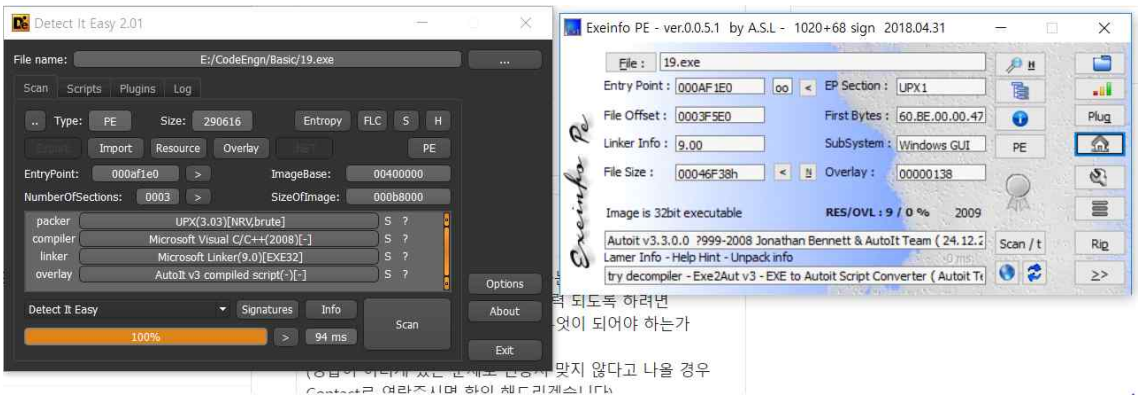
2019.02.21. CodeEngn basic 19
Tree to Tree

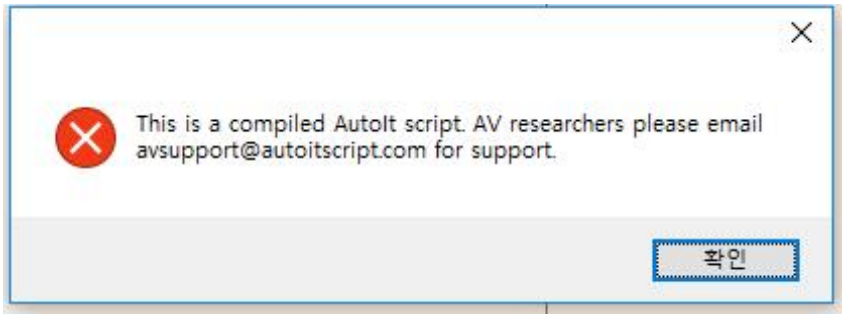
몇 밀리세컨드 후에 종료되는지 찾아야되는 문제
basic지금까지 문제 중 가장 오래걸림...

우선 UPX로 팩되어있고 AutoIt이라는 Window응용프로그램 쉽게 만들어주는 툴? 로 만들어졌다고 나온다.

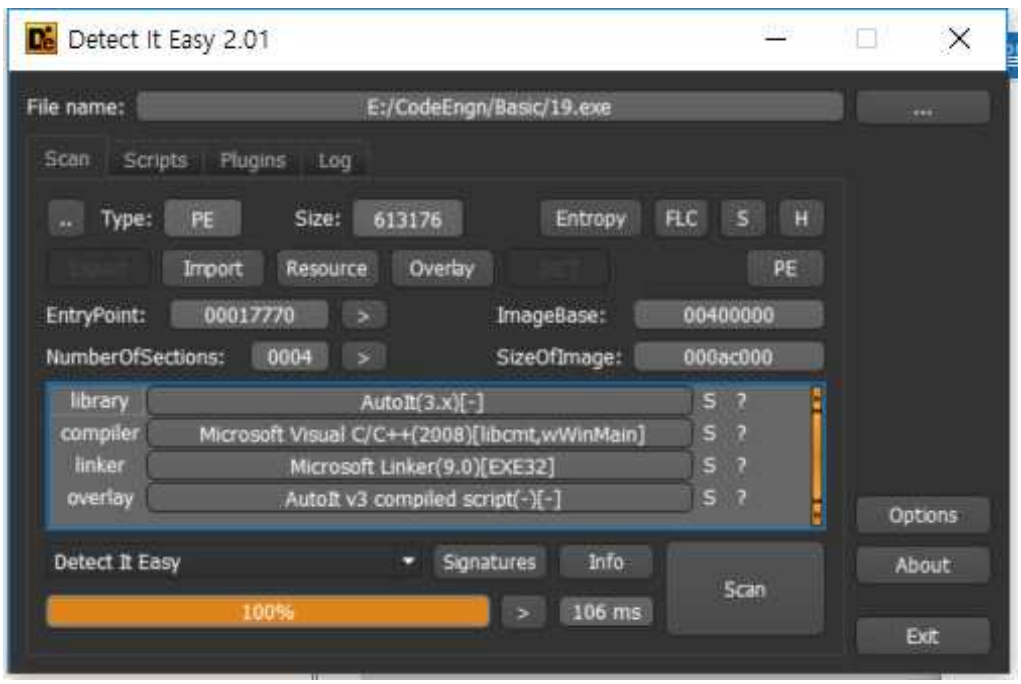


일반적으로 실행시키면 위처럼 창이 뜨고 약 11초정도 후에 꺼진다.

디버거로 실행시키니까 아래 창처럼 뜨고 종료됨.
안티디버깅 되어있음.

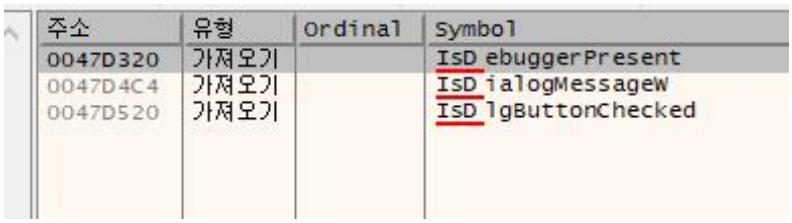


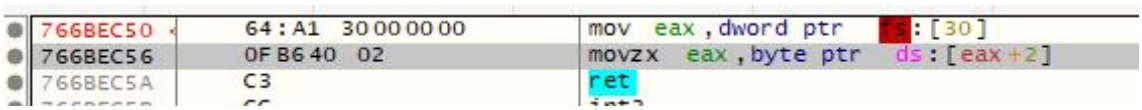
우선 완벽하게 풀기위해 UPX만든 사람이 배포한 툴을 이용해서 unpack



언팩된 모습.

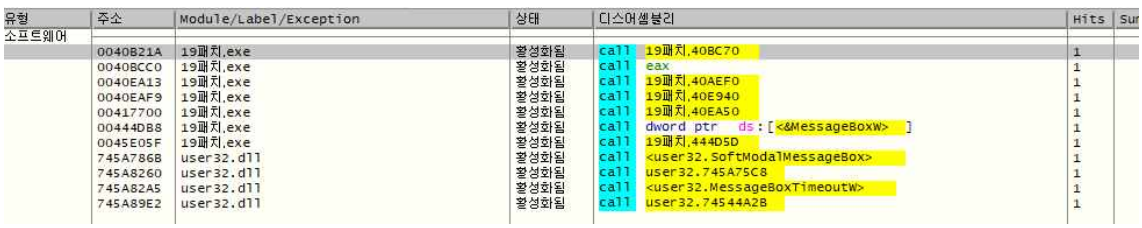
어떤종류의 안티디버깅인지 찾다보니 IsDebuggerPresent를 사용한다는 사실을 찾음
다행이다 가장 쉽다고생각하는 안티디버깅! TLS도 한번 풀어보고싶다.



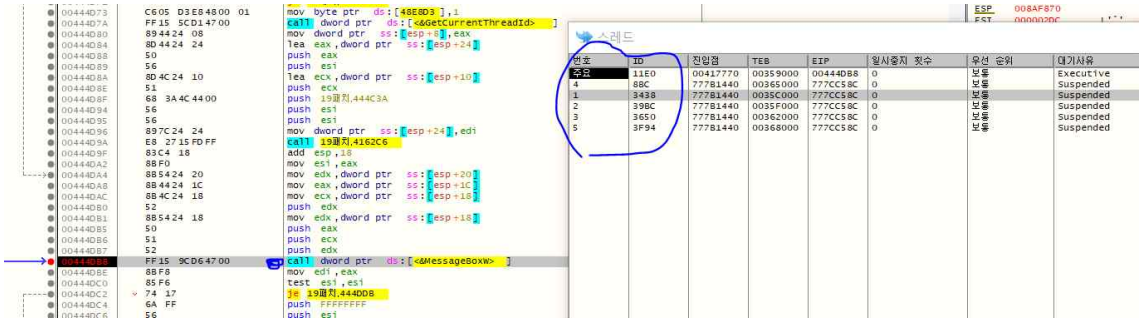


PEB+2에 있는 값만 00으로 바꿔주면 회피가능

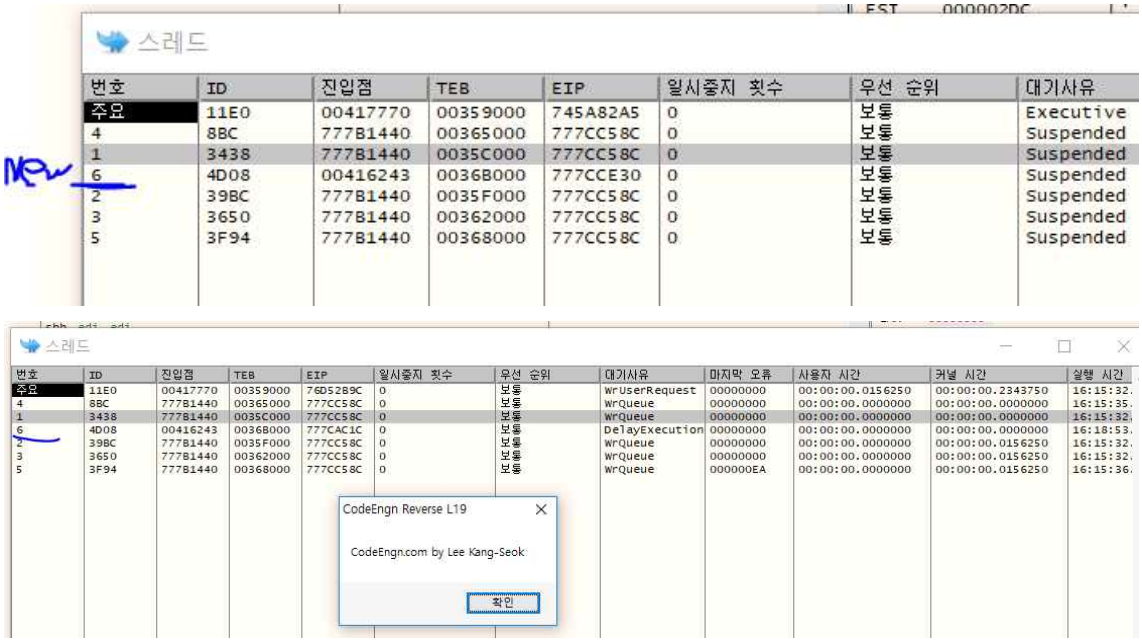
그 후에 Message창이 띄워지는 부분을 계속 트레이싱하면서 변화들을 관찰하던중에



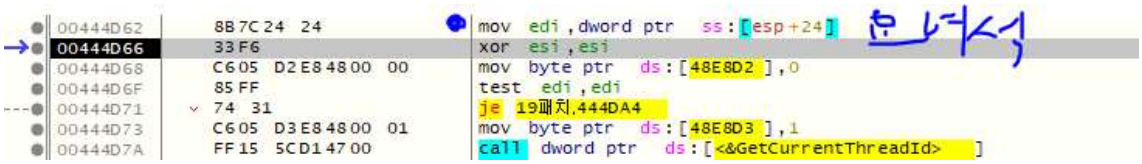
MessageBoxW로 진입하는 순간에 스레드가 실행되고 약 11초뒤에 6번스레드가 종료됨



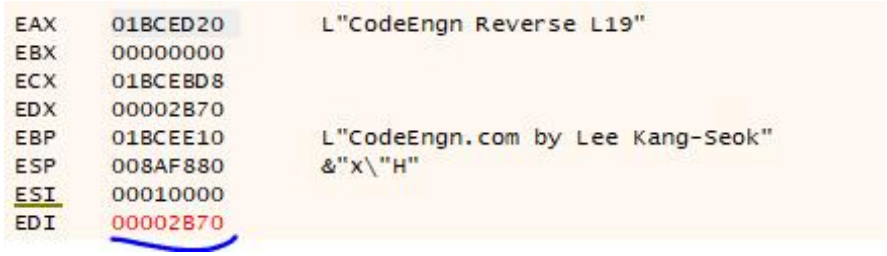
6번스레드가 실행된모습

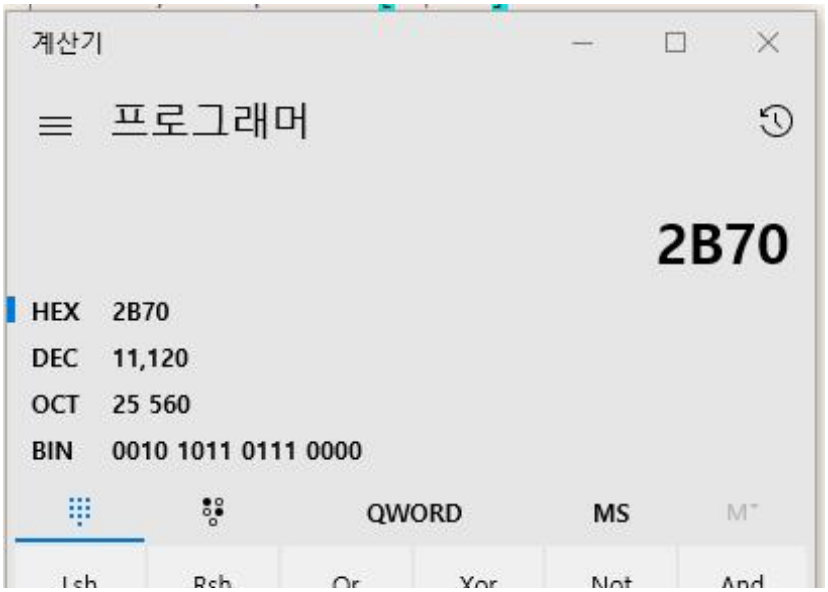


이제 MessageBoxW전 명령어들만 보면 된다고 생각하여 레지스터들을 유심히 확인



mov edi, dword ptr ss:[esp+24] 부분이 밀리세컨드를 저장하는 부분




계산기
프로그래머
2B70
HEX 2B70
DEC 11,120
OCT 25 560
BIN 0010 1011 0111 0000
QWORD
MS
Lsh
Rsh
Or
Xor
Not
And

11120
Clear