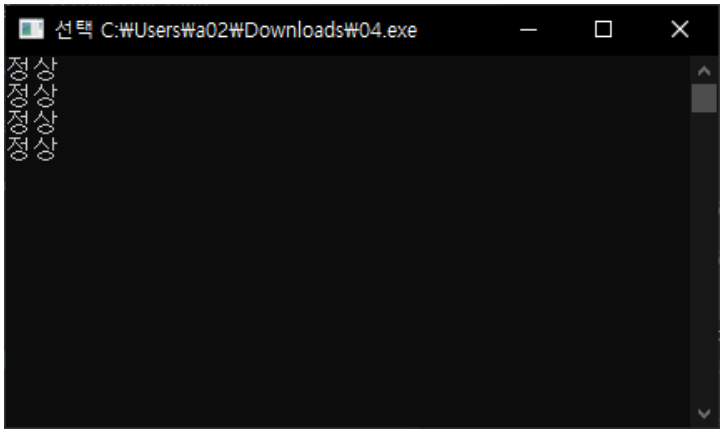
# codeengn-basic-L04 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 11. 10:35



그냥 실행 시켰을 때는 정상이라고 뜨지만 디버거로 열었을 때는 저를 굉장히 싫어하네요.

F8로 실행시켜보면서 확인하던 도중,

```
00408454 |.  E8 B68BFFFF        call <04.sub_40100F>
```

sub_40100F 함수가 호출되니 디버깅 당함이라고 뜨기 시작했습니다. 이 함수를 따라 들어가봅시다.

```
.   CC              int3
>   55              push ebp
.   8BEC            mov ebp,esp
.   83EC 40         sub esp,40
.   53              push ebx
.   56              push esi
.   57              push edi
.   8D7D C0         lea edi,dword ptr ss:[ebp-40]
.   B9 10000000     mov ecx,10
.   B8 CCCCCCCC     mov eax,CCCCCCCC
.   F3:AB           rep stosd
>   8BF4            mov esi,esp
.   68 E8030000     push 3E8
.   FF15 68B14300   call dword ptr ds:[<&Sleep>]
.   3BF4            cmp esi,esp
.   E8 B4710000     call <04.sub_408210>
.   8BF4            mov esi,esp
.   FF15 64B14300   call dword ptr ds:[<&IsDebuggerPresent>]
.   3BF4            cmp esi,esp
.   E8 A5710000     call <04.sub_408210>
.   85C0            test eax,eax
.v  74 0F           je 04.40107E
.   68 24104300     push 04.431024                  431024:"디버깅 당함 \n"
.   E8 17710000     call <04.sub_408190>
.   83C4 04         add esp,4
.v  EB 0D           jmp 04.401088
>   68 1C104300     push 04.43101C                  43101C:"정상 \n"
.   E8 08710000     call <04.sub_408190>
.   83C4 04         add esp,4
>^  EB BB           jmp 04.401048
    CC              int3
```

여기에 해당하는 메시지를 띄우는 구문이 있습니다. IsDebuggerPresent 함수가 궁금하네요 검색해봅시다.

## Return value

If the current process is running in the context of a debugger, the return value is nonzero.

If the current process is not running in the context of a debugger, the return value is zero.

리턴값 value가 디버깅 당하면 0이 아니고, 디버깅 당하지 않으면 0이라고 합니다.

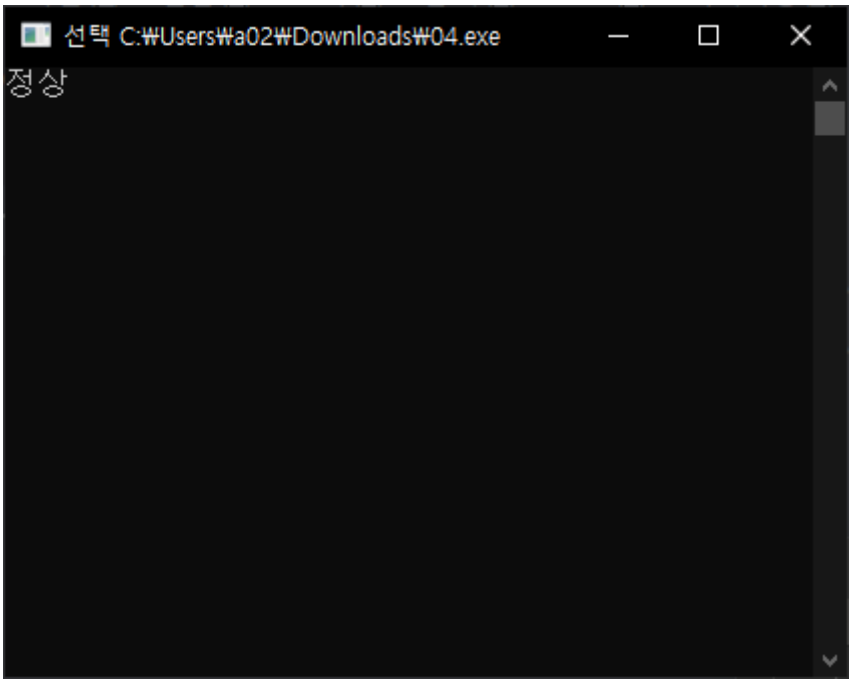
eax를 0으로 바꿔주면 될 거 같아요.

```
0040105E  .   FF15 64B14300   call dword ptr ds:[<&IsDebuggerPresent>]
00401064  .   3BF4            cmp esi,esp
00401066  .   E8 A5710000     call <04.sub_408210>
0040106B  .   85C0            test eax,eax
0040106D  .v  74 0F           je 04.40107E
0040106F  .   68 24104300     push 04.431024                  431024:"디버깅 당함 \n"
00401074  .   E8 17710000     call <04.sub_408190>
00401079  .   83C4 04         add esp,4
0040107C  .v  EB 0D           jmp 04.401088
0040107E  >   68 1C104300     push 04.43101C                  43101C:"정상 \n"
00401083  .   E8 08710000     call <04.sub_408190>
00401088  .   83C4 04         add esp,4
0040108B  >^  EB BB           jmp 04.401048
```

함수 바로 다음 구문에 브레이크 포인트를 걸고,

```
EAX   00000001
```

eax레지스터의 값이 1로 되어 있는데 0으로 바꿔주면




정상을 출력하는 구문으로 점프를 뛰며 정상으로 출력 됩니다.  문제는 함수의 이름을 원했으니 "IsDebuggerPresent"