Basic 01 문제 화면

Challenges : Basic 01

Author: abex

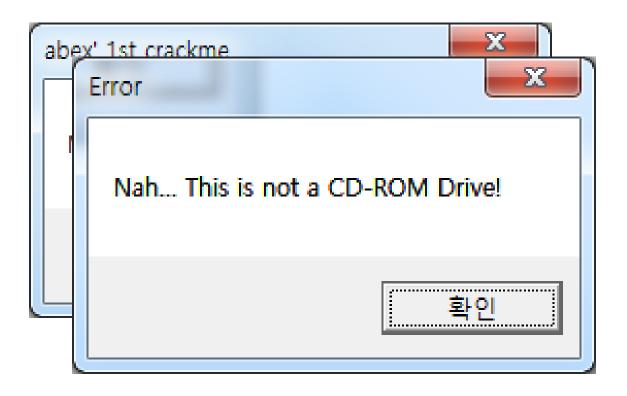
Korean:

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

English:

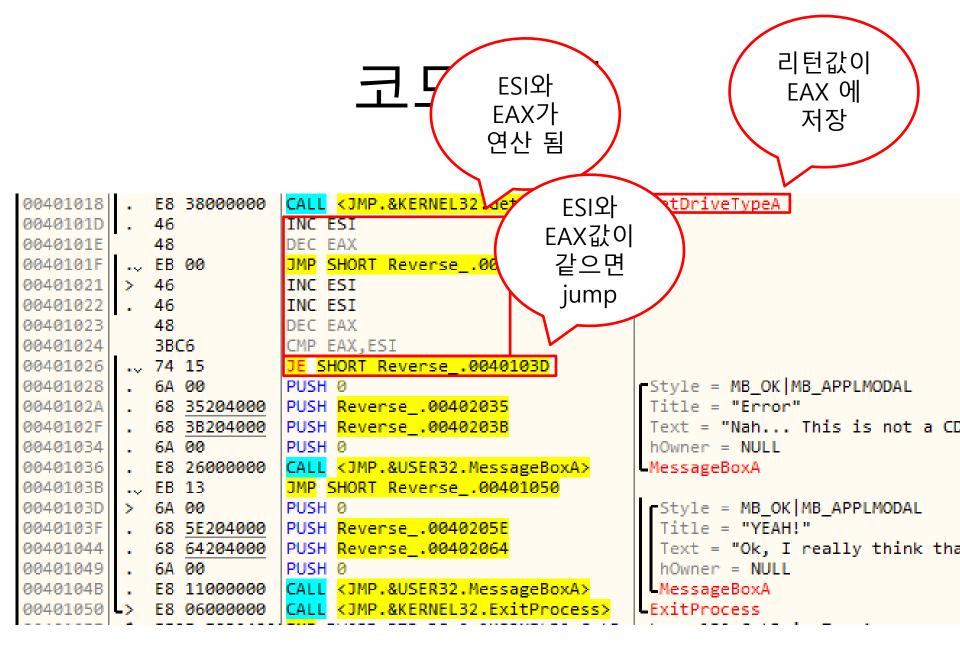
What value must GetDriveTypeA return in order to make the computer recognize the HDD as a CD-Rom

문제 실행 시



문제 코드

```
00401000 rs
            6A 00
                         PUSH 0
                                                            rStyle = MB OK MB APPLMODAL
          . 68 00204000
                         PUSH Reverse .00402000
                                                             Title = "abex' 1st crackme"
00401002
          . 68 12204000
                         PUSH Reverse .00402012
                                                            Text = "Make me think your HD is a CD-Rom."
00401007
         . 6A 00
                                                             hOwner = NULL
0040100C
                          PUSH 0
0040100E . E8 4E000000
                         CALL <JMP.&USER32.MessageBoxA>
                                                            -MessageBoxA
          . 68 94204000
                         PUSH Reverse .00402094
                                                            rRootPathName = "c:\"
00401013
00401018 . E8 38000000
                         CALL <JMP.&KERNEL32.GetDriveTypeA> LGetDriveTypeA
0040101D . 46
                         INC ESI
0040101E
            48
                         DEC EAX
          .. EB 00
0040101F
                         JMP SHORT Reverse .00401021
00401021
         > 46
                         INC ESI
00401022 . 46
                         INC EST
                         DEC EAX
00401023
            48
                         CMP EAX, ESI
00401024
            3BC6
                         JE SHORT Reverse .0040103D
00401026 ... 74 15
00401028 . 6A 00
                                                            Style = MB_OK MB_APPLMODAL
                         PUSH 0
                         PUSH Reverse .00402035
                                                             Title = "Error"
0040102A | . 68 35204000
                         PUSH Reverse .0040203B
                                                             Text = "Nah... This is not a CD-ROM Drive!"
0040102F . 68 3B204000
                                                            hOwner = NULL
00401034 . 6A 00
                         PUSH 0
00401036 . E8 26000000
                         CALL <JMP.&USER32.MessageBoxA>
                                                            -MessageBoxA
0040103B ... EB 13
                         JMP SHORT Reverse .00401050
0040103D|| > 6A 00
                         PUSH 0
                                                             rStyle = MB OK MB APPLMODAL
0040103F . 68 5E204000
                                                              Title = "YEAH!"
                         PUSH Reverse .0040205E
00401044 . 68 64204000
                         PUSH Reverse .00402064
                                                              Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049 | . 6A 00
                         PUSH 0
                                                              hOwner = NULL
                         CALL <JMP.&USER32.MessageBoxA>
                                                             -MessageBoxA
0040104B . E8 11000000
00401050 L> E8 06000000
                         CALL <JMP.&KERNEL32.ExitProcess>
                                                            -ExitProcess
```





```
00401018
                         CALL <JMP.&KERNEL32. etDriveTypeA> LGetDriveTypeA
            E8 38000000
0040101D .
            46
                         INC ESI
0040101E
            48
                         DEC EAX
0040101F ... EB 00
                         JMP SHORT Reverse .00401021
00401021 > 46
                         INC EST
00401022 . 46
                         INC ESI
                         DEC EAX
00401023
          48
00401024
          3BC6
                         CMP EAX,ESI
                         JE SHORT Reverse .0040103D
00401026 ... 74 15
00401028 . 6A 00
                         PUSH 0
                                                           Style = MB OK MB APPLMODAL
                                                            Title = "Error"
0040102A . 68 35204000
                        PUSH Reverse .00402035
0040102F|| . 68 3B204000
                        PUSH Reverse .0040203B
                                                            Text = "Nah... This is not a CD
00401034 . 6A 00
                         PUSH 0
                                                            hOwner = NULL
00401036 .
            E8 26000000
                        CALL <JMP.&USER32.MessageBoxA>
                                                            -MessageBoxA
0040103B . EB 13
                         JMP SHORT Reverse .00401050
                                                            rStyle = MB OK MB APPLMODAL
0040103D| > 6A 00
                         PUSH 0
0040103F | . 68 5E204000
                        PUSH Reverse .0040205E
                                                             Title = "YEAH!"
00401044 . 68 64204000
                        PUSH Reverse .00402064
                                                             Text = "Ok, I really think that
00401049 . 6A 00
                         PUSH 0
                                                             hOwner = NULL
                         CALL <JMP.&USER32.MessageBoxA>
0040104B .
            E8 11000000
                                                            MessageBoxA
                                                            FxitProcess
00401050 ->
            E8 06000000
                         CALL <JMP.&KERNEL32.ExitProcess>
```

문제 풀이

```
00401000 r$ 6A 00
                         PUSH 0
                                                               Registers (FPU)
00401002
         . 68 00204000 PUSH Reverse .00402000
                                                               EAX 00000003
                         PUSH Reverse .00402012
00401007 . 68 12204000
                                                               ECX 77D338AA ntdll.77D338AA
0040100C . 6A 00
                         PUSH 0
                                                               EDX 0049B3F0
0040100E . E8 4E000000
                        CALL <JMP.&USER32.MessageBoxA>
                                                               EBX 7EFDE000
00401013 . 68 94204000
                         PUSH Reverse_.00402094
                                                               ESP 0018FF8C ASCII "j3?"
00401018 . E8 38000000
                         CALL <JMP.&KERNEL32.GetDriveTypeA>
                                                               EBP 0018FF94
0040101D
         . 46
                         INC ESI
                                                               ESI 00000000
0040101E
            48
                         DEC EAX
                                                               EDI 00000000
0040101F ... EB 00
                         JMP SHORT Reverse .00401021
```

GetDriveTypeA의 리턴값(EAX에 저장되는 값)은 3

문제 풀이

```
00401002
            68 00204000
                          PUSH Reverse .00402000
                                                                 EAX 00000001
00401007 . 68 12204000
                          PUSH Reverse .00402012
                                                                 FCX 77D338AA
0040100C . 6A 00
                          PUSH 0
                                                                 FDX 0049B3F0
                          CALL <JMP.&USER32.MessageBoxA>
0040100E|| . E8 4E000000
                                                                 FBX 7FFDF000
00401013 . 68 94204000
                          PUSH Reverse .00402094
                                                                 ESP 0018FF8C
00401018 . E8 38000000
                          CALL <JMP.&KERNEL32.GetDriveTypeA>
                                                                 EBP 0018FF94
0040101D . 46
                          TNC FST
                                                                 ESI 00000003
0040101E
         48
                          DEC EAX
                                                                 FDT 00000000
0040101F|| ... EB 00
                          JMP SHORT Reverse .00401021
                                                                 EIP 00401024
00401021 > 46
                          INC ESI
                          TNC FST
00401022 . 46
                                                                      ES 002B
                                                                 \subset \Theta
00401023
         48
                          DEC FAX
                                                                      CS 0023
             3BC6
                          CMP EAX.ESI
```

CMP EAX, ESI가 일어나기 전, 연산과정 이후

- EAX: 1(**3->1**)

- ESI: 3

EAX가 3이 되어야 하므로, GetDriveTypeA의 리턴값은 5가 되어야 한다.