[Code_Engn] Basic RCE L04

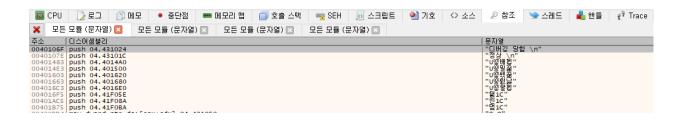


Basic RCE L04

이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

— Author: CodeEngn— File Password: codeengn





문자열 참조에서 "디버깅 당함" 으로 이동해보겠다.

```
push 3E8
call dword ptr ds:[<&Sleep>]
cmp esi,esp
                                               esi:EntryPoint
call 04.408210
mov esi,esp
call dword ptr ds:[<&IsDebuggerPresent>
                                               esi:EntryPoint
cmp esi,esp
call 04.408210
test eax,eax
                                               esi:EntryPoint
   04.40107E
push 04.431024
                                               431024:"디버깅 당함 \n"
call 04.408190
add esp,4
jmp 04.40108B
push 04.43101C
                                               43101C: "정상 \n"
call 04.408190
add esp,4
jmp 04.401048
```

바로 위에 IsDebuggerPresent라는 함수가 있길래 이것이 디버거를 탐지하는 프로그램이라고 유추하였습니다.