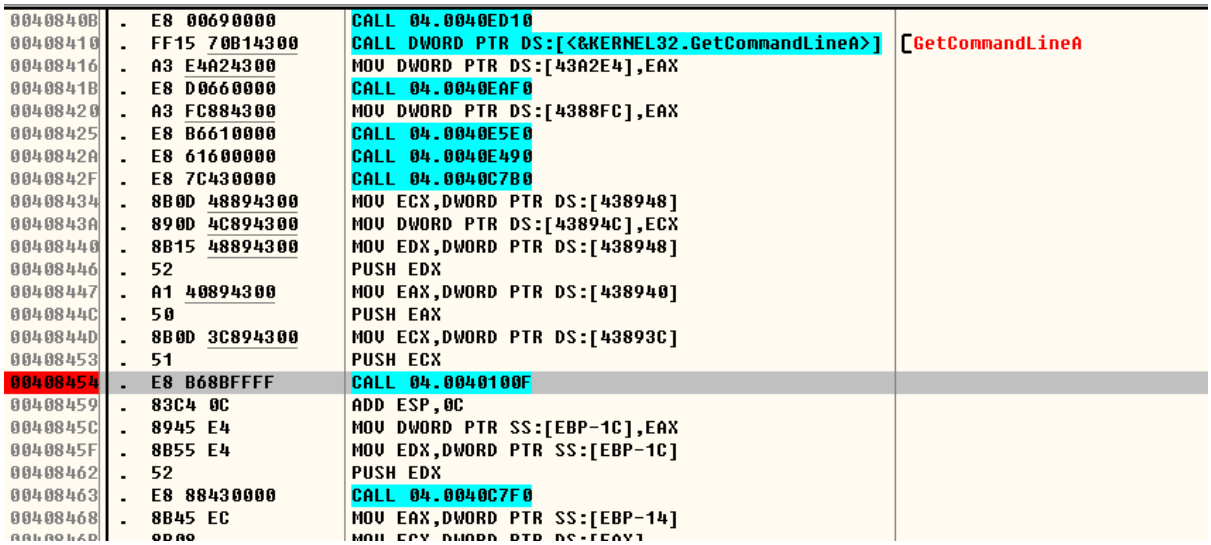
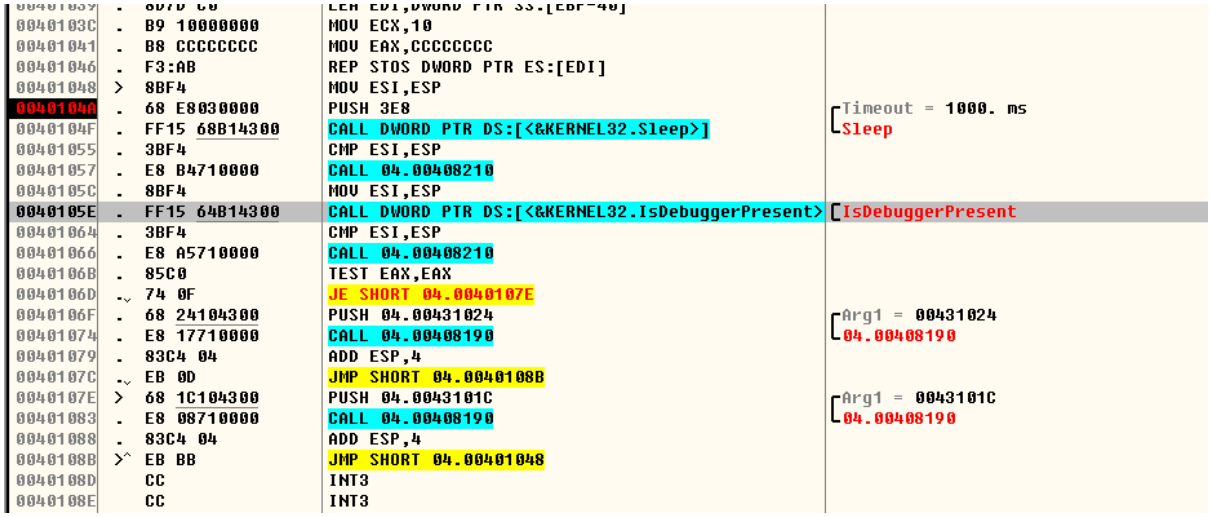
정상동작하면 정상만이 찍힌다.

디버거로 실행!



BP걸어둔부분을 F8로 지나치자 디버깅당함이 떴다

그래서 BP걸고 들어가보았다.

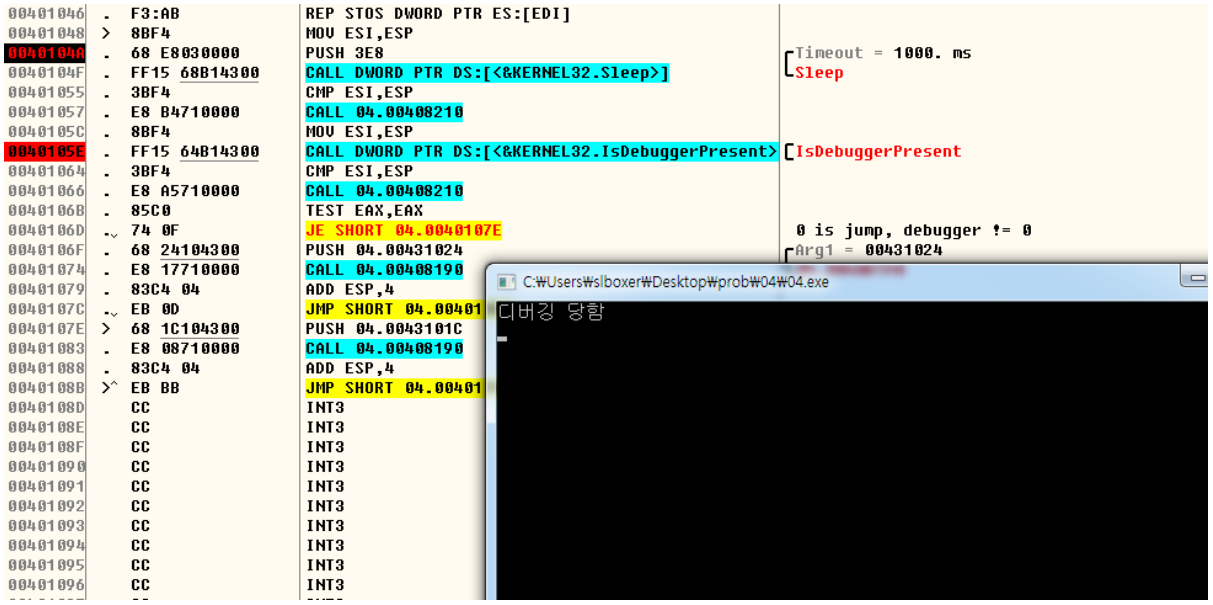


위쪽 잘린부분은 스택에 공간만들어주는 작업이니 무시하고

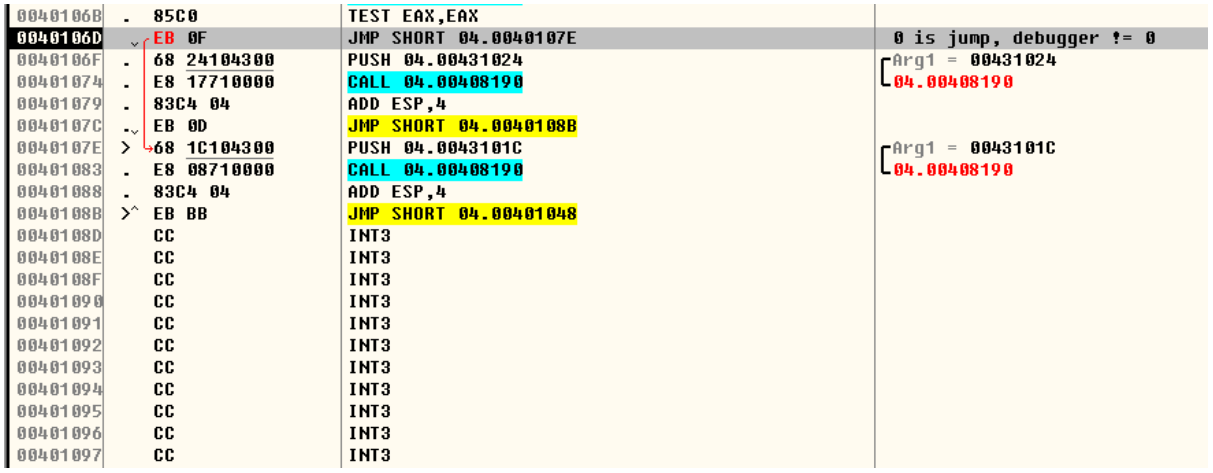
1000ms씩 쉬는 함수가 있다(sleep) 동작할때 보면 1초마다 글씨 찍히는걸 볼수있다.

그리고 아래에 IsDebuggerPresent로 디버거가 있는지 알아본다.

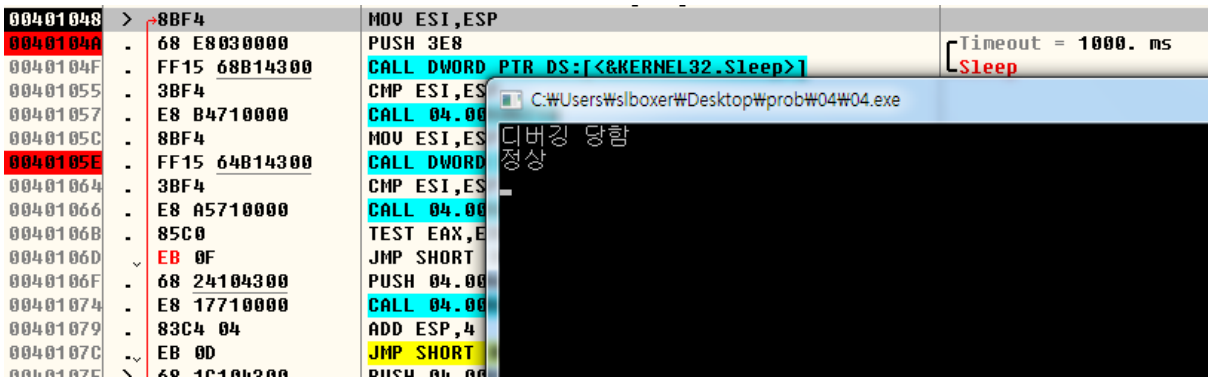
TEST EAX, EAX가 0이면 점프하는데 IsDebuggerPresent에서 EAX가 0이 아니었는지 점프하지 않고 push 00431024를 진행하였다.



그대로 진행했더니 이렇게 디버깅당함이 떴다.



디버거 탐지 함수는 찾았지만 난 이 프로그램을 속일것이다. JE를 JMP로 바꿨다.



속이기까지 성공했다.

따라서 디버거 탐지함수는 IsDebuggerPresent