Back To User를 이용한 lena 4번 문제풀이

Pwn&play 박석은

Back To User Mode란?

특정 이벤트를 이벤트가 일어나기 전으로 설정해두고 Call 명령이 일어난 다음 바로 다음 위치를 잡을 수 있는 기능이다.

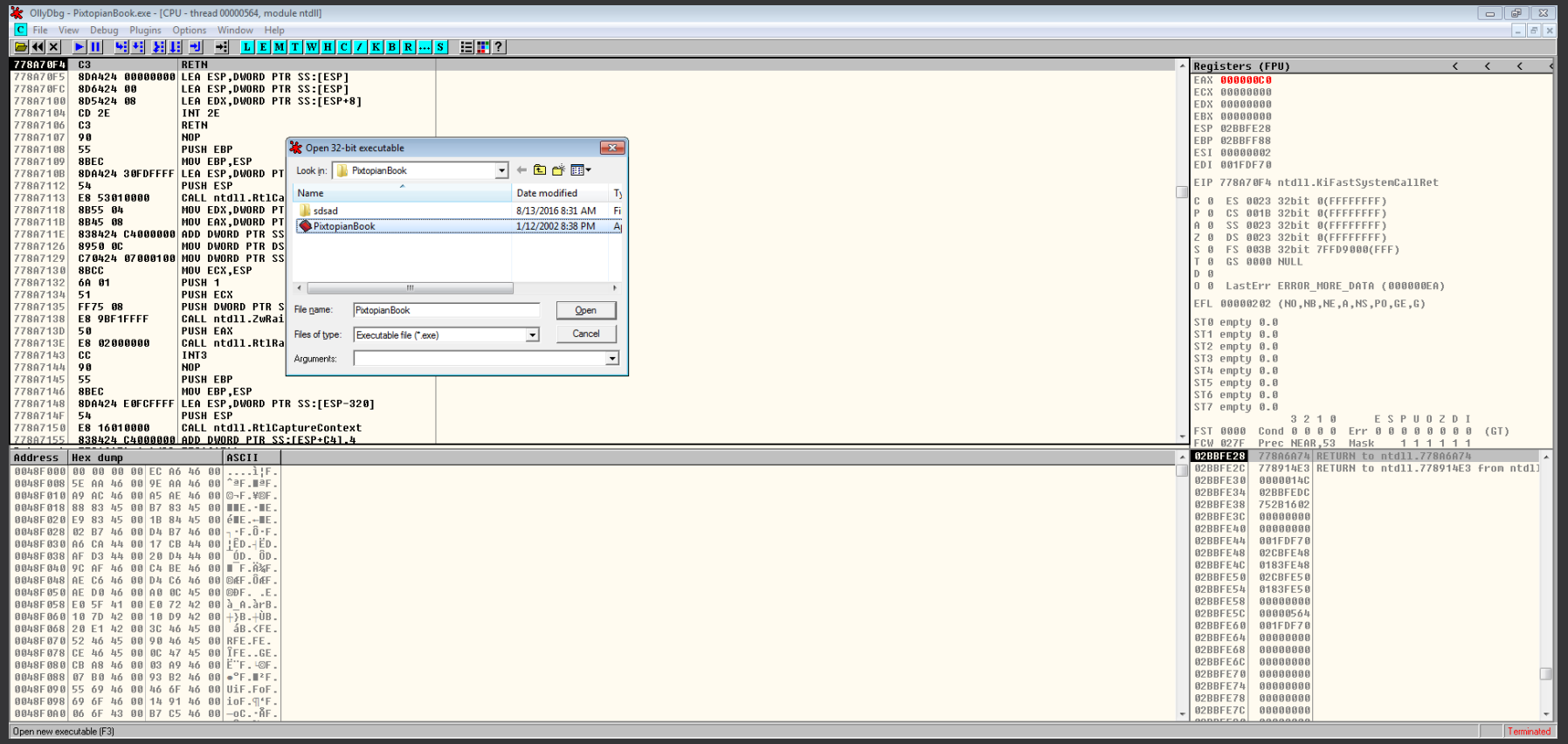
참고사항

필자의 PC 환경은 win10 64bit이다.
필자의 PC에서 Back To User 기능을
사용해보려 했지만, 되지 않아 구글링을 해본 결과
64bit에서는 해당 기능이 되지 않는다고 한다.

그래서 Vitual Box에 32bit 운영체제를 올렸다.

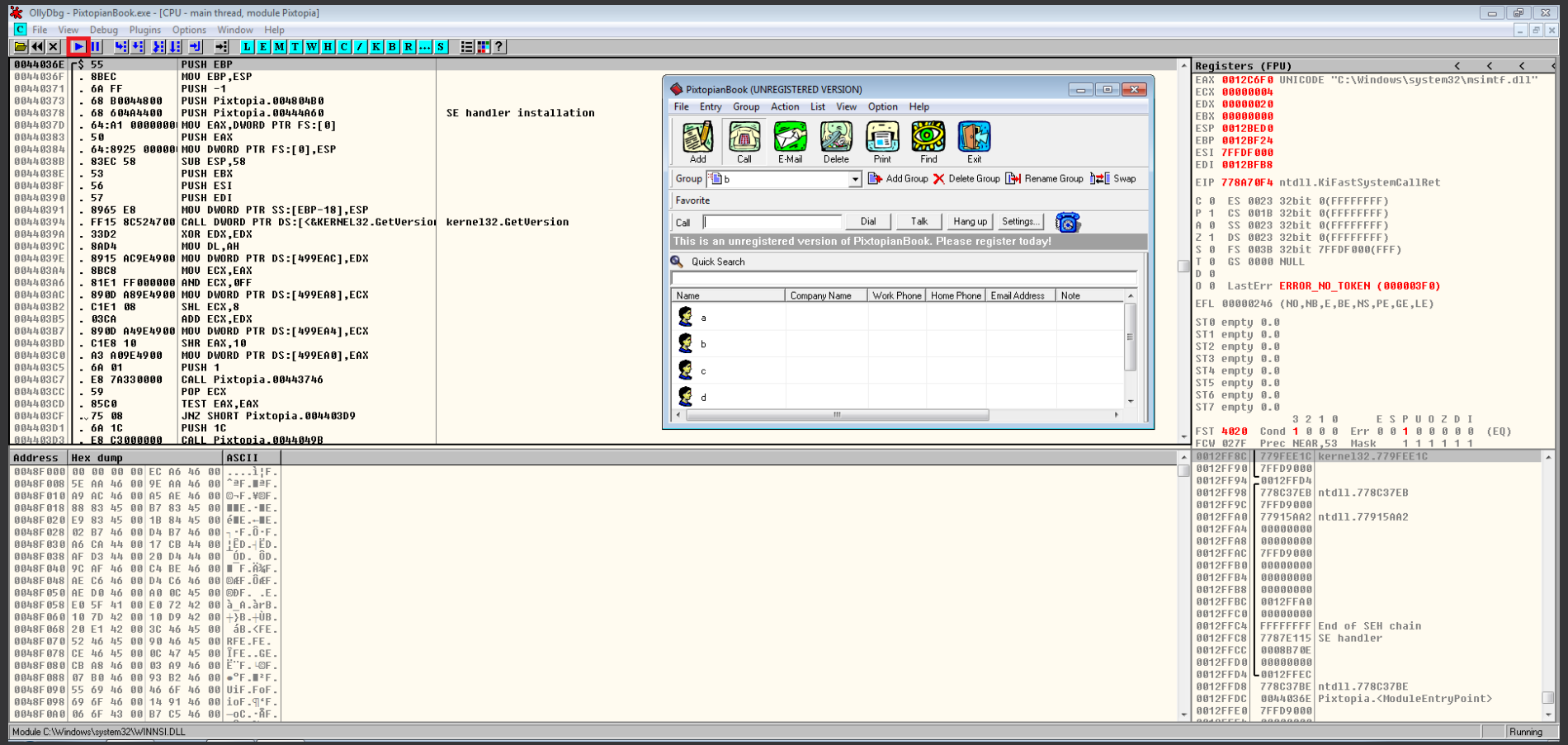
추가적으로 Ollydbg는 1.10버전을 사용했다.

문제 풀이1



Ollydbg를 이용해 PixtopianBook.exe를 Open한다.

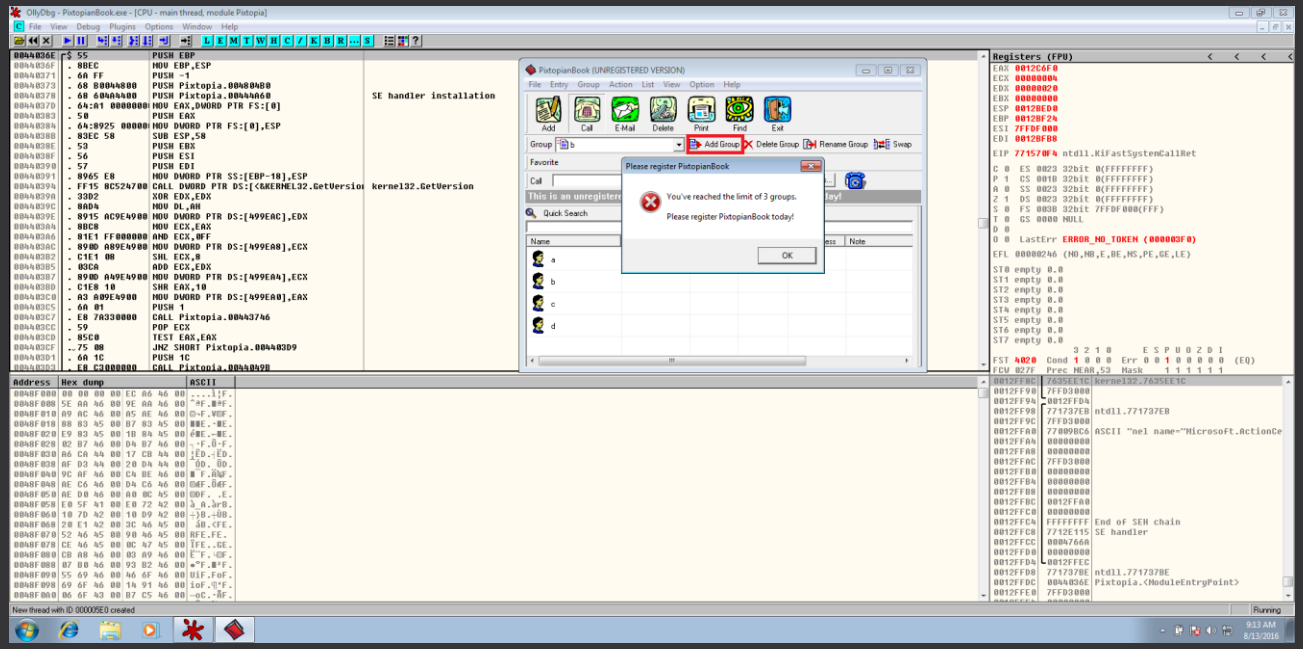
문제 풀이2



프로그램을 열고 F9(Run) 또는 빨간색 박스를

클릭 하면 프로그램이 실행되는 것을 볼 수 있다.

문제 풀이3



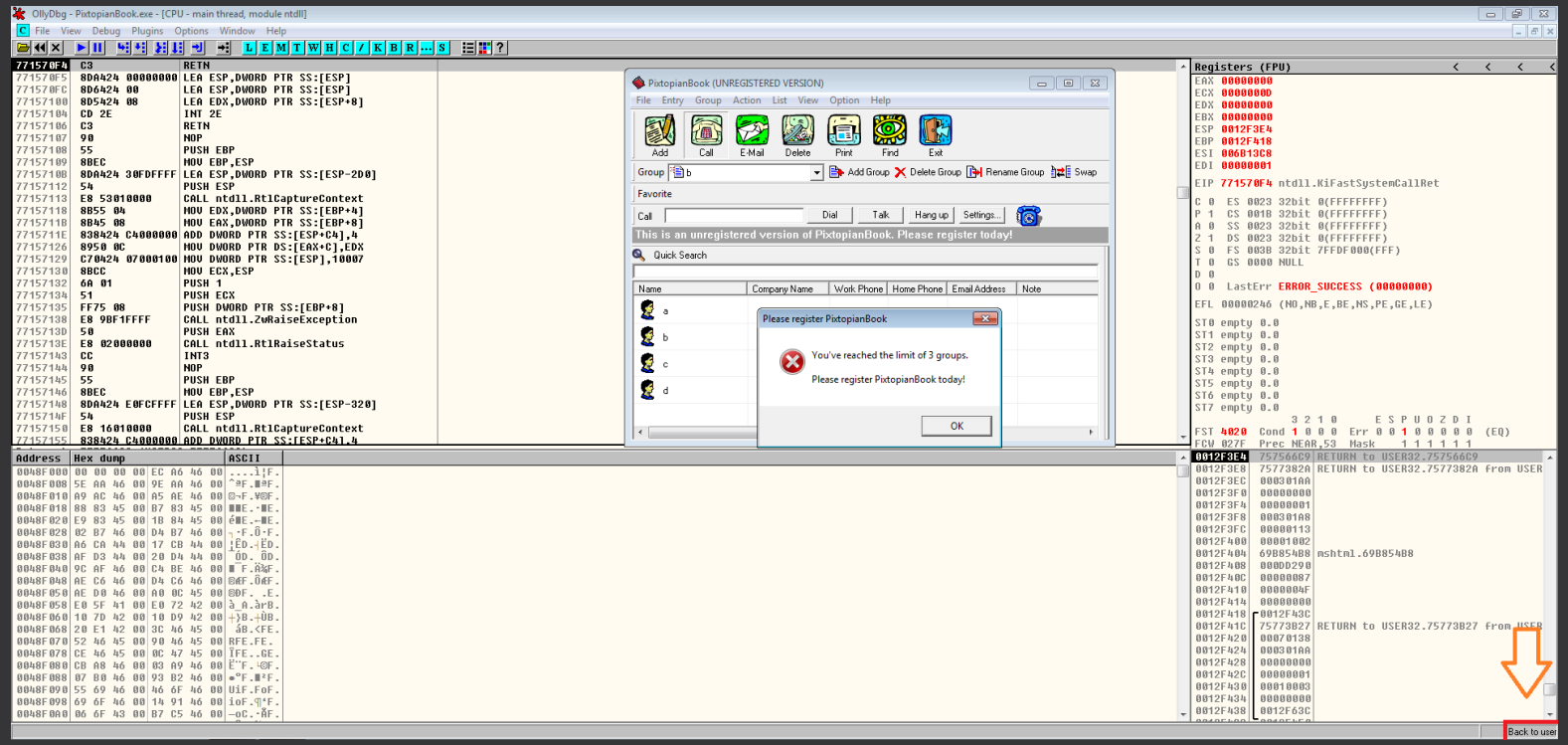
빨간색 박스를 클릭하면 그룹을 만들 수 있는데

기존에는 3개이상 만들려고 하면 화면과 같이

에러창이 출력된다.

이제 패치를 통해 그룹을 더 생성해보도록 할 것이다.

문제 풀이4

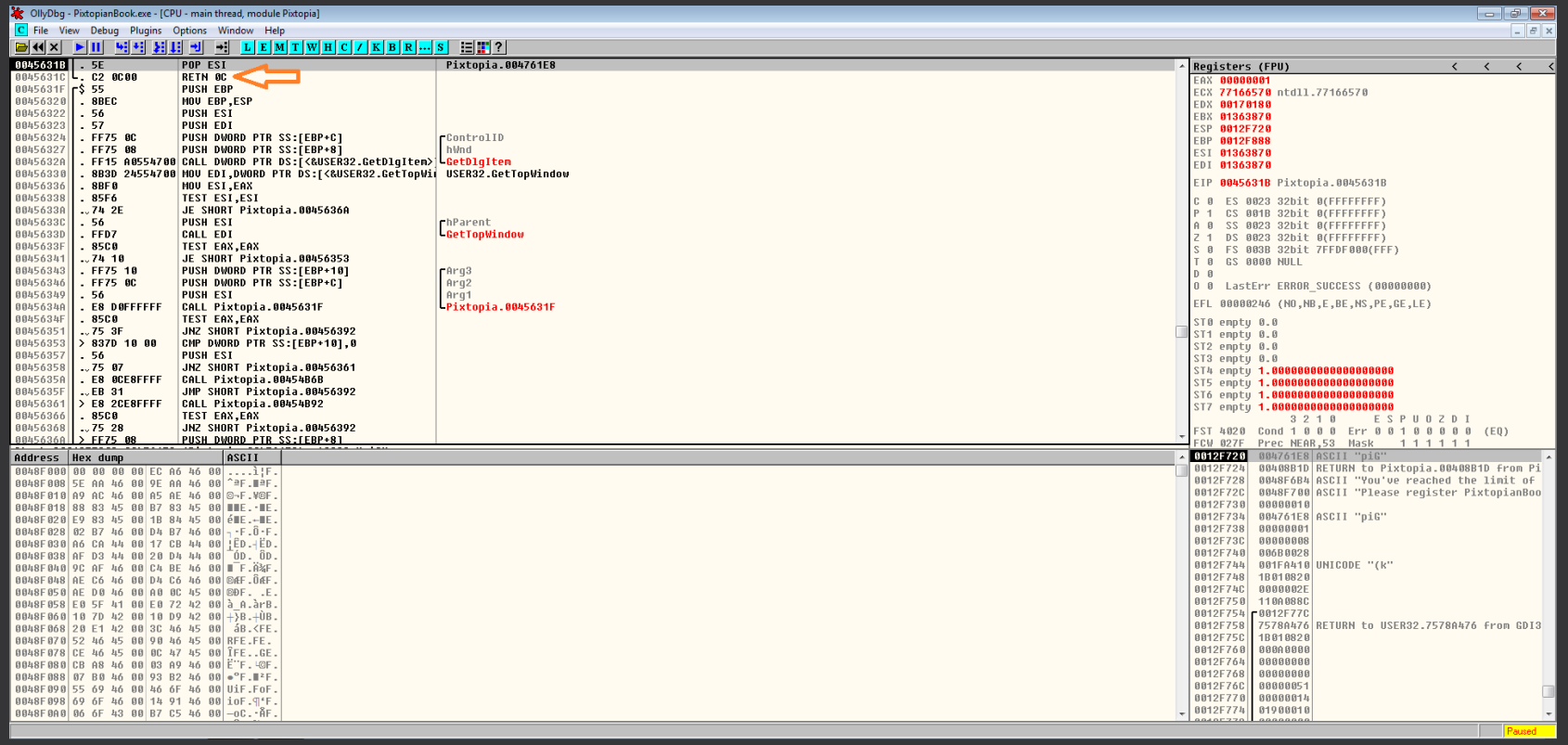


에러메시지 창이 뜬 상태에서 Ollydbg에서 Pasue(F12)를 하고

Execute till user code (Alt + F9)를 누르면 우측 하단 처럼

Back To User mode로 진입하는걸 확인 할 수 있다.

문제 풀이5

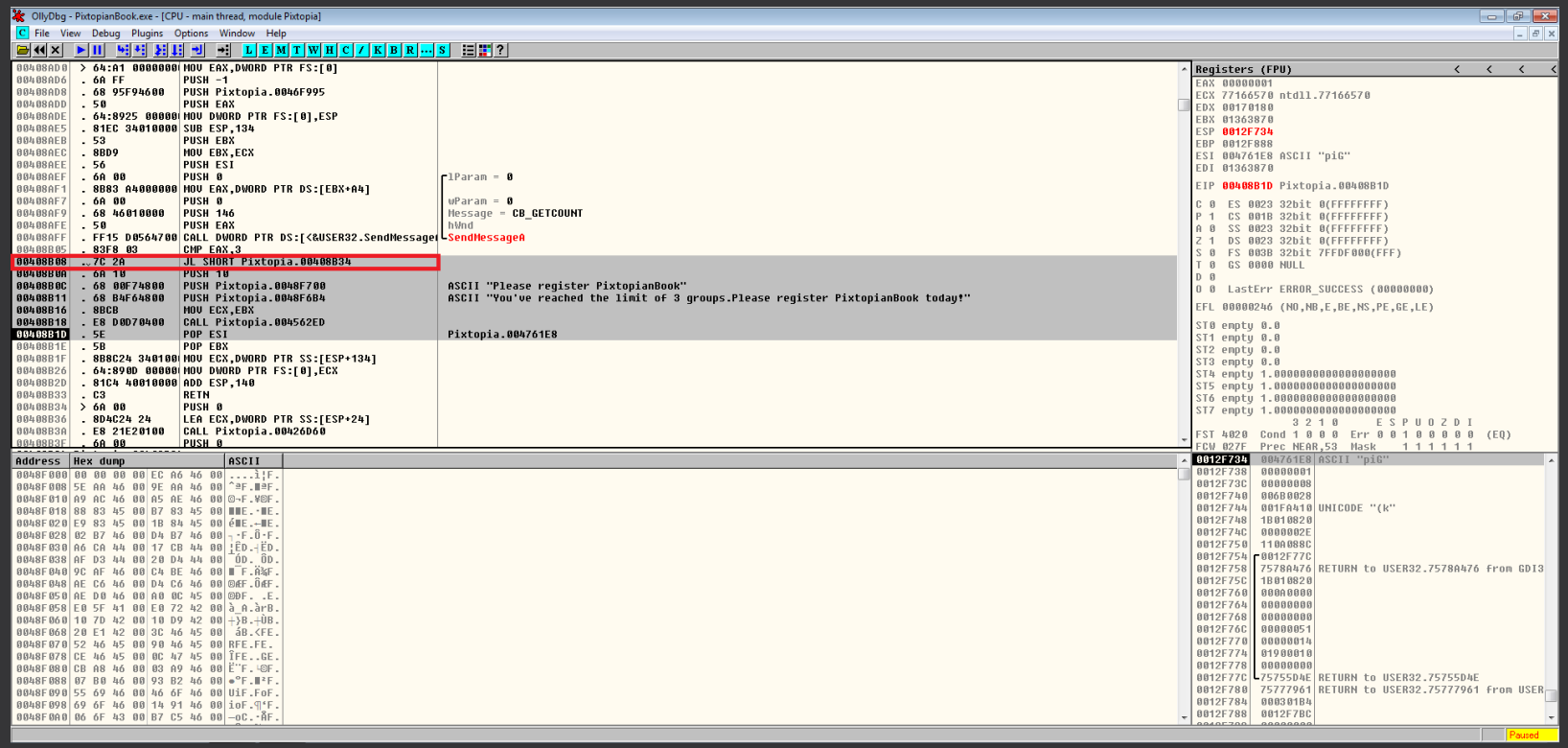


이전 페이지에서 봤던 에러메시지 창에 있는 OK 버튼을 누르면

해당 코드창으로 넘어가게 된다.

그럼 F8을 눌러서 화살표가 가리키고 있는 RETN으로 진입해보자.

문제 풀이6



RETN을 타고 넘어오면 00408B1D로 오게되는데

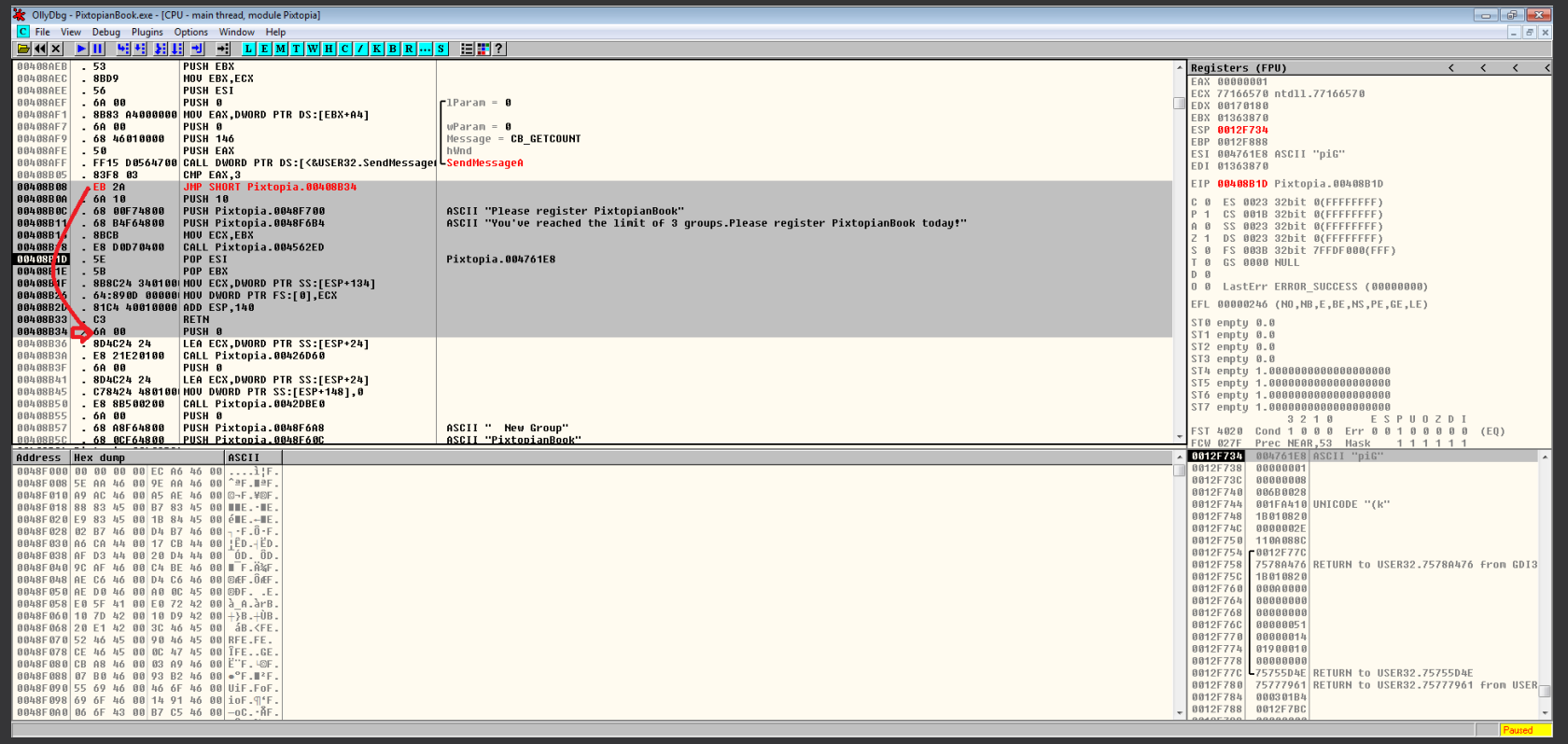
스크롤을 조금 올려보면 아까 봤던 메시지가 적혀있는 부분을 보게된다.

자세히 보면 빨간 박스 부분의 JL문을 지나면서 해당 에러창이

출력되는 것을 알 수 있다. 그렇다면 해당 부분을 JMP(무조건 점프)로

바꿔주게 되면 어떻게 될까?

문제 풀이7

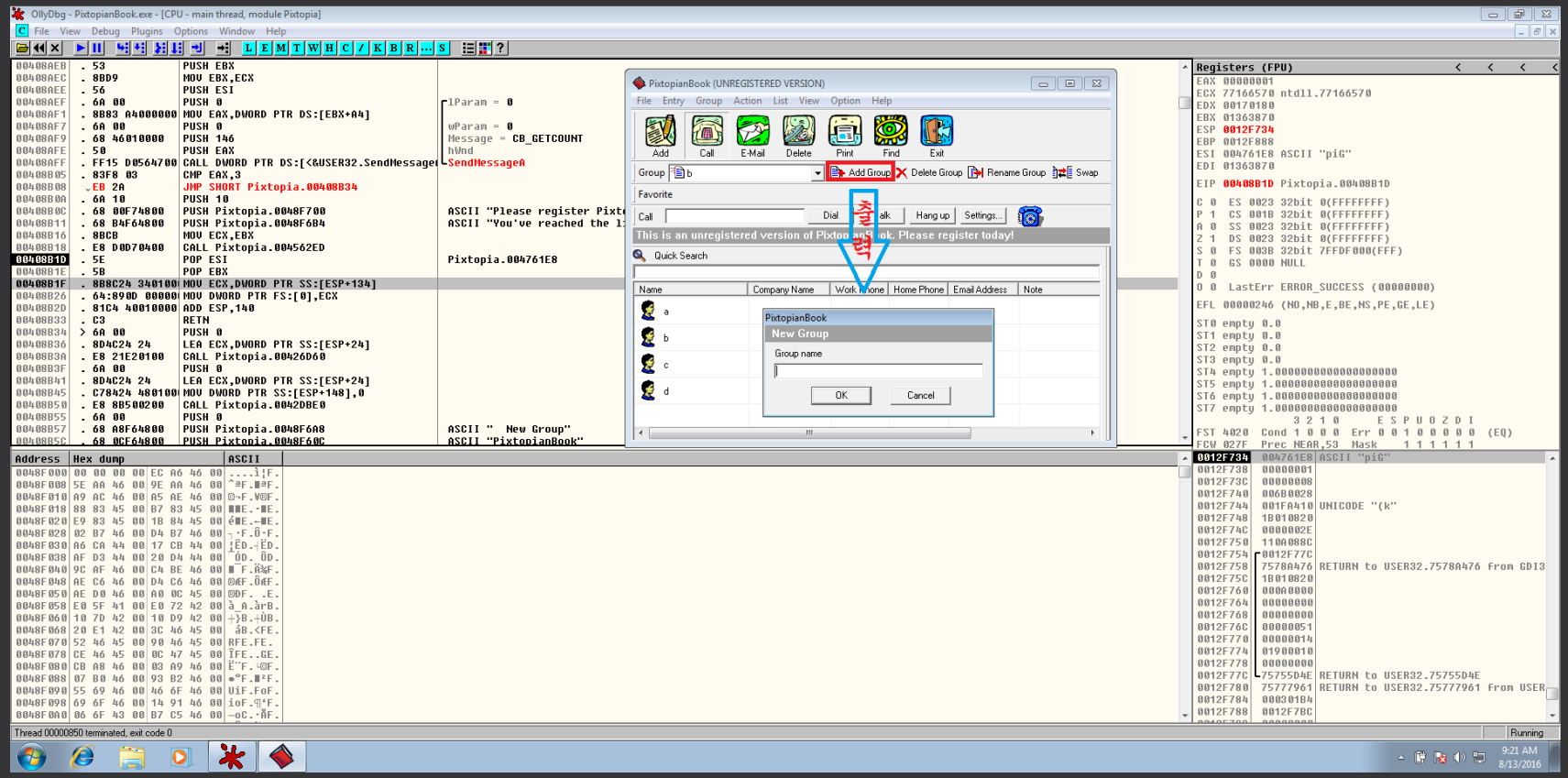


JMP문으로 바꾸어주게 되면서 표기된 00408B34부분으로 점프(Jump)하게 되어

해당 메시지가 출력이 되지 않을 것이다.

확인해보도록 하자.

결과 확인



처음과 같이 그룹 추가 버튼을 누르면 아까와는 다르게

그룹추가가 가능 하게 된 것을 확인 할 수 있다.

GOOD~~~~

감사합니다.^^