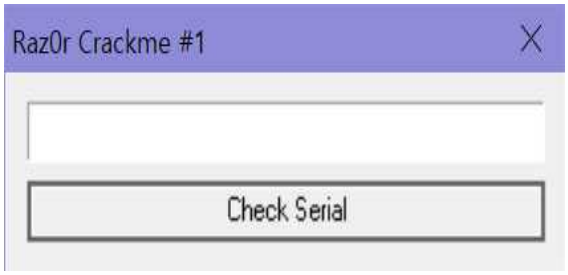
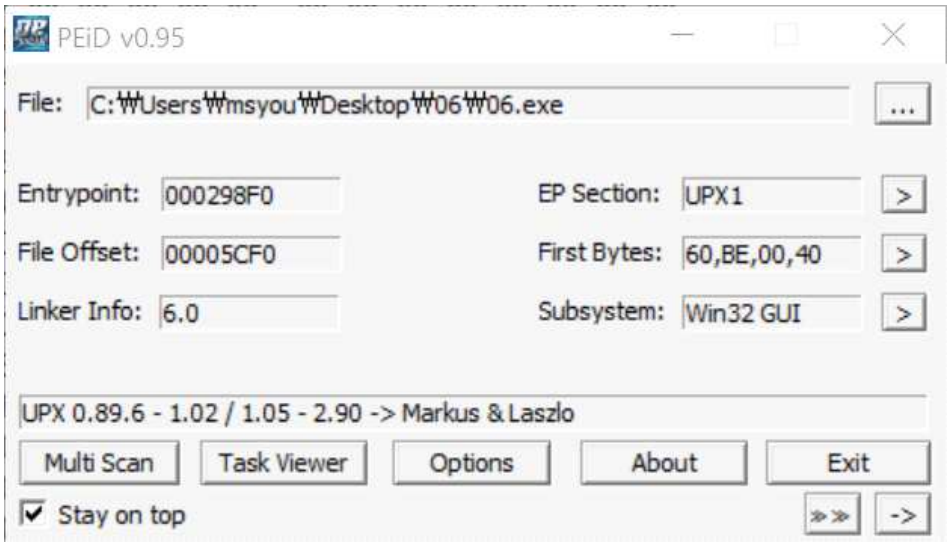
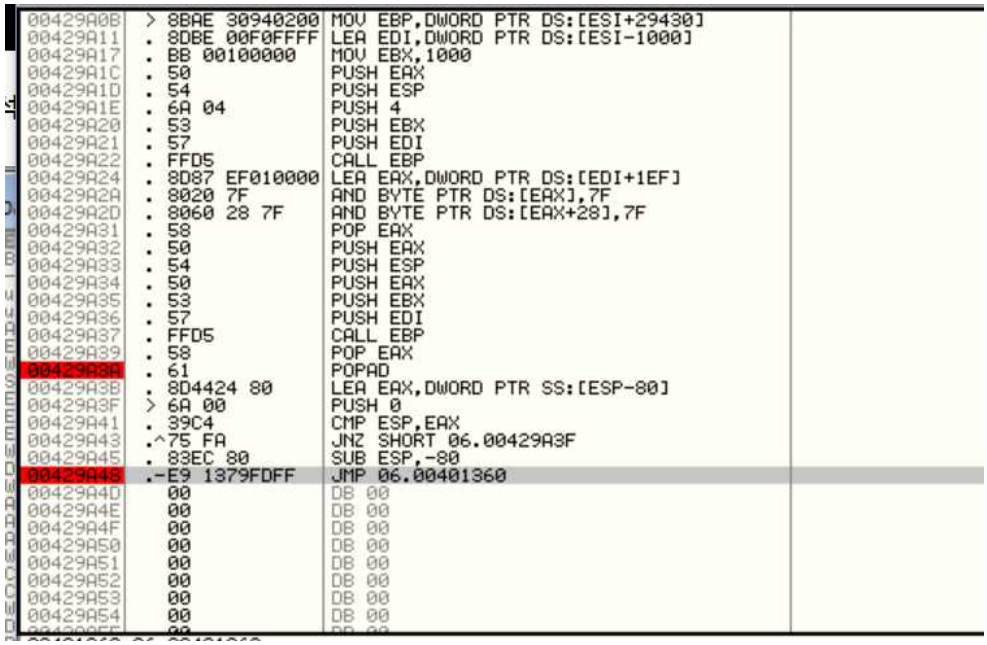
CodeEngn Basic RCE L06
: Unpack을 한 후 Serial을 찾으시오.
정답인증은 OEP + Serial
Ex) 00400000PASSWORD



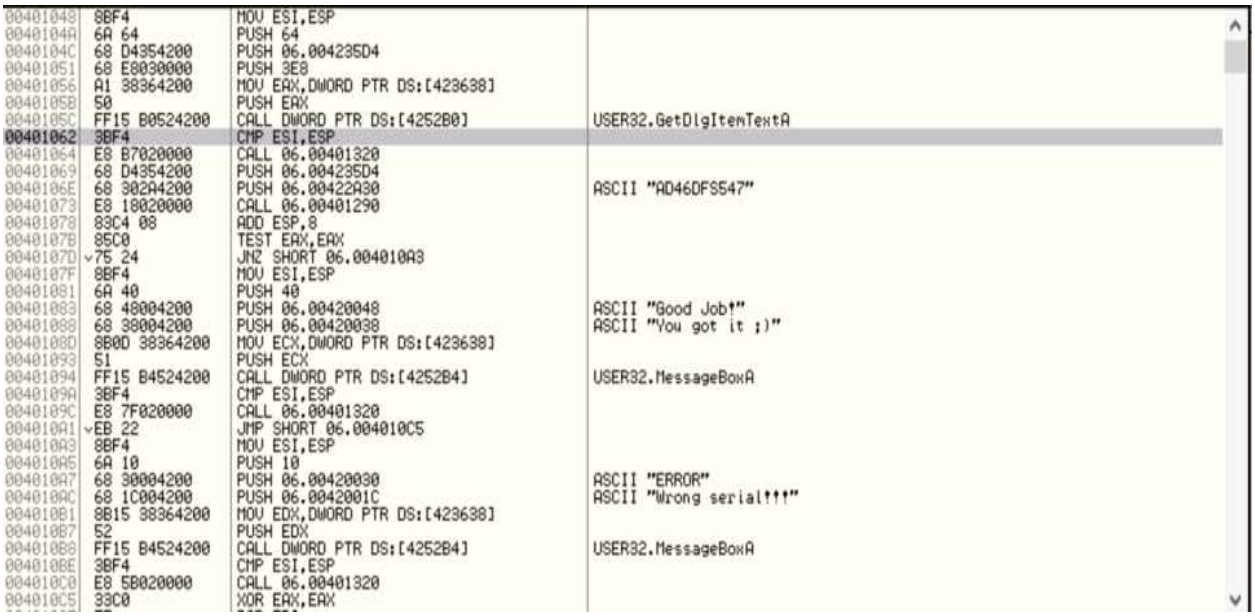
06.exe 실행하면 위와 같이 에러메세지가 나온다.



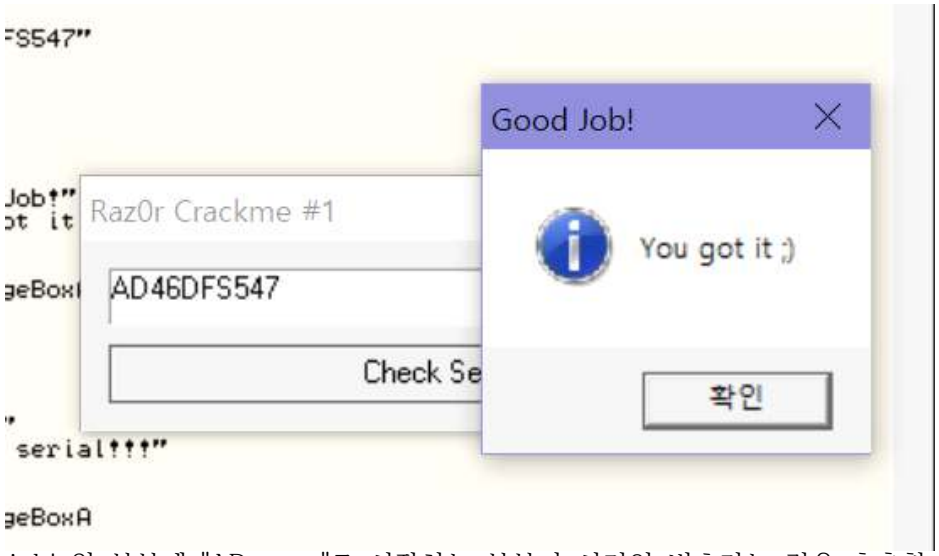
코드엔진 베이직을 5문제 풀어서 그런지 문제 풀때마다 루트가 일단 실행 한번 해보고 -> PEView로 봐주고, 패킹 의심되면 PEiD 틀어서 보는데 이번 문제는 5번 문제처럼 UPX로 패킹되어있었다.



search for로 popad를 찾아주고, 그 뒤로의 명령어들을 읽어보면 BP걸어둔 JMP명령어가 위치하는 곳이 OEP라는 것을 알 수 있다. 즉 00401360이 OEP시작주소이다.



OEP로 들어가는 해당 명령어에 BP를 걸고 F9->F8을 누르면 위와 같은 화면이 나오는데, 나는 우연인지 모르겠지만 바로 Wrong serial 부분이 나왔다.아닌 사람들은 string 찾기로 Wrong을 검색하면 될것이라고 생각한다.



Good job! 윗 부분에 "AD~~~~~"로 시작하는 부분이 시리얼 번호라는 것을 추측할 수 있다.