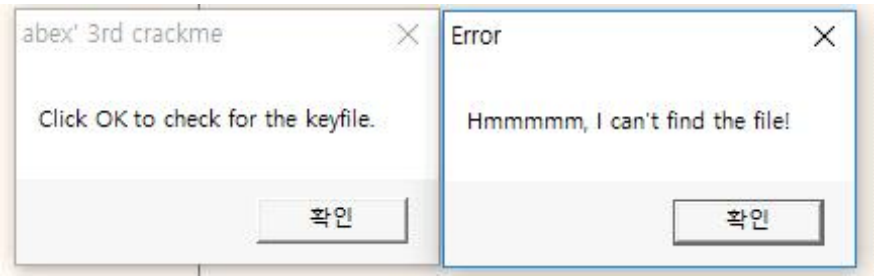
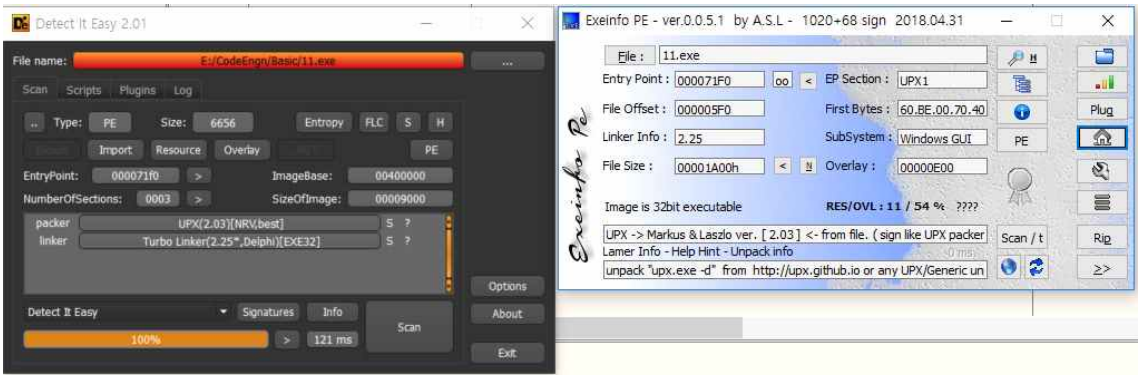
19.02.16 CodeEngn Basic RCE L11

Tree to Tree

Stolyenbyte를 찾아보자



실행했을 때 나오는 창

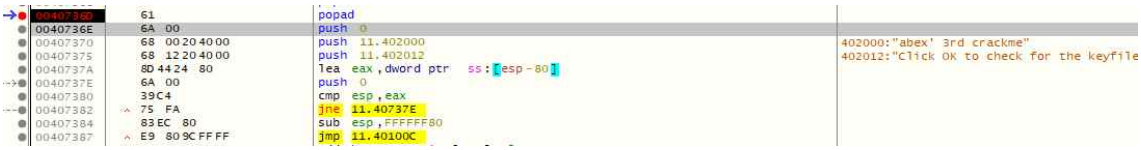


UPX 2.0버전으로 pack되어있음

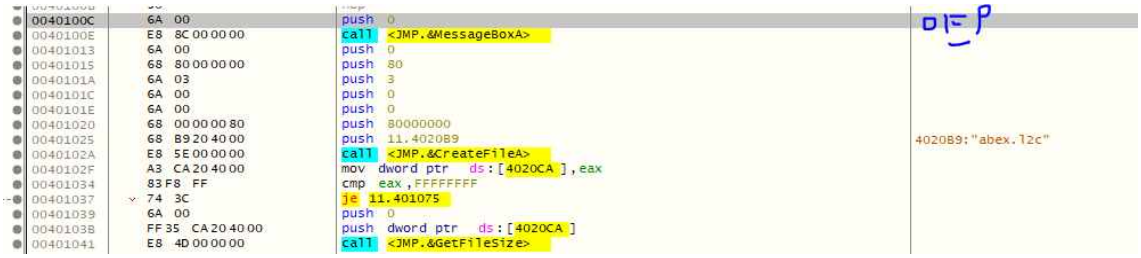
pushad breakpoint

주소	Module/Label/Exception	상태	디스어셈블리
004071F0	<11.exe.EntryPoint>	One-time	pushad

실행 후 popad 찾으러 감.
밑으로 쭉내려서 popad에 breakpoint걸고 실행



실행시켰을 때 나오는 문자열들이 push되는 모습
Stolenbyte 6A006800204000 6812204000



OEP 0040100C - C(opset) = 00401000
004010006A006800204000 6812204000
Clear