**wirte-up**

1. hook.exe 라는 이름에서 후킹을 써야겠다 생각이 듦.
2. Exe 파일을 실행해보았더니 엄청 많은 메시지 박스가 뜸. 그 중 이름이 다른 몇 개가 있는 것 같음. Ida로 까보겠다
3. Ida로 분석을 하려하니 메시지 박스를 띄우는 곳들의 내용이 두 개로 갈리는 것을 알 수 있음. 하나는 standard고, 하나는 special key 임. 모든 것이 무작위로 나오는데 그 중 33개만 특정한 문자열이 출력되는 것을 알 수 있음. 여기를 후킹해야겠다고 마음 먹음

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

1. 이 부분을 보고, 메시지 박스를 후킹할 때 제목이 Special Key인 부분만 빼오면 되겠다 라고 생각을 함
2. Frida로 후킹을 진행. 막상 해보니 모든 메시지 박스의 제목 값이 null 인걸 알게 되었고, 제목을 가지고는 특정 내용을 뺴올 수 없겠다고 생각함
3. 따라서 내용 중 key: 인 부분이 포함되어 있는 부분을 후킹해야겠디고 젼략을 바꿈.
4. 내용들을 빼와서 숫자 순서대로 조합해보니 dec0d1ng\_K3y!s\_<s3cR3t\_k3y!s\_AES> 라는 문자열이 나왔다.

내용을 보니 decoding 키가 s3cR3t\_k3y!s\_AES 이거라는 것을 알 수 있다.

1. 키 내용을 보니 AES 암호화 알고리즘을 사용한 것 같다. 이거에 대해서 공부를 해봐야겠다..
2. AES 암호화와 관련한 pycryptodome 라는 것이 있는 것을 알게 되었고, 이를 이용해서 복호화 알고리즘을 짤 수 있음
3. 미리 주어진 암호화된 flag 파일을 디코딩 알고리즘으로 복호화 Pay1oad{mast3r1ng\_r3v3rs3\_sk1lls!}