

DUM DUM :P

32기 김효주

포렌식 문제 풀이가 익숙해졌으니 또 다른 포렌식 문제를 도전해 보았다

먼저 dump.bin 파일에서 png 파일 시그니처를 찾았더니 png 파일을 두 개 찾을 수 있었다

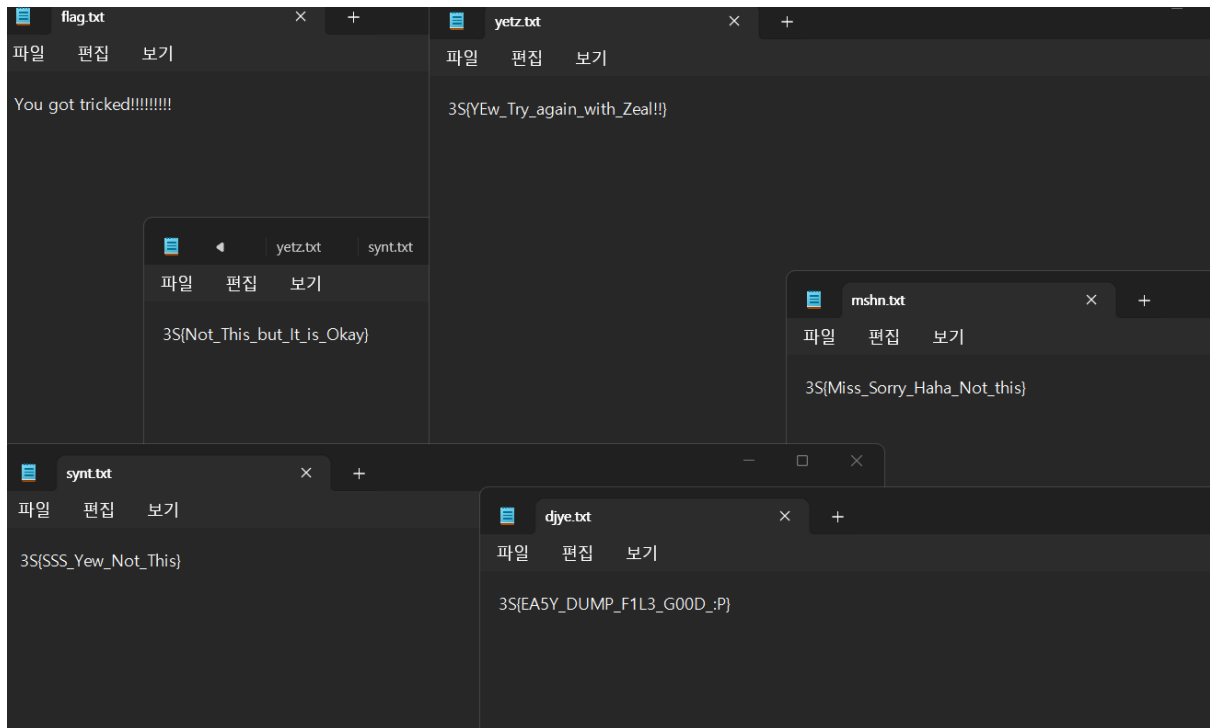
00001010	97 EB 6D C0 2B 00 00 00 00 43 43 4E 44 4E 42 00	FORMAT.....IENDb6D
00001020	82 44 4F 5F 59 4F 55 5F 46 49 4E 44 5F 41 5F 46	,DO_YOU_FIND_A_F
00001030	4C 41 47 3F 00 00 00 00 00 00 00 00 00 00 00 00	LAG?.....
00001040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001060	00 00 00 00 00 00 00 D9 50 4E 47 0D 0A 1A 0A 00 00PNG.....
00001070	00 0D 49 48 44 52 00 00 01 90 00 00 01 2C 08 06	..IHDR.....
00001080	00 00 00 ED B7 E5 C2 00 00 00 09 70 48 59 73 00	...i.ãÄ....pHYs.
00001090	00 0E C4 00 00 0E C4 01 95 2B 0E 1B 00 00 09 65	..Ä...Ä..*+.....e
000010A0	49 44 41 54 78 9C ED DD DB 6E F3 B6 16 46 D1 A8	IDATxœiYÜnóq.FÑ
000010B0	E8 FB BF B2 7A 53 6F B8 DE 4E 7E E7 D3 81 6B 91	èû¿²zSo,ßN~çÓ.k`
000010C0	63 00 BD 69 D1 44 56 24 4E 93 92 E5 6D DF F7 FD	c.¿iNDV\$N''ãmß÷ý
000010D0	0B 00 7E E9 AF D1 1B 00 40 4F 02 02 40 44 40 00	..~eÑ...@O...@D@.

체크섬 검색 (2개의 검색 결과)		
오프셋	잘라내기 (16진수)	잘라내기 (텍스트)
401	2B 7D 68 4B 58 3A 2F 38 78 2F 39 42 68 55 38 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 ...	+}hK[:/8x/9BhU8%oPNG.....IHDR.
1067	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D9 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48...PNG.....IHDR.

찾은 파일을 추출해서 열어보니

이름	수정한 날짜	유형
djye.txt	2024-07-25 오후 4:54	텍스트
flag.txt	2024-07-25 오후 2:50	텍스트
mshn.txt	2024-07-25 오후 2:49	텍스트
ntio.txt	2024-07-25 오후 2:51	텍스트
synt.txt	2024-07-25 오후 2:53	텍스트
tzou.txt	2024-07-25 오후 2:53	텍스트
yetz.txt	2024-07-25 오후 2:53	텍스트

파일이 여러 개 있었다



이 중에서 진짜 플래그는 3S{EA5Y_DUMP_F1L3_G00D_:P} !!!!