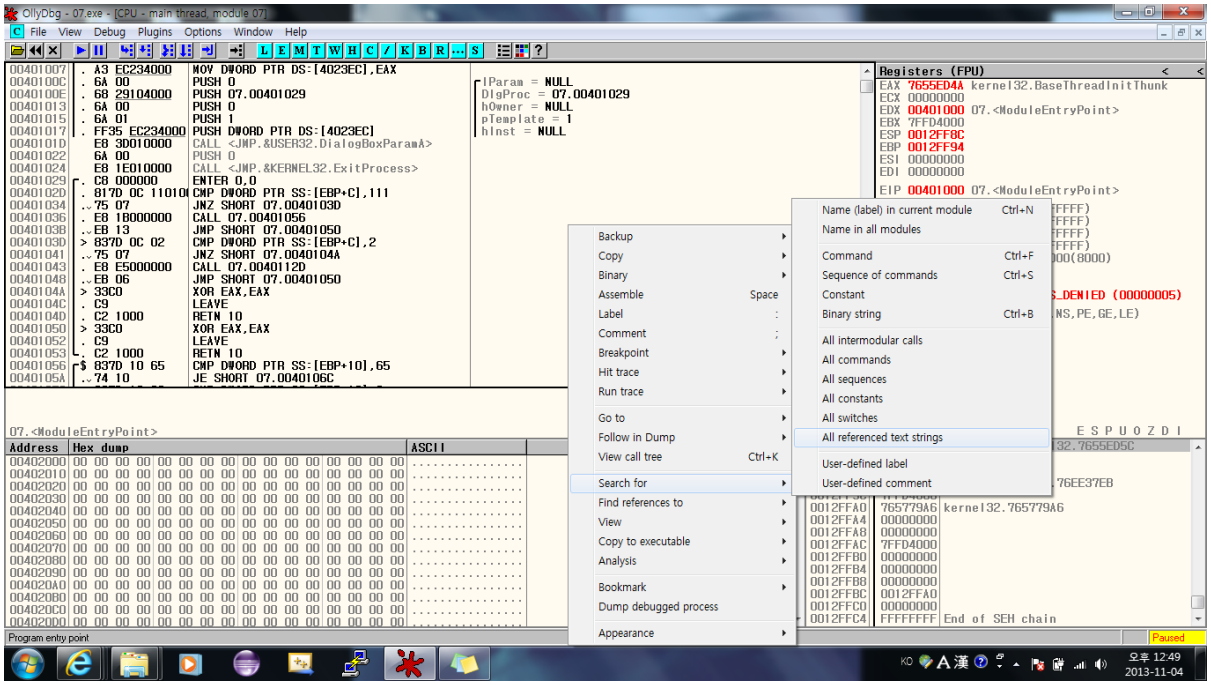
Challenges : Basic 07

Author : abex

Korea :
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 "어떤것"으로 변경되는가

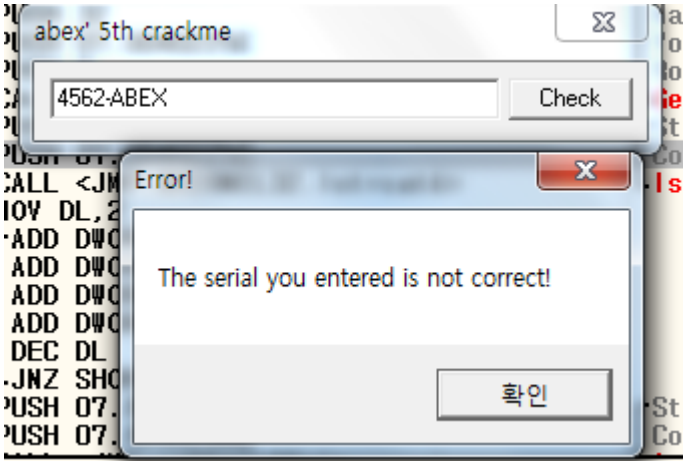
그럼 일단 07.exe 파일을 디버깅 해보자

올리디버거로 들어가서 search for -> all referenced text strings



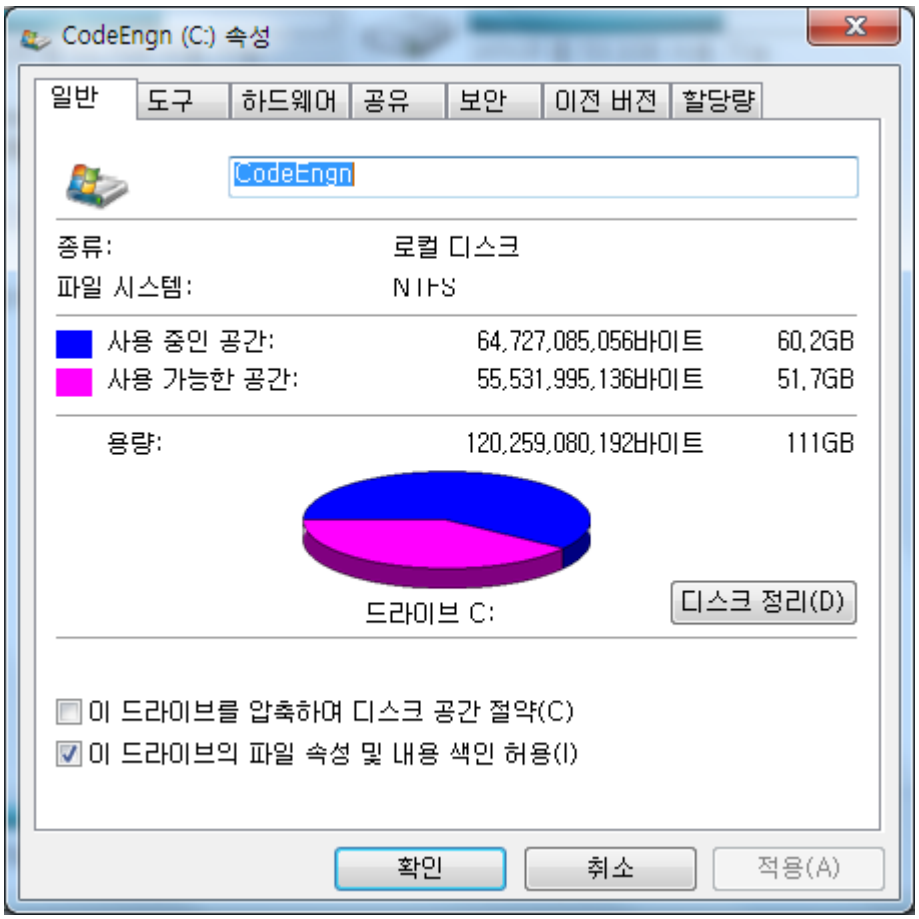
00401000	PUSH 0	(Initial CPU selection)
0040109E	PUSH 07.004023F3	ASCII "4562-ABEX"
004010CF	PUSH 07.004023FD	ASCII "L2C-5781"
00401103	PUSH 07.00402434	ASCII "Error!"
00401108	PUSH 07.0040243B	ASCII "The serial you entered is not correct!"
00401119	PUSH 07.00402406	ASCII "Well Done!"
0040111E	PUSH 07.00402411	ASCII "Yep, you entered a correct serial!"

저 둘 중 하나가 시리얼번호 아니면 두개를 조합해서 한번 입력해보자

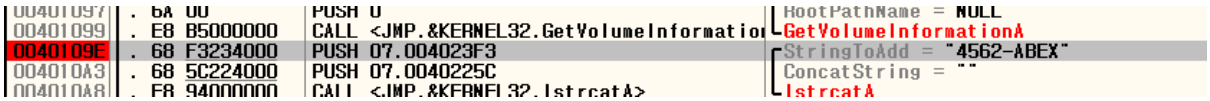


역시,,,에러다

그러면 문제대로 C드라이버의 이름을 CodeEngn 으로 바꾸고 다시 실행시켜보자



다시 실행~



여기에 브레이크 포인트를 걸고 실행시켜보자

체크를 누르면 브레이크 포인트 걸었던 곳부터 f8 로 한 단계씩 들어가보자

```
00401097  . 6A 00          PUSH 0                                  RootPathName = NULL
00401099  . E8 B5000000    CALL <JMP.&KERNEL32.GetVolumeInformatio GetVolumeInformationA
0040109E  . 68 F3234000    PUSH 07.004023F3                        StringToAdd = "4562-ABEX"
004010A3  . 68 5C224000    PUSH 07.0040225C                        ConcatString = "CodeEngn"
004010A8  . E8 94000000    CALL <JMP.&KERNEL32.lstrcatA>           lstrcatA
004010AD  . B2 02          MOV DL,2
004010AF  > 8305 5C224000  ADD DWORD PTR DS:[40225C],1
004010B6  . 8305 5D224000  ADD DWORD PTR DS:[40225D],1
004010BD  . 8305 5E224000  ADD DWORD PTR DS:[40225E],1
004010C4  . 8305 5F224000  ADD DWORD PTR DS:[40225F],1
004010CB  . FECA           DEC DL
004010CD  .^75 E0          JNZ SHORT 07.004010AF
```

그럼 ConcatString 에 CodeEngn 이라고 들어가있다.

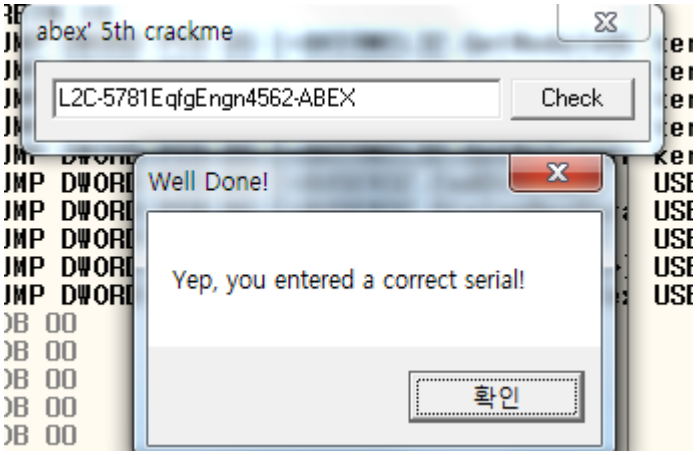
```
00401097  . 6A 00          PUSH 0                                  RootPathName = NULL
00401099  . E8 B5000000    CALL <JMP.&KERNEL32.GetVolumeInformatio GetVolumeInformationA
0040109E  . 68 F3234000    PUSH 07.004023F3                        StringToAdd = "4562-ABEX"
004010A3  . 68 5C224000    PUSH 07.0040225C                        ConcatString = "EqfgEngn4562-ABEX"
004010A8  . E8 94000000    CALL <JMP.&KERNEL32.lstrcatA>           lstrcatA
004010AD  . B2 02          MOV DL,2
004010AF  > 8305 5C224000  ADD DWORD PTR DS:[40225C],1
004010B6  . 8305 5D224000  ADD DWORD PTR DS:[40225D],1
004010BD  . 8305 5E224000  ADD DWORD PTR DS:[40225E],1
004010C4  . 8305 5F224000  ADD DWORD PTR DS:[40225F],1
004010CB  . FECA           DEC DL
004010CD  .^75 E0          JNZ SHORT 07.004010AF
004010CF  . 68 FD234000    PUSH 07.004023FD                        StringToAdd = "L2C-5781"
004010D4  . 68 00204000    PUSH 07.00402000                        ConcatString = ""
```

계속 진행시키다보면 004010AF~004010CD 까지 두바퀴 돌고 ConcatString 은 EqfgEngn4562-ABEX 로 바뀐다

```
004010CB  . FECA           DEC DL
004010CD  .^75 E0          JNZ SHORT 07.004010AF
004010CF  . 68 FD234000    PUSH 07.004023FD                        StringToAdd = "L2C-5781"
004010D4  . 68 00204000    PUSH 07.00402000                        ConcatString = "L2C-5781EqfgEngn4562-ABEX"
004010D9  . E8 63000000    CALL <JMP.&KERNEL32.lstrcatA>           lstrcatA
004010DE  . 68 5C224000    PUSH 07.0040225C                        StringToAdd = "EqfgEngn4562-ABEX"
004010E3  . 68 00204000    PUSH 07.00402000                        ConcatString = "L2C-5781EqfgEngn4562-ABEX"
004010E8  . E8 54000000    CALL <JMP.&KERNEL32.lstrcatA>           lstrcatA
004010ED  . 68 24234000    PUSH 07.00402324                        String2 = "Enter your serial"
004010F2  . 68 00204000    PUSH 07.00402000                        String1 = "L2C-5781EqfgEngn4562-ABEX"
004010F7  . E8 51000000    CALL <JMP.&KERNEL32.lstrcmpiA>          lstrcmpiA
```

그리고 이것이 최종 시리얼 번호이다.

그러므로 CodeEngn 은 EqfgEngn 으로 바뀐다.


abex' 5th crackme
L2C-5781EqfgEngn4562-ABEX
Check
Well Done!
Yep, you entered a correct serial!
확인

성공~!