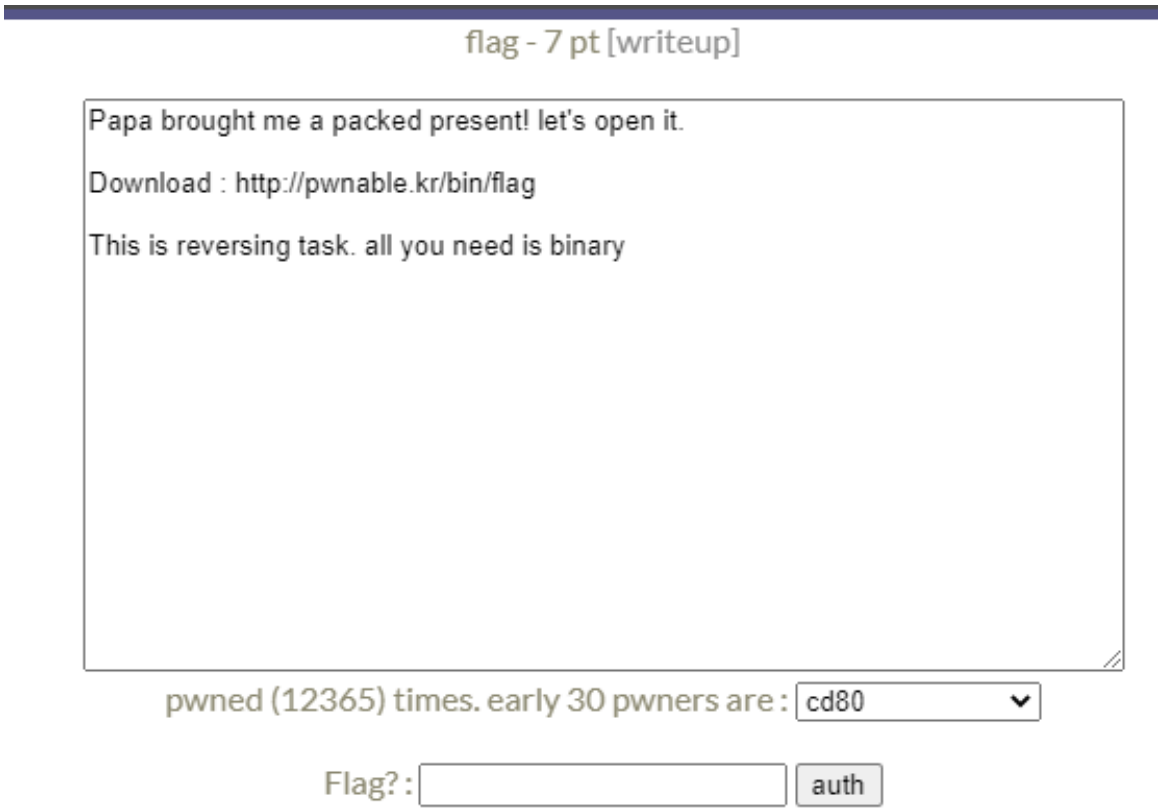
flag



wget으로 다운받아서 gdb로 살펴보앗으나 나오는게 없다..
packed present!.. unpack하면 될거 같은데.. 그게 뭐징?ㅋㅋㅋㅋ
This is reversing task. 리버싱.. 하하 처음들어보는 거 리버싱이 뭔지 살펴보자

리버싱(reversing)

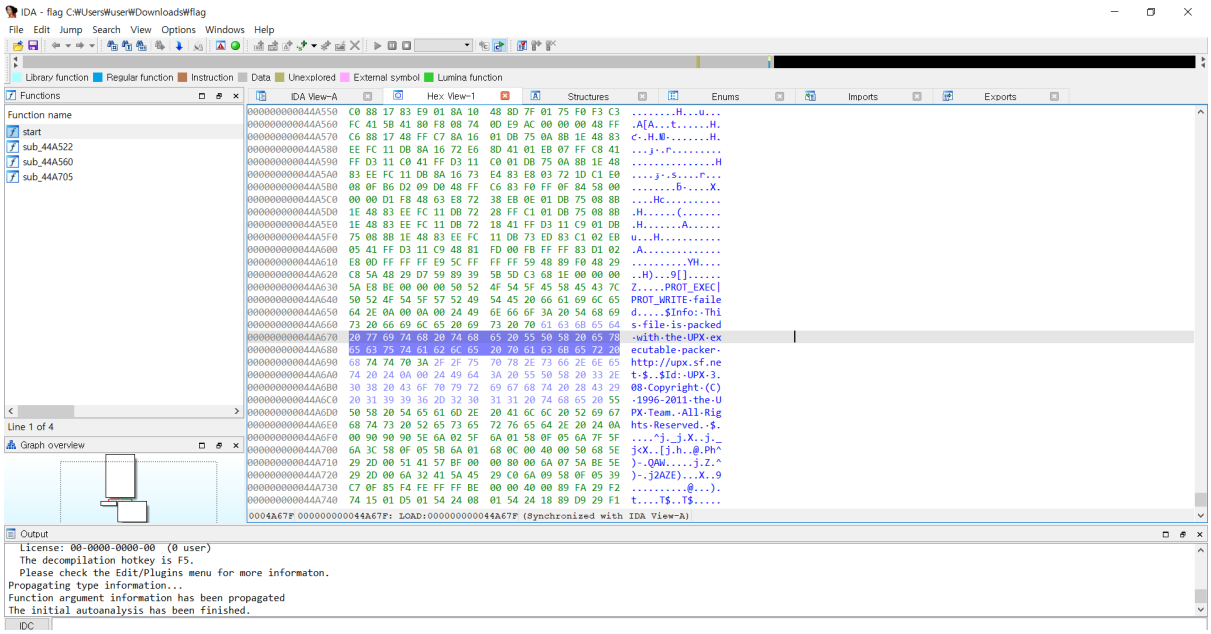
리버스(reverse)와 엔지니어링(engineering)을 합친 엔지니어링을 줄인 말로써 역공학의 한 분야이다

리버스 엔지니어링

- 소스를 역추적하는 것을 말함
- 소스코드를 빌드해서 만들어진 exe, dll의 바이너리르 ㄹ분석해 원래의 소스코드가 어떤 식으로 만들어져 있는지 파악한다.

리버싱은 해야할 것 같으니 리버싱 도구중 IDA를 설치해봤다...

ida로 파일을 열어서 보니까

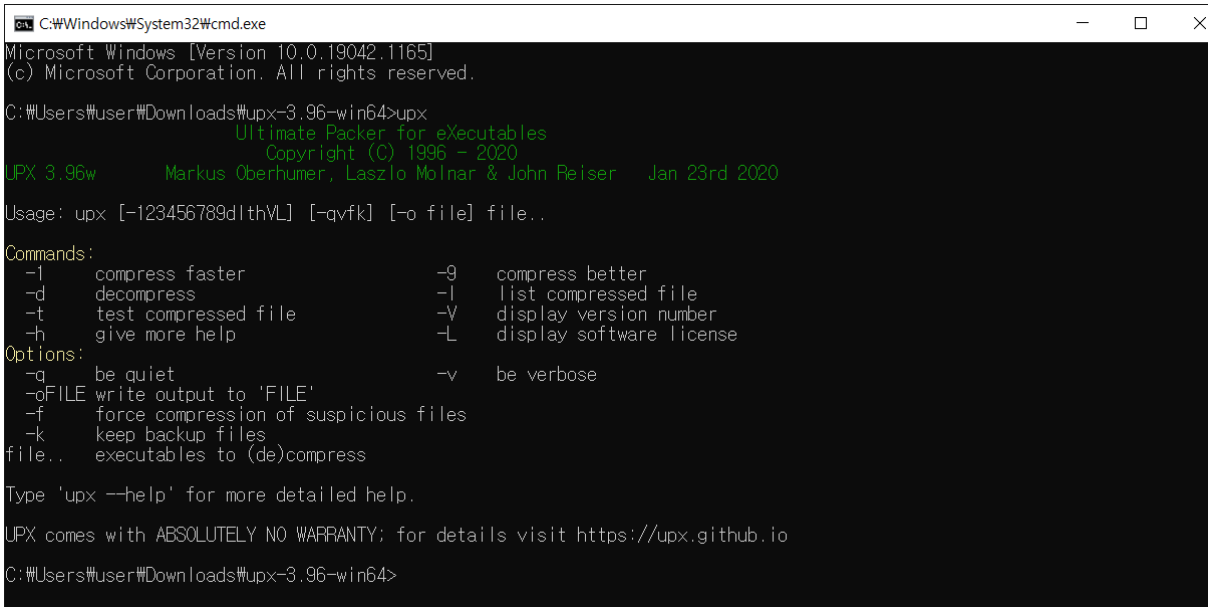


Info This file is packed with the UPX executable packer 이라는 말이 보인다. 그럼이제 UPX executable packer를 구글링해보자ㅋㅋㅋㅋ아놔!!!!!!

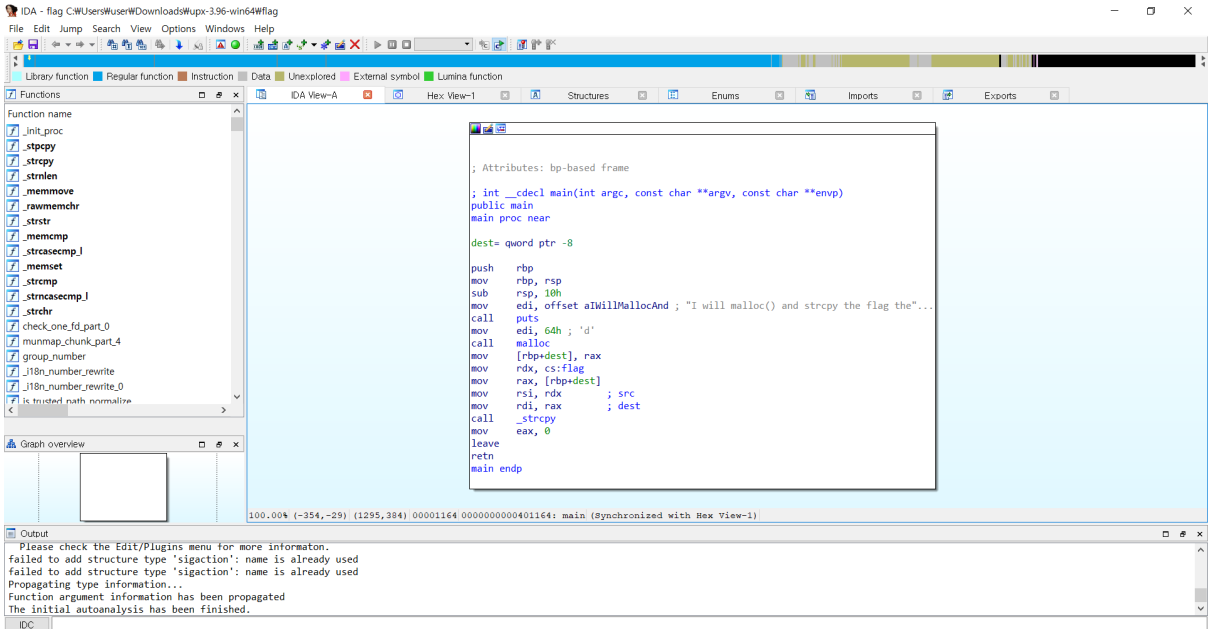
UPX를 언패킹하기 위해선 이 사이트에서 upx를 다운받아야한다고 한다.

그 다음 upx.exe와 언패킹할 flag파일을 같은 폴더에 두고 해당 폴더에서 cmd를 실행시킨다.

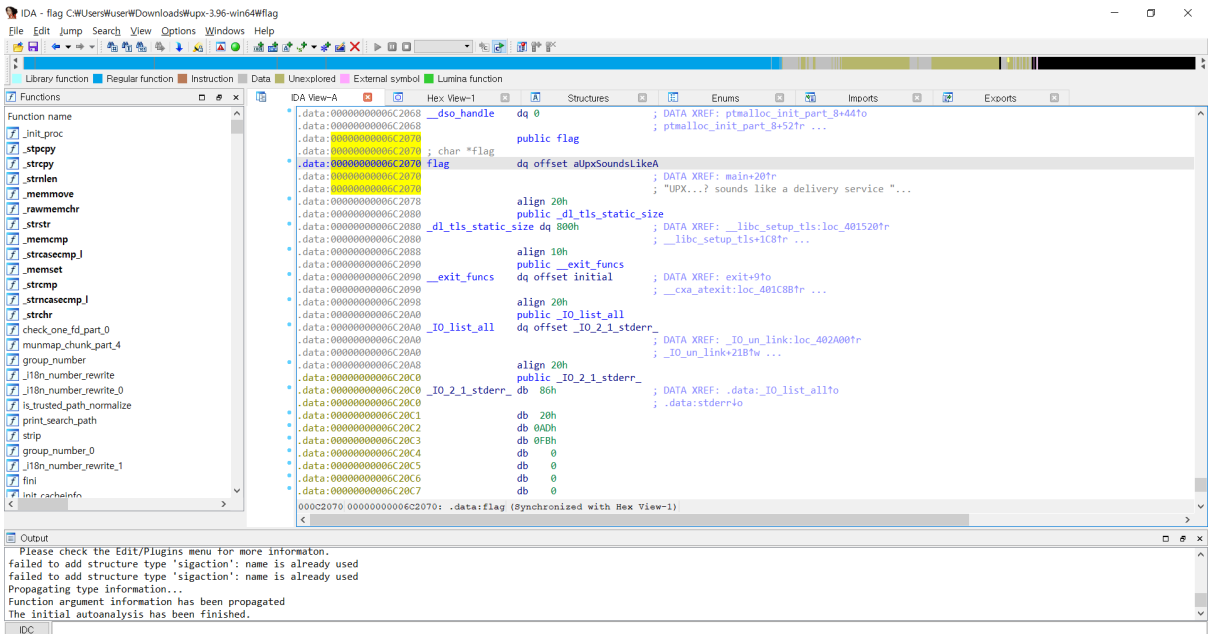
cmd에 upx라고 치면 upx사용법을 보여준다



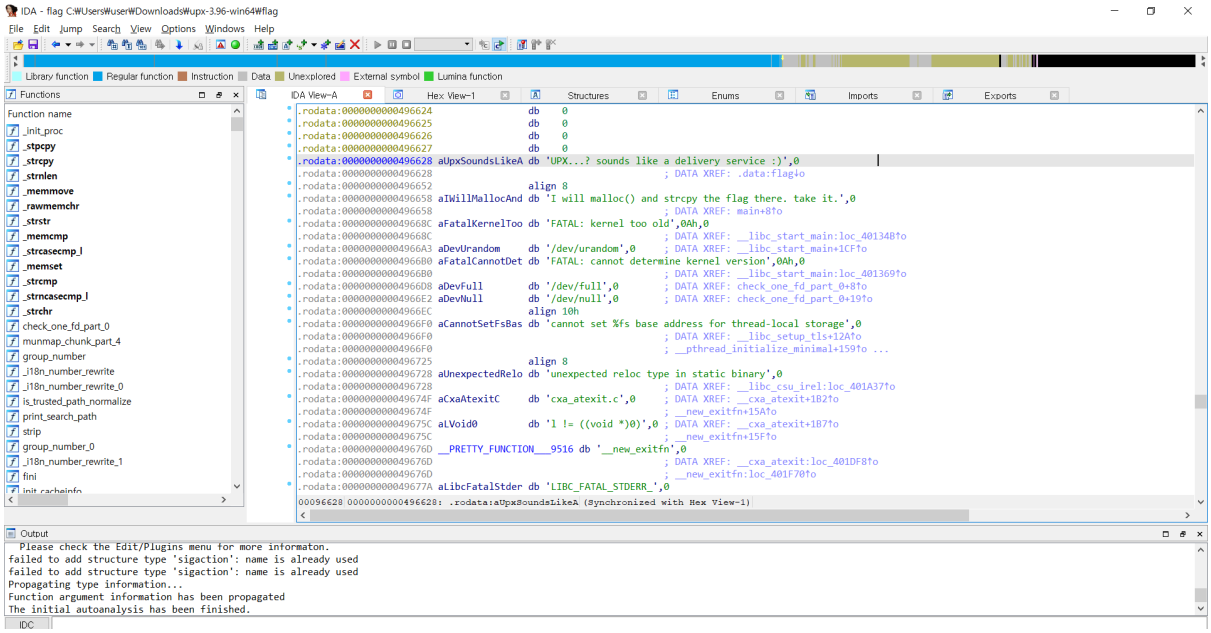
decompress : 압출을 풀다 `upx -d flag` 라고 입력하면 압축이 풀리는 것을 볼 수 있다. 풀린 flag를 ida로 열어보면 이렇게 뜨는데



여기서 cs:flag가 눈에 뜬다 더블 클릭으로 들어가보자



들어가보니 'UPX..? ~~'라고 보이는 부분이 있길래 그것이 flag인줄 알았으나.. 해봤을때 wrong이라고 뜬다ㅜㅜ
dq offset이 뭔지 모르겠으나 그 옆의 aUpxSoundsLikeA를 클릭할 수 있어서 들어가보니



다음과 같이 뜬다. 그래서 초록색 줄을 입력해보니 정답이더라!! 근데 아직 뭐가 뭔지 모르겠는 기분..... 아 그리고 peid를 이용하면 따로 안 찾아봐도 upx packing인지 아닌지 알려주는 듯 하다.

간지나게 적고싶다.....