

PNG

≡ 문제 분류	forensic
≡ poc 작성자	김재환
≡ 문제 개발자	김재환

1. 문제

문제를 읽어보면 **PNG 파일을 잘 아는가?** 에 대해서 물어보고 있습니다.

챌린지

0명 해결함

×

PNG

550

PNG 파일에 대해서 잘 아시나요? 그럼 풀어보세요!

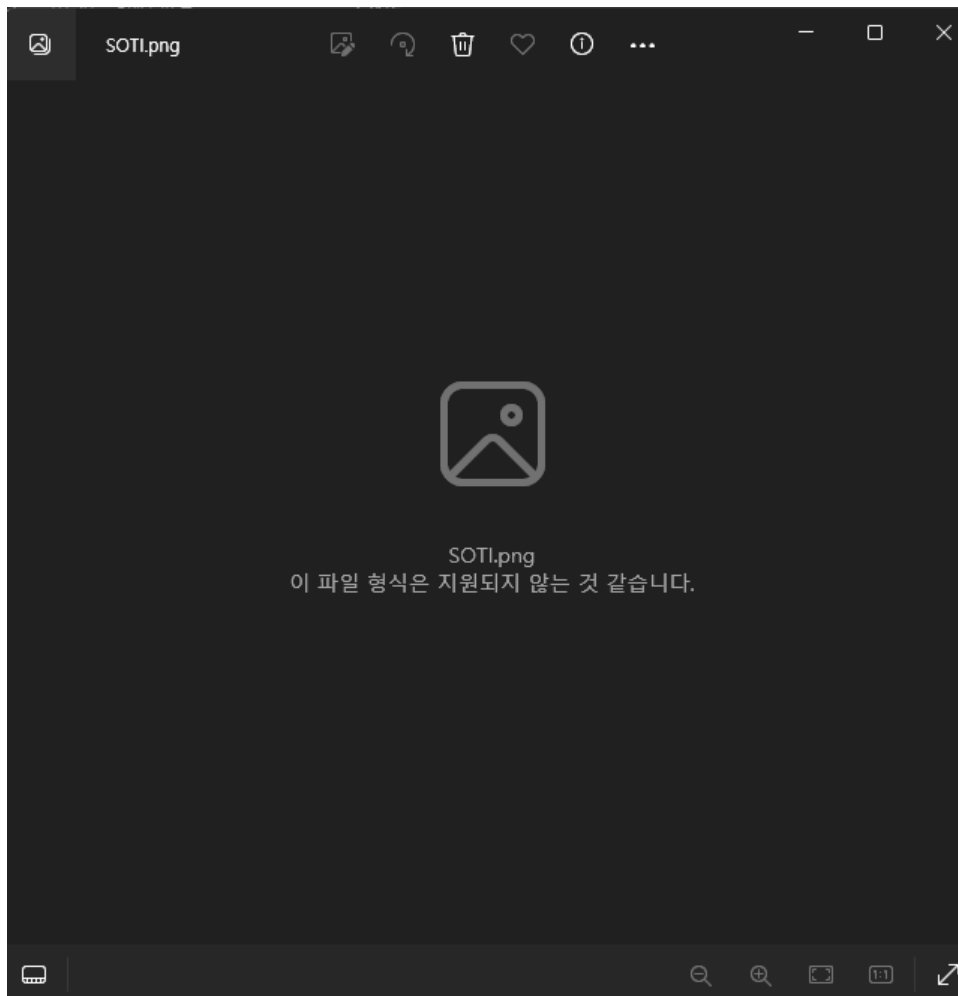
 SOTI.png

플래그

제출

- ~~어서 이 건방진 녀석을 혼내주려 갑시다.~~

soti.png 파일을 다운로드해서 보면, 파일이 깨져 보이지 않는 것을 볼 수 있습니다.



- 무언가 복구를 해야 할 것 같습니다.

2. 풀이

2.1 PNG 헤더 복구

모든 파일에는 **시그니처** 라는 것이 존재합니다. 파일 최상단 헤더에 위치하며, 자신을 어떤 형태로 분석해야 할지 표시하는 문구라고 생각하면 됩니다.

일반적인 PNG 파일을 HxD를 이용하여, HEX값으로 열어 보겠습니다.

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	00	D1	00	00	00	D2	08	06	00	00	00	D4	AE	25	...Ń...Ò.....Ô@%
00000020	41	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	A....sRGB.®İ.é..
00000030	20	00	49	44	41	54	78	5E	EC	5D	07	7C	54	55	F6	7E	.IDATx^i]. TUö~
00000040	D3	13	7A	93	DD	95	16	40	6C	B4	50	45	32	99	24	54	Ó.z"Ý•.@1'PE2™\$T
00000050	0B	25	14	B1	41	42	55	57	A5	5A	50	4A	42	12	40	01	.%.±ABUW¥ZPJB.®.
00000060	69	62	07	21	09	C5	86	10	8A	AB	90	3E	09	45	40	48	ib.!.Ă†.Š«.>.E@H
00000070	00	51	7A	D5	DD	FF	AA	40	02	A4	4C	FD	EF	77	DF	3B	.QzÔÝŸ*®.ŁŁýiwß;
00000080	93	CB	90	CC	4C	66	12	08	F0	9E	3F	7F	13	66	5E	B9	"Ē.İLf..ðž?...f^¹
00000090	EF	DE	FB	DD	73	EE	29	DF	51	08	B7	F0	38	73	E6	CC	iBúÝsi)BQ.·88sæİ
000000A0	3F	2E	9C	3E	DD	0C	4D	B0	4B	87	B7	CD	51	28	14	8A	?œ>Ý.M°K†·İQ(.Š
000000B0	B2	AE	C5	AD	4B	FB	CD	56	CA	F7	6A	95	EA	86	73	CB	*@Ă.KŮİVĚ÷j·ê†sĚ
000000C0	BA	BE	BC	6D	2D	ED	3E	76	B5	ED	BA	E7	A9	6D	6A	C7	*%4m-i>vui°ç@mjÇ
000000D0	BF	9D	DB	67	B7	5D	7F	2E	3D	5F	A1	54	96	F9	EE	A5	ç.Ŭg·j..=_;T-ùİ¥
000000E0	B5	91	BF	8F	5D	53	D2	37	36	E9	D9	1A	A9	5F	6C	D2	µ'ç.]S076éŬ.©.lò
000000F0	F3	70	0E	FF	1B	5D	6F	D3	D8	EC	36	9B	C6	AE	95	CE	óp.ÿ.]oÓ0i6>B@·İ
00000100	43	7B	6D	1A	2B	6B	BF	D2	AC	52	28	15	0A	85	49	A9	C{m.+kçÔ-R(.....I@
00000110	54	A8	AC	56	AD	D5	6A	55	FE	AD	49	93	2B	0F	3F	FC	T"-V.ŬjUp.I"+.¿ü
00000120	F0	D9	F2	F6	5B	55	3F	BF	5C	9D	EF	CD	CB	EC	DD	BB	8Ŭòò[U?ç\..İİĚİŸ»
00000130	B7	CD	D1	A3	47	02	F7	EE	DD	D7	E9	60	4E	6E	C7	E3	·İŇŁG.÷İŸ×é`NnÇă
00000140	27	8E	37	FF	E3	8F	3F	9A	98	CD	16	76	3B	65	A9	D3	'Ž7Ÿă.¿š~İ.v;e@Ó
00000150	DB	9B	27	C9	D7	54	C5	1E	00	BE	35	1A	8D	50	5C	6C	Ŭ>'Ē×TĂ...%5..P\l
00000160	12	68	A8	31	E9	EE	B9	A7	C1	95	56	AD	5A	ED	FF	DB	.h"léi'šĂ·V.ZiŸŬ
00000170	BD	8D	F2	9A	05	04	EC	EB	D0	A1	C3	99	B6	6D	DB	E6	%..òš...İēĐ;Ă™ŹmŬæ
00000180	B4	6B	D7	EE	50	55	7C	0F	57	6D	AA	14	10	FD	B0	75	'k×iPU .Wm*...Ÿ°u
00000190	EB	93	5F	AF	FF	66	50	A6	31	B3	CF	F9	F3	E7	9B	98	ē" _ŸfP l'İùóç>~
000001A0	CD	56	D6	06	8D	46	05	89	23	58	2C	36	F6	6F	95	4A	İVŬ..F.%#X,6öo·J
000001B0	21	08	E2	C2	25	1F	77	68	0F	60	74	31	C9	A0	27	A8	!.ăĂ%..wh.`tİĚ' "
000001C0	54	73	01	03	83	40	53	40	BE	13	BE	50	6C	B6	33	60	T*...ŸŹŹŹ...ŸŹŹŹ

- 89 50 4E 0D 0A 1A 0A 라는 헤더 값이 존재합니다.
- 우측에 디코드 된 문자열을 보면, 헤더 부분이 존재하는 것을 볼 수 있습니다.
- 그 뒤는 파일의 넓이, 포맷 형식 등 다양한 정보가 저장되어 있습니다.

그렇다면 우리가 분석해야 할 파일인 `soti.png` 는 어떨까요?

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	00	00	0D	49	48	44	52	00	00	00	D1	00	00	00	D2IHDR...Ñ...Ò
00000010	08	06	00	00	00	D4	AE	25	41	00	00	00	01	73	52	47Ö%A....sRG
00000020	42	00	AE	CE	1C	E9	00	00	00	04	67	41	4D	41	00	00	B.®İ.é....gAMA..
00000030	B1	8F	0B	FC	61	05	00	00	00	09	70	48	59	73	00	00	±..üa....pHYs..
00000040	12	74	00	00	12	74	01	DE	66	1F	78	00	00	58	82	49	.t...t.řf.x...X,I
00000050	44	41	54	78	5E	ED	9D	09	9C	54	C5	B5	FF	BB	7B	A6	DATx^i...œTÄÿ»{!
00000060	BB	A7	99	8D	61	11	45	76	04	65	15	06	D4	44	98	19	»\$™.a.Ev.e..ÖD~.
00000070	40	71	17	70	79	89	31	6C	62	34	89	51	42	4C	CC	A2	@q.py%llb4%QBLİc
00000080	30	80	18	4D	A2	2C	6A	92	97	97	88	80	C6	18	5F	94	0€.Mc,j'—^€Æ._"
00000090	C5	25	3E	14	98	61	73	43	19	10	D0	88	B2	6B	FC	E4	Å%>."asC..Đ^"küä
000000A0	AF	32	2C	B2	CC	D6	FD	AF	6F	DD	7B	9A	9A	A6	A7	BB	~2,"İÖÿ"oÝ{šš!\$»
000000B0	A7	7B	86	F5	FE	86	43	D5	AD	AE	5B	CB	A9	73	EA	54	\$!†öþ†CÖ.®[Ë@sêT
000000C0	D5	AD	5B	D7	ED	3A	8E	D8	BE	7D	FB	59	BB	B6	6D	6B	Ö.[×i:ŽØ%}ûY»qmk
000000D0	8F	3F	04	82	C1	90	FE	21	09	B8	3D	9E	3A	EB	52	57	.?.,Á.p!.,=ž:ëRW
000000E0	BA	64	69	7B	C3	48	4F	4F	3F	2A	2C	5A	BC	64	10	8C	°di{ÄHOO?*,Z¼d.Æ
000000F0	52	8F	50	7A	FD	B4	D3	55	80	FD	3D	AA	DC	75	95	C3	qžPzı'ónŋı=ıřıı.ž

- 이런... PNG 부분이 없어져 있군요



근데 이게 PNG파일인줄 어떻게 아나요??

좋은 질문입니다. 이는 시그니처 뿐만이 아니라 파일을 구분하는 **청크**를 보면 됩니다

청크는 반드시 필요한 청크가 있고, 그 이외에는 따로 요구되거나, 특정 데이터를 저장하는데 사용됩니다.

PNG에서 반드시 포함되어야 하는 청크는 다음과 같습니다.

- IHDR
- IDAT
- IEND

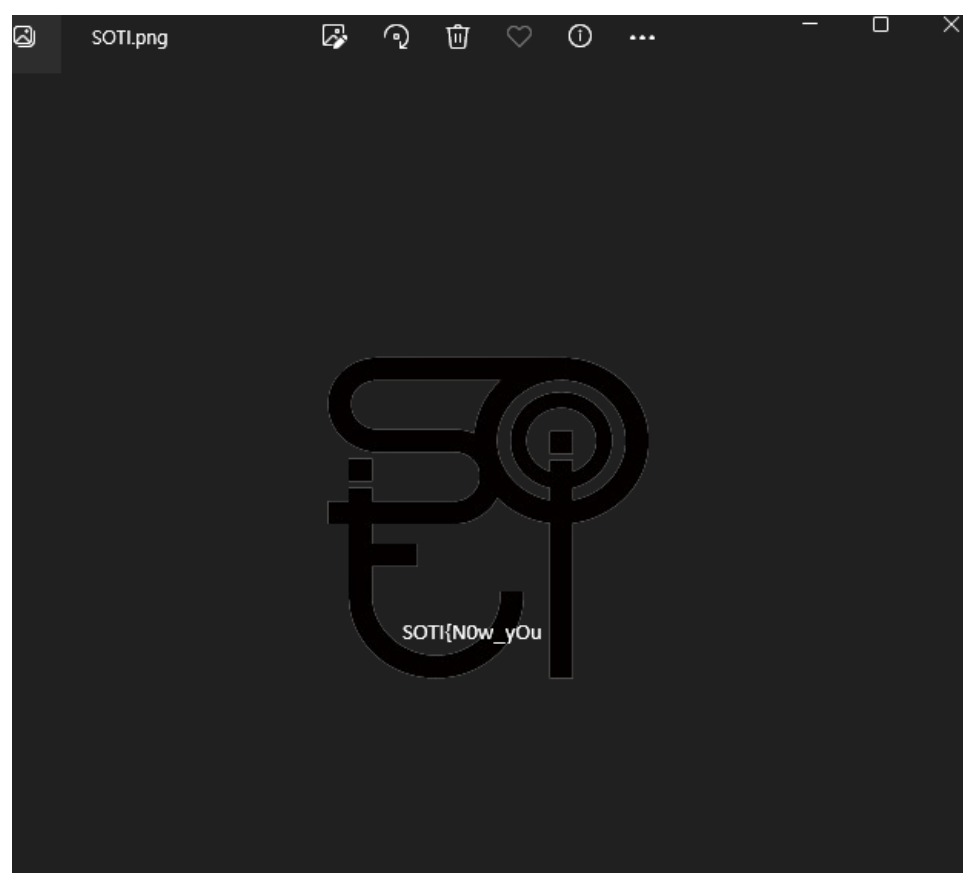
따라서 그림에 **IHDR**이 존재하기 때문에, PNG 파일임을 알 수 있습니다.

복구

PNG 헤더를 표기하는 시그니처를 손상된 파일에 덧붙여 보겠습니다.

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	00	D1	00	00	00	D2	08	06	00	00	00	D4	AE	25	...Ñ...Ò.....Ô@%
00000020	41	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	A....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	12	74	00	00	12	74	01	DE	..pHYs...t...t.Þ
00000050	66	1F	78	00	00	58	82	49	44	41	54	78	5E	ED	9D	09	f.x...X,IDATx^i...
00000060	9C	54	C5	B5	FF	BB	7B	A6	BB	A7	99	8D	61	11	45	76	æTÄuÿ»{ »\$™.a.Ev
00000070	04	65	15	06	D4	44	98	19	40	71	17	70	79	89	31	6C	.e...ÔD".@q.py%11
00000080	62	34	89	51	42	4C	CC	A2	30	80	18	4D	A2	2C	6A	92	b4%QBLİç0€.Mç,j'
00000090	97	97	88	80	C6	18	5F	94	C5	25	3E	14	98	61	73	43	—^€Æ. "Å&>."asC
000000A0	19	10	D0	88	B2	6B	FC	E4	AF	32	2C	B2	CC	D6	FD	AF	..Ð^"küä"2,"İÖý"
000000B0	6F	DD	7B	9A	9A	A6	A7	BB	A7	7B	86	F5	FE	86	43	D5	oÝ{šš!\$»\$†töþ+CÕ
000000C0	AD	AE	5B	CB	A9	73	EA	54	D5	AD	5B	D7	ED	3A	8E	D8	.@[Ë@sêTÕ. [xı:Žø

오~ 복구된 파일을 볼 수 있습니다.



- 근데... FLAG가 반쪽이 잘려있습니다. 나머지 어딘가에 FLAG가 숨겨져 있는 듯 합니다.

2.2 반쪽짜리 FLAG 찾기(footer)

앞서 PNG 파일에는 여러가지 **체크** 가 존재한다고 했습니다. 여기서 **IEND** 는 PNG 데이터의 끝을 알리는 부분으로, 해당 부분에 데이터를 숨기는 **스태가노그래피** 기법이 존재합니다.

- 해당 섹션에 데이터를 숨기게 되면, PNG는 이를 표시하지 않기 때문입니다.

아니! 근데 해당 체크 이후에 무슨 데이터가 있네요

00005890	43 87 CF 89 E3 C0 E5 FA 62 C7 8E D6 8F 3C F6 D8	C#I%ãÄáúbcŽÖ.<øØ
000058A0	B8 DC DC 5C 77 45 45 55 88 4D B3 5E AF 9F 57 47	,ÜÜ\wEEU^M^'^~YWG
000058B0	42 35 35 35 21 AF 37 CD 4D 47 C5 8E 0C FD CA 4B	B555!~7íMGĀŽ.ýĚK
000058C0	55 8D BE 4E 4B 73 BB BB 9E DB 7D DB 77 46 7E E7	U.%NKs»»žŮ}ŮwF~ç
000058D0	69 3B A9 93 14 2E D7 FF 07 36 1D 7C 8D 87 17 49	i;@".*.xÿ.6. .+.I
000058E0	84 00 00 00 00 49 45 4E 44 AE 42 60 82 5F 4B 6EIEND@B` , Kn
000058F0	4F 77 5F 41 62 30 75 74 5F 70 6E 39 21 7D	Ow Ab0ut pn9!}

- 이로써 FLAG를 모두 찾게 되었습니다.