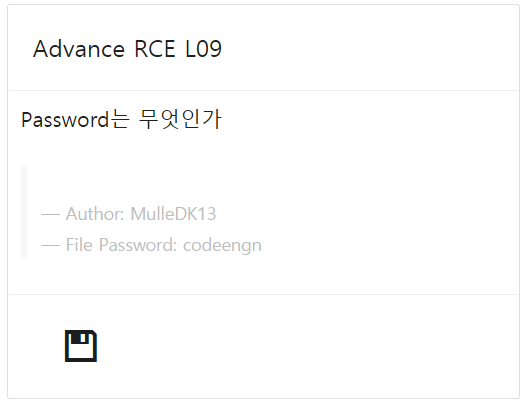
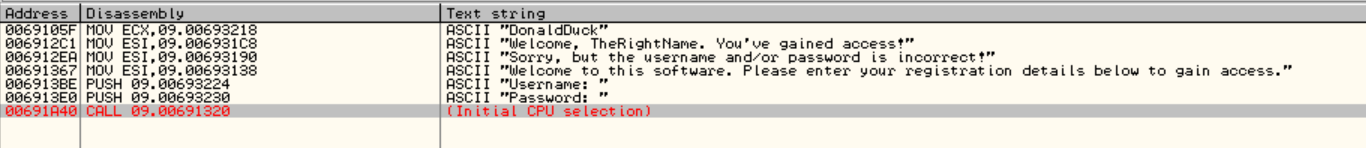
1. 문제확인



2. 과정

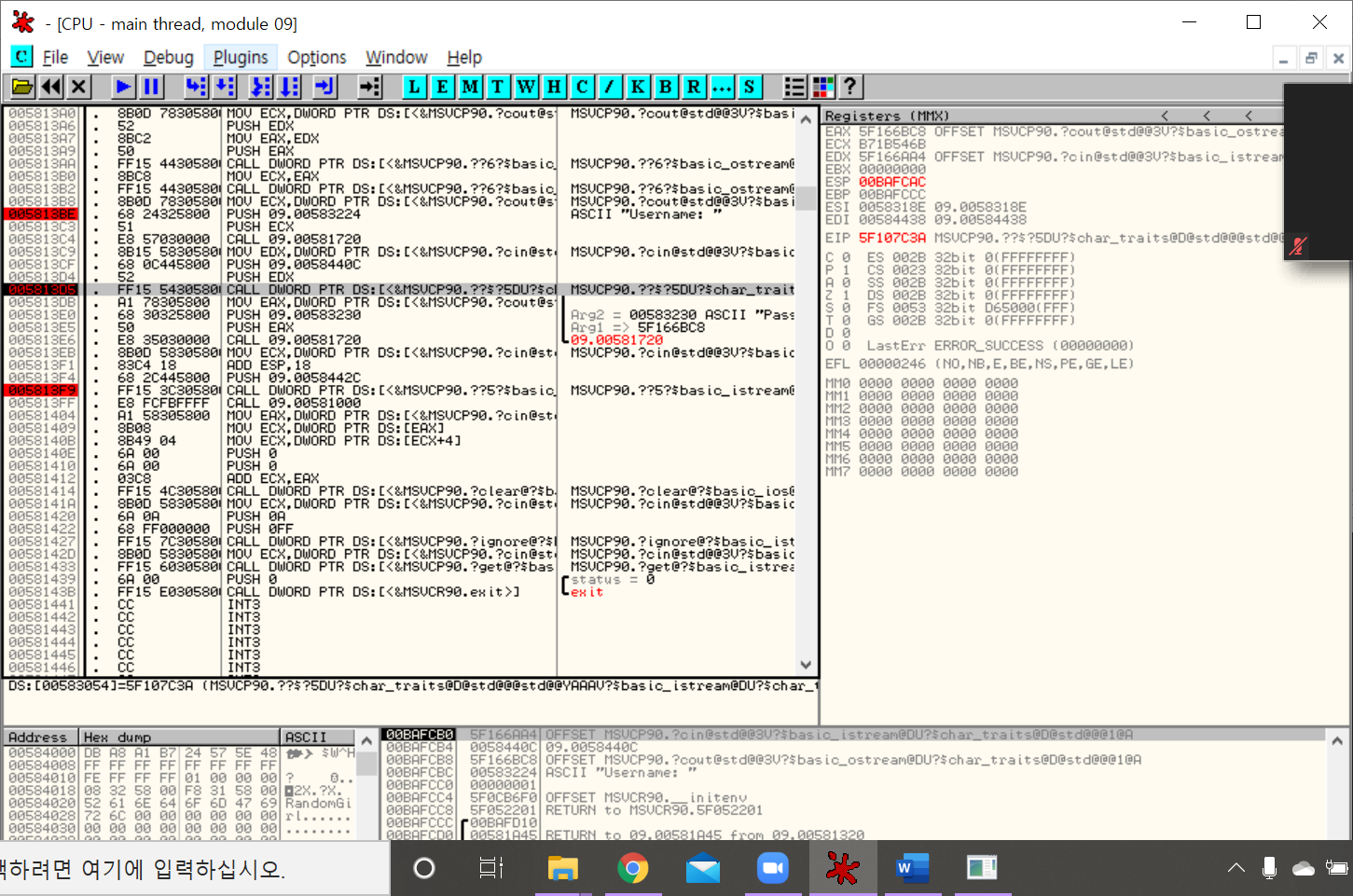
문자열을 확인해보았다.



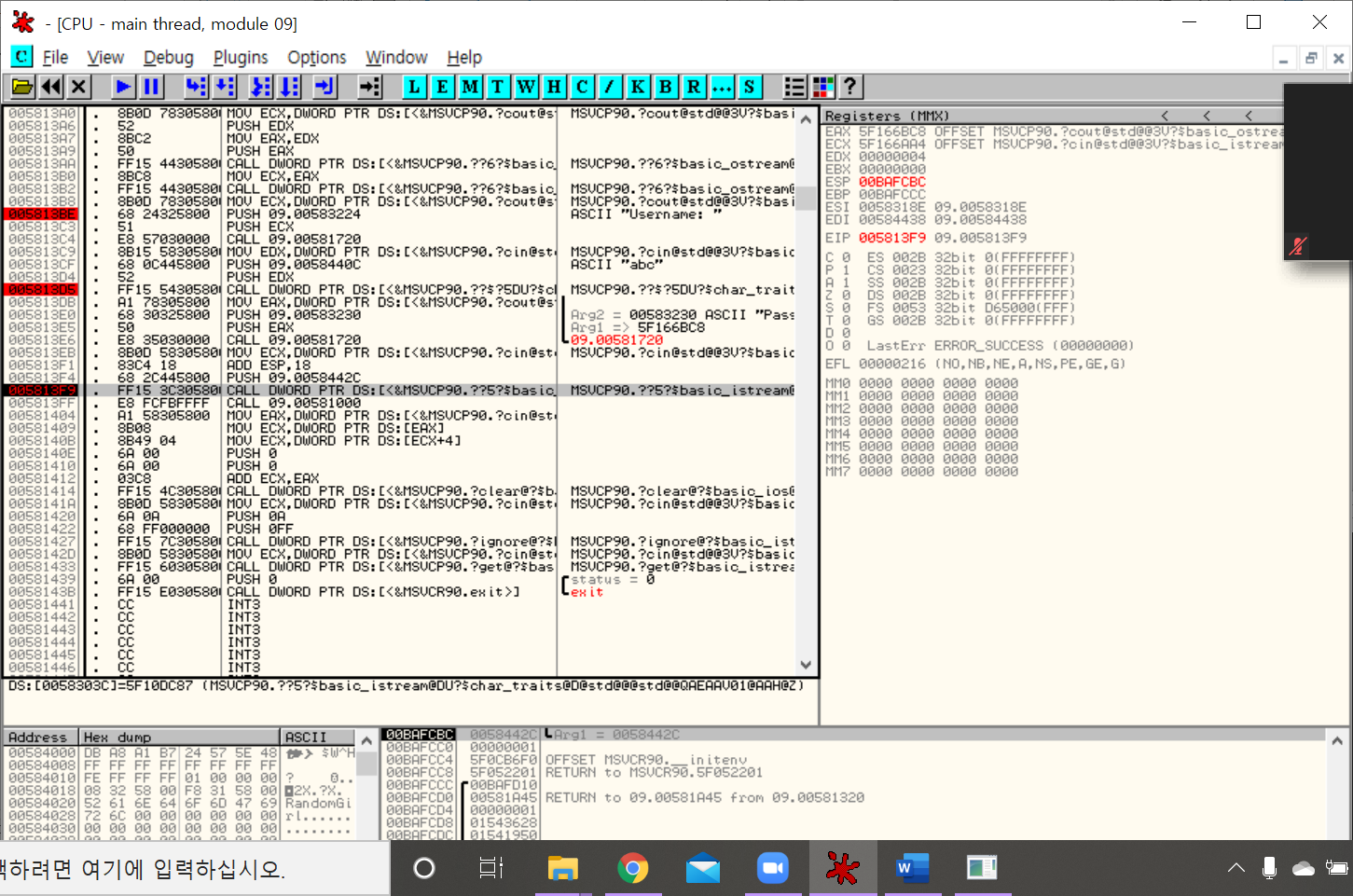
도날드덕?과 성공문자열, 실패문자열을 찾았다.

해당 문자열이 있는 곳까지 실행해봐야겠다.

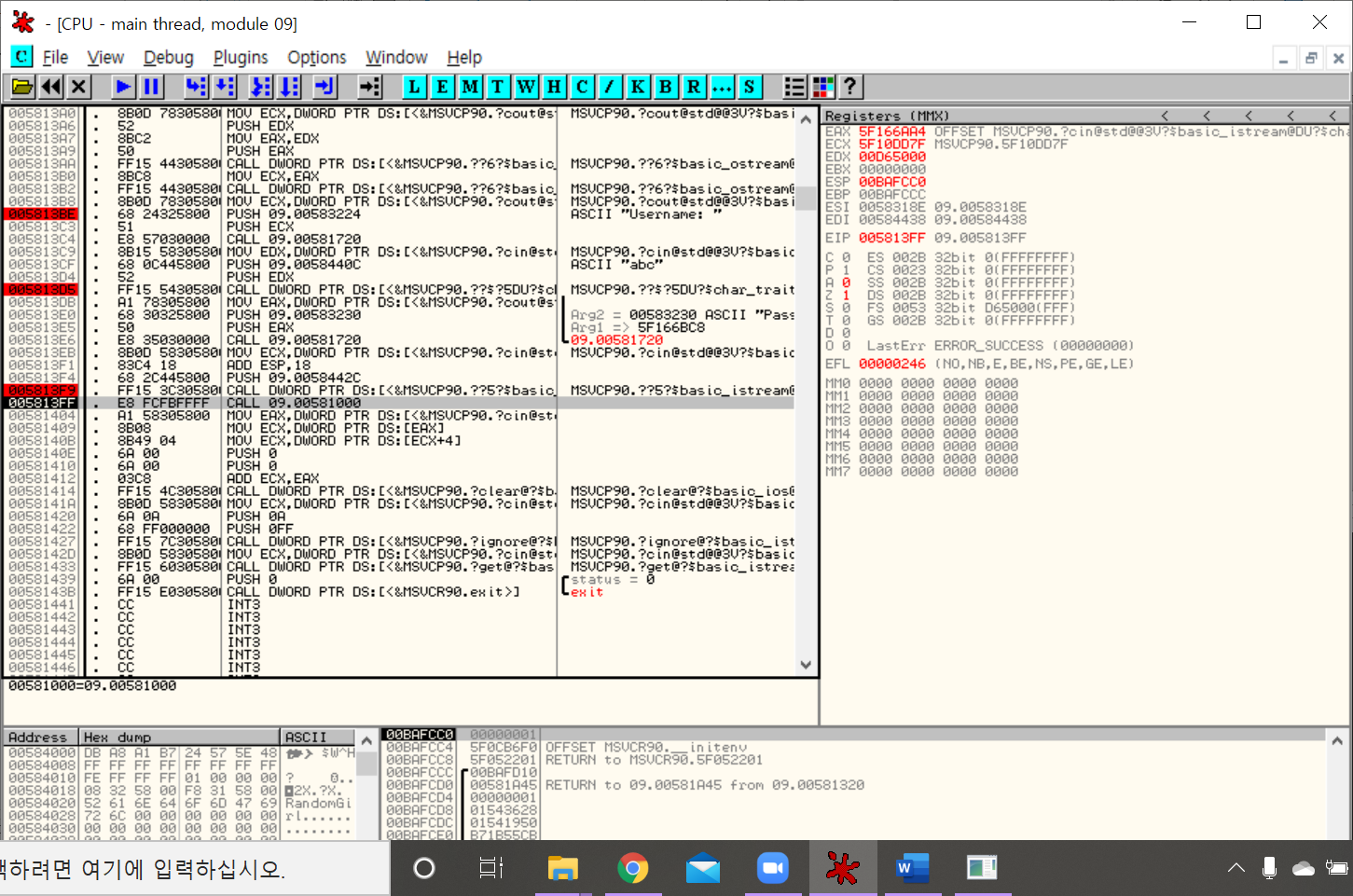
아이디를 입력 받는 함수가 실행된다.



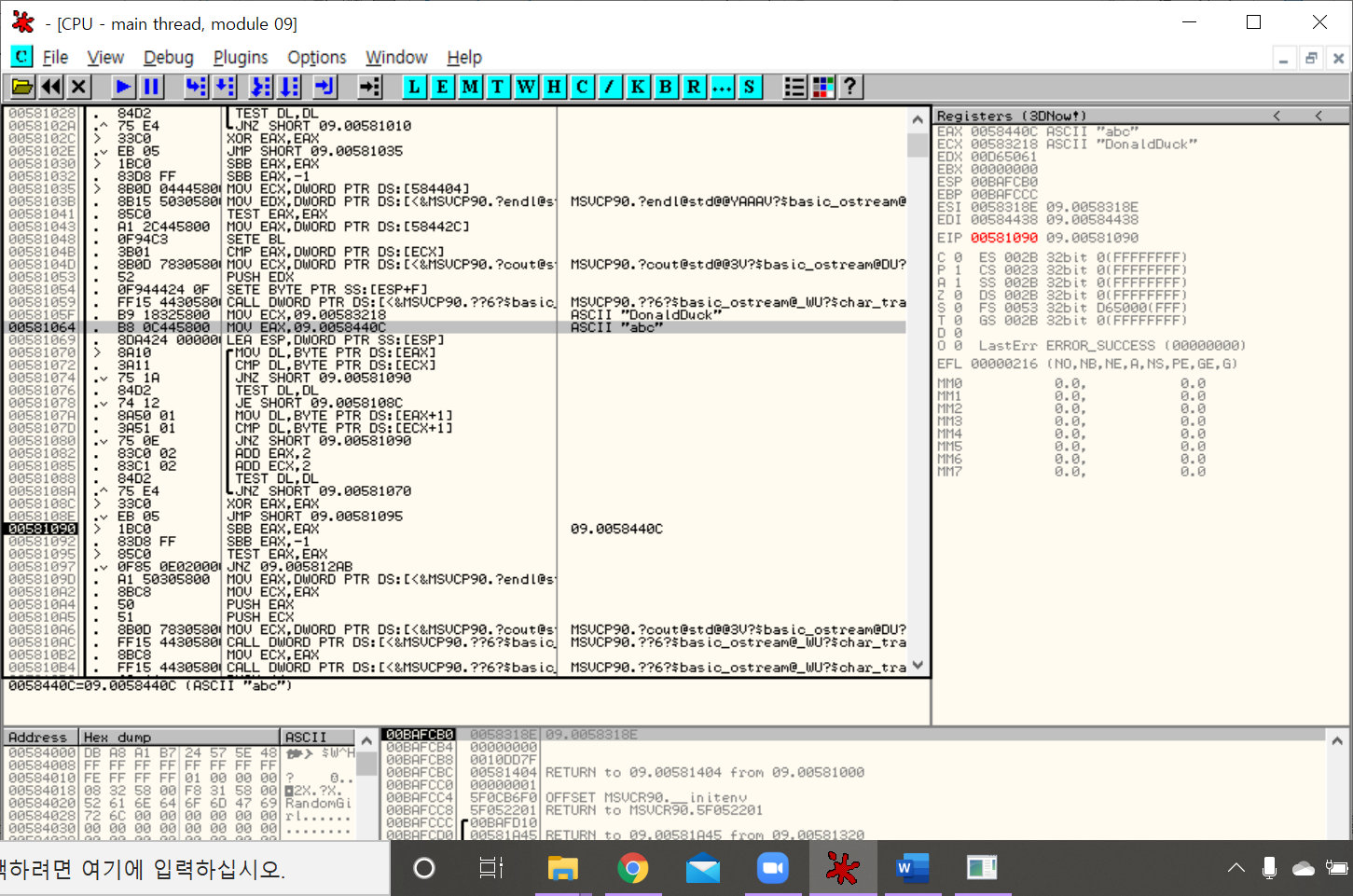
비밀번호를 입력 받는 함수가 실행된다.



아이디와 비밀번호를 비교하는 곳을 찾아 함수 내부로 F7을 눌러 살펴보았다.

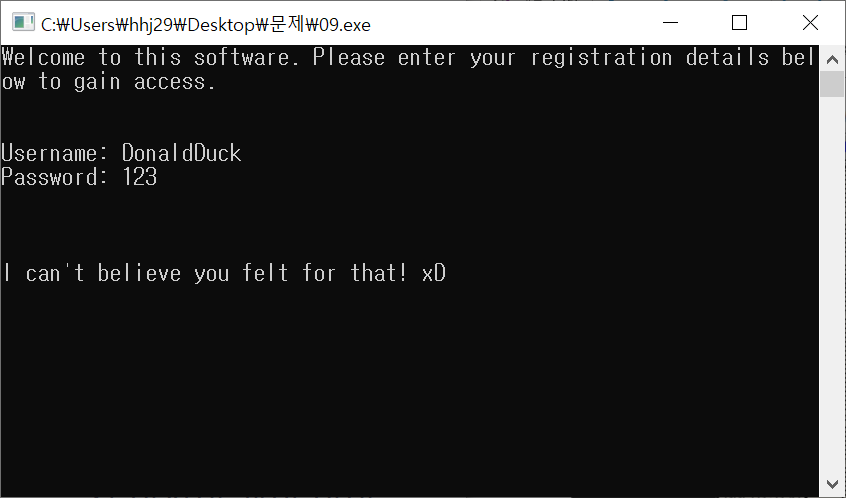


5813FF 함수 내부로 들어가니까 내가 username으로 입력한 abc와 DonaldDuck을 비교하는 루프문을 발견할 수 있었다.

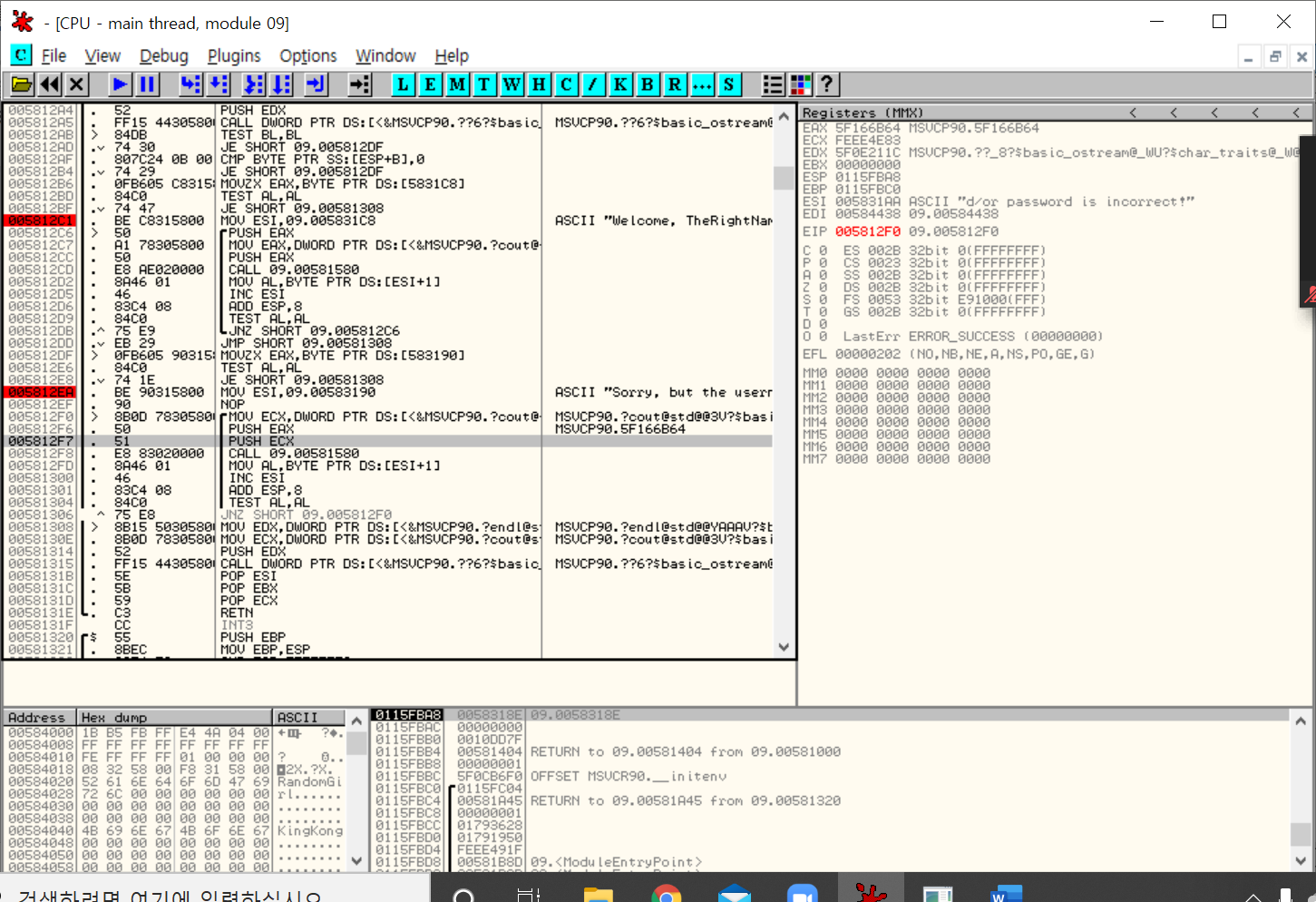


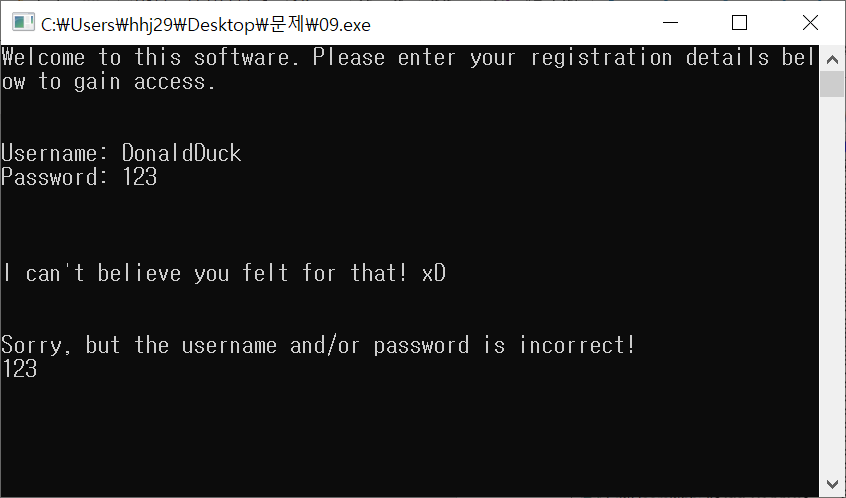
아무래도 username은 DonaldDuck인가보다.

이제 username을 DonaldDuck으로 설정하고 다시 리버싱해보았다.



찾던 중 실패문자열이 출력되는 루프문을 발견할 수 있었다.



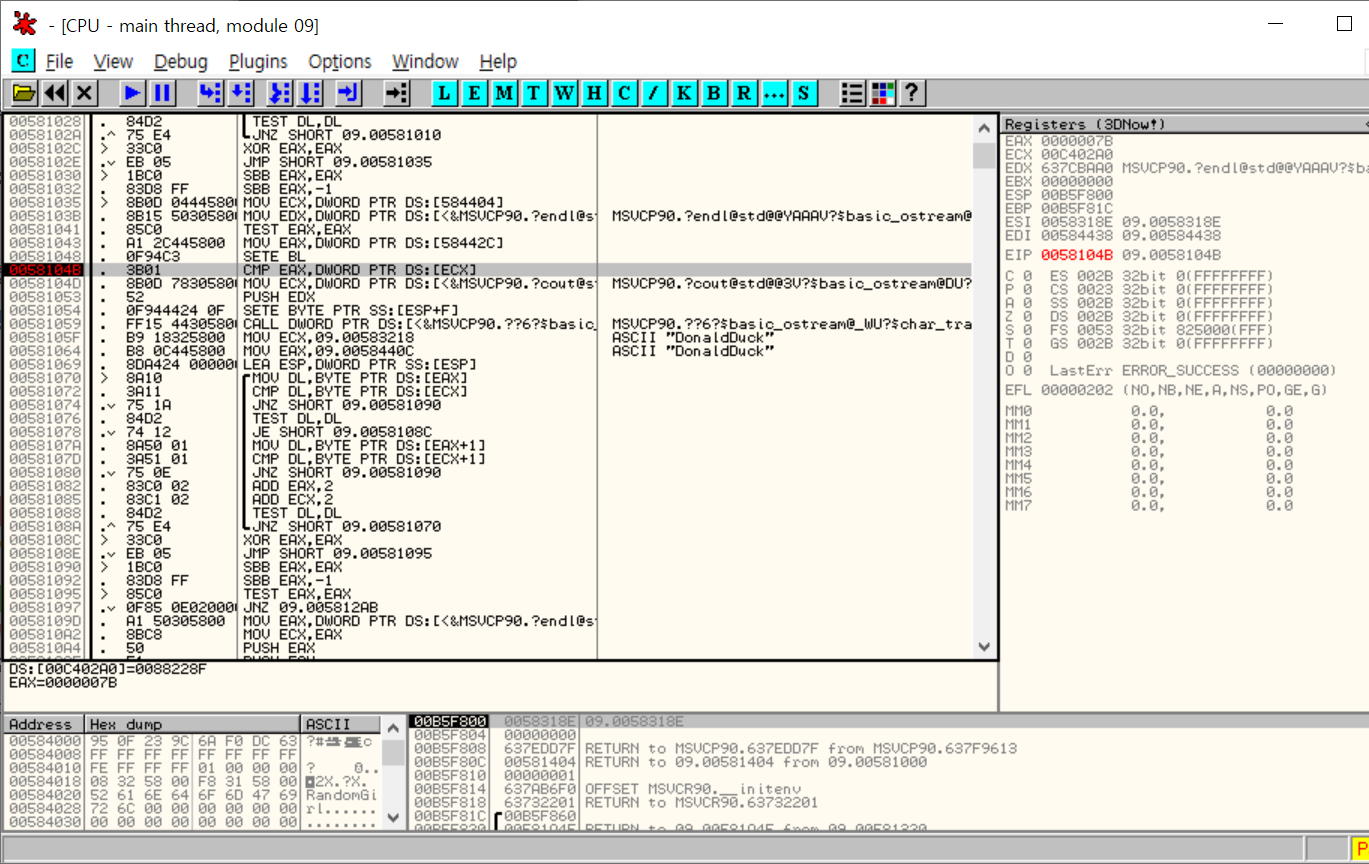


실패문자열이 출력되기 전 password를 비교하는 문이 있었던 것 같다.

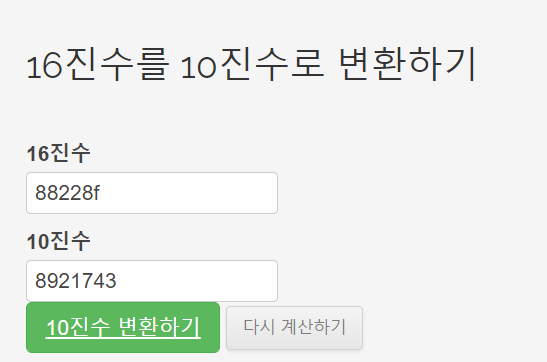
이 부분을 찾아 한참 헤매다가 못 풀고 있었는데 스터디원 분께서 풀이해주시는 것을 듣고

해결 실마리를 찾을 수 있었다.

내가 입력한 password가 (123/16진수로 7B)가 EAX값에 들어있고, 이 값과 ECX에 있는 값 비교하는 CMP문을 발견했다. (58104B)

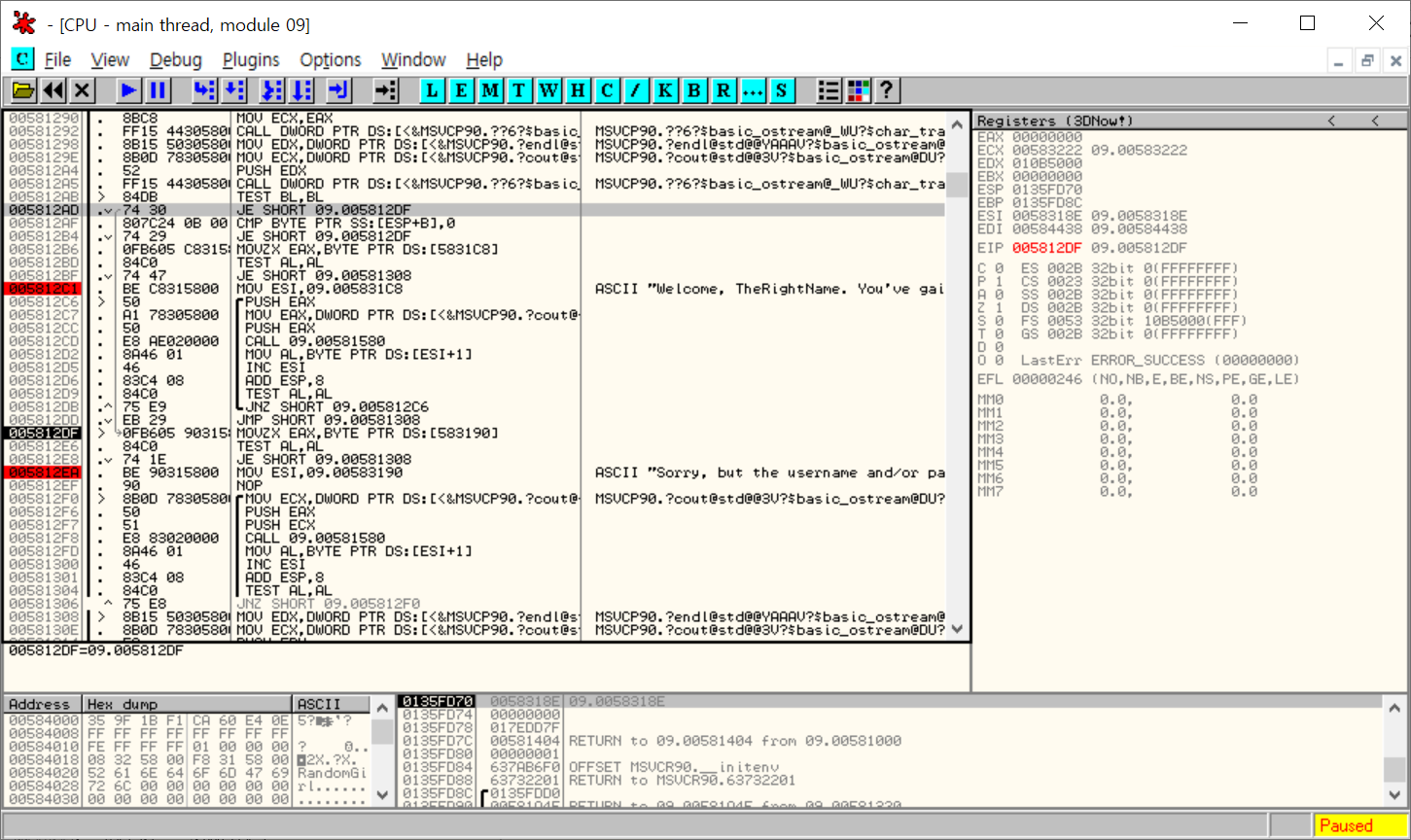


88228F를 10진수로 바꾼 값이 password일 것이다.



Username과 password를 입력했지만 문제가 해결되지 않았다.

이 문제를 해결하기 위해서는 점프문을 잘 조절해서 성공문자열로 가도록 실행시켜야 했는데



\*

Test BL, BL (BL값이 0이면 점프)

CMP BYTE PTR SS:[ESP+B], 0 (값이 0이면 점프)

\*

5812AD에서 JE ->를 JNZ로 수정해주면 성공 플래그로 갈 수 있다.

\*

JE: 0이면 점프

JNZ: 0이 아니면 점프

\*

