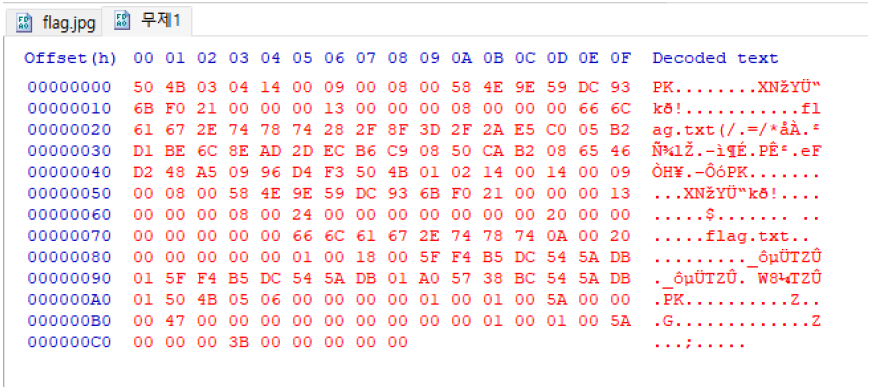


```
000011C0  8A 26 4F 43 2E 59 FE D9 AB 5C 4A BF 72 1F DD 47  Š&OC.YþÙ«\J¿r.ÝG
000011D0  E9 EE 69 F5 15 BC 1F 66 B4 45 FE 3F E2 FA 9E 4D  éîiõ.¼.f´Eþ?âúžM
000011E0  3B 35 EB D1 85 A2 78 38 89 73 48 EB FC DA 3C CA  ;5ëÑ…¢x8‰sHëüÚ<Ê
000011F0  A5 E7 52 19 AB 97 90 E9 F6 A5 EF 36 82 D5 9D E7  ¥çR.«—.éö¥ï6‚Õ.ç
00001200  D3 50 4B 03 04 14 00 09 00 08 00 58 4E 9E 59 DC  ÓPK........XNžYÜ
00001210  93 6B F0 21 00 00 00 13 00 00 00 08 00 00 00 66  "kð!...........f
00001220  6C 61 67 2E 74 78 74 28 2F 8F 3D 2F 2A E5 C0 05  lag.txt(/.=/*åÀ.
00001230  B2 D1 BE 6C 8E AD 2D EC B6 C9 08 50 CA B2 08 65  ²Ñ¾lŽ.-ì¶É.PÊ².e
00001240  46 D2 48 A5 09 96 D4 F3 50 4B 01 02 14 00 14 00  FÒH¥.–ÔóPK......
00001250  09 00 08 00 58 4E 9E 59 DC 93 6B F0 21 00 00 00  ....XNžYÜ"kð!...
00001260  13 00 00 00 08 00 24 00 00 00 00 00 00 00 20 00  ......$....... .
00001270  00 00 00 00 00 00 66 6C 61 67 2E 74 78 74 0A 00  ......flag.txt..
00001280  20 00 00 00 00 00 01 00 18 00 5F F4 B5 DC 54 5A  ........._ôµÜTZ
00001290  DB 01 5F F4 B5 DC 54 5A DB 01 A0 57 38 BC 54 5A  Û._ôµÜTZÛ. W8¼TZ
000012A0  DB 01 50 4B 05 06 00 00 00 00 01 00 01 00 5A 00  Û.PK..........Z.
000012B0  00 00 47 00 00 00 00 00 00 00 00 00 01 00 01 00  ..G.............
000012C0  5A 00 00 00 3B 00 00 00 00 00 C5 C5 1C 81 ED 2E  Z...;.....ÅÅ..í.
000012D0  4D 2A D5 39 17 FB DF 73 EE B7 D0 F5 AB 1E 75 41  M*Õ9.ûßsî·Ðõ«.uA
000012E0  21 AA 48 C9 B3 87 D7 74 68 AF 2D 1F 4D 9F FE 5D  !ªHÉ³‡×th¯-.MŸþ]
000012F0  D8 F9 6D FE C3 74 6F A0 3C 56 57 80 AF A5 86 3B  Øùmþãto <VW€¯¥†;
```

.zip 확장자의 시그니처인 PK 시그니처(50 4B 03 04) 를 확인할 수 있고 PK signature로 시작하는 zip파일을 확인해 볼 수 있다.

PK 시그니처부터 해당 부분을 카빙해보았다.

2. 새로운 파일로 저장 후 FTK Imager로 확인

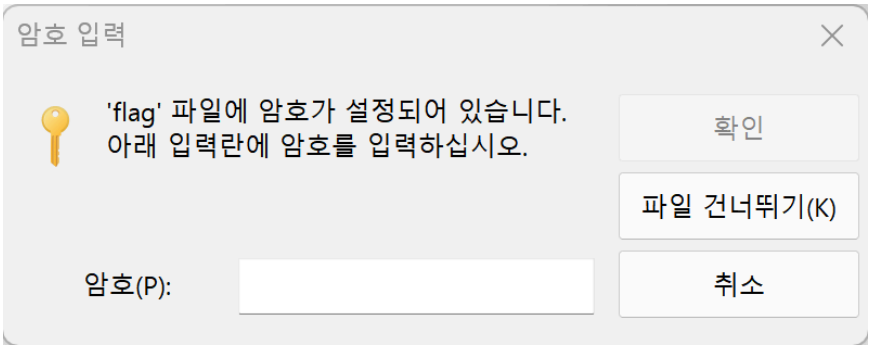


flag.jpg | 무제1

```
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 09 00 08 00 58 4E 9E 59 DC 93  PK........XNžYÜ"
00000010  6B F0 21 00 00 00 13 00 00 00 08 00 00 00 66 6C  kð!...........fl
00000020  61 67 2E 74 78 74 28 2F 8F 3D 2F 2A E5 C0 05 B2  ag.txt(/.=/*åÀ.²
00000030  D1 BE 6C 8E AD 2D EC B6 C9 08 50 CA B2 08 65 46  Ñ¾lŽ.-ì¶É.PÊ².eF
00000040  D2 48 A5 09 96 D4 F3 50 4B 01 02 14 00 14 00 09  ÒH¥.–ÔóPK.......
00000050  00 08 00 58 4E 9E 59 DC 93 6B F0 21 00 00 00 13  ...XNžYÜ"kð!....
00000060  00 00 00 08 00 24 00 00 00 00 00 00 00 20 00 00  .....$....... ..
00000070  00 00 00 00 00 66 6C 61 67 2E 74 78 74 0A 00 20  .....flag.txt.. 
00000080  00 00 00 00 00 01 00 18 00 5F F4 B5 DC 54 5A DB  ........._ôµÜTZÛ
00000090  01 5F F4 B5 DC 54 5A DB 01 A0 57 38 BC 54 5A DB  ._ôµÜTZÛ. W8¼TZÛ
000000A0  01 50 4B 05 06 00 00 00 00 01 00 01 00 5A 00 00  .PK..........Z..
000000B0  00 47 00 00 00 00 00 00 00 00 00 01 00 01 00 5A  .G.............Z
000000C0  00 00 00 3B 00 00 00 00 00                       ...;.....
```

해당 부분을 붙여넣은 새 파일을 만든 후 .zip으로 저장했다.

저장 후 압축풀기를 시도했으나 암호가 걸려있었다.



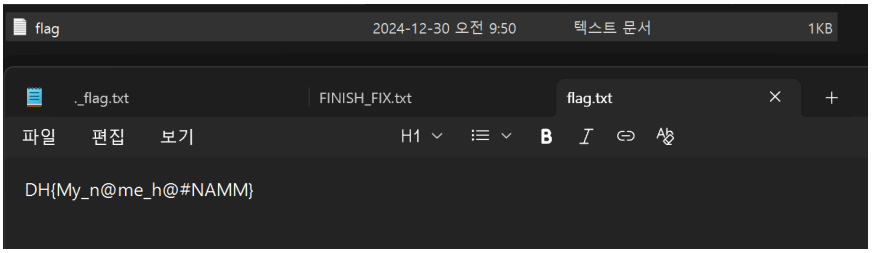
flag.jpg aes.zip

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	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	....ÿÛ.C.....
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	.....
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	..... $.'
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",#..(7),01444.'
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ.C...
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	........2!.!2222
00000070	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000080	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000090	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	22222222222222ÿÀ
000000A0	00	11	08	00	C9	00	FB	03	01	22	00	02	11	01	03	11	....É.û..".....
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	.ÿÄ.....
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	.....
000000D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	..ÿÄ.µ.....
000000E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	......}.....!
000000F0	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23	1A..Qa."q.2.'¡.#
00000100	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	B±Á.RÑð$3br,....
00000110	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	...%&'()*456789:
00000120	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	CDEFGHIJSTUVWXYZ
00000130	63	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A	cdefghijstuvwxyz
00000140	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	ƒ„…†‡ˆ‰Š‘’“”•–—˜™
00000150	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	š¢£¤¥¦§¨©ª²³´µ¶·
00000160	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
00000170	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1	Ö×ØÙÚáâãäåæçèéêñ
00000180	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	00	1F	01	00	03	òóôõö÷øùúÿÄ.....
00000190	01	01	01	01	01	01	01	01	01	00	00	00	00	00	00	01	.....
000001A0	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	11	00	.....ÿÄ.µ..
000001B0	02	01	02	04	04	03	04	07	05	04	04	00	01	02	77	00	.....w.
000001C0	01	02	03	11	04	05	21	31	06	12	41	51	07	61	71	13	.....!1..AQ.aq.
000001D0	22	32	81	08	14	42	91	A1	B1	C1	09	23	33	52	F0	15	"2...B‘¡±Á.#3Rð.
000001E0	62	72	D1	0A	16	24	34	E1	25	F1	17	18	19	1A	26	27	brÑ..$4á%ñ....&'
000001F0	28	29	2A	35	36	37	38	39	3A	43	44	45	46	47	48	49	()*56789:CDEFGHI
00000200	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	JSTUVWXYZcdefghi
00000210	6A	73	74	75	76	77	78	79	7A	82	83	84	85	86	87	88	jstuvwxyz,ƒ„…†‡ˆ
00000220	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6	‰Š‘’“”•–—˜™š¢£¤¥¦
00000230	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4	§¨©ª²³´µ¶·¸¹ºÂÃÄ
00000240	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E2	ÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâ
00000250	E3	E4	E5	E6	E7	E8	E9	EA	F2	F3	F4	F5	F6	F7	F8	F9	ãäåæçèéêòóôõö÷øù
00000260	FA	FF	DA	00	0C	03	01	00	02	11	03	11	00	3F	00	EA	úÿÚ.....?.ê
00000270	69	71	4A	05	3D	56	BE	91	C8	F9	E1	98	A5	C5	48	23	iqJ.=V¾‘Èùá˜¥ÅH#
00000280	A9	02	56	4E	45	28	99	D7	B6	11	6A	56	37	16	33	FF	©.VNE(™×¶.jV7.3ÿ

flag.jpg에서 암호가 될만한 것들을 다 입력해봤으나 풀리지 않았다.

이 flag.jpg외에는 주어진 파일이 없어 문제 제목을 입력해봤더니 암호를 풀 수 있었다..

- 이 부분에서 시간을 오래 썼다



파일 속에 있는 flag.txt를 통해 flag값을 찾을 수 있다.

FLAG

DH{My_n@me_h@#NAMM}