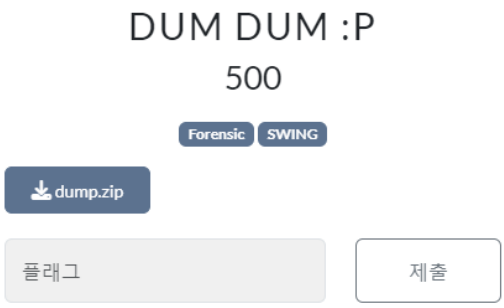
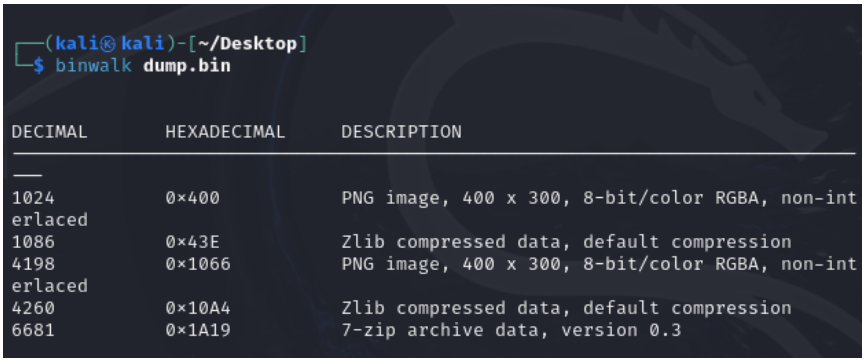
3S CTF
Forensic-DUM DUM :P

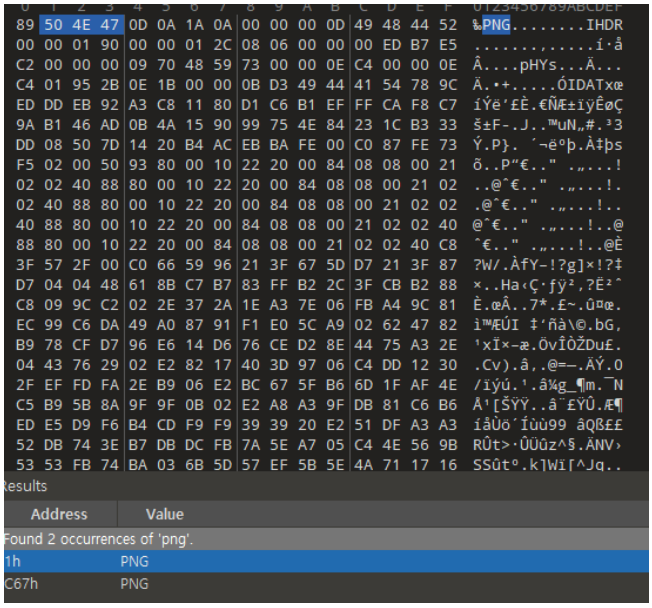
SWING 32 기 한재희



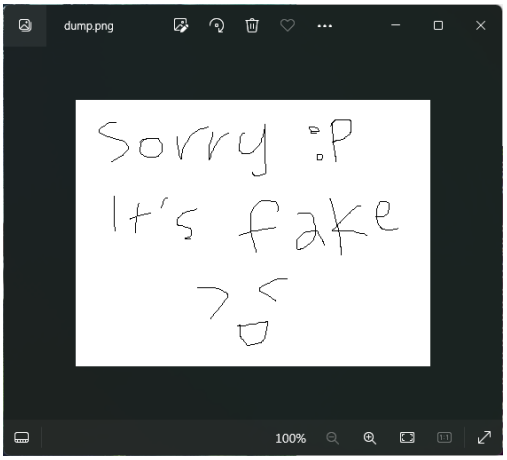
파일을 다운 받으면 dump.bin 파일이 나온다.
bin 파일을 열고 확인하기 위해 칼리리눅스에 들어가 binwalk 를 사용해줬다.



bin 파일 안에 png 파일이랑 zip 파일 두개가 있는 것으로 확인이 되었다.
010 editor 로 확인해보자.

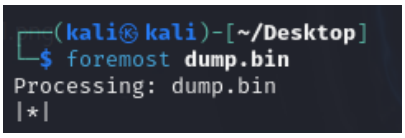


ctrl F 로 png 를 검색해보니 두 개가 나와서 그 두 부분을 앞뒤로 보니 파일 시그니처가 맞아서 그 부분만 남겨두고 그 앞과 뒤는 다 삭제하고 dump.png 로 저장해 사진을 확인해봤다.

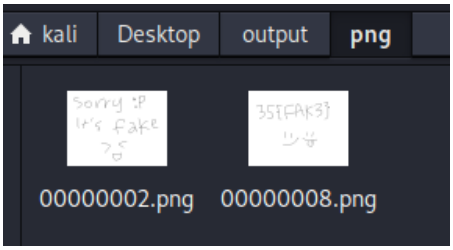


상상치도못한정체가...
좌절을 느끼며 다시 찾아보러 갔다.

검색을 해보니 binwalk 에서 파일 안에 파일이 있다는 걸 알았다면 foremost 명령어를 사용해 파일 안에 있는 파일을 열 수 있다고 해서 사용해봤다.



프로세싱 되면서 output 폴더가 새로 생겼다.



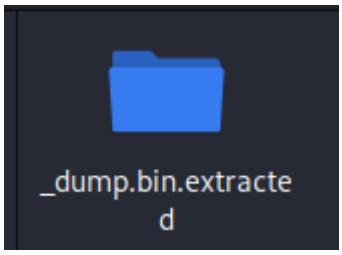
png 파일이 두 개가 나왔는데 02 는 아까 본 fake 사진 이었고 08 이 플래그 값이 적혀 있는 사진이었다.

근데 플래그에 넣었는데 제출이 안돼서.. 이것또한 가짜 플래그 같았다.....
binwalk 에서 봤었던 png 사진 두 개말고 맨 아래 있는 zip 파일을 열어야 할 것 같아서 파일 안에 있는 파일을 여는 방법을 찾아봤다.

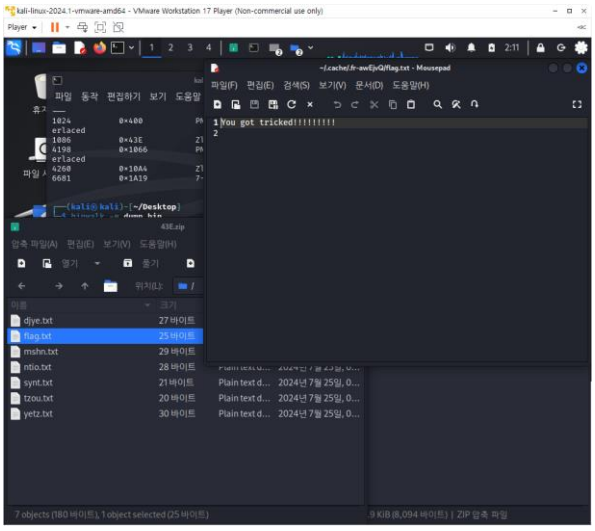
```
┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk -e dump.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1024          0x400           PNG image, 400 x 300, 8-bit/color RGBA, non-i
erlaced
1086          0x43E           Zlib compressed data, default compression
4198          0x1066          PNG image, 400 x 300, 8-bit/color RGBA, non-i
erlaced
4260          0x10A4          Zlib compressed data, default compression
6681          0x1A19          7-zip archive data, version 0.3
```

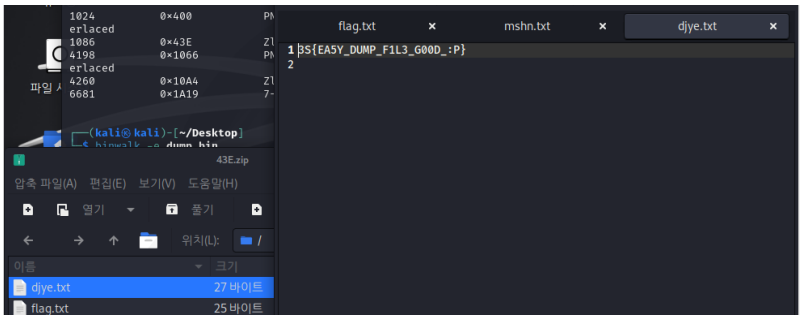
$ binwalk -e 명령어를 사용하면 파일이 열린다고 해서 사용해봤더니



이렇게 폴더 하나가 생성 되어 있었다.



여니까 텍스트 파일이 많았는데 flag.txt 를 보고 황급히 열어보니 또속...
그래서 처음부터 다 열어봤다.



맨 처음 파일에 플래그 값이 적혀 있었다..ㅎ

3S{EA5Y_DUMP_F1L3_G00D_:P}