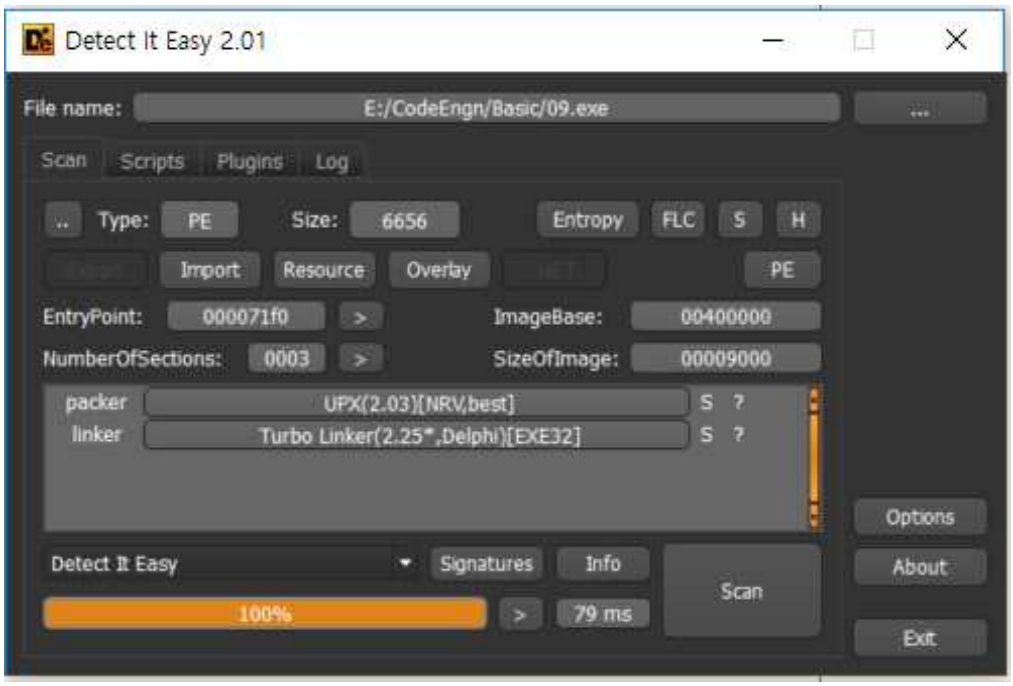
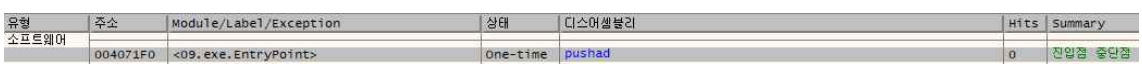
2019.02.14. CodeEngn Basic RCE L09
Tree to Tree

StolenByte가 뭔지 하고 한참 생각하다가 일단 돌려봤다.

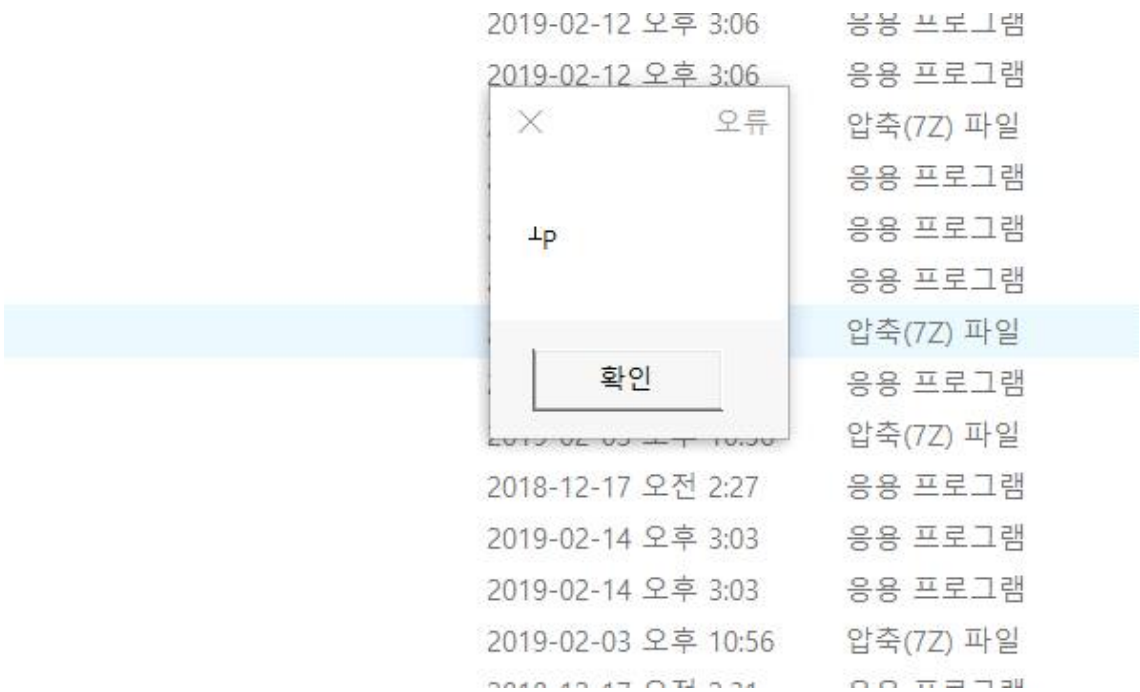


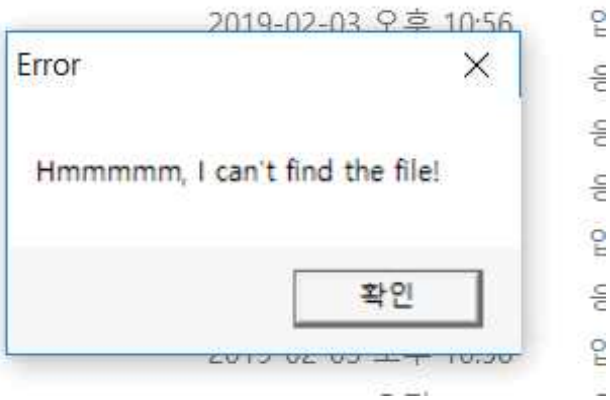
이번에도 UPX패커!
습관적으로 언패킹을 시작



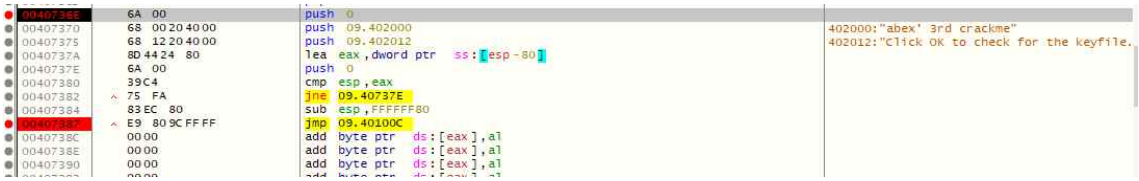
pushad와 popad를 찾은 순간 실행했을 때 나오는 문구들이 들어있다.
일단 UPX OEP를 찾고 덤프했다.

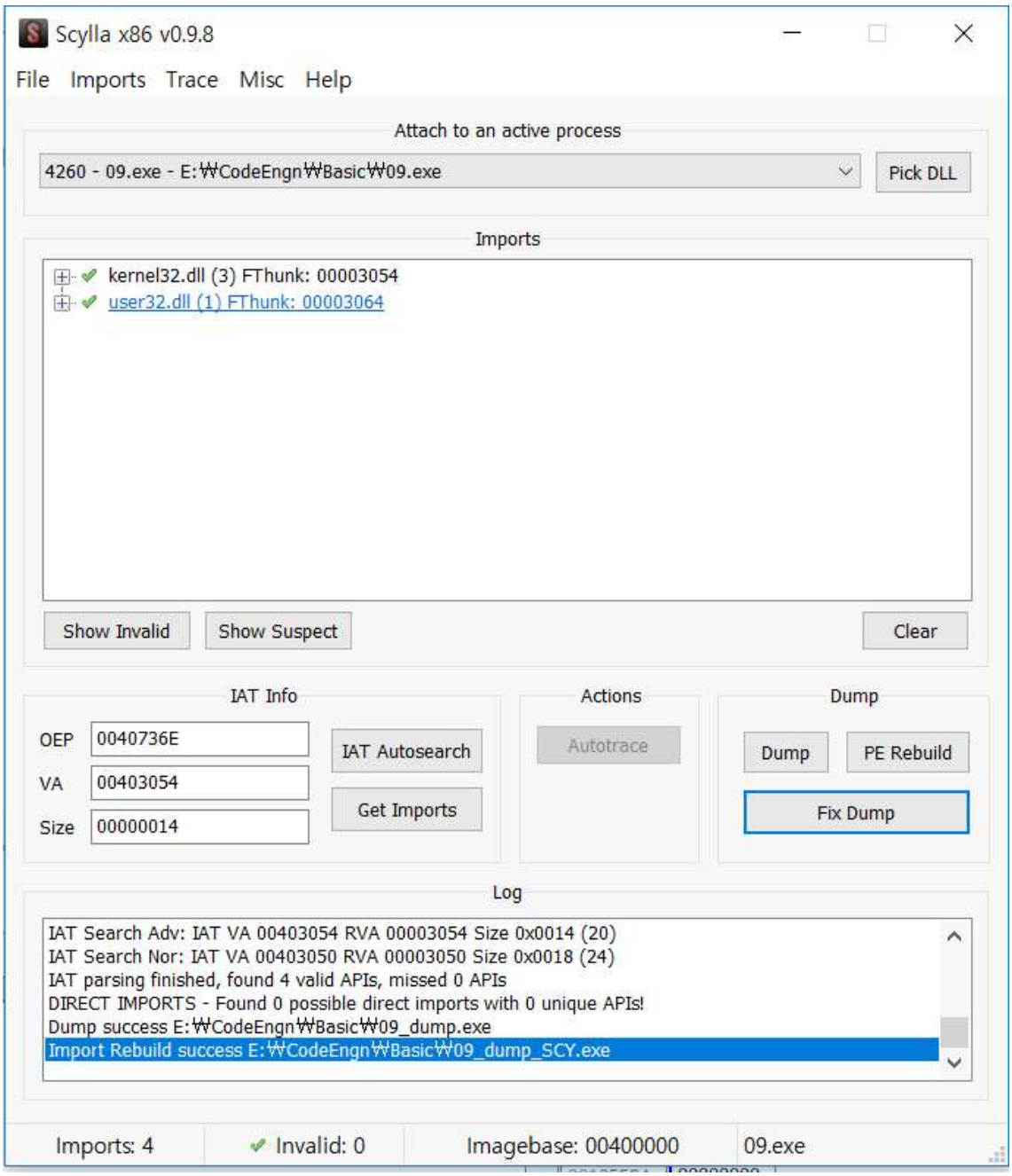
오류가 난다. 저 위에 문구 때문이라고 생각하고 StolenByte를 검색해봤더니
언팩을 막기 위해 코드 일부분을 숨겨놓는 행위



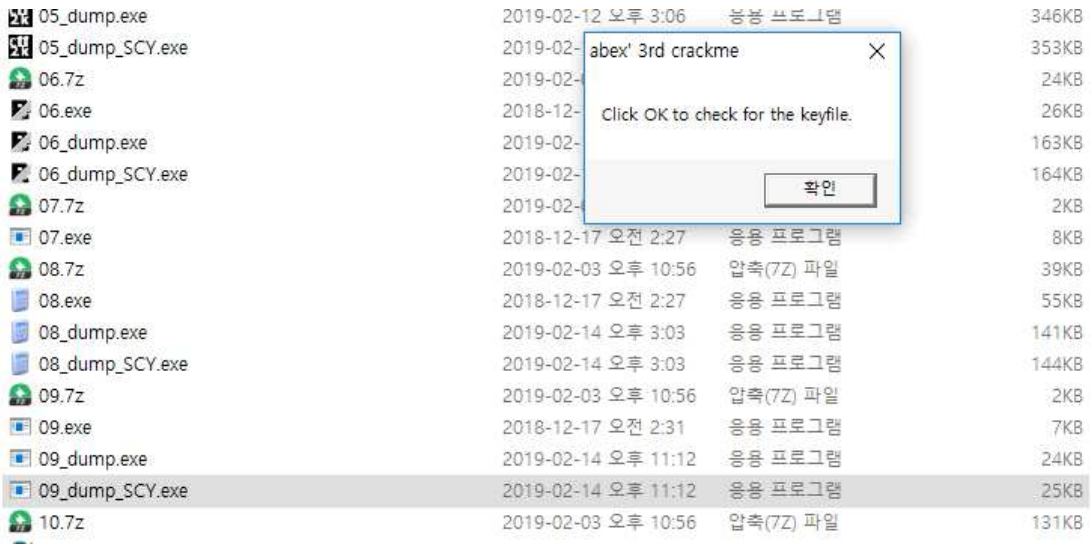


이번에는 문자열이 push되는 부분에 breakpoint를 걸고





덤프해서 실행해봤다.



잘된다. StolenByte는 12byte

6A0068002040006812204000