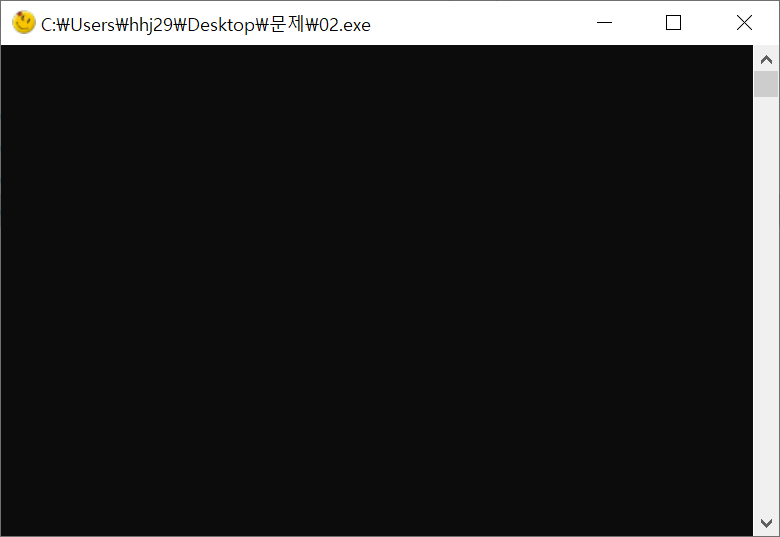
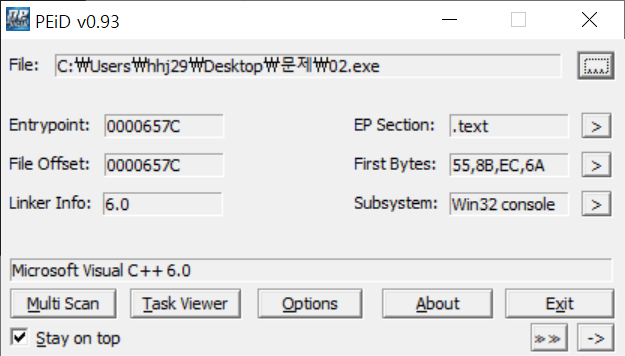
[Codeengn basic RCE L02]

1. 문제 확인



2. 과정

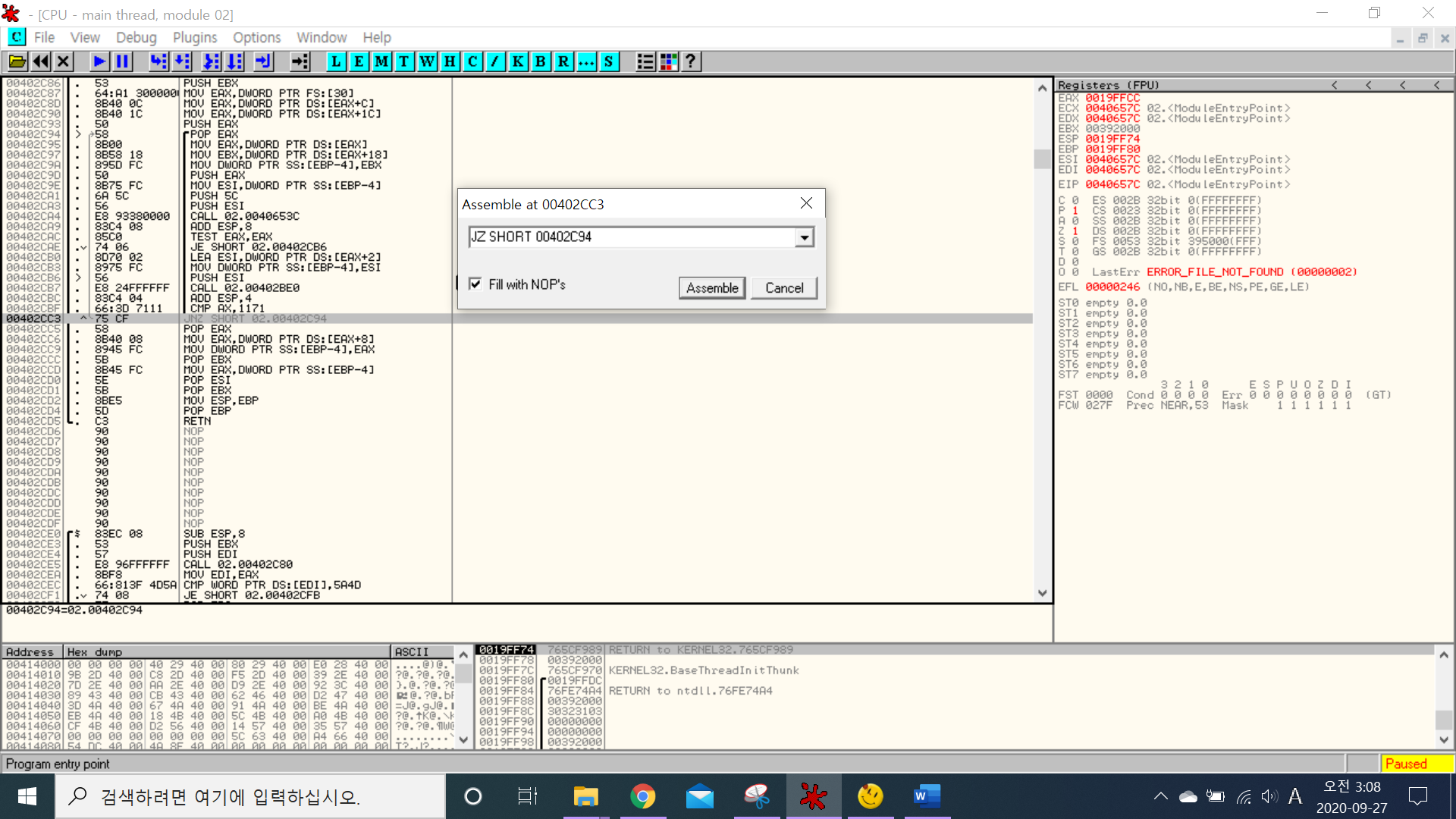
처음 PIED로 패킹이 되어있는지 확인해주었다.



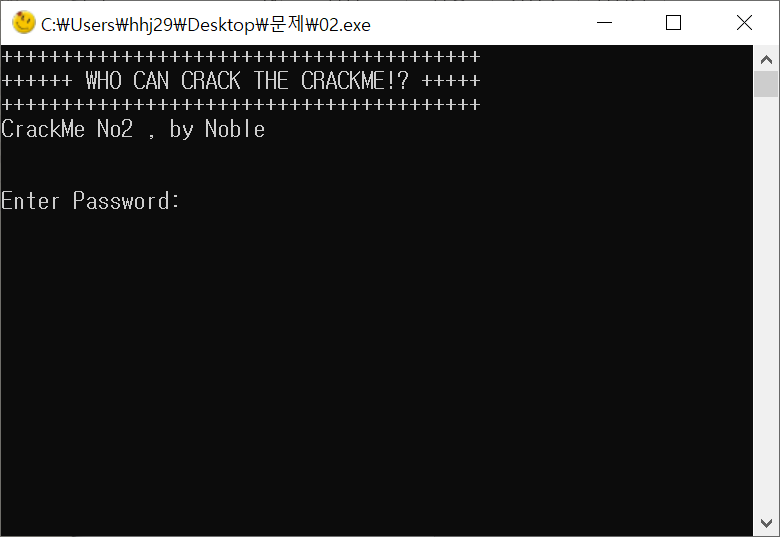
패킹이 되어 있지 않은 것을 확인하고 문제파일 exe를 실행했을 때

무슨 오류가 있는지 문제가 뜨지 않아서 먼저 수정해야 한다.

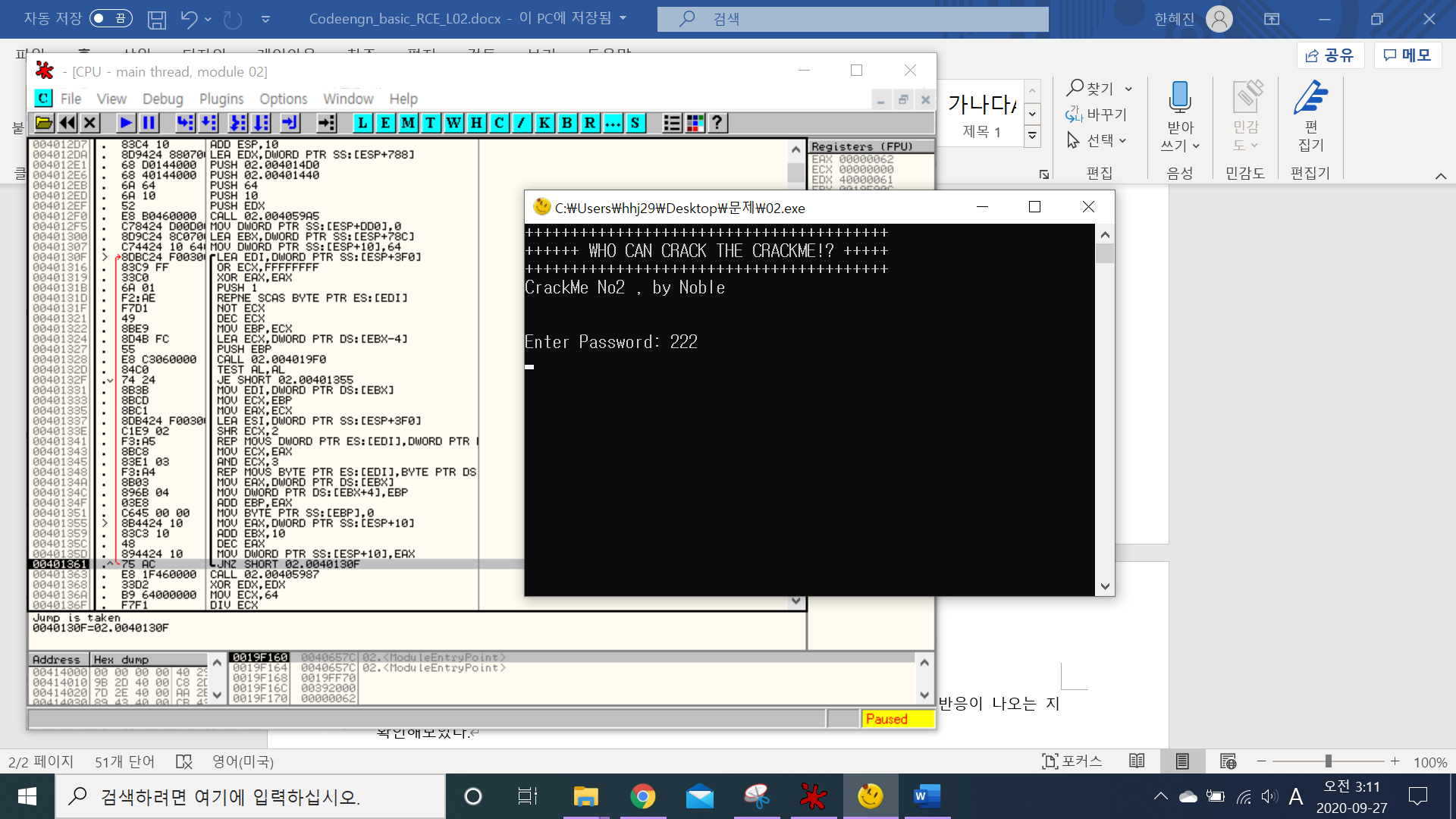
Ollydbg를 켜서 먼저 수정해보았다.



수정한 후 원래 문자열이 출력되는지 F8을 누르면서 확인해보았다.

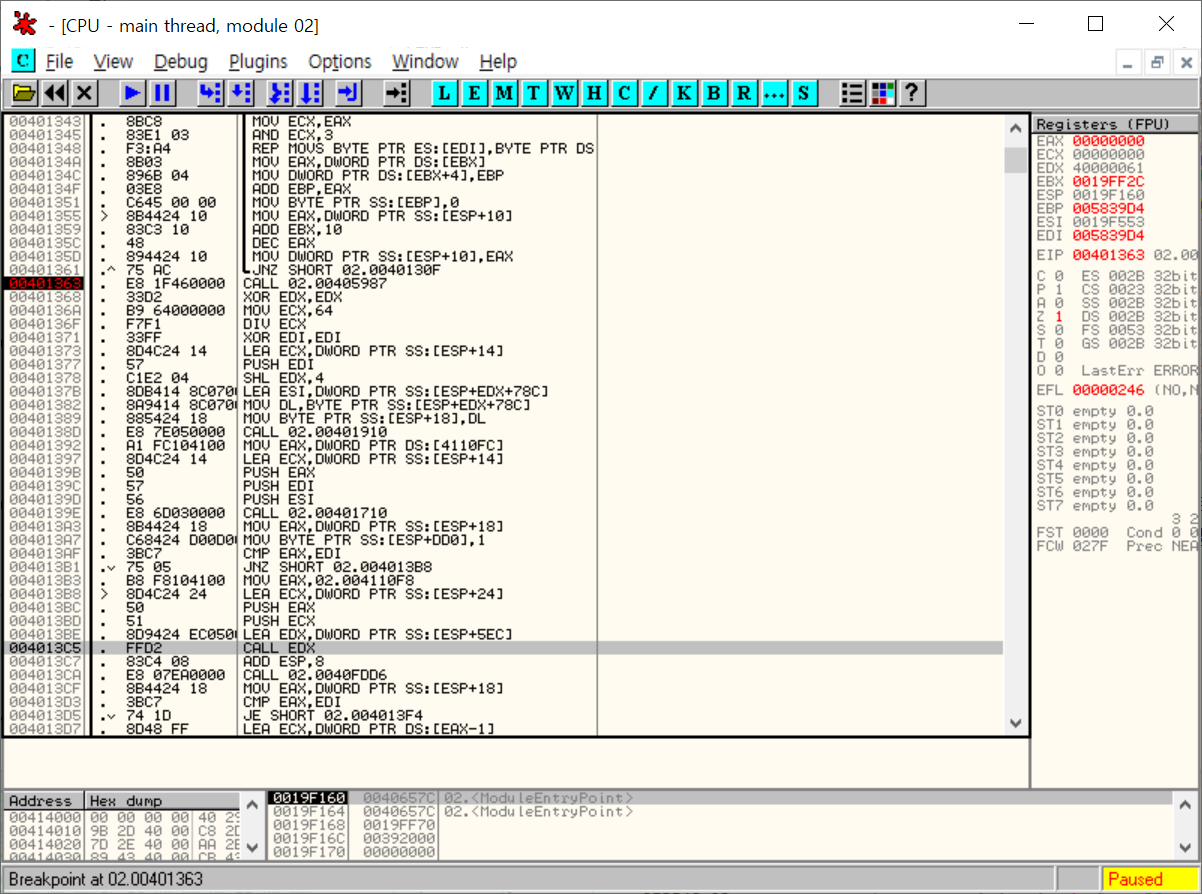


잘 뜨는 것을 확인하고 이제 아무 키나 눌렀을 때 어떤 곳으로 넘어가고 어떤 반응이 나오는 지 확인해보았다.



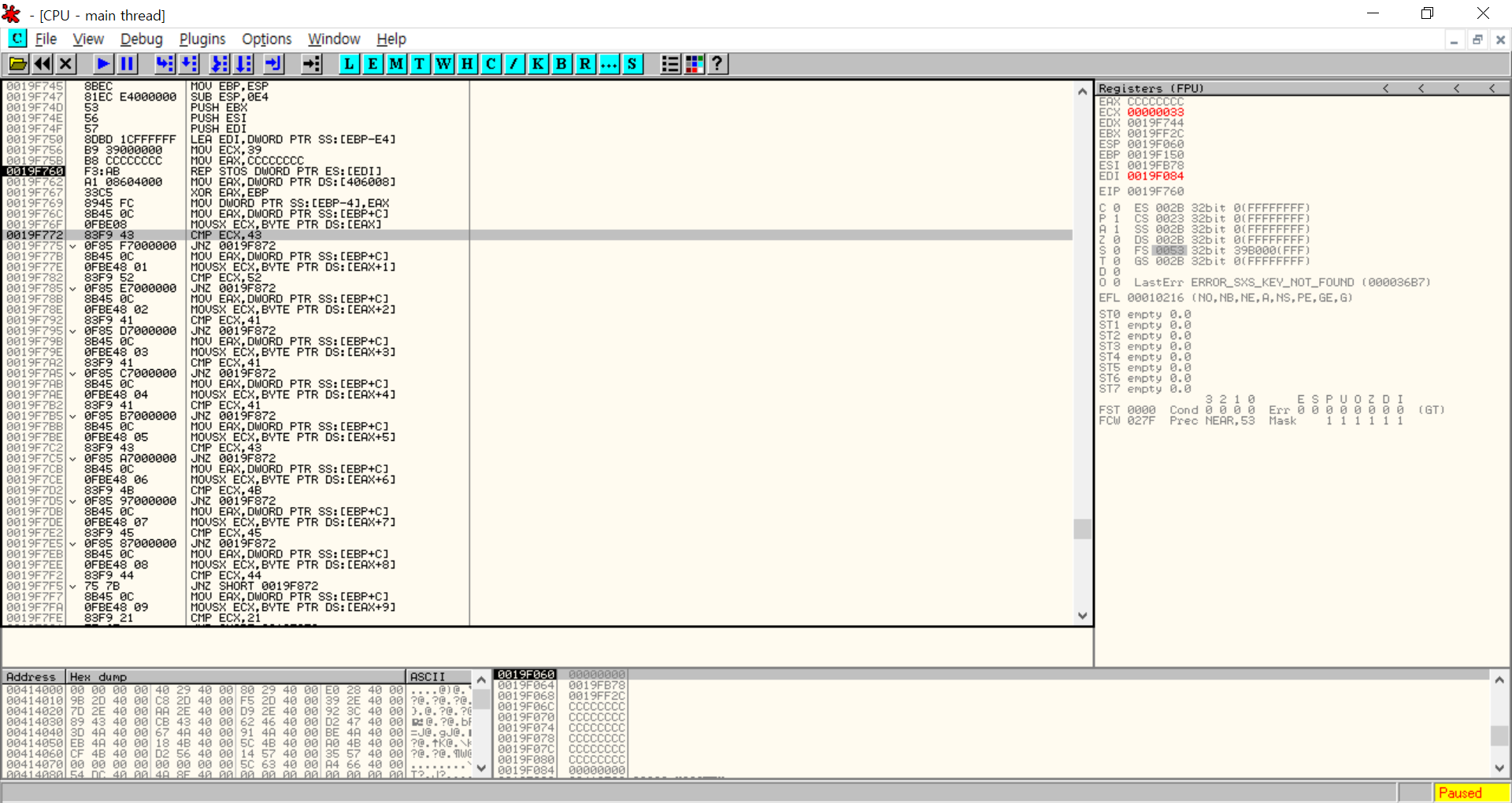
222를 누르고 넘어간 뒤 계속 f8을 눌러 확인하다가 계속 loop가 되는 곳을 발견했다.

Ctrl+f9를 눌러 함수루프를 탈출하고 계속 한줄씩 실행해보았다.



쭉 내리다가 보면 call edx라는 코드를 볼 수 있는데 이 구문을 실행시키면 종료된다.

call edx로 들어가 살펴보면



입력값 eax의 값을 mousx로 ecx로 복사하고

CMP로 ecx의 값을 계속 비교하고 달면 JNZ문으로 인해 0019F872로 일관되게 이동하는 것을 볼 수 있다.

43, 52, 41, 41, … , 21 이 값들을 아스키 코드로 변환하면 문제의 답을 구할 수 있다고 한다.

3. 결과

