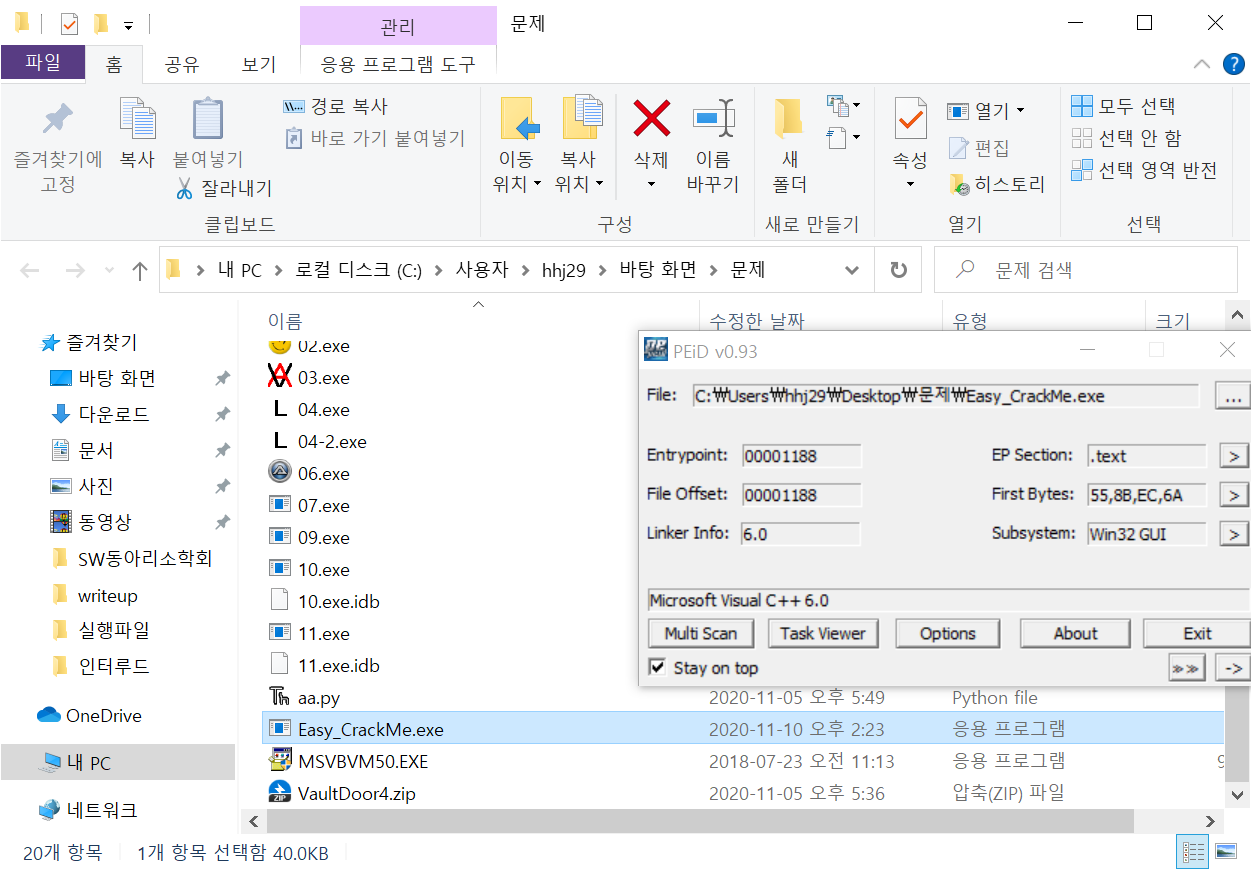
1. 문제 확인



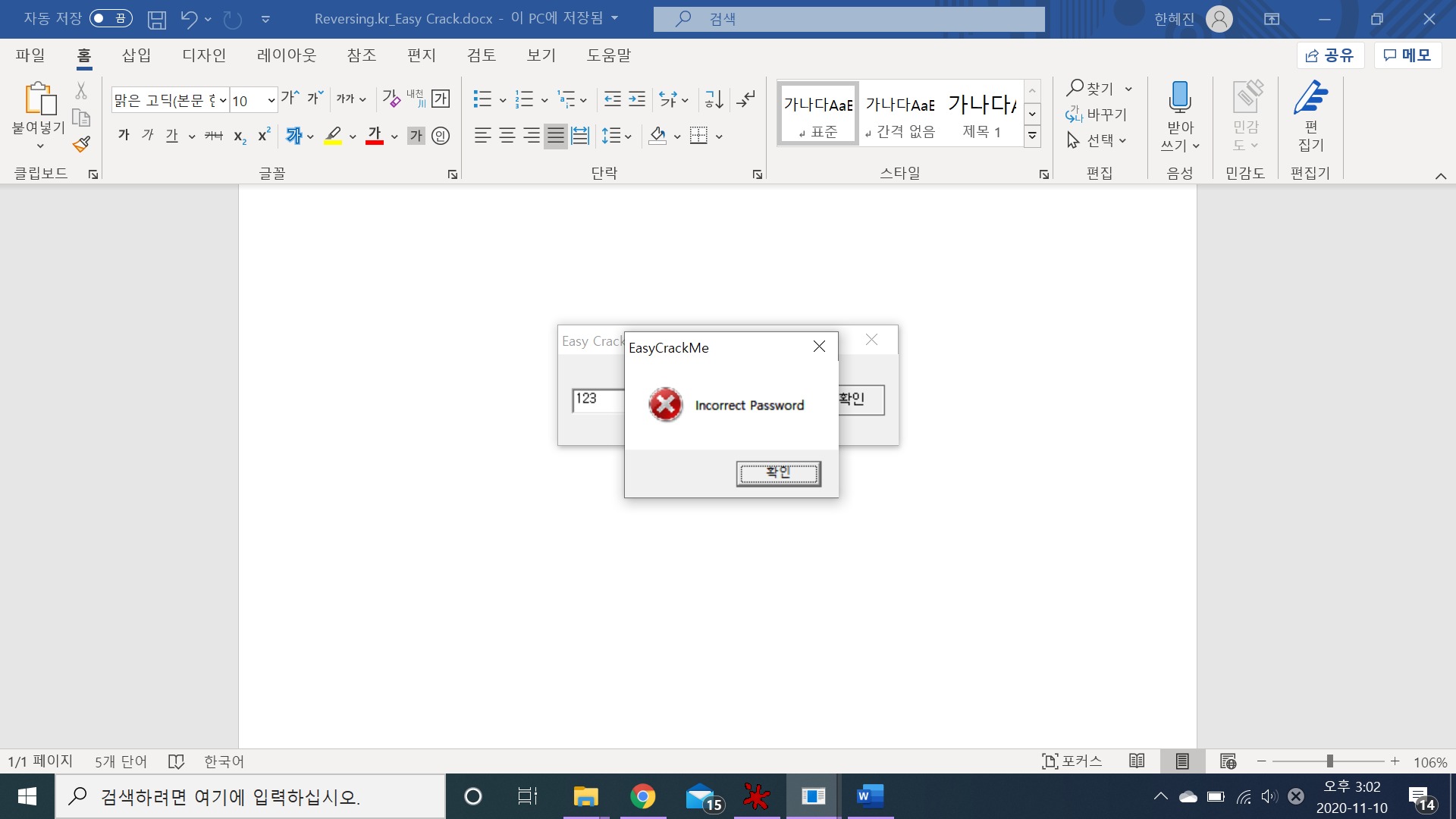
2. 과정

우선 PEiD로 패킹여부를 확인해보았다.



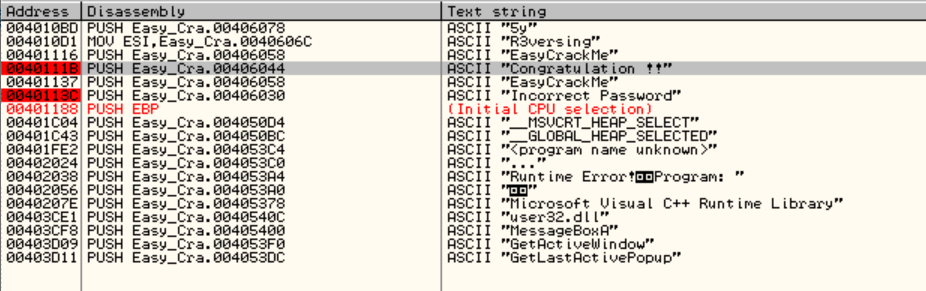
패킹은 되어 있지 않고 C++로 작성되어 있는 것 같다.

실행 파일을 열어 123을 입력해보았다.

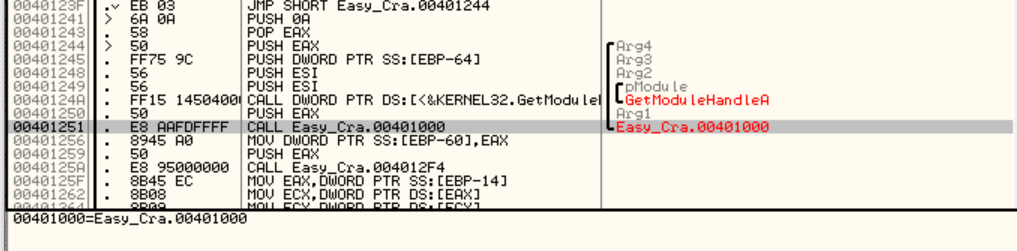


다음처럼 incorrect password라는 창이 뜨고 다른 반응은 없었다.

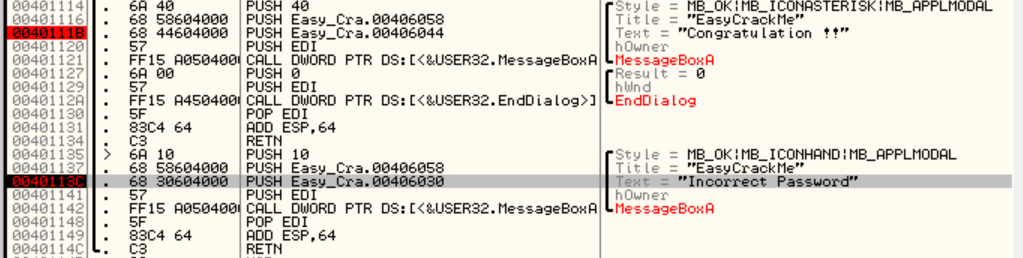
올리디버거로 열어서 위와 같은 문자열이 어디에 나오는지 확인해보았다.



401251에서 password를 불러오는 함수가 실행됐다.



Password에 123을 입력하니까



위처럼 Incorrect Password 문자열이 있는 곳으로 왔다.

내가 입력한 password 값과 어떤 문자열을 비교하는 부분을 찾아야할 것 같다.

아까 password를 입력하라는 함수 내부로 F7를 눌러 들어가서

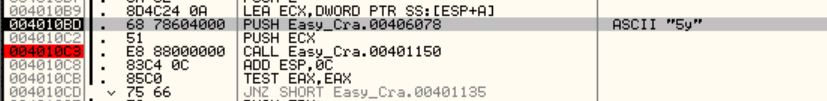
CMP 구문을 찾아 breakpoint를 걸고 살펴보았다.

첫 번째 CMP 문에서는 내가 입력한 ‘123’ 중 2와 61(a)을 비교하는데

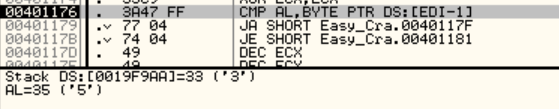


밑에 실패문으로 가는 점프문이 있어서 JZ로 변경하고 계속 진행해보았다.

5y라는 값을 스택에 넣고 함수를 실행하길래 함수 내부를 살펴보았다.

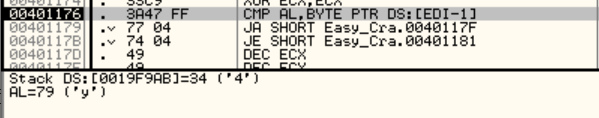


여기서도 마찬가지로 CMP 문으로 내가 입력한 3과 5를 비교하는 것 같았다.



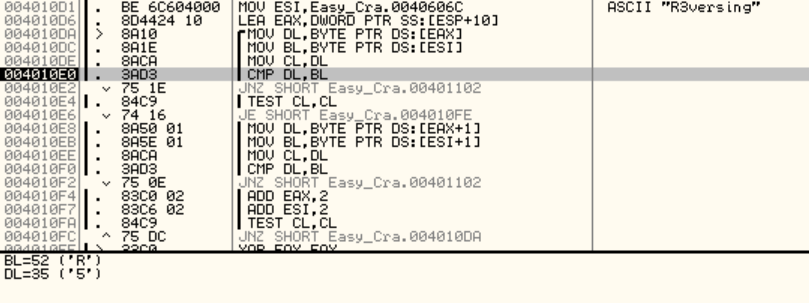
그래서 입력 문자열을 1a54567로 변경해서 다시 실행해보았다.

이젠 4와 y를 비교하는 것을 보니 4가 있던 자리에 y가 들어가야 하는 것 같다.



1a5y567

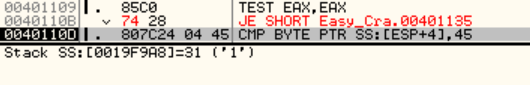
4010DA부터 시작하는 루프문을 돌면서



루프 내의 CMP 구문으로 내가 입력한 문자 5부터 ‘R3versing’ 이라는 문자열을 비교하는 것을 알았다.

1a5yR3versing

이 루프문이 끝나고 40110D CMP 문에서는 내가 입력한 1과 45(E)를 비교한다.



Ea5yR3versing

비교 후 일치하면 바로 성공문자열로 이동할 수 있다.



패스워드는 Ea5yR3versing이다.

