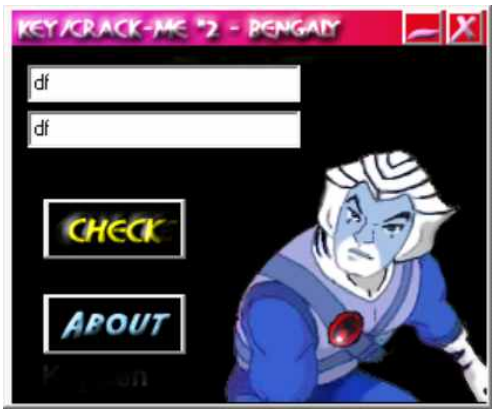
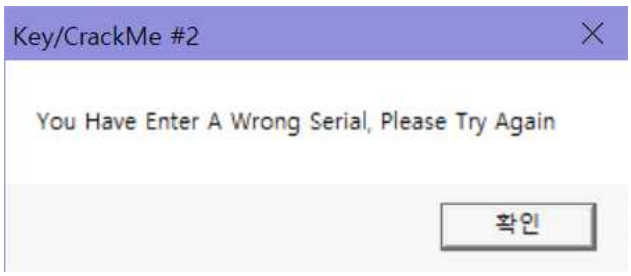
CodeEngn Basic RCE L14
: Name이 CodeEngn 일때 Serial을 구하시오
(이 문제는 정답이 여러개 나올 수 있는 문제이며 5개의 숫자로 되어있는 정답을 찾아야함, bruteforce 필요)

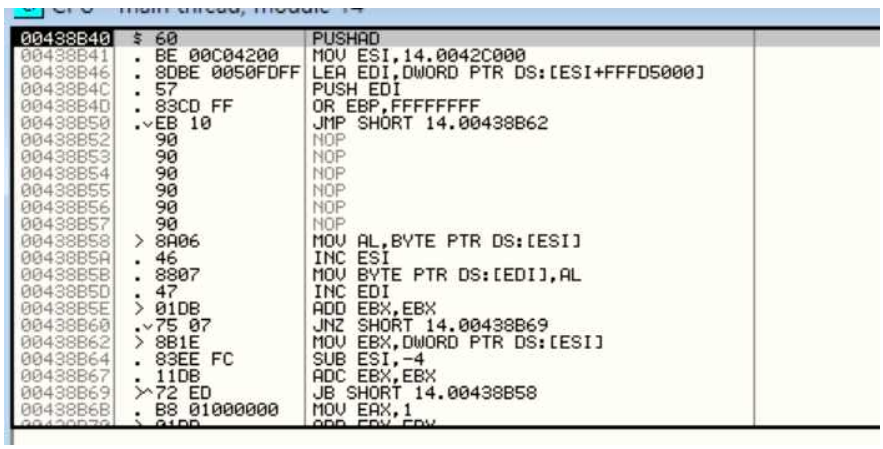
Ex) 11111



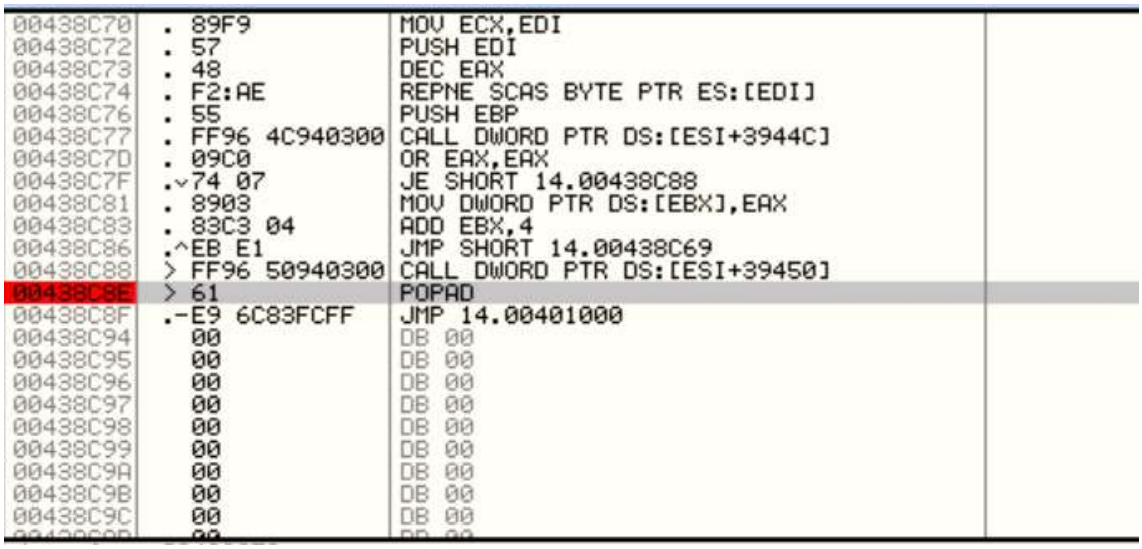
exe 파일 실행 시 위와 같은 실행창이 뜨고, 아무거나(df) 누르고 CHECK를 눌렀더니



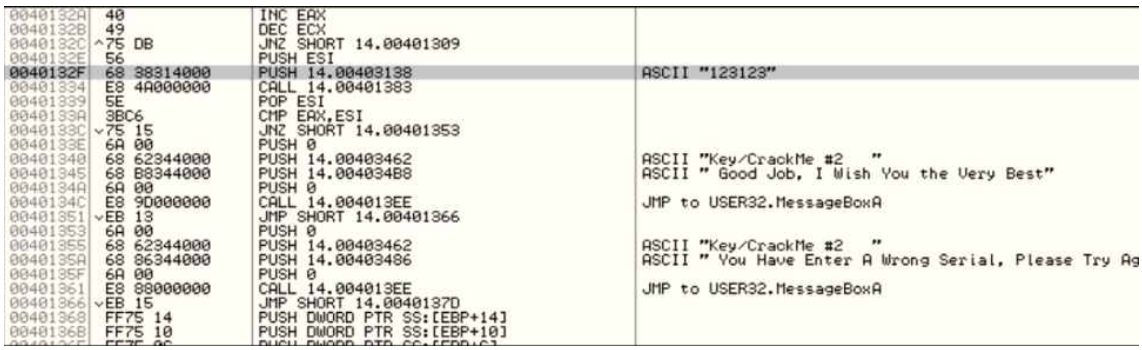
이런 경고창이 뜬다. serial을 찾아야 하니 올리디버거로 열어주었다.



PUSHAD 가 떴다! pushad가 뜨면 popad를 찾아주어야 한다.



popad 밑에 jmp 한 줄 밖에 없기 때문에 00401000이 OEP이고, 엔터를 눌러서 해당 주소로 이동한다.

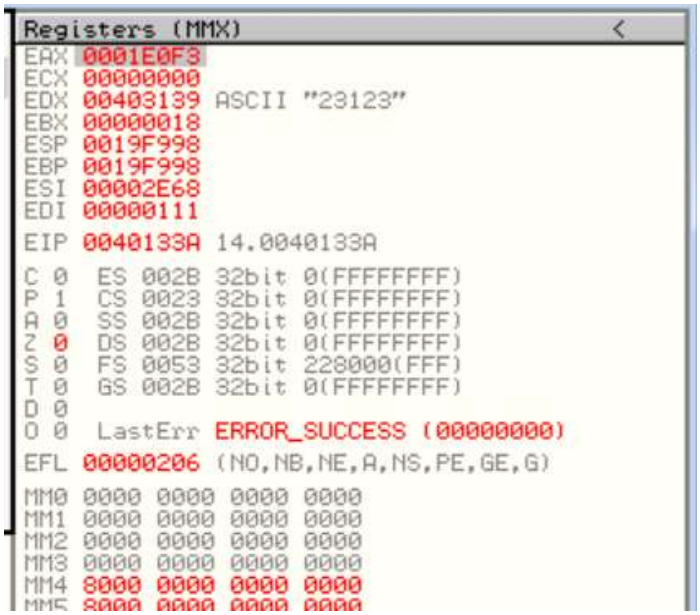


어셈블리어를 더 쉽게 살펴보기 위해서 실행 후 11111과 123123을 입력하였고, 올리디버거에 123123라는 부분이 에러/성공메세지 전에 띄워지는 것을 볼 수 있다. 즉 시리얼 넘버는 실행화면에 아랫줄이라는 것을 알 수 있었다.

이제 시리얼 넘버를 찾아야 하니 wrong seial 문구가 뜨는 지점을 기준으로 앞 뒤로 분석해보자 !

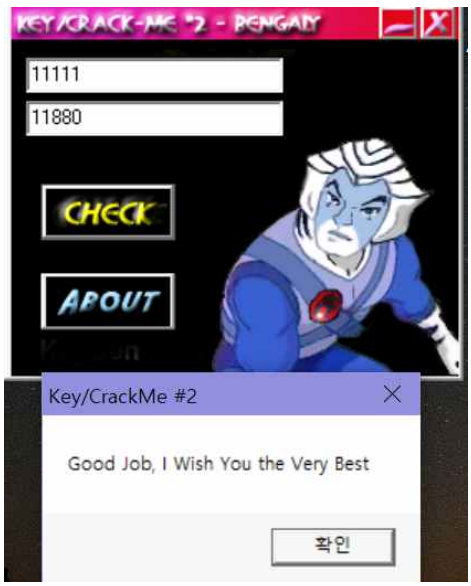
0040133A CMP EAX,ESI
0040133C JNZ 00401353

이 부분을 해석해보면 EAX - ESI의 값이 0이 아니라면 00401353으로 이동해서 "YOU HAVE ENTER A WRONG SERIAL"이라는 에러메세지를 출력하도록 하고 있다. 그러면 JNZ 에서 점프를 하지 않아야 "GOOD JOB. ~~~" 이라는 성공메세지를 출력할 수 있다.
즉 EAX - ESI = 0 이 되어야 하고, EAX와 ESI의 값이 같아야 한다.



레지스터 값에 각각 어떤것이 들어가는지 알아보기 위해서 CMP명령어에 F2를 눌러 BP를 걸고 실행시켰다. 우선 EAX에 들어가있는 값을 10진수로 변환 시켰더니 123123이 나온다. 즉 EAX와 ESI 중에서 EAX의 값이 사용자가 입력하는 시리얼 넘버라는 것을 알 수 있고, ESI가 진짜 시리얼 넘버라는 것을 알 수 있다.

ESI를 10진수로 변환시키면 11880이고, 이를 다시 대입해 보겠다.



성공메세지가 뜬다.
근데 문제에서 이름이 CodeEngn일 때, 시리얼 넘버를 구하라고 했으므로 똑같은 방법으로 시리얼 넘버를 구하면 76193이 나오므로, 답은 76193이다 !