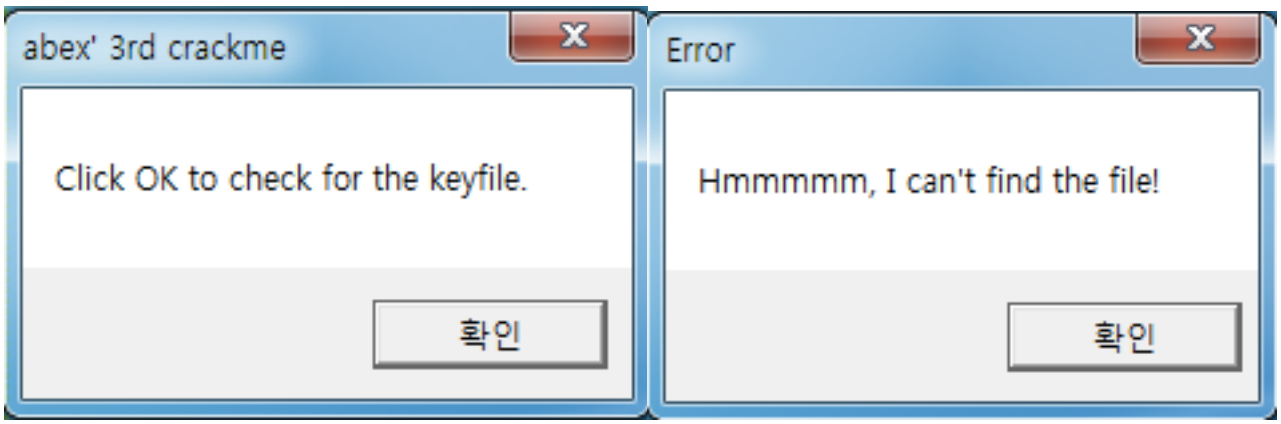
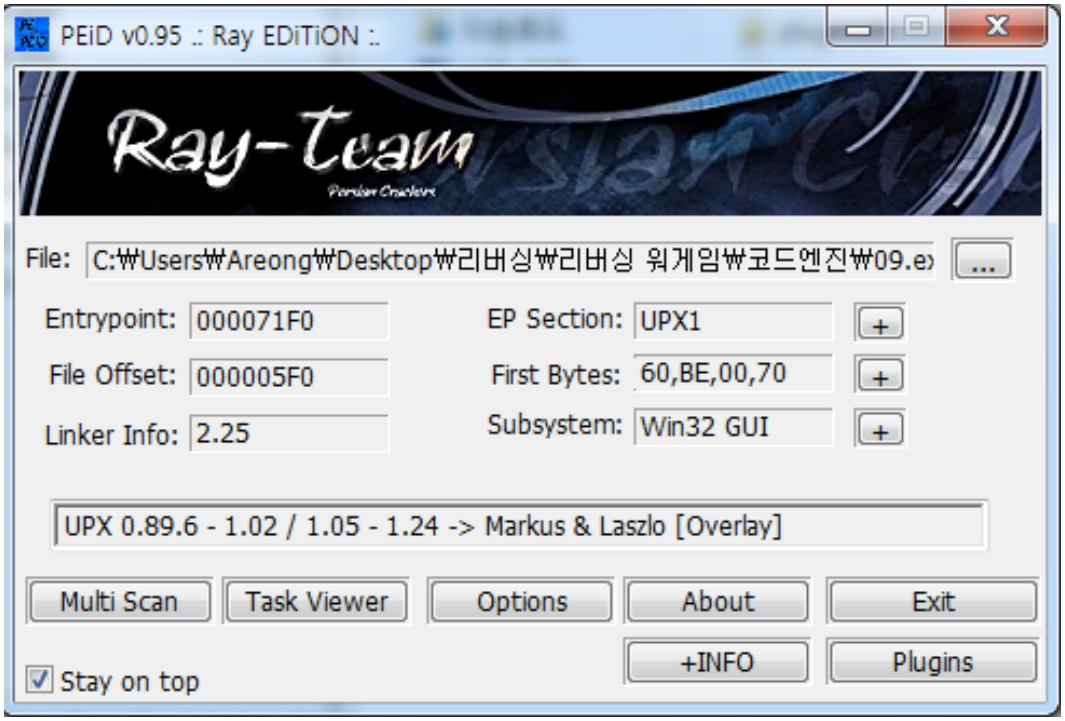
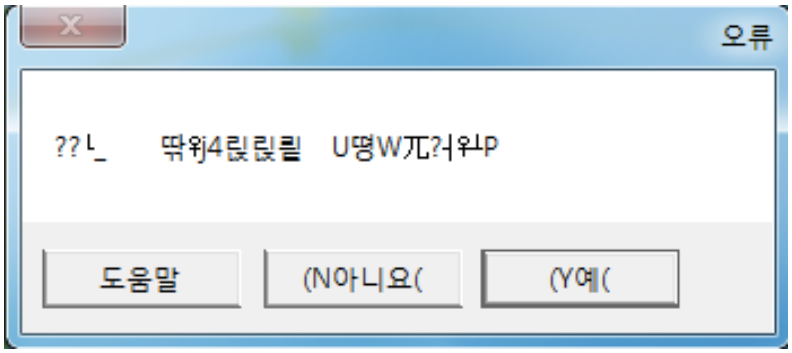


프로그램 실행 화면입니다. keyfile을 찾을 수 없다고 나옵니다.

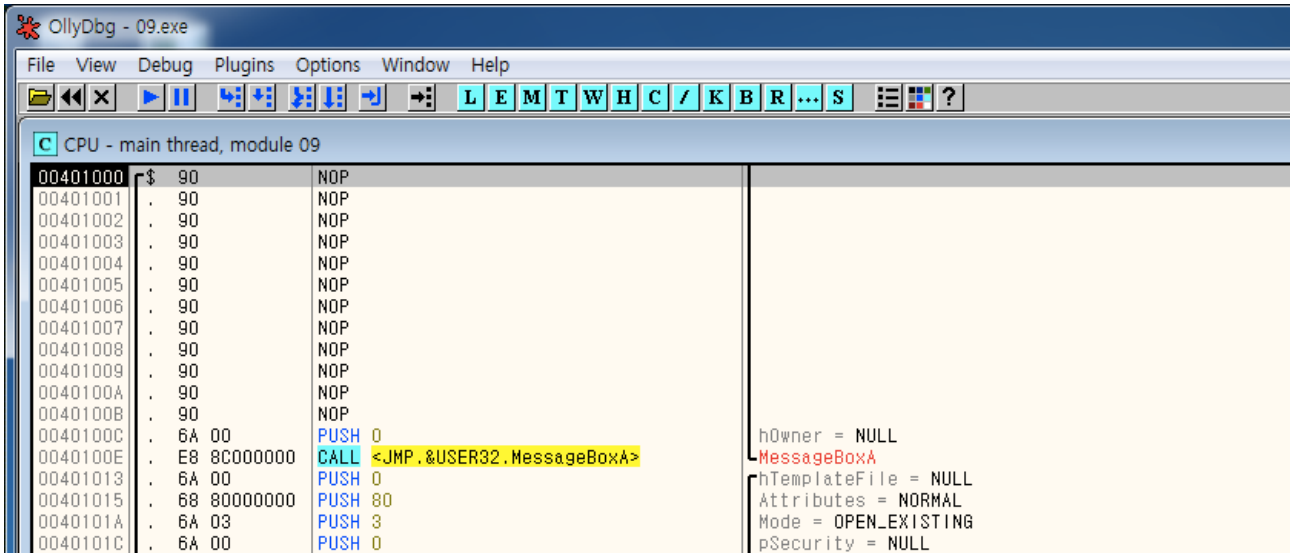


해당 프로그램은 UPX로 패킹되어 있음을 알 수 있습니다.

언패킹을 하고 진행하도록 하겠습니다.



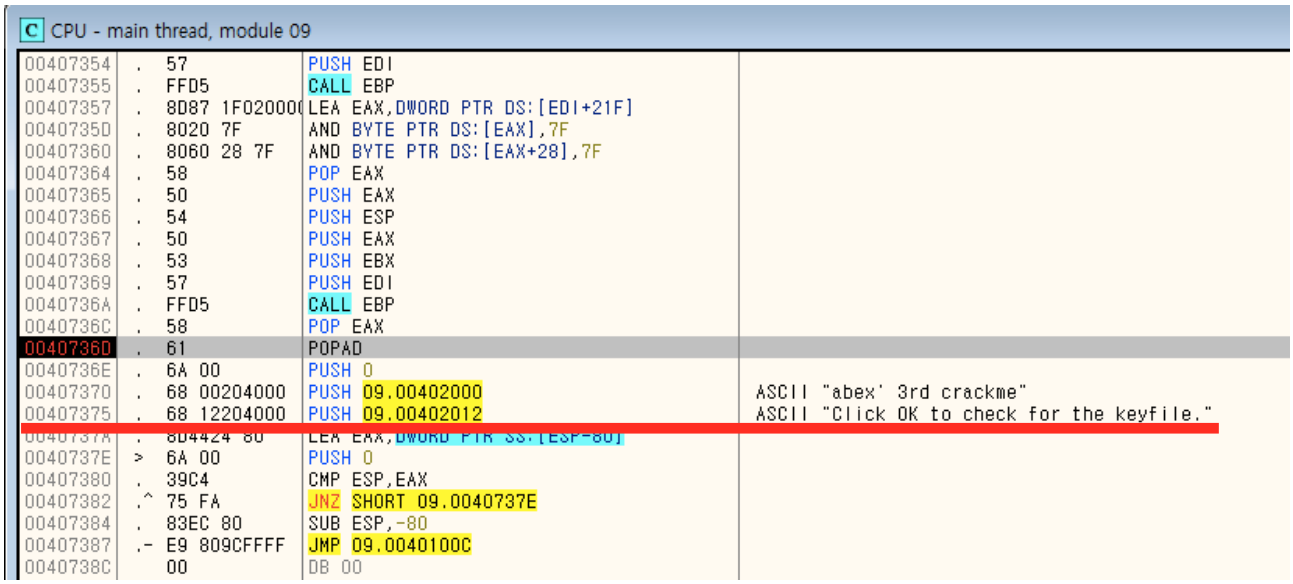
언패킹 후, 프로그램을 실행해보면 글자가 깨져있는 것을 알 수 있습니다.



이유가 무엇인지 올리디버거로 살펴보도록 하겠습니다.

MessageBox 함수를 호출하는 부분에 인자값 부분이 NOP으로 채워져 있습니다.

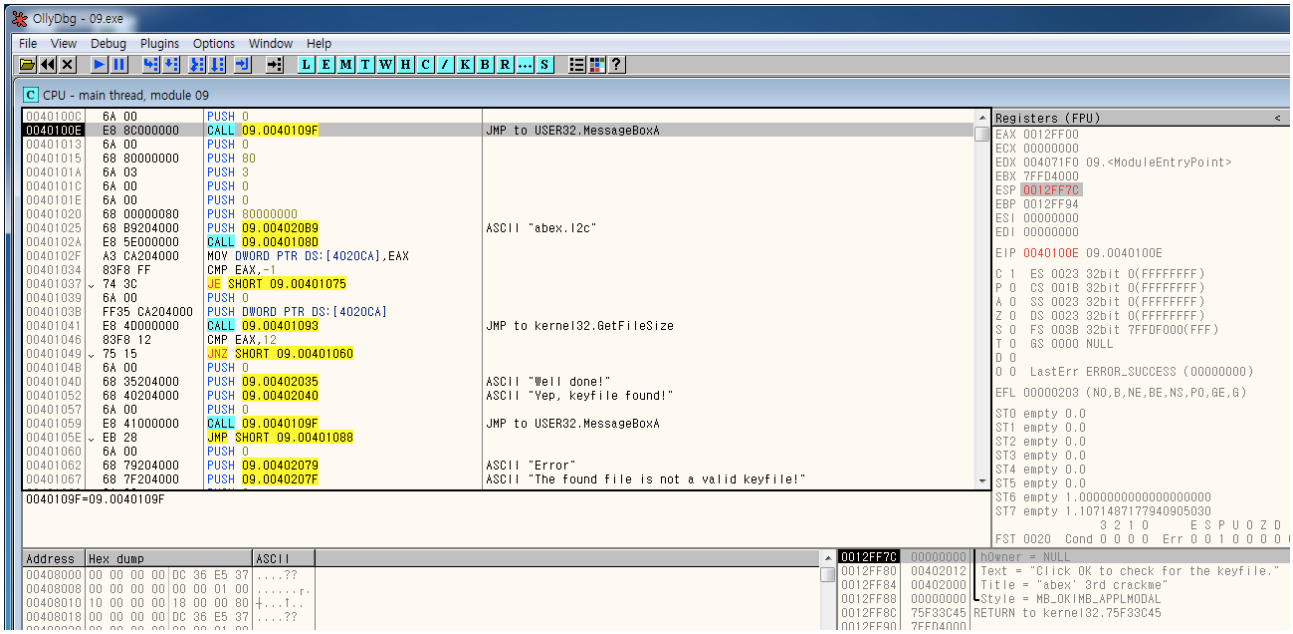
인자값이 NOP라서 메세지 박스의 글자가 깨지는 것을 알 수 있습니다.



언패킹을 하지 않은 코드입니다.

잘 보시면 POPAD뒤에 MessageBox의 인자값으로 보이는 문자열들이 있습니다.

그 문자열들이 JMP를 통해 원래 소스코드 흐름으로 돌아가기 전에 스택에 저장되어 있습니다.



JMP한 후 바로 MessageBox를 호출하기 됩니다.

이처럼 특정 소스코드 라인을 숨겨놓는 방법이 Stolen byte라는 일종의 안티 디버깅 기법입니다.

원래의 흐름으로 돌아오기 전에 중요한 함수의 인자값을 스택에 저장하고 그 후 사용하게 됩니다.

이런 상태에서 툴이나 일반적인 방법으로 언패킹을 하게 되면 인자값을 가져오지 못하게 되는 경우가 발생합니다.