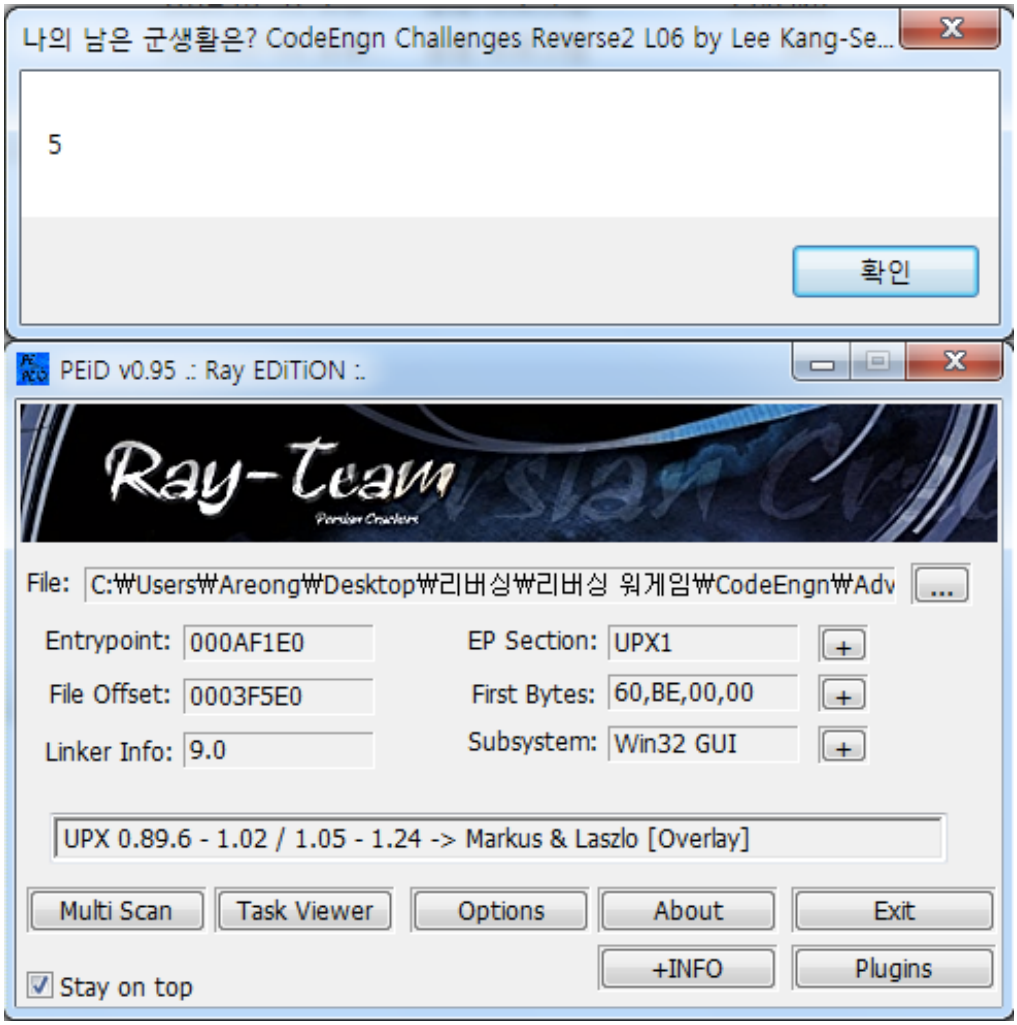
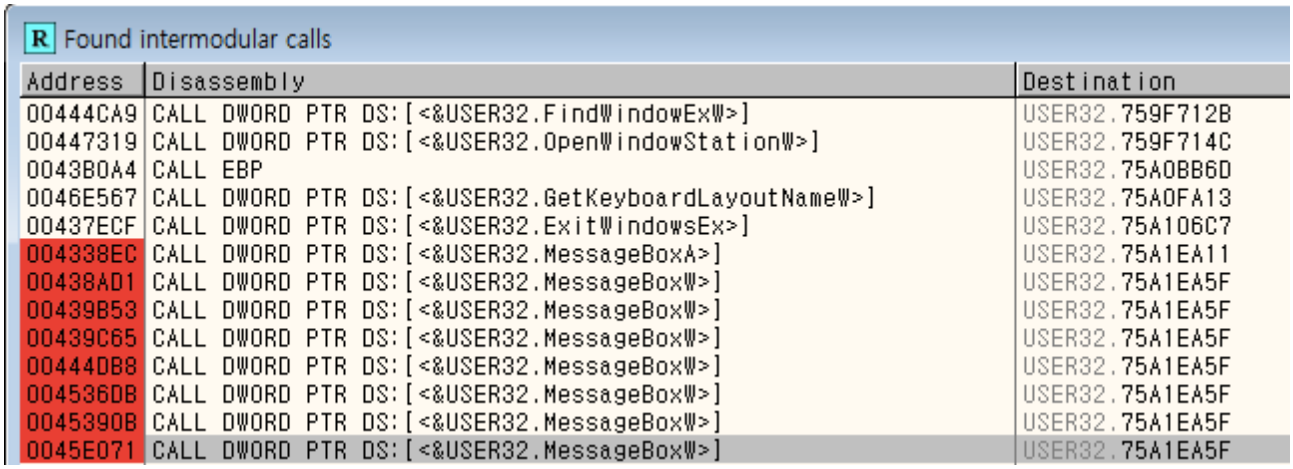


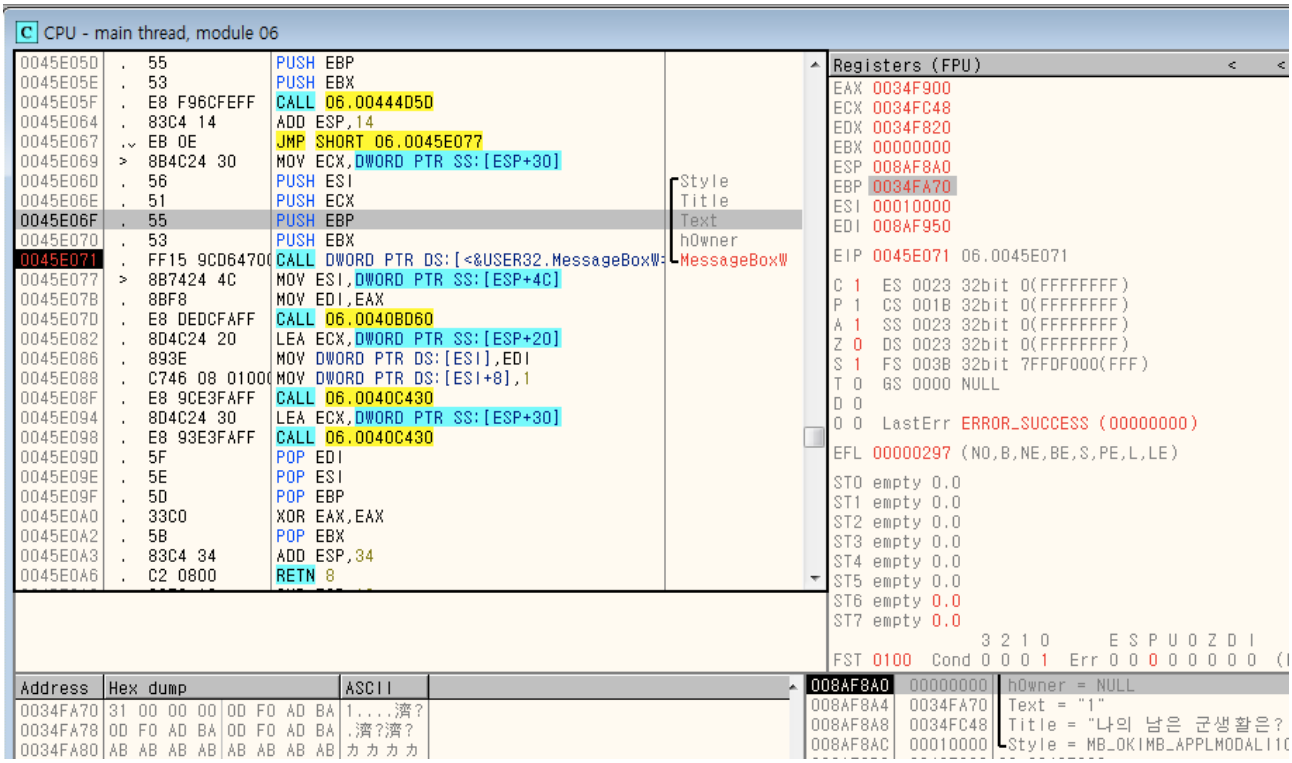
확인을 누르면 카운트가 증가하는 프로그램입니다.

숫자가 남은 군생활인 것 같습니다.

패킹은 UPX패킹이 되어있어 언패킹 후 진행하도록 하겠습니다.

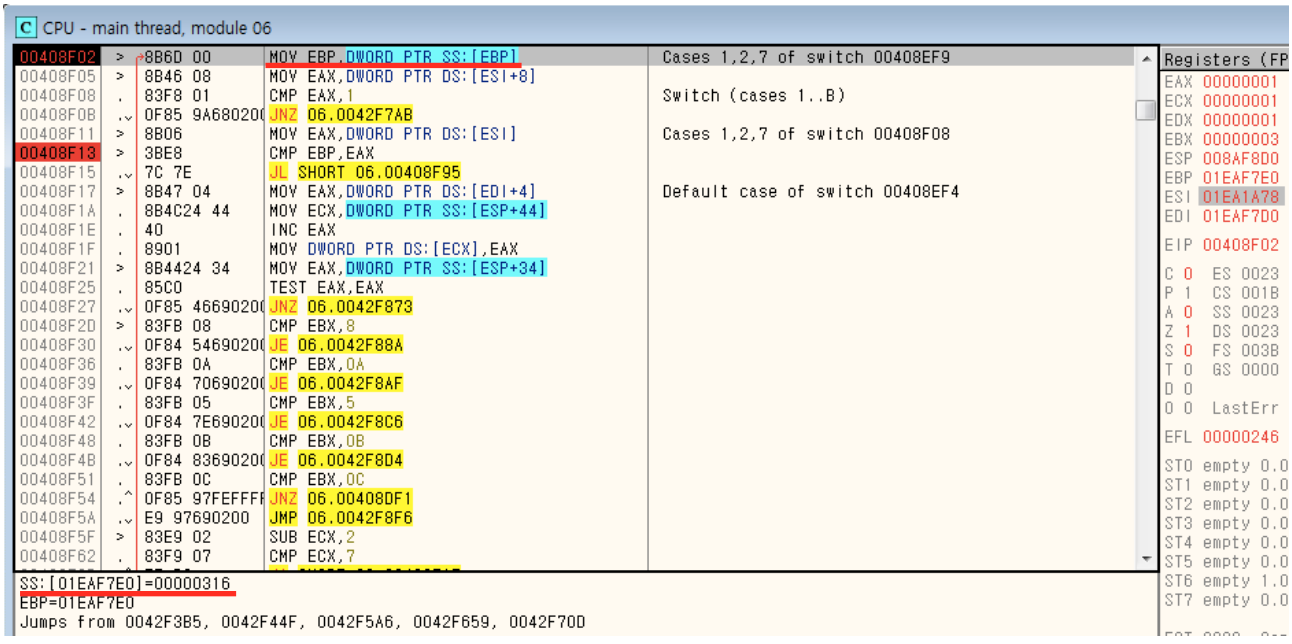


메세지박스를 통해 문구를 출력하기 때문에 메세지 박스에 BreakPoint를 설정하고 실행합니다.

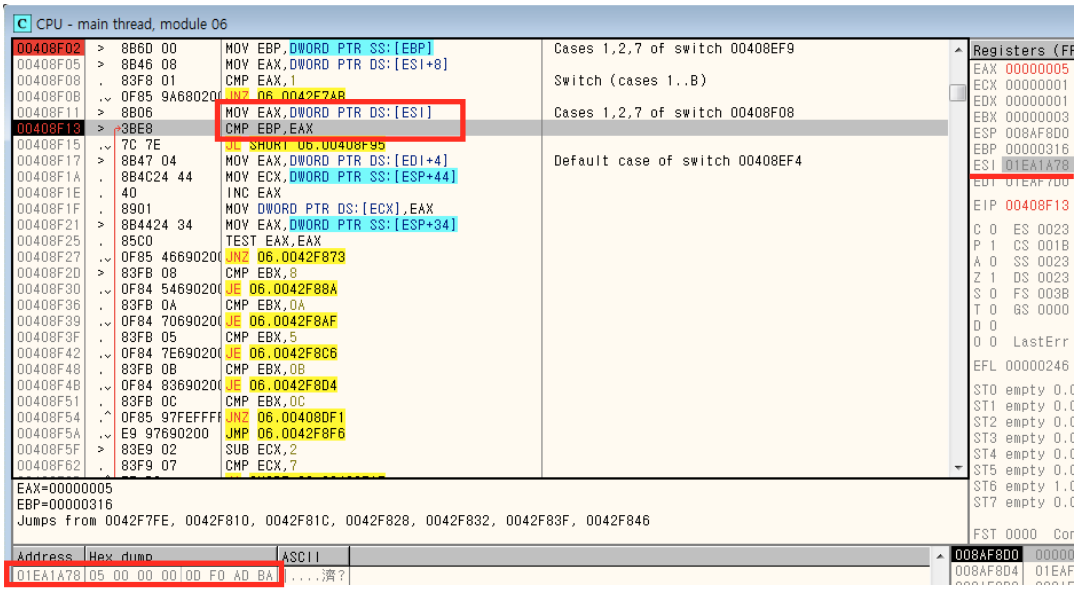


메세지 박스를 통해 문구를 출력하는 것을 알 수 있습니다.

밑으로 실행하면서 함수콜을 전부 뒤져보도록 하겠습니다.



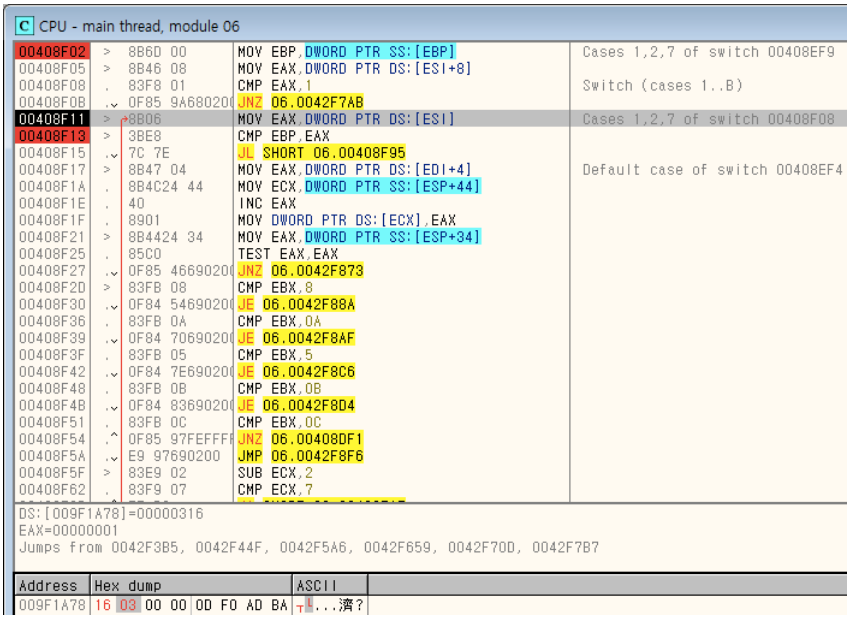
함수콜을 분석하면서 발견한 부분입니다. EBP에 0x316의 값을 넣는 것을 확인할 수 있습니다.



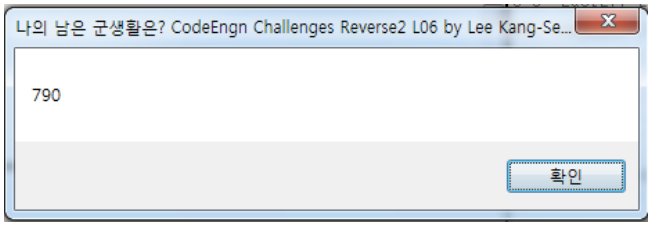
EAX에 ESI주소가 담고있는 값을 이동시킵니다.

ESI의 주소는 0x01EA1A78이고 그 값은 0x5입니다. 이 값은 메세지박스에 출력되는 숫자와 값이 같습니다.

이 값과 EBP에 저장된 값과 비교한 뒤 나머지 연산을 처리하게 됩니다.



ESI의 값을 EBP의 값과 똑같게 바꿔서 실행하면



위 그림처럼 출력되고 프로그램이 종료됩니다.