입력값을 1234567890 으로 넣고.. 대충 프로그램 실행중에 중간에 멈출만한 부분을 bp 걸어보자.

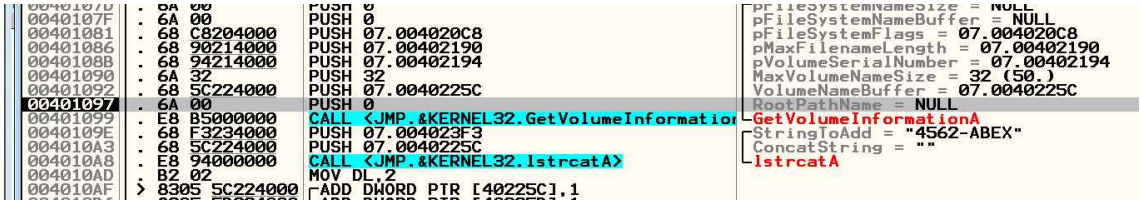
```
004010AF  > 8305 5C224000  ADD DWORD PTR [40225C],1
004010B6  . 8305 5D224000  ADD DWORD PTR [40225D],1
004010BD  . 8305 5E224000  ADD DWORD PTR [40225E],1
004010C4  . 8305 5F224000  ADD DWORD PTR [40225F],1
004010CB  . FECA           DEC DL
004010CD  .^75 E0          JNZ SHORT 07.004010AF
004010CF  . 68 FD234000    PUSH 07.004023FD                 ; StringToAdd = "L2C-5781"
004010D4  . 68 00204000    PUSH 07.00402000                 ; ConcatString = ""
004010D9  . E8 63000000    CALL <JMP.&KERNEL32.lstrcatA>    ; lstrcatA
004010DE  . 68 5C224000    PUSH 07.0040225C                 ; StringToAdd = ""
004010E3  . 68 00204000    PUSH 07.00402000                 ; ConcatString = ""
004010E8  . E8 54000000    CALL <JMP.&KERNEL32.lstrcatA>    ; lstrcatA
004010ED  . 68 24234000    PUSH 07.00402324                 ; String2 = ""
004010F2  . 68 00204000    PUSH 07.00402000                 ; String1 = ""
004010F7  . E8 51000000    CALL <JMP.&KERNEL32.lstrcmpiA>   ; lstrcmpiA
004010FC  . 83F8 00        CMP EAX,0
004010FF  .v74 16          JE SHORT 07.00401117
00401101  . 6A 00          PUSH 0                           ; Style = MB_OK|MB_APPLMODAL
00401103  . 68 34244000    PUSH 07.00402434                 ; Title = "Error!"
00401108  . 68 3B244000    PUSH 07.0040243B                 ; Text = "The serial you entered is not cor
0040110D  . FF75 08        PUSH [ARG.1]                     ; hOwner
00401110  . E8 56000000    CALL <JMP.&USER32.MessageBoxA>   ; MessageBoxA
00401115  .v EB 16         JMP SHORT 07.0040112D
00401117  > 6A 00          PUSH 0                           ; Style = MB_OK|MB_APPLMODAL
00401119  . 68 06244000    PUSH 07.00402406                 ; Title = "Well Done!"
0040111E  . 68 11244000    PUSH 07.00402411                 ; Text = "Yep, you entered a correct serial
00401123  . FF75 08        PUSH [ARG.1]                     ; hOwner
00401126  . E8 40000000    CALL <JMP.&USER32.MessageBoxA>   ; MessageBoxA
```

필자는 0040106C, 004010CF, 00401117 3개 걸었다. (그림에는 2개 bp만 나왔다)

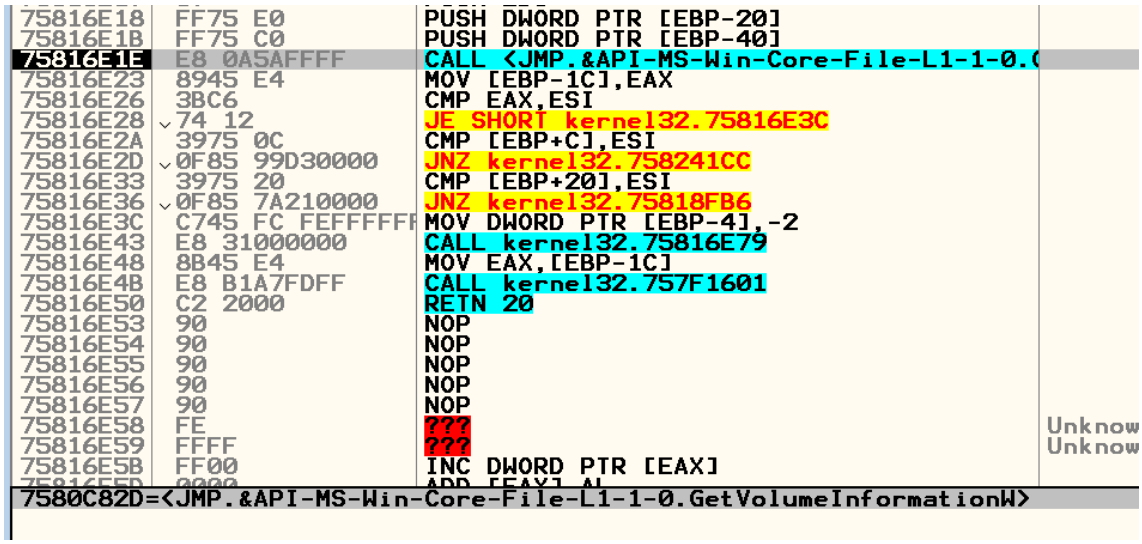
```
004010A3  . 68 5C224000    PUSH 07.0040225C                 ; ConcatString = "6784-ABEX"
004010A8  . E8 94000000    CALL <JMP.&KERNEL32.lstrcatA>    ; lstrcatA
004010AD  . B2 02          MOV DL,2
004010AF  > 8305 5C224000  ADD DWORD PTR [40225C],1
004010B6  . 8305 5D224000  ADD DWORD PTR [40225D],1
004010BD  . 8305 5E224000  ADD DWORD PTR [40225E],1
004010C4  . 8305 5F224000  ADD DWORD PTR [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 = "L2C-57816784-ABEX"
004010D9  . E8 63000000    CALL <JMP.&KERNEL32.lstrcatA>    ; lstrcatA
004010DE  . 68 5C224000    PUSH 07.0040225C                 ; StringToAdd = "6784-ABEX"
004010E3  . 68 00204000    PUSH 07.00402000                 ; ConcatString = "L2C-57816784-ABEX"
004010E8  . E8 54000000    CALL <JMP.&KERNEL32.lstrcatA>    ; lstrcatA
004010ED  . 68 24234000    PUSH 07.00402324                 ; String2 = "1234567890"
004010F2  . 68 00204000    PUSH 07.00402000                 ; String1 = "L2C-57816784-ABEX"
004010F7  . E8 51000000    CALL <JMP.&KERNEL32.lstrcmpiA>   ; lstrcmpiA
004010FC  . 83F8 00        CMP EAX,0
004010FF  .v74 16          JE SHORT 07.00401117
00401101  . 6A 00          PUSH 0                           ; Style = MB_OK|MB_APPLMODAL
00401103  . 68 34244000    PUSH 07.00402434                 ; Title = "Error!"
00401108  . 68 3B244000    PUSH 07.0040243B                 ; Text = "The serial you entered is not cor
0040110D  . FF75 08        PUSH [ARG.1]                     ; hOwner
00401110  . E8 56000000    CALL <JMP.&USER32.MessageBoxA>   ; MessageBoxA
00401115  .v EB 16         JMP SHORT 07.0040112D
00401117  > 6A 00          PUSH 0                           ; Style = MB_OK|MB_APPLMODAL
00401119  . 68 06244000    PUSH 07.00402406                 ; Title = "Well Done!"
0040111E  . 68 11244000    PUSH 07.00402411                 ; Text = "Yep, you entered a correct serial
00401123  . FF75 08        PUSH [ARG.1]                     ; hOwner
```

보면 004010AF부터 004010CB까지 ADD와 DEC를 하면서 입력한 문자열값이 바뀌는데.. 결국 최종적으로 L2C-57816784-ABEX 이러한 문자열로 바뀌고 확인해보니 맞았다.

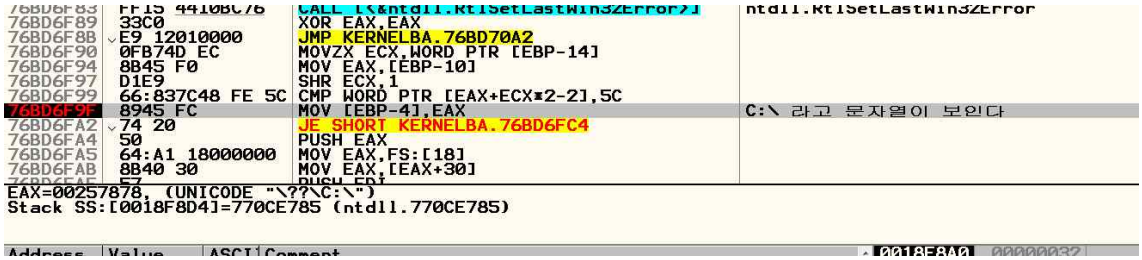
근데.. “컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 "어떤것"으로 변경되는가” 라고 하는걸 보니 문제가 드라이브 명을 따오는거같다;



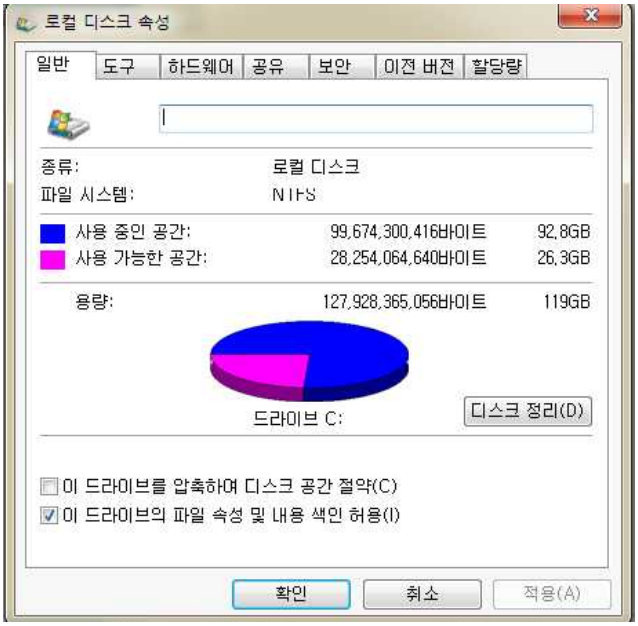
다시한번 살펴보니, GetVolumeInformationA라는 함수가 있는데 아마 이게 드라이브정보를 따오는 함수로 추측된다. 여기로 step into로 들어가보자.

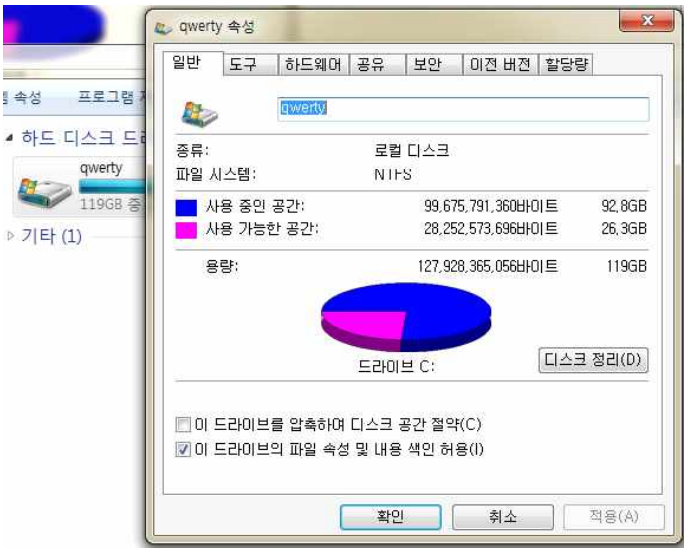


음 뭔가 또 나오긴했다.. ?



보면 EAX값에 C:₩라고 대충 문자열이 들어감을 알 수 있다.

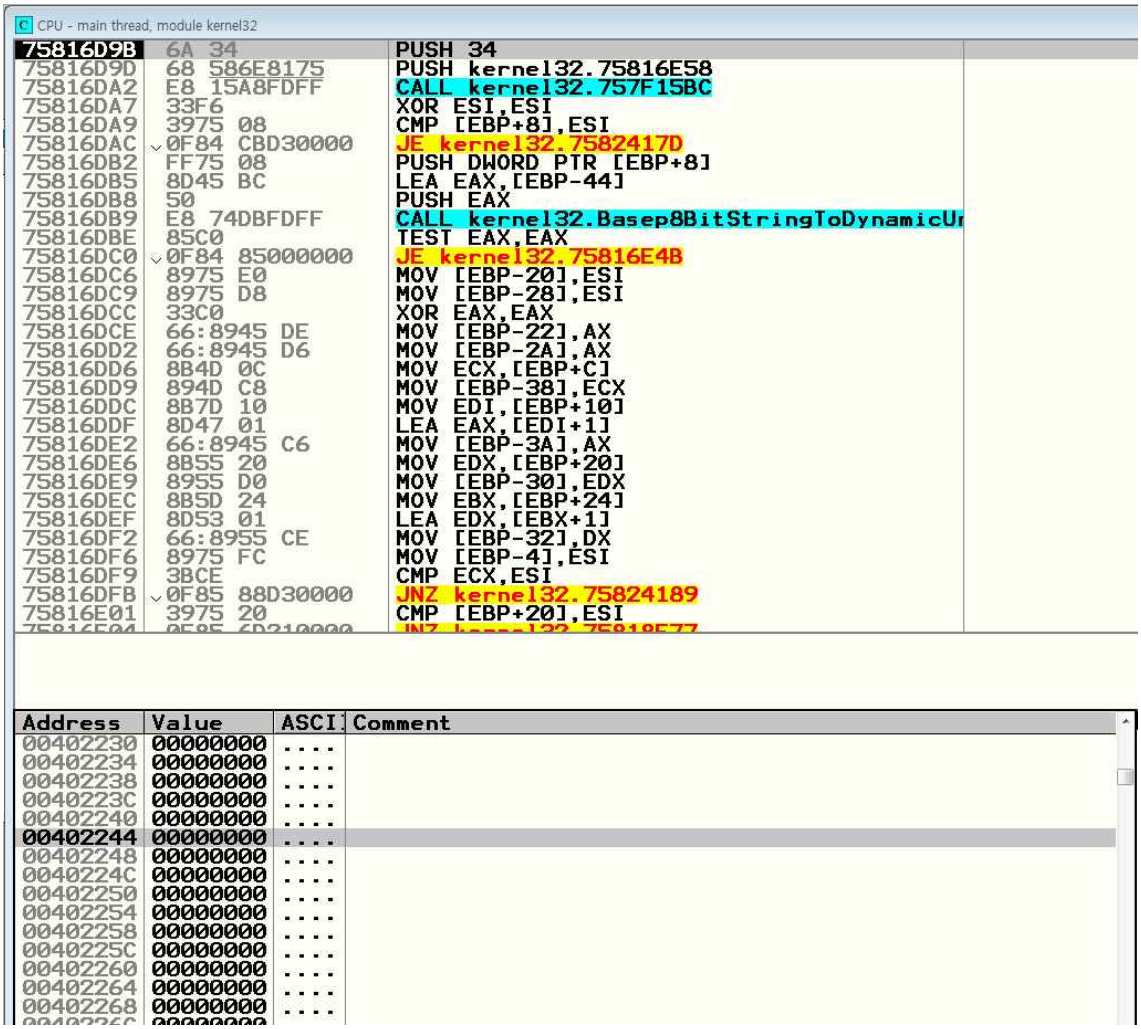




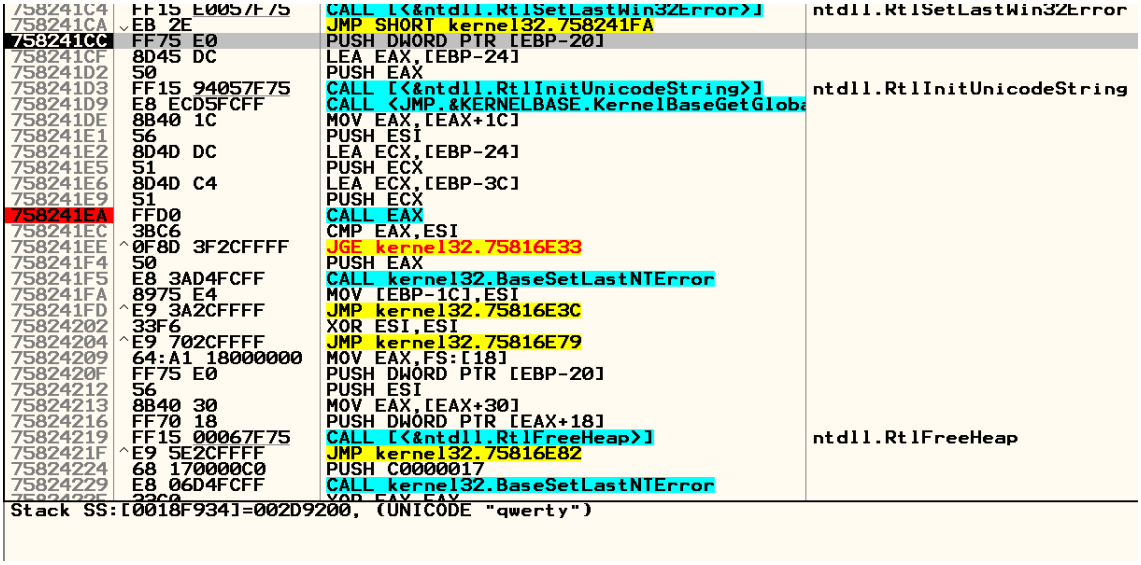
그런데 리버싱하던도중 생각해보니 기본으로 c:₩으로 들어가는게 맞나 싶어서 확인해보니 아예 이름이 없엇다? ㄷ.ㄷ
default값이 잇겟지만 일단 테스트해보기 위해서 임의로 qwerty라고 넣어서 다시해보자!..

```
00401075  . FF75 08         PUSH [ARG.1]                    hWnd
00401078  . E8 F4000000     CALL <JMP.&USER32.GetDlgItemTextA>  GetDlgItemTextA
0040107D  . 6A 00           PUSH 0                          pFileSystemNameSize = NULL
0040107F  . 6A 00           PUSH 0                          pFileSystemNameBuffer = NULL
00401081  . 68 C8204000     PUSH 07.004020C8                pFileSystemFlags = 07.004020C8
00401086  . 68 90214000     PUSH 07.00402190                pMaxFilenameLength = 07.00402190
0040108B  . 68 94214000     PUSH 07.00402194                pVolumeSerialNumber = 07.00402194
00401090  . 6A 32           PUSH 32                         MaxVolumeNameSize = 32 (50.)
00401092  . 68 5C224000     PUSH 07.0040225C                VolumeNameBuffer = 07.0040225C
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 = "qwerty"
004010A8  . E8 94000000     CALL <JMP.&KERNEL32.lstrcatA>   lstrcatA
004010AD  . B2 02           MOV DL,2
004010AF  > 8305 5C224000   ADD DWORD PTR [40225C],1
004010B6  . 8305 5D224000   ADD DWORD PTR [40225D],1
004010BD  . 8305 5E224000   ADD DWORD PTR [40225E],1
004010C4  . 8305 5F224000   ADD DWORD PTR [40225F],1
```

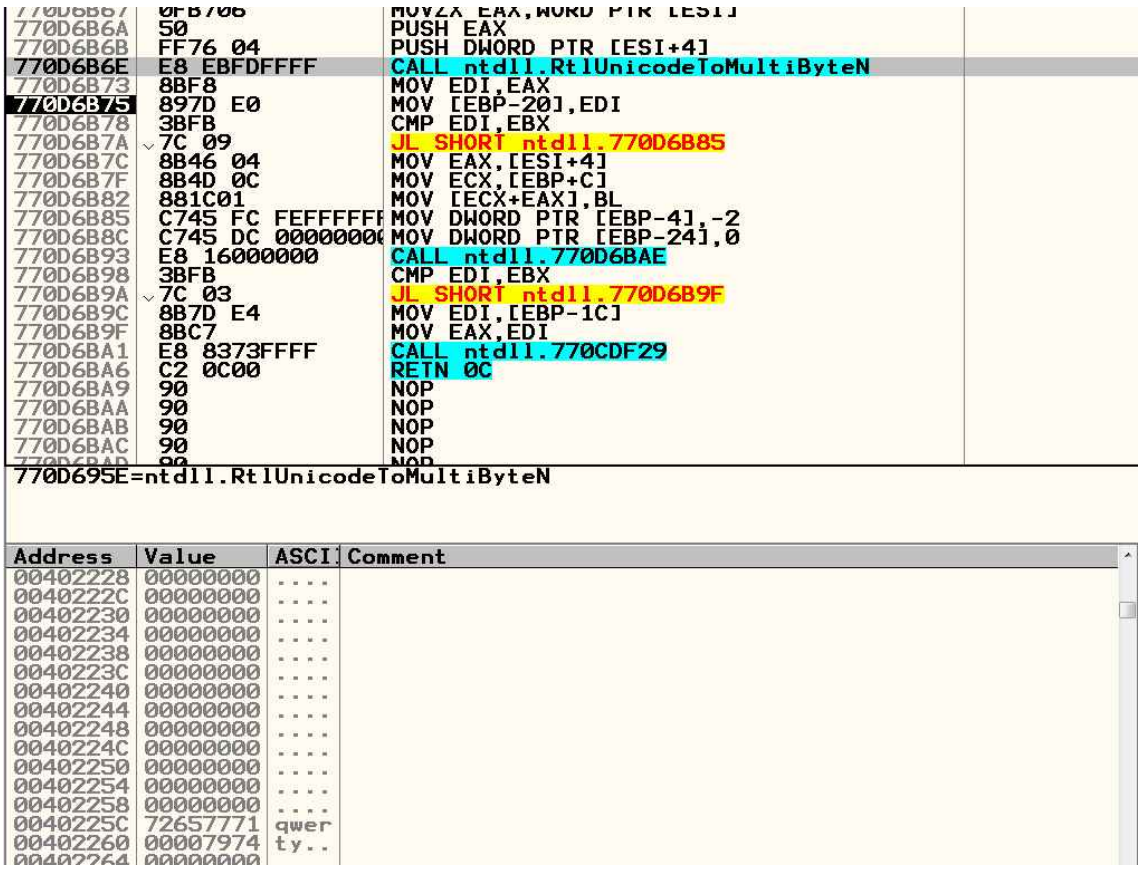
아 혹시나 Concat에 문자열붙어서 넣을까 싶어서 일단 분석안해보고 f8로 step over해보니 qwerty로 그냥 문자열 붙여서 들어간다 ..ㅡㅡ; 그래도 공부할겸 분석 한번 해보자!
보면 일단 0040225C에 문자열을 붙이는걸 알수있다.



일단 0040225C 기준으로 값이 들어가고 나오는걸 체크하게 메모리 값을 확인하고
위에 75816D98은 GetVolumnInformation을 타서 들어가자마자 찍은 주소다.

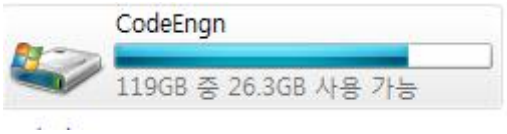


보면 EBP기준으로 20byte만큼 빼서 qwerty라는 값을 넣는것을 확인할 수 있다.
이곳을 찾게된 경로는 757816E1E라고 MS-Win-Core ??? <GetVolumeInformation>에서 몇 번 넘어가다보면 보인다.



음 CALL인지 어느 주소에서 정확히 0040225C에 qwerty라 저장되는지 모르겟는데 여튼

이 부근이다. 대충 분석했으니 넘어가자;



드라이브명을 CodeEngn으로 바꾸고 해보면..

```
004010CB  . FEC8          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 = "01234567890"
004010F2  . 68 00204000   PUSH 07.00402000                ; String1 = "L2C-5781EqfgEngn4562-ABEX"
004010F7  . E8 51000000   CALL <JMP.&KERNEL32.lstrcmpiA>  ; lstrcmpiA
004010FC  . 83F8 00       CMP EAX,0
004010FF  . 74 16         JE SHORT 07.00401117
00401101  . 6A 00         PUSH 0                          ; Style = MB_OK|MB_APPLMODAL
00401103  . 68 34244000   PUSH 07.00402434                ; Title = "Error!"
00401108  . 68 3B244000   PUSH 07.0040243B                ; Text = "The serial you entered is not cor
0040110D  . FF75 08       PUSH [ARG.1]                    ; hOwner
00401110  . E8 56000000   CALL <JMP.&USER32.MessageBoxA>  ; MessageBoxA
00401115  . EB 16         JMP SHORT 07.0040112D
00401117  > 6A 00         PUSH 0                          ; Style = MB_OK|MB_APPLMODAL
00401119  . 68 06244000   PUSH 07.00402406                ; Title = "Well Done!"
0040111E  . 68 11244000   PUSH 07.00402411                ; Text = "Yep, you entered a correct serial
00401123  . FF75 08       PUSH [ARG.1]                    ; hOwner
00401126  . E8 40000000   CALL <JMP.&USER32.MessageBoxA>  ; MessageBoxA
0040112B  . EB 00         JMP SHORT 07.0040112D
0040112D  $ 6A 00         PUSH 0                          ; Result = 0
0040112F  . FF75 08       PUSH [ARG.1]                    ; hWnd
00401132  . E8 22000000   CALL <JMP.&USER32.EndDialog>    ; EndDialog
00401137  . C9            LEAVE
00401138  . C2 1000       RETN 10
0040113B  $ FF25 6C304000 JMP [<&KERNEL32.GetModuleHandleA>]  ; kernel32.GetModuleHandleA
EAX=00000001
```

보면 CMP에서 부면 EAX값하고 0 비교하는거보니 틀렸다고 인증될텐데,

위에 004010F2주소에 string1을 보면 L2C-5781EqfgEngn4562-ABEX이걸 입력해야 정답인것을 알수 있으니 그냥 넘어가자 ㅋ.

인증해보니 틀렷다고 해서 머지햇는데..

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

문제좀 잘읽자 zz..

EgfgEngn 이거겟네.