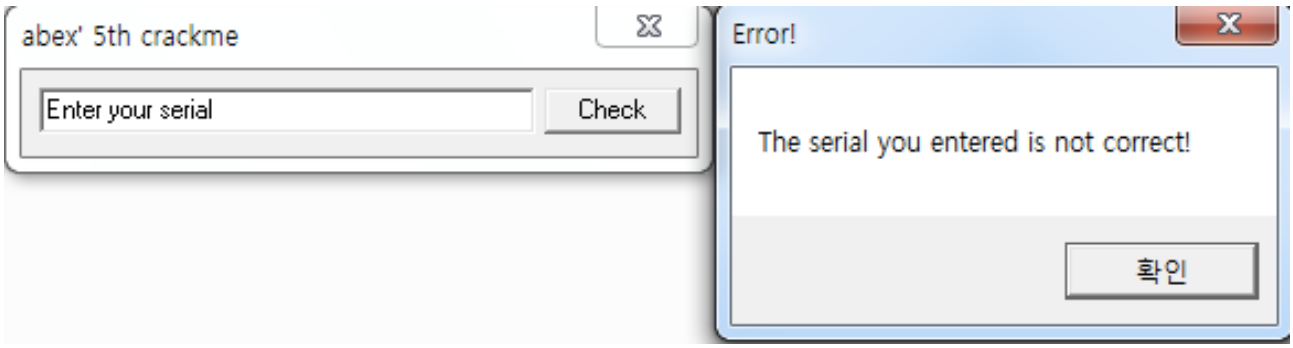
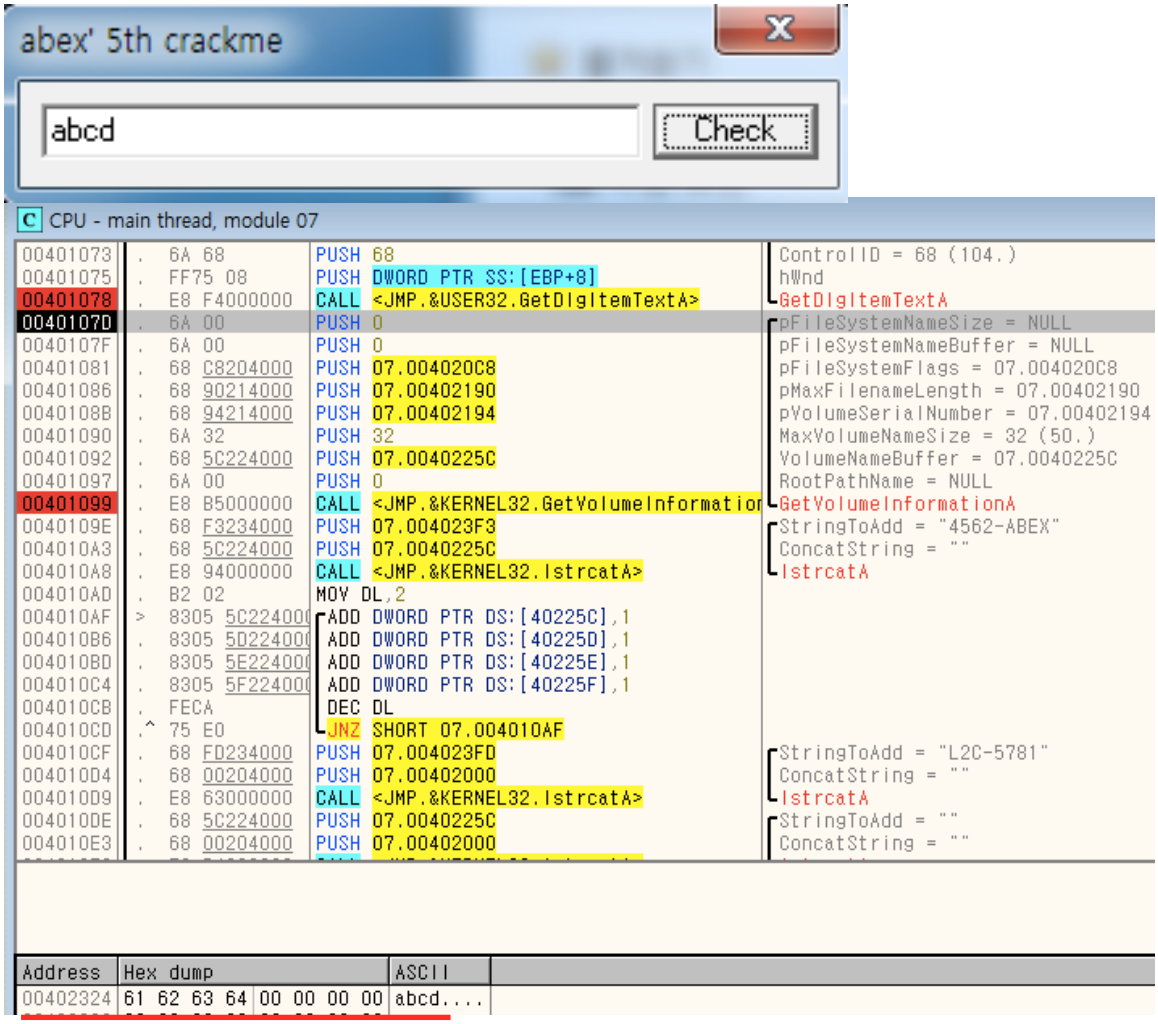


처음 실행화면입니다. 그냥 체크버튼을 눌러보니 에러메세지가 발생합니다.

올바른 시리얼을 찾기 위해서 프로그램 분석을 해보도록 하겠습니다.



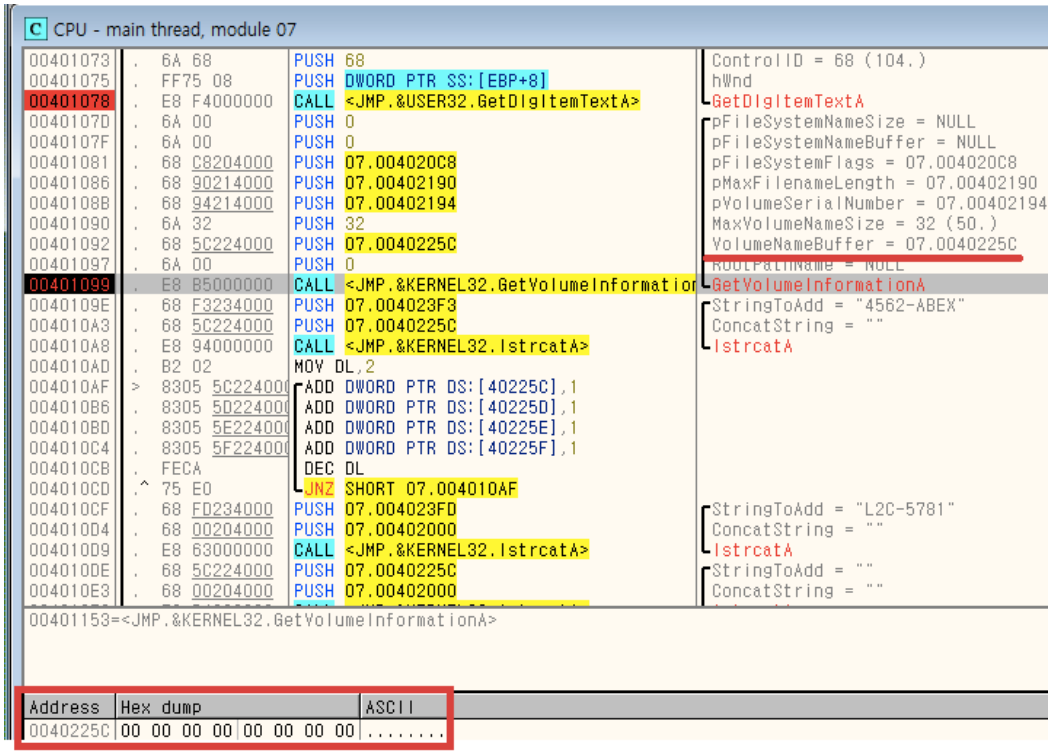
보다 확실하게 하기 위해 입력값을 abcd로 입력하도록 하겠습니다.

break point가 설정 된 00401078 번지를 보면 GetDigItemTextA라는 함수를 호출합니다.

이는 프로그램에서 텍스트박스에 입력한 값을 가져오는 함수입니다.

호출 뒤에 밑에 보시면 abcd가 들어간 것을 볼 수 있습니다.

이 함수를 통해 입력 값을 가져오는 것을 확인했습니다.

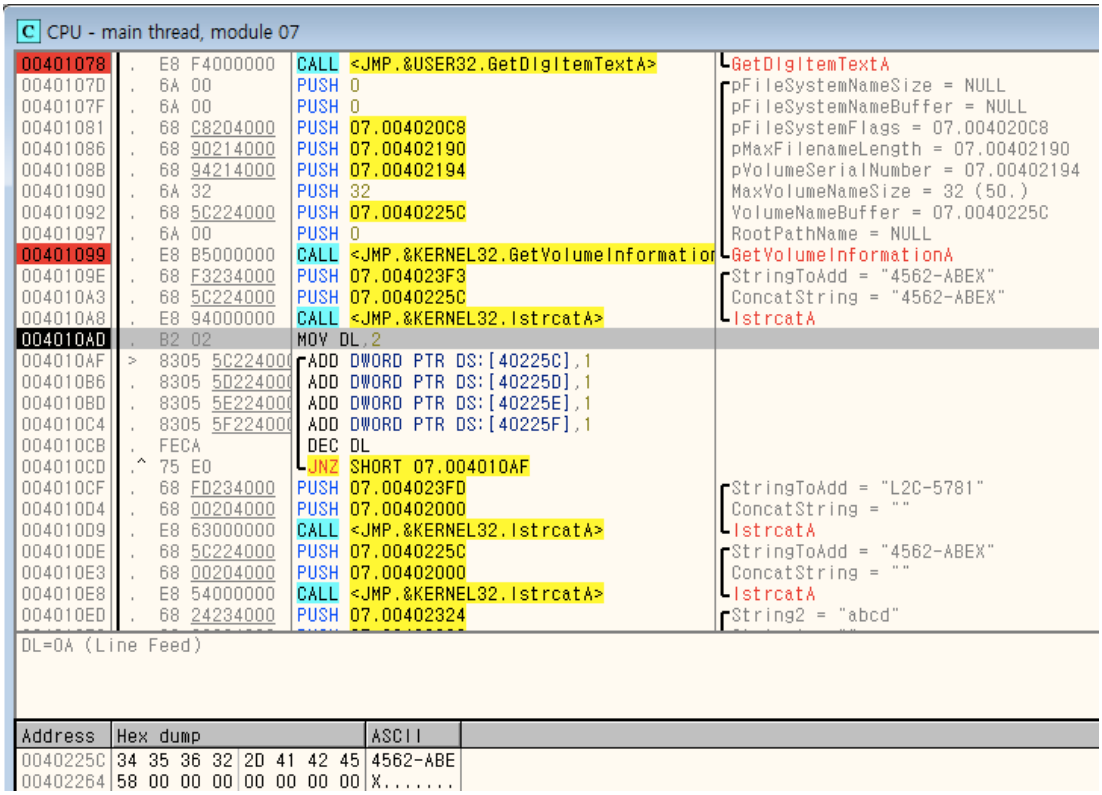


두 번째 break point인 GetVolumeInformation 함수는 드라이버의 정보를 가져올 때 사용하는 함수입니다.

밑줄과 박스로 표시한 것은 드라이버의 이름을 얻어오는 버퍼입니다.

그리고 밑줄 바로 밑에 RootPathName=NULL이라고 되어 있는데 이 값이 NULL이면 C:\를 가리키게 됩니다.

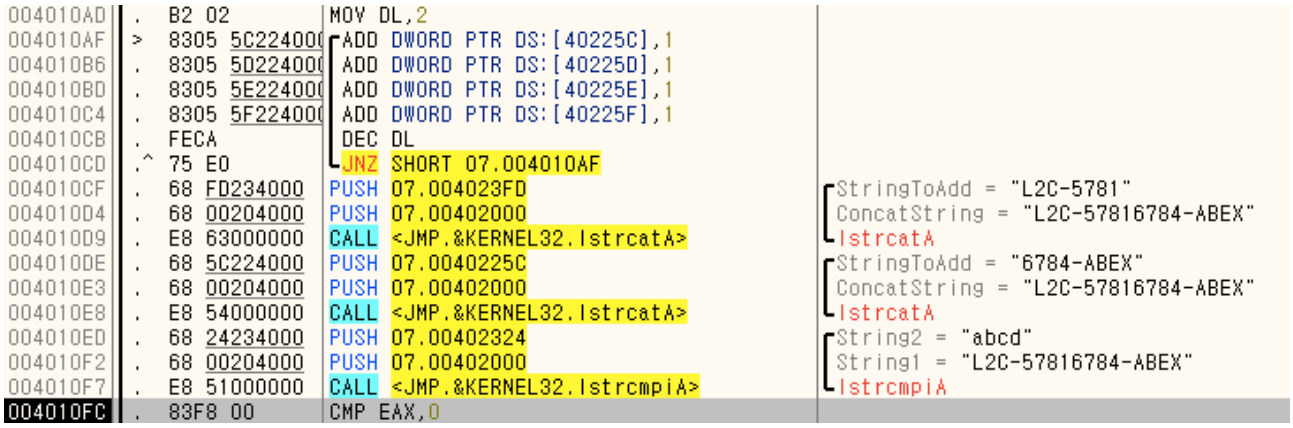
지금 빈 칸인 이유는 로컬 디스크라는 이름이 비어있는 이름을 뜻하기 때문입니다.



현재 라인을 보시면 위에 두 변수를 가지고 strcat 함수를 호출하는 것을 알 수 있습니다.

strcat 함수는 문자열을 붙히는 함수인데 인자값으로 4562-ABEX와 07.0040225C 값을 가지고 옵니다.

07.0040225C는 드라이버의 이름인 빈 값이므로 strcat 함수를 지나도 4562-ABEX라는 값이 됩니다.

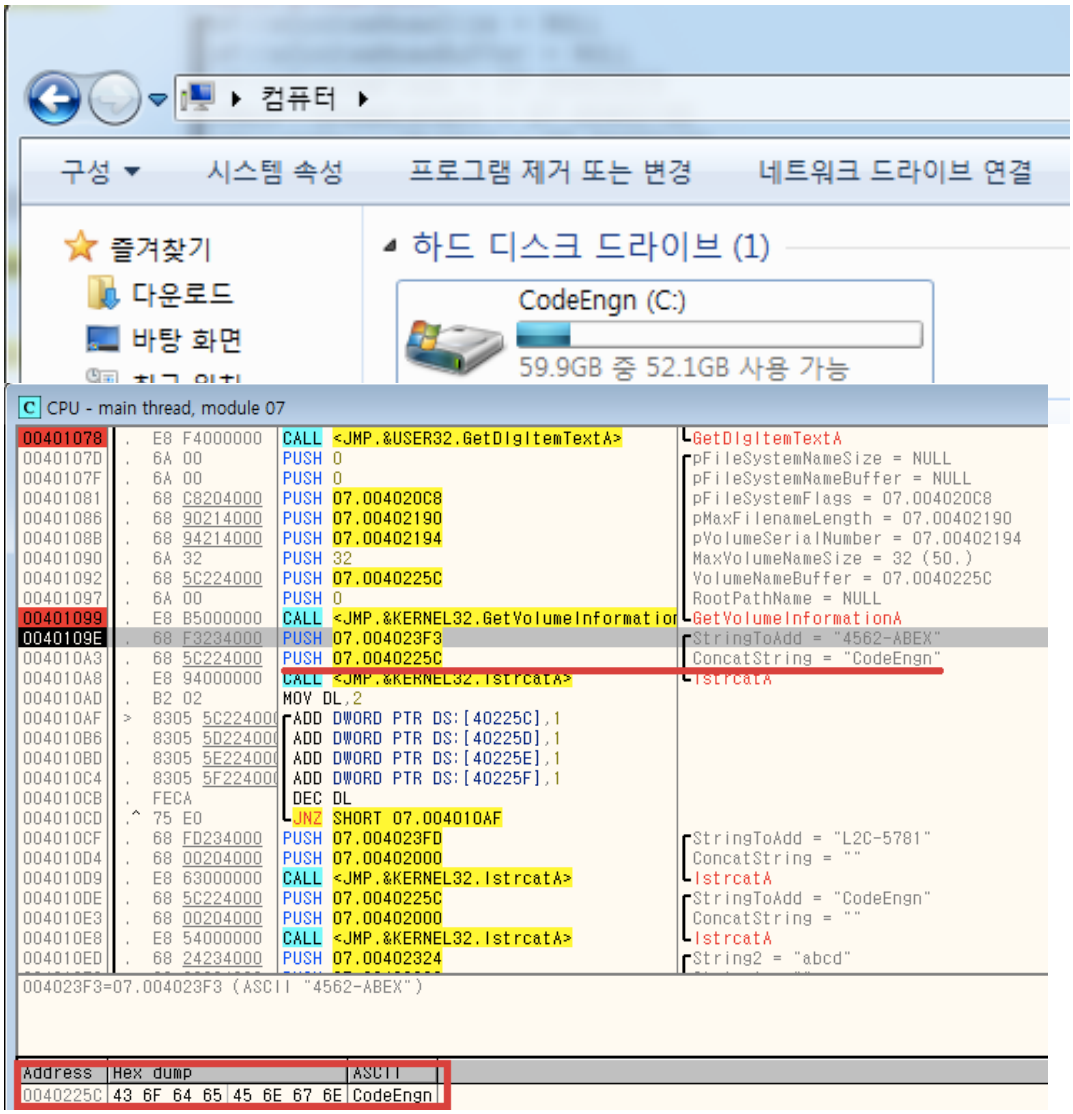


DL에 2를 넣고 두 번 반복하는데 0040225C의 값 앞의 4자리 각각 1씩 더합니다.

4562 + 1 1 1 1 = 6784-ABEX 값이 되고 그 후에 L2C-5781 + 연산한 값을 한 것이 시리얼 값입니다.

```
00401FC   .  83F8 00      CMP EAX,0
00401FF   .v 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 correct!"
0040110D  .  FF75 08      PUSH DWORD PTR SS:[EBP+8]               ; 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 DWORD PTR SS:[EBP+8]               ; hOwner
00401126  .  E8 40000000  CALL <JMP.&USER32.MessageBoxA>          ; MessageBoxA
0040112B  .v EB 00        JMP SHORT 07.0040112D
0040112D  $  6A 00        PUSH 0                                  ; Result = 0
0040112F  .  FF75 08      PUSH DWORD PTR SS:[EBP+8]               ; hWnd
00401132  .  E8 22000000  CALL <JMP.&USER32.EndDialog>            ; EndDialog
00401137  .  C9           LEAVE
00401138  L. C2 1000      RETN 10
```

L2C-57816784-ABEX와 abcd를 비교하고 그 결과를 메세지박스로 출력해줍니다.



아까 빈칸이었던 0040225C 번지에 CodeEngn값이 들어갔습니다.

이를 이용해서 연산하게 되면 원하는 결과를 얻을 수 있습니다.