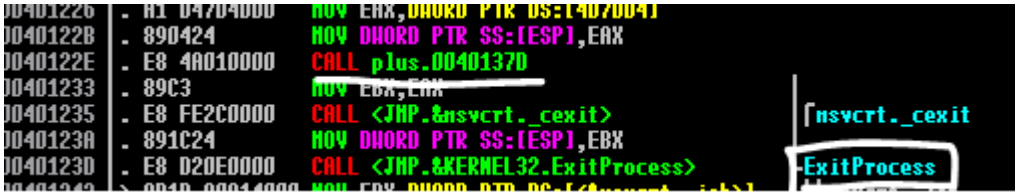
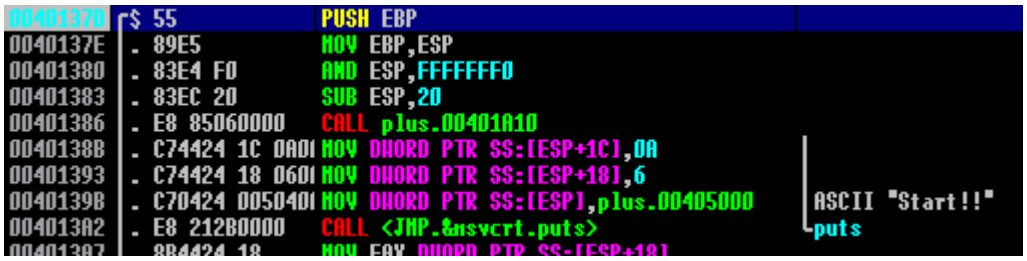
실습과제 1

exe 파일을 디버거에서 열고 한줄씩 실행을 해보았다.

먼저 main 함수를 찾기 위해 가장 먼저 보이는 함수에 f7을 이용하여 들어가봤다.

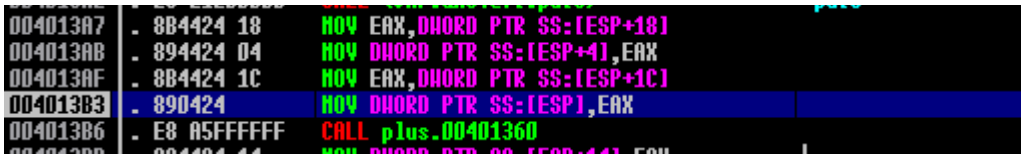


들어가보니 exitprocess라는 주석이 보이고, 저번 예제처럼 exitprocess 윗 부분에 있는 함수가 main 함수 아닐까? 하고 바로 위에 보이는 함수에 f7을 통해 들어가봤다.



그랬더니 다음과 같이 main 함수를 찾을 수 있었다.

이 부분에선 함수의 시작을 알리는 push ebp, mov ebp, esp 후에 start!!를 출력해주는 것 같다.



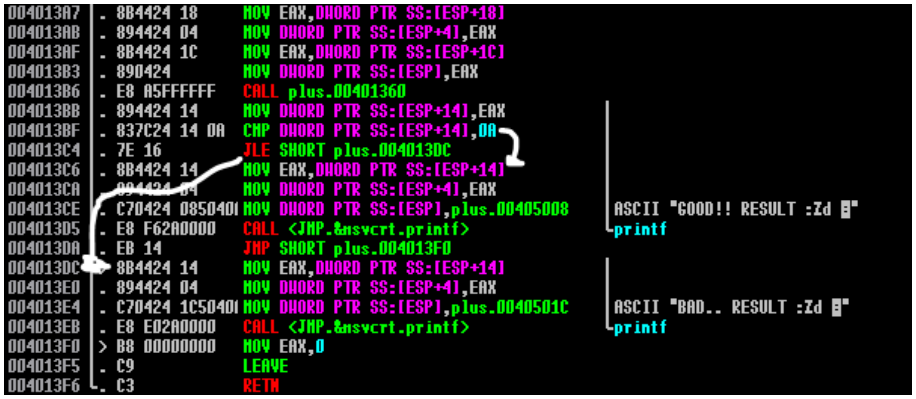
이 부분에서는 6과 10이라는 값을 eax로 가져와 스택에 저장하고,

Call plus.00401360 부분에서 서브루틴을 호출하는 것을 알 수 있다.

서브루틴 부분을 보면 10과 6을 순서대로 edx, eax 레지스터로 가져온 후에

둘을 add 하여 eax에 저장한다는 것을 알 수 있다. 그리고 그 결과를 스택에 저장하고 서브루틴을 마친다.

서브루틴을 마칠 때 retn 부분에서 eip에 서브루틴 call 했던 라인의 바로 밑에 주소가 저장되어 있는 것을 확인했다.



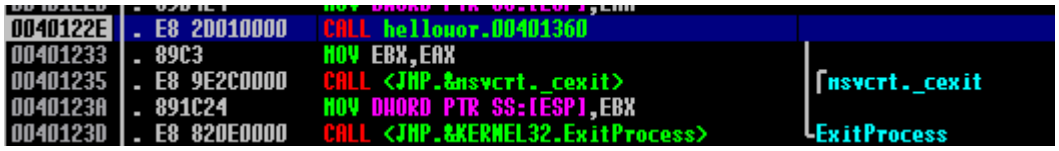
서브루틴의 결과가 eax에 저장되었었는데 이 결과를 10과 비교(cmp)하고 작거나 같다면 0040230c 부분(bad 출력)으로 점프하고, 크다면 바로 밑에 004013ca 부분(good!! 출력)이 실행되는 것을 확인했다.

위의 부분을 보고 if문은 if문 조건이 cmp로 비교되고 jmp를 이용해 cmp결과에 따라 분기하게 하여 if문이 실행되는 것을 알았다.

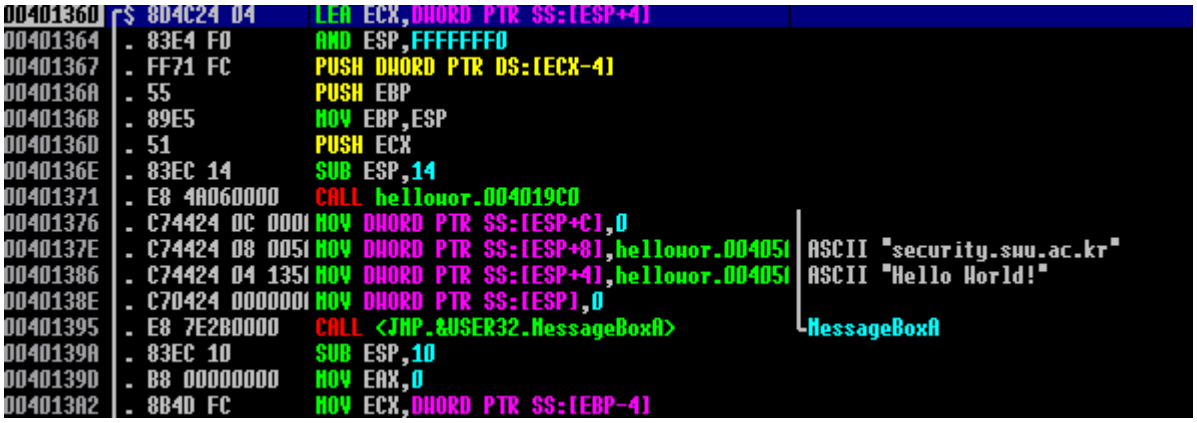
실습과제 2

Exe 파일을 생성 후 디버거를 통해 열었다.

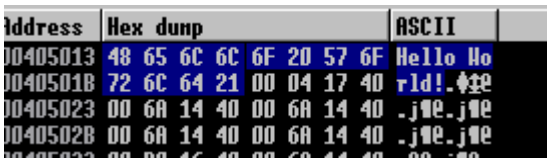
가장 먼저 보이는 함수를 f7를 통해 내부를 보았다.



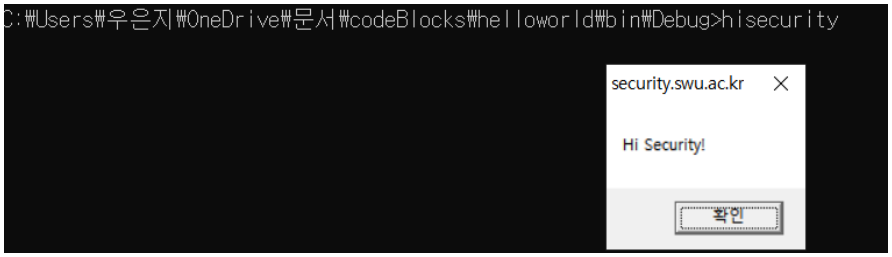
이번 실습도 실습1과 동일하게 exitprocess 위에 있는 call 함수에서 호출하는 부분이 main 함수였다.



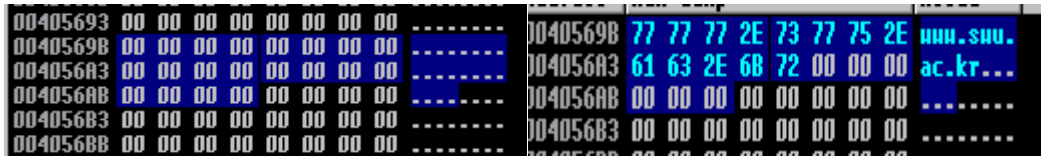
Security.swu.ac.kr과 Hello World를 스택에 저장하고 messagebox를 call하는 것을 알 수 있다.



Hello world가 저장되어 있는 곳에 ctrl+g 키를 통해 와서 문자열을 변경하기 위해 컨트롤+e로 Hi Security로 수정하였다. 그 후 copy to executable 후 save file을 하여 복사본을 저장한 후 그 파일을 실행해본 결과



다음과 같이 원하는 결과가 출력되었다.



다음으론 덤프에서 문자열이 저장된 곳 아래에 00000으로 패딩되어 있는 곳에 가서 칸을 선택한 후에 컨트롤+e 키로 security.swu.ac.kr을 www.swu.ac.kr로 변경하였다. (0040569B의 주소에)

다음은 0040137E 부분을 두번 클릭해 참조하는 주소를 0040569B로 바꿔서 실행해보았다.

다음과 같이 원하는 결과를 얻을 수 있었다.