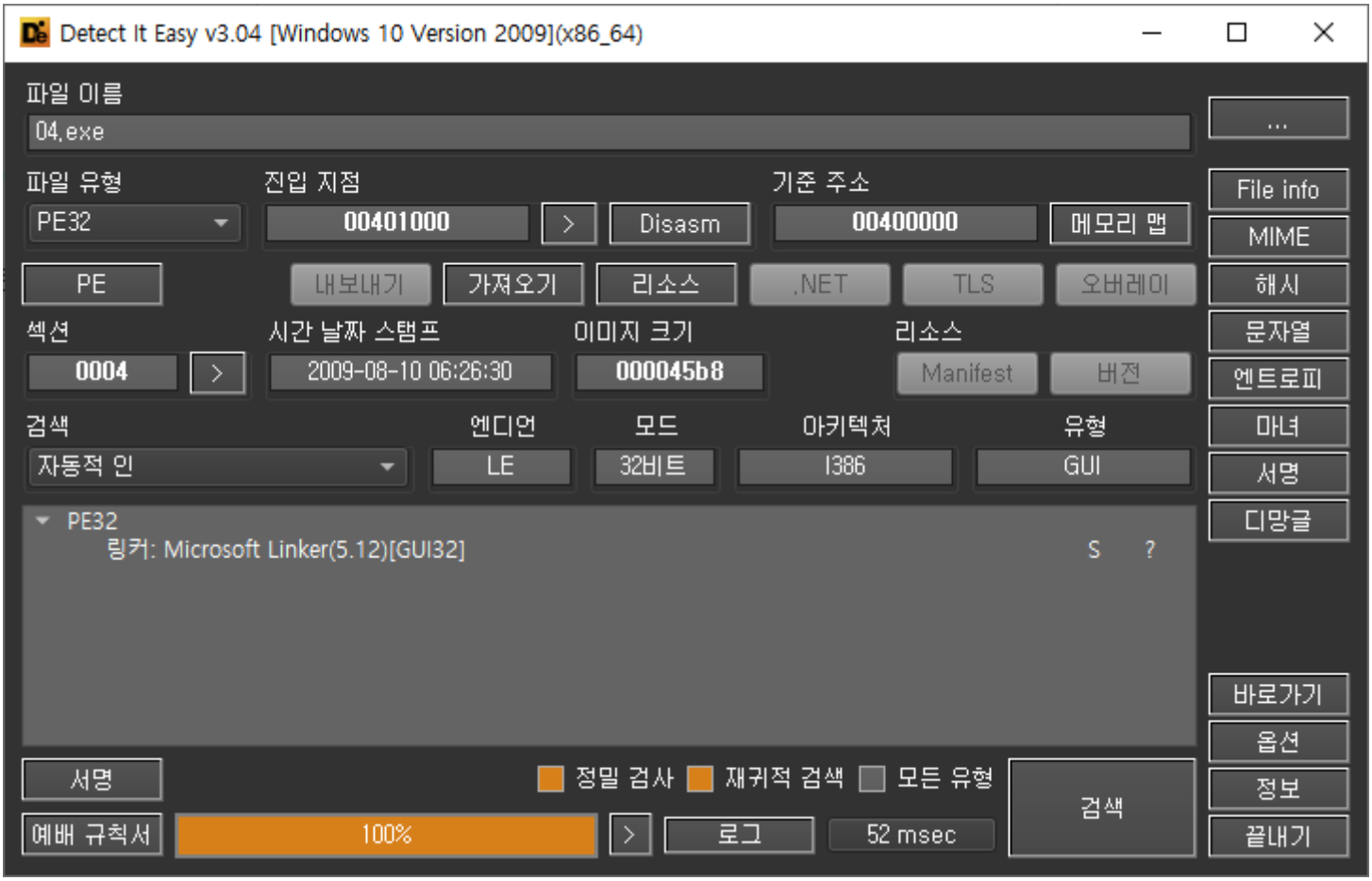
codeengn-advance-L04 풀이

리버싱 문제풀이 / Wonlf / 2022. 5. 4. 16:29

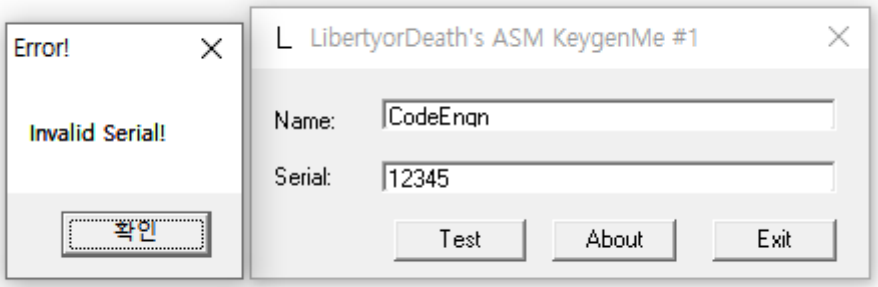
문제는 Name이 CodeEngn 일때 Serial을 원하고 있다.

Die로 열어본다.



아무런 특이사항이 없다.

실행시켜본다.



문제에서 원하는 Serial은 여기를 말하는 것 같다.

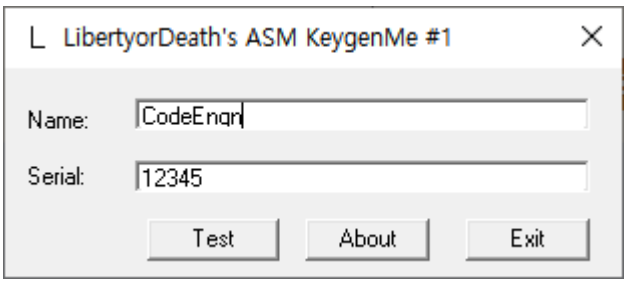
디버거로 열어본다.

```
00401160    E8 75000000     call <JMP.&wsprintfA>
00401165    83C4 10         add esp,10
00401168    68 E0304000     push 04.4030E0
0040116D    68 04314000     push 04.403104
00401172    E8 5D000000     call <JMP.&lstrcmpA>
00401177    83F8 00         cmp eax,0
0040117A    5F              pop edi
0040117B    75 14           jne <04.sub_401191>
0040117D    6A 00           push 0                          sub_40117D
0040117F    68 92304000     push 04.403092                  403092:"Yay!"
00401184    68 84304000     push 04.403084                  403084:"Valid Serial!"
00401189    6A 00           push 0
0040118B    E8 6E000000     call <JMP.&MessageBoxA>
00401190    C3              ret
00401191    6A 00           push 0                          sub_401191
00401193    68 A7304000     push 04.4030A7                  4030A7:"Error!"
00401198    68 97304000     push 04.403097                  403097:"Invalid Serial!"
0040119D    6A 00           push 0
```

실패 문자열을 검색하여 통과와 실패로 분기하는 구문을 찾아 냈다.

아마 4030E0 과 403104 둘 중 한곳에는 내가 입력한 값이 있을 것이다.

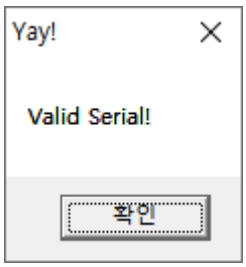
임의의 값을 넣어본다.



```
00401155    56              push esi
00401156    68 AE304000     push 04.4030AE                  4030AE:"LOD-%lu-%lX"
0040115B    68 04314000     push 04.403104                  403104:"LOD-59919-A0024900"
00401160    E8 75000000     call <JMP.&wsprintfA>
00401165    83C4 10         add esp,10
00401168    68 E0304000     push 04.4030E0                  4030E0:"12345"
0040116D    68 04314000     push 04.403104                  403104:"LOD-59919-A0024900"
00401172    E8 5D000000     call <JMP.&lstrcmpA>
00401177    83F8 00         cmp eax,0
0040117A    5F              pop edi
0040117B    75 14           jne <04.sub_401191>
0040117D    6A 00           push 0                          sub_40117D
0040117F    68 92304000     push 04.403092                  403092:"Yay!"
00401184    68 84304000     push 04.403084                  403084:"Valid Serial!"
00401189    6A 00           push 0
0040118B    E8 6E000000     call <JMP.&MessageBoxA>
00401190    C3              ret
00401191    6A 00           push 0                          sub_401191
00401193    68 A7304000     push 04.4030A7                  4030A7:"Error!"
00401198    68 97304000     push 04.403097                  403097:"Invalid Serial!"
0040119D    6A 00           push 0
0040119F    E8 5A000000     call <JMP.&MessageBoxA>
```

예상한대로 내가 입력한 값과 특정 값을 비교하는 구문이 있다.

특정 값을 serial에 넣어주면,



성공 하였다

Serial을 홈페이지에 인증해주면 된다.

성공!