Snowing!

Description

> 드림이 : 우와! 밖에 눈이 많이와요!
> 드림맘 : 그렇네~
> 드림이 : 거의 모두 하얀공간뿐이네요.

사용한 도구

HxD, snow.exe

Background

스테가노그래피 (Steganography)

- 사진, 음악, 동영상 같은 일반적인 파일 안에 데이터를 숨기는 기술
- 겉으로는 일반적인 사진,음악,동영상 파일 → 실제론 데이터가 숨겨져 있음

▼ 스테가노 그래피 원리

- 사진,동영상,오디오와 같은 파일에는 불필요한 데이터가 상당수 포함되어있음
- 위와 같은 노이즈를 다른 메시지로 대치해도 겉으로 보면 확인 X
- 사람의 눈으로는 미세한 차이를 인식하지 못하기 때문에 아주 작은 값을 변형시켜 메시지를 숨기기도 함 → 원본의 외형적(화질,음질 등)변화를 최소화 하면서 유의미한 정보를 넣는 것이 핵심

▼ 스테가노 그래피 방법

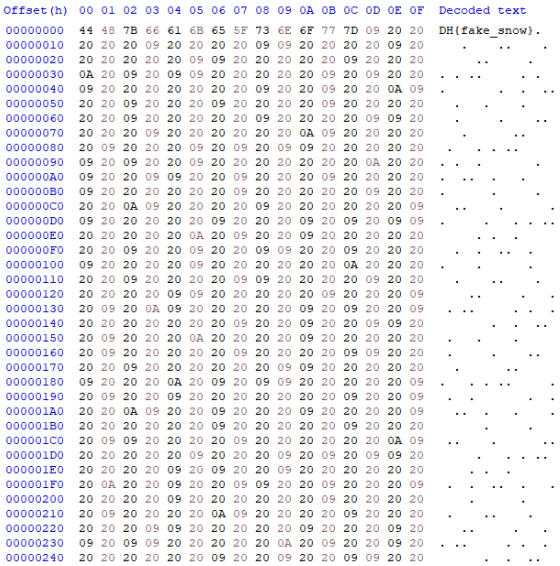
1. 비트 플레인 분산 방식
    - 상위 비트로 갈수록 영향력이 크고(MSB), 하위 비트로 갈수록 인지성이 감소(LSB)하는것을 이용해 적절한 연산 방식으로 비밀 정보를 삽입하는 방법
    - JPEG 파일에서 LSB를 사용하여 은닉하는 방법이 대표적
        - LSB(Least Significant Bit) 즉 중요도가 낮은 bit 들을 원하는 정보로 바꿔 넣는 방식

        - LSB를 1~2 bit 만큼 바꿔도 사람의 눈으로는 인식하기 어려움
    - LSB 에만 정보를 삽입하면 LSB만 추출한 경우 삽입한 정보가 바로 드러나기 때문에 비트플레인 분산 방식 사용
        - LSB 외에 8 bit에서 MSB를 피해 하위 비트들에 랜덤하게 정보 삽입
        - MSB(Most Significant Bit)는 주로 색상을 결정하기 때문에 피함
2. 파일 뒤에 삽입하는 방식
    - 파일의 끝을 알리는 시그니처 뒤의 데이터는 무시된다는 방식을 이용하여 푸터 시그니처 뒤에 원하는 파일을 삽입

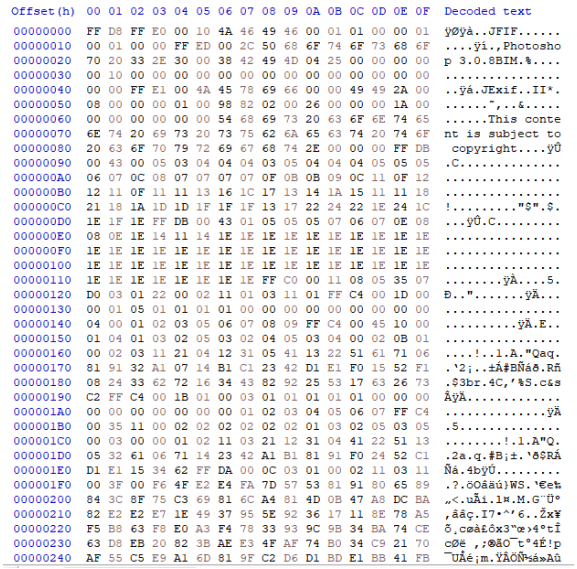
White Space

- 공백부분에 데이터를 은닉하는 스테가노그래피 기법
- https://darkside.com.au/snow/ → whitespace 스테가노 그래피를 찾아서 복호화를 시켜줌
    - SHOW.EXE [옵션] [파일명]

1. HxD로 flag.txt, snow.jpeg 분석



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	44	48	7B	66	61	6B	65	5F	73	6E	6F	77	7D	09	20	20	DH{fake_snow}.
00000010	20	20	20	09	20	20	20	20	09	09	20	20	20	20	09	20	. . .. .
00000020	20	20	20	20	20	09	09	20	20	20	20	20	09	20	20	20	.. .
00000030	0A	20	09	20	09	09	20	20	20	20	20	09	20	09	20	20	. . .. . .
00000040	09	20	20	20	20	20	20	20	09	20	20	09	20	20	0A	09	. . . ..
00000050	20	20	09	20	20	20	09	20	20	20	20	09	20	20	20	20	. . . .
00000060	20	20	09	20	20	20	20	20	09	20	20	20	20	09	09	20	. . . ..
00000070	20	20	20	09	20	20	20	20	20	20	0A	09	20	20	20	20	. ..
00000080	20	09	20	20	20	09	20	09	20	09	09	20	20	20	20	20	. . . .. .
00000090	09	20	09	20	20	09	20	20	20	20	20	20	20	0A	20	20	. . . . .
000000A0	09	20	20	09	09	20	20	09	20	20	20	09	20	20	20	20	. .. . .
000000B0	09	20	20	20	20	20	20	09	20	20	20	20	20	09	20	20	. . .
000000C0	20	20	0A	09	20	20	20	20	09	20	20	20	20	20	20	09	.. . .
000000D0	09	20	20	20	20	20	09	20	20	20	09	20	09	20	09	09	. . . . ..
000000E0	20	20	20	20	20	0A	20	09	20	20	09	20	20	20	20	20	. . .
000000F0	20	20	09	20	20	09	20	20	09	09	20	20	09	20	20	20	. . .. .
00000100	09	20	20	20	20	09	20	20	20	20	20	0A	20	20	20	20	. . . .
00000110	20	20	09	20	20	20	20	09	09	20	20	20	20	09	20	20	. .. .
00000120	20	20	20	20	09	09	20	20	20	20	20	09	20	20	20	09	.. . .
00000130	20	09	20	0A	09	20	20	20	20	20	09	20	09	20	20	09	. .. . . .
00000140	20	20	20	20	20	20	20	09	20	20	09	20	20	09	09	20	. . . ..
00000150	20	09	20	20	20	0A	20	20	20	20	09	20	20	20	20	20	. . . .
00000160	20	09	20	20	20	20	20	09	20	20	20	20	09	09	20	20	. . . ..
00000170	20	20	09	20	20	20	20	20	20	09	09	20	20	20	20	20	. . ..
00000180	09	20	20	20	0A	20	09	20	09	09	20	20	20	20	20	09	. . . .
00000190	20	09	20	20	09	20	20	20	20	20	20	20	09	20	20	09	. . . . .
000001A0	20	20	0A	09	20	20	09	20	20	20	09	20	20	20	20	09	.. . . . .
000001B0	20	20	20	20	20	20	09	20	20	20	20	20	09	20	20	20	. . .
000001C0	20	09	09	20	20	20	20	09	20	20	20	20	20	20	0A	09	.. . ..
000001D0	20	20	20	20	20	20	09	20	20	20	09	20	09	20	09	09	. . . . ..
000001E0	20	20	20	20	09	20	09	20	20	09	20	20	20	20	20	20	. . .
000001F0	20	0A	20	20	09	20	20	20	09	20	20	09	20	20	20	09	. . .. . .
00000200	20	20	20	20	09	20	20	20	20	20	20	09	20	20	20	20	. . .
00000210	20	09	20	20	20	20	0A	09	20	20	20	20	09	20	20	20	. . .. .
00000220	20	20	20	09	09	20	20	20	20	20	09	20	20	20	09	20	.. . .
00000230	09	20	09	09	20	20	20	20	20	0A	20	09	20	20	09	20	. .. . .
00000240	20	20	20	20	20	20	09	20	20	09	20	20	09	09	20	20	. . ..



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	ED	00	2C	50	68	6F	74	6F	73	68	6F	....ÿí.,Photosho
00000020	70	20	33	2E	30	00	38	42	49	4D	04	25	00	00	00	00	p 3.0.8BIM.%....
00000030	00	10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	00	00	FF	E1	00	4A	45	78	69	66	00	00	49	49	2A	00	..ÿá.JExif..II*.
00000050	08	00	00	00	01	00	98	82	02	00	26	00	00	00	1A	00	......˜‚..&.....
00000060	00	00	00	00	00	00	54	68	69	73	20	63	6F	6E	74	65	......This conte
00000070	6E	74	20	69	73	20	73	75	62	6A	65	63	74	20	74	6F	nt is subject to
00000080	20	63	6F	70	79	72	69	67	68	74	2E	00	00	00	FF	DB	copyright....ÿÛ
00000090	00	43	00	05	03	04	04	04	03	05	04	04	04	05	05	05	.C..............
000000A0	06	07	0C	08	07	07	07	0F	0B	0B	09	0C	11	0F	12		....
000000B0	12	11	0F	11	11	13	16	1C	17	13	14	1A	15	11	11	18	....
000000C0	21	18	1A	1D	1D	1F	1F	1F	13	17	22	24	22	1E	24	1C	!.........."$".$.
000000D0	1E	1F	1E	FF	DB	00	43	01	05	05	05	07	06	07	0E	08	...ÿÛ.C.........
000000E0	08	0E	1E	14	11	14	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	....
000000F0	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	....
00000100	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	....
00000110	1E	1E	1E	1E	1E	1E	1E	FF	C0	00	11	08	05	35	07		.......ÿÀ....5.
00000120	D0	03	01	22	00	02	11	01	03	11	01	FF	C4	00	1D	00	Ð.."........ÿÄ...
00000130	00	01	05	01	01	01	01	00	00	00	00	00	00	00	00	00	....
00000140	04	00	01	02	03	05	06	07	08	09	FF	C4	00	45	10	00	..........ÿÄ.E..
00000150	01	04	01	03	02	05	03	02	04	05	03	04	00	02	0B	01	....
00000160	00	02	03	11	21	04	12	31	05	41	13	22	51	61	71	06	....!..1.A."Qaq.
00000170	81	91	32	A1	07	14	B1	C1	23	42	D1	E1	F0	15	52	F1	.'2¡..±Á#BÑáð.Rñ
00000180	08	24	33	62	72	16	34	43	82	92	25	53	17	63	26	73	.$3br.4C,'%S.c&s
00000190	C2	FF	C4	00	1B	01	00	03	01	01	01	01	01	00	00	00	ÂÿÄ.............
000001A0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	FF	C4	..............ÿÄ
000001B0	00	35	11	00	02	02	02	02	02	02	01	03	02	05	03	05	.5..............
000001C0	00	03	00	00	01	02	11	03	21	12	31	04	41	22	51	13	........!.1.A"Q.
000001D0	05	32	61	06	71	14	23	42	A1	B1	81	91	F0	24	52	C1	.2a.q.#B¡±.'ð$RÁ
000001E0	D1	E1	15	34	62	FF	DA	00	0C	03	01	00	02	11	03	11	Ñá.4bÿÚ.........
000001F0	00	3F	00	F6	4F	E2	E4	FA	7D	57	53	81	91	80	65	89	.?.öOâäú}WS.'€e‰
00000200	84	3C	8F	75	C3	69	81	6C	A4	81	4D	0B	47	A8	DC	BA	„<.uÃi.l¤.M.G¨Ü°
00000210	82	E2	E2	E7	1E	49	37	95	5E	92	36	17	11	8E	78	A5	‚ââç.I7•^'6..Žx¥
00000220	F5	B8	63	F8	E0	A3	F4	78	33	93	9C	9B	34	BA	74	CE	õ¸cøà£ôx3"œ›4°tÎ
00000230	63	D8	EB	20	82	3B	AE	E3	4F	AF	74	B0	34	C9	21	70	cØë ‚;®ãO¯t°4É!p
00000240	AF	55	C5	E9	A1	6D	81	9F	C2	D6	D1	BD	E1	BB	41	FB	¯UÅé¡m.ŸÂÖÑ½á»Aû

→ flag.txt 에서 whitespace strganography 가능

처음엔 snow.jpeg에서 시도. 암호화 되어있는 부분 검색(en~, md5, base64 등 → 아무런 내용 X)

스테가노 그래피 해독 사이트 → 아무것도 안나옴 → snow.jpeg로는 아무것도 발견할 수 없었음.

2. Whitespace steganography

background에서 알아본 snow.exe툴 사용

(cmd에서 입력, flag.txt를 snow.exe와 같은 경로에 두고 사용)

```
C:₩Users₩user₩Downloads₩snwdos32>SNOW.EXE -C flag.txt
SnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnow
SnowSnowSnowSnowSnowDH{w0w_1t_Sn0w5}SnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnowSnow
Snow
```

FLAG

DH{w0w_1t_Sn0w5}