

3S CTF

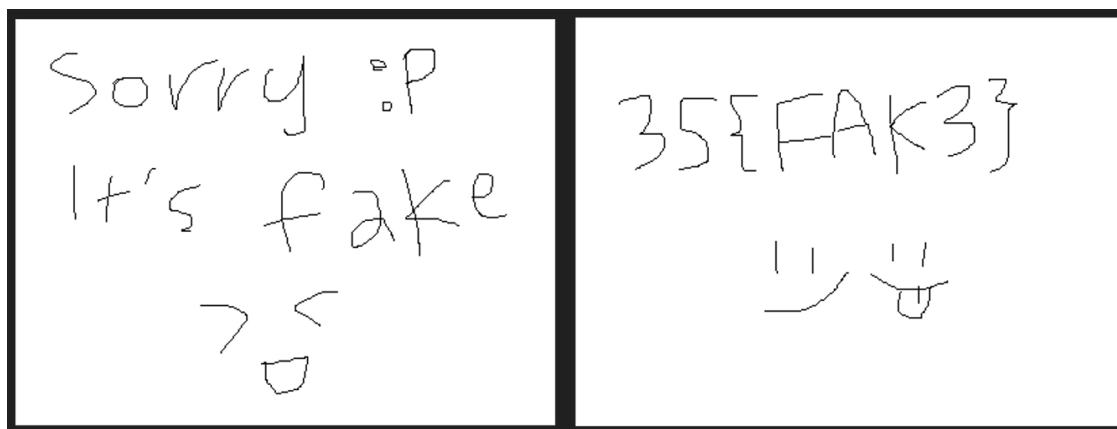
DUMDUM :p



해당 dump.bin 파일에 두 가지 형태의 png 값이 있었다.

010 Hex Editor로 png의 IHDR부터 IEND 부분만 가져와 새로운 파일로 저장했다.

dump.bin	Untitled3.png x																Untitled4															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF															
0000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR															
0010	00	00	01	90	00	00	01	2C	08	06	00	00	00	ED	B7	E5í.ä															
0020	C2	00	00	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	Â....pHYs...Ä...															
0030	C4	01	95	2B	0E	1B	00	00	09	65	49	44	41	54	78	9C	Ä.*+.....eIDATxæ															
0040	ED	DD	DB	6E	F3	B6	16	46	D1	A8	E8	FB	BF	B2	7A	53	íÝÛnó¶.FÑ¨èû¿²zS															
0050	6F	B8	DE	4E	7E	E7	D3	81	6B	91	63	00	BD	69	D1	44	o, pN~çÓ.k'c.½iÑD															

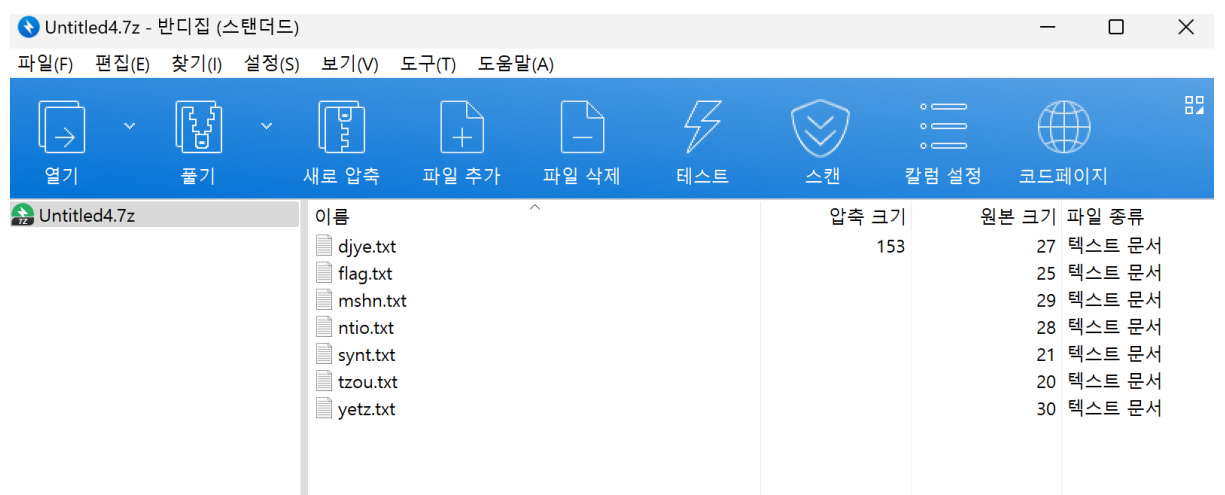


두 가지 형태의 PNG값을 각각 저장해 나타난 fake 이미지이다.

IEND 뒤의 시그니처를 확인해보니 HeX값이 37 7A BC AF 27 1C 형식이라는 것을 알게 되었고 이를 찾아보니 이는 7-Zip 형식의 파일이었다.

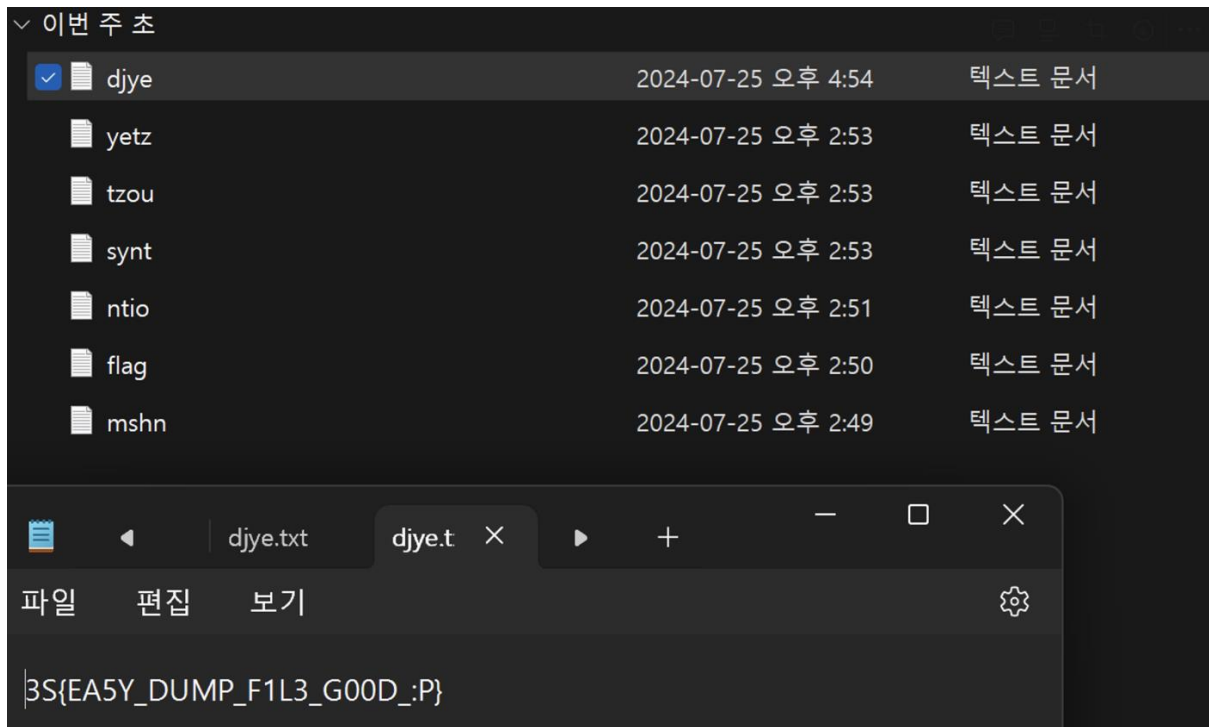
dump.bin	Untitled3.png				Untitled4 x															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3
0000	37	7A	BC	AF	27	1C	00	03	DA	72	1D	2A	7C	01	00	00	7z	¼	'	...
0010	00	00	00	00	23	00	00	00	00	00	00	00	D0	BA	BB	D2	#	Đ°»Ò
0020	00	19	94	CB	64	52	18	E3	EB	BA	33	A5	EA	50	3D	E9	..	"	ĚdR	.ãë°3¥êP=é
0030	29	98	E4	7A	3F	73	6F	D0	35	47	AD	86	29	23	A3	20)	~	äz?	soĐ5G-†)#£
0040	97	3C	08	59	E3	EF	9B	DF	32	34	05	21	92	04	31	71	-<	.Yăĩ>	ß24.!	'
0050	39	A2	6E	EF	B3	7C	59	9E	0C	6B	46	0D	BA	FC	47	E0	9ç	nĩ³	Yž.kF.	°üGà
0060	56	C2	A8	0D	49	E0	83	75	C3	60	9F	26	DC	02	B7	E1	VÂ"	.Iàfu	Ã`Ÿ&Ü.	·á
0070	18	9D	47	F0	67	CD	4A	03	66	6F	7E	EF	B2	19	B8	D3	..	GđgÍJ.	fo~ĩ².	Ó
0080	71	5D	57	30	22	74	58	3B	05	32	13	EA	3A	41	B9	7B	q]W0"	tX;	.2.ê:A¹{	
0090	88	B3	5F	53	F9	F2	E6	06	B3	7E	9B	0A	CF	6F	EC	FD	^³	_Sùòæ.	³~>.	İoiy
00A0	DC	73	C1	FD	B6	85	4A	AE	4E	A0	C0	5F	7B	EC	83	6A	ÜsÁý¶	...J@N	À_	{ifj
00B0	12	98	8D	79	FF	BB	81	00	00	00	00	81	33	07	AE	0F	..	.yŸ»	3.®.
00C0	D5	30	35	43	56	6C	29	1F	48	2B	41	32	68	C6	C0	4C	Ö05CV1)	.H+A2h	ÆÀL	
00D0	D3	47	16	3D	C8	CC	11	D3	BA	6A	9E	5E	96	2E	9E	68	ÓG.	=ÈÌ.	Ó°jž^	-..žh
00E0	E1	12	5C	D5	E6	2E	CA	34	4E	C2	29	A5	5B	A4	C2	A7	á.	\\Öæ.	Ê4NÂ)	¥[̣ôÎš

또한 dump.bin에는 37 7A BC AF 27 ...로 시작하는 값이 나타났는데, 구글링을 통해 이 값이 압축 파일의 일종인 7z파일 형식이라는 것을 알 수 있었다. 따라서 이 영역을 선택해 마찬가지로 새로운 파일로 만들어주었다.



확장자명을 7z로 저장하면 7개의 txt 파일이 나타나는 것을 알 수 있었다.

이 압축파일을 해제 하면 flag가 나타날 것이라는 걸 예측해볼 수 있었다.



Djye.txt에서 flag를 찾아낸 것을 확인할 수 있었다.