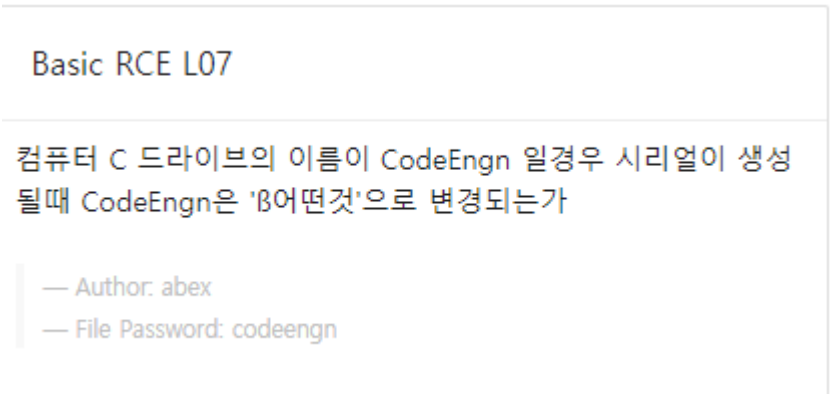
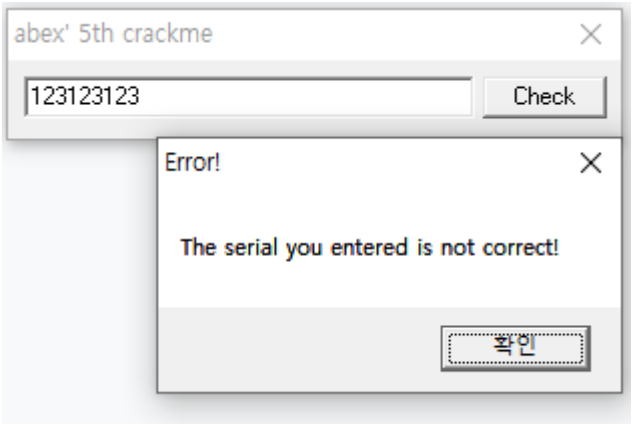
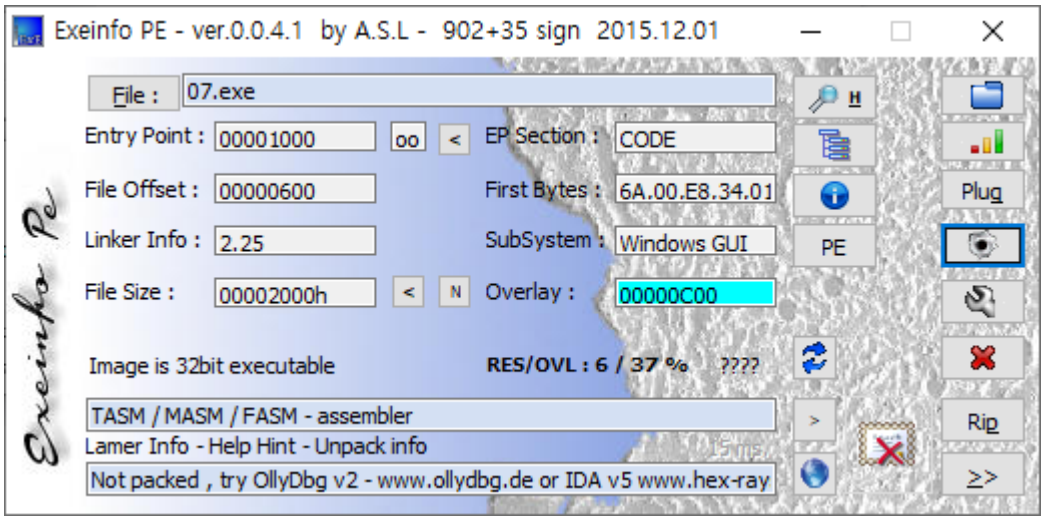
CodeEngn Basic RCE

7. Level 07

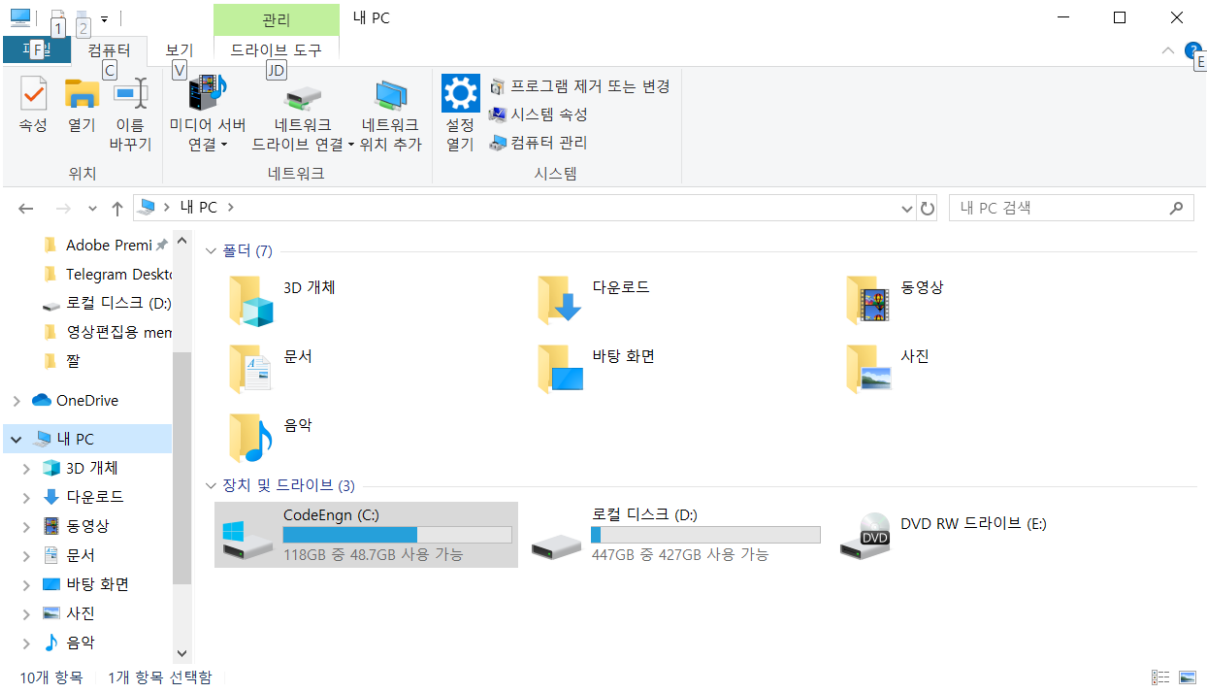




프로그램 실행화면이다.



07.exe는 확인결과 패킹되지 않았고 어셈블리어로 코딩됐다는 것을 알 수 있다.



다음과 같이 C드라이브의 이름을 CodeEngn으로 바꿔보았다.

```
004010F7    E8 51000000          call <JMP.&lstrcmpiA>
004010FC    83F8 00              cmp eax,0
004010FF    74 16                je 07.401117
00401101    6A 00                push 0
00401103    68 34244000          push 07.402434                  402434:"Error!"
00401108    68 3B244000          push 07.40243B                  40243B:"The serial you entered is not correct!"
0040110D    FF75 08              push dword ptr ss:[ebp+8]
00401110    E8 56000000          call <JMP.&MessageBoxA>
00401115    EB 16                jmp 07.40112D
00401117    6A 00                push 0
00401119    68 06244000          push 07.402406                  402406:"Well Done!"
0040111E    68 11244000          push 07.402411                  402411:"Yep, you entered a correct serial!"
00401123    FF75 08              push dword ptr ss:[ebp+8]
00401126    E8 40000000          call <JMP.&MessageBoxA>
0040112B    EB 00                jmp 07.40112D
0040112D    6A 00                push 0
0040112F    FF75 08              push dword ptr ss:[ebp+8]
00401132    E8 22000000          call <JMP.&EndDialog>
```

방금 프로그램 시 나오는 문자열을 검색해 비교함수인 CMP 함수가 있는 것을 확인

```
00401090    6A 32                push 32
00401092    68 5C224000          push 07.40225C                  40225C:"EqfgEngn4562-ABEX"
00401097    6A 00                push 0
00401099    E8 B5000000          call <JMP.&GetVolumeInformationA>
0040109E    68 F3234000          push 07.4023F3                  4023F3:"4562-ABEX"
004010A3    68 5C224000          push 07.40225C                  40225C:"EqfgEngn4562-ABEX"
004010A8    E8 94000000          call <JMP.&lstrcatA>
004010AD    B2 02                mov dl,2
004010AF    8305 5C224000 01     add dword ptr ds:[40225C],1     0040225C:"EqfgEngn4562-ABEX"
004010B6    8305 5D224000 01     add dword ptr ds:[40225D],1     0040225D:"qfgEngn4562-ABEX"
004010BD    8305 5E224000 01     add dword ptr ds:[40225E],1     0040225E:"fgEngn4562-ABEX"
004010C4    8305 5F224000 01     add dword ptr ds:[40225F],1     0040225F:"gEngn4562-ABEX"
004010CB    FECA                 dec dl
004010CD    75 E0                jne 07.4010AF
004010CF    68 FD234000          push 07.4023FD                  4023FD:"L2C-5781"
004010D4    68 00204000          push 07.402000                  402000:"L2C-5781EqfgEngn4562-ABEX"
004010D9    E8 63000000          call <JMP.&lstrcatA>
004010DE    68 5C224000          push 07.40225C                  40225C:"EqfgEngn4562-ABEX"
004010E3    68 00204000          push 07.402000                  402000:"L2C-5781EqfgEngn4562-ABEX"
004010E8    E8 54000000          call <JMP.&lstrcatA>
004010ED    68 24234000          push 07.402324                  402324:"Enter your serial"
004010F2    68 00204000          push 07.402000                  402000:"L2C-5781EqfgEngn4562-ABEX"
004010F7    E8 51000000          call <JMP.&lstrcmpiA>
004010FC    83F8 00              cmp eax,0
004010FF    74 16                je 07.401117
```

중단점 설정되지 않음

CMP 함수에 BP를 걸어두고 실행하니 안보이던 문자열이 보임

GetVolumeInformationA : 하드드라이브의 정보를 얻어오는 함수

코드의 흐름을 보아 L2C-5781EqfgEngn4562-ABEX 가 시리얼임