Dreamhack-ascetic_zip(level1)

[forensics]

Description

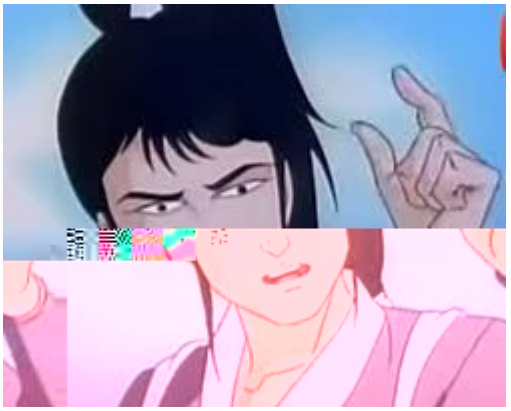
JPG 파일과 반딧불이가 사고가 나서 큰 충돌이 났다.

충돌한 지점을 찾아서 flag를 제출해라. (2024.12.30)

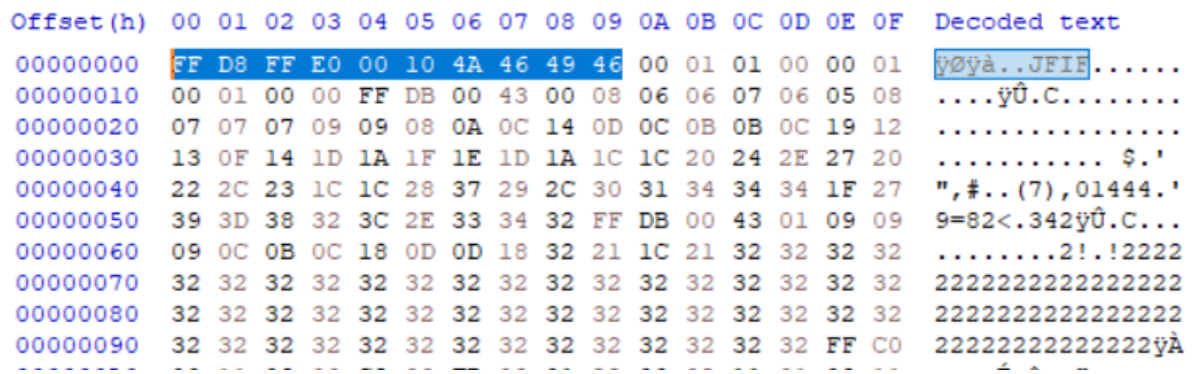
Write up

- 사용 도구: HxD

- 손상된 상태의 `flag.jpg`

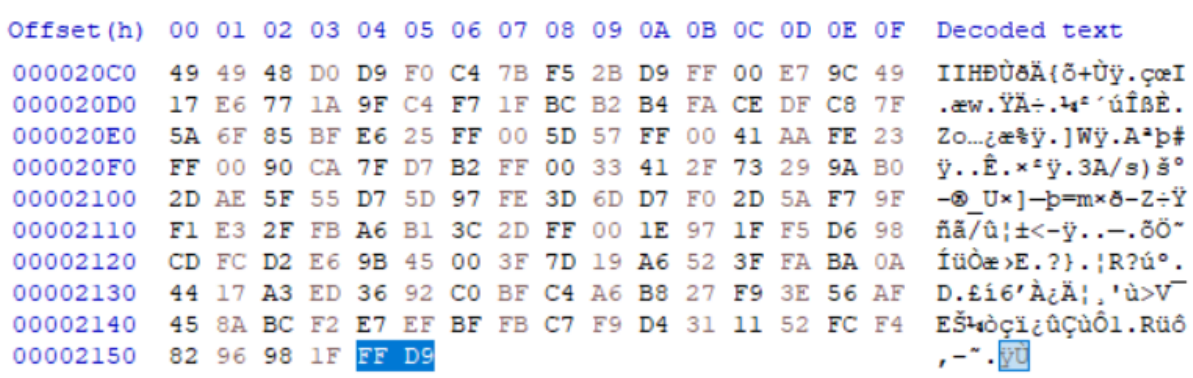


- HxD를 통해 분석 시작
- JPG 시작 부분 → `FF D8` 시작 시그니처 확인



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

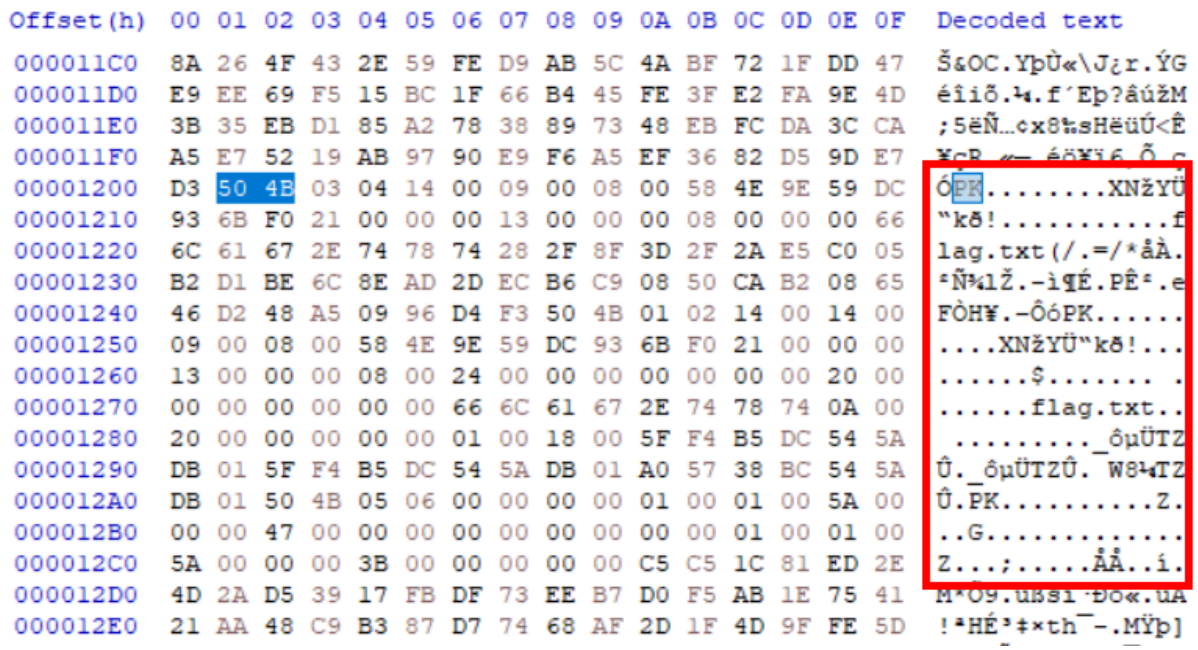
- JPG 끝 부분 → `FF D9` 종료 시그니처 확인



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000020C0	49	49	48	D0	D9	F0	C4	7B	F5	2B	D9	FF	00	E7	9C	49	IIHÐÙðÄ{õ+Ùÿ.çœI
000020D0	17	E6	77	1A	9F	C4	F7	1F	BC	B2	B4	FA	CE	DF	C8	7F	.æw.ŸÄ÷.¼²´úÎßÈ.
000020E0	5A	6F	85	BF	E6	25	FF	00	5D	57	FF	00	41	AA	FE	23	Zo…¿æ%ÿ.]Wÿ.Aªþ#
000020F0	FF	00	90	CA	7F	D7	B2	FF	00	33	41	2F	73	29	9A	B0	ÿ..Ê.×²ÿ.3A/s)š°
00002100	2D	AE	5F	55	D7	5D	97	FE	3D	6D	D7	F0	2D	5A	F7	9F	-®_U×]—þ=m×ð-Z÷Ÿ
00002110	F1	E3	2F	FB	A6	B1	3C	2D	FF	00	1E	97	1F	F5	D6	98	ñã/û¦±<-ÿ..—.õÖ˜
00002120	CD	FC	D2	E6	9B	45	00	3F	7D	19	A6	52	3F	FA	BA	0A	ÍüÒæ›E.?}.¦R?ú°.
00002130	44	17	A3	ED	36	92	C0	BF	C4	A6	B8	27	F9	3E	56	AF	D.£í6'À¿Ä¦¸'ù>V¯
00002140	45	8A	BC	F2	E7	EF	BF	FB	C7	F9	D4	31	11	52	FC	F4	EŠ¼òçï¿ûÇùÔ1.Rüô
00002150	82	96	98	1F	FF	D9											,–˜.ÿÙ

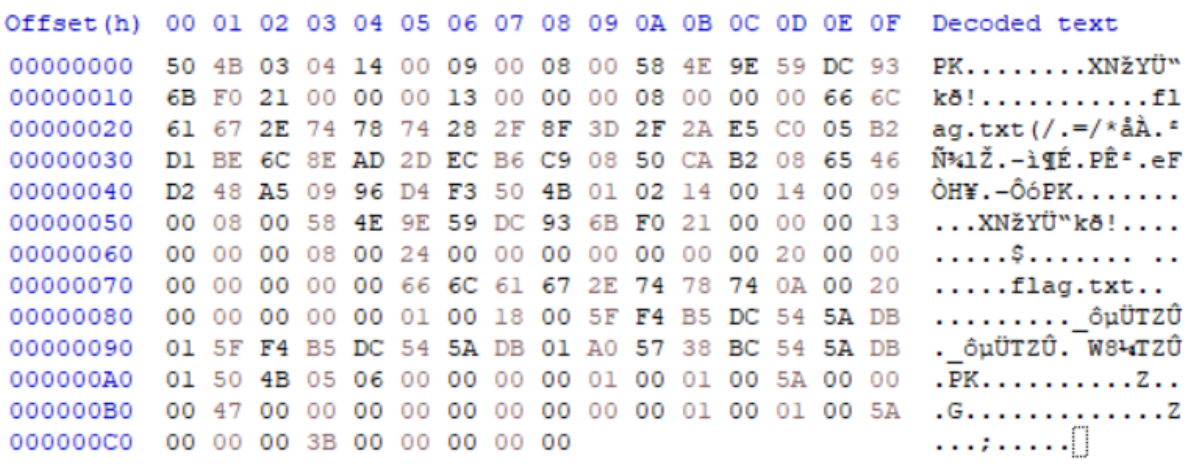
- 즉, 시작과 끝은 손상되지 않았으며 중간에서 파일이 손상된 것으로 추정

- PK 시그니처(`50 4B`) 발견 → 중간 영역에 .zip 파일 구조가 삽입되어 있음을 확인



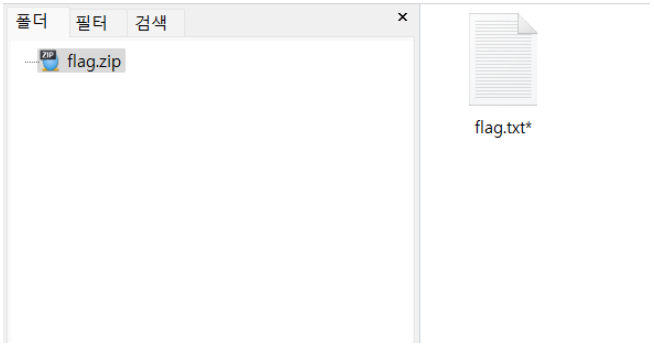
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000011C0	8A	26	4F	43	2E	59	FE	D9	AB	5C	4A	BF	72	1F	DD	47	Š&OC.YþÙ«\J¿r.ÝG
000011D0	E9	EE	69	F5	15	BC	1F	66	B4	45	FE	3F	E2	FA	9E	4D	éîiõ.¼.f´Eþ?âúžM
000011E0	3B	35	EB	D1	85	A2	78	38	89	73	48	EB	FC	DA	3C	CA	;5ëÑ…¢x8‰sHëüÚ<Ê
000011F0	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]

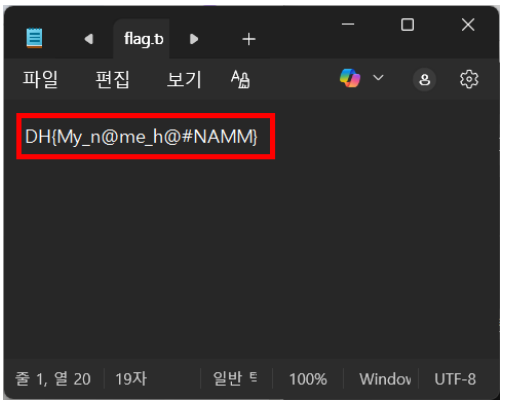
- 해당 부분만 따로 추출하여 flag.zip으로 저장



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								...;.....□

- 내부에 flag.txt 파일 존재 확인 → But, 암호가 걸려있음
  - 시도 1) 반딧불이를 영어로 입력(**firefly)** → 실패 X
  - 시도 2) 문제 제목 입력(**ascetic**) → 성공





- FLAG는, DH{My_n@me_h@#NAMM}

- 추가적으로 손상된 사진 복구 시도
- zip 영역으로 추정되는 부분을 삭제 후 jpg로 저장 ⇒ 복구 성공

FLAG

DH{My_n@me_h@#NAMM}