Basic 01 문제 화면

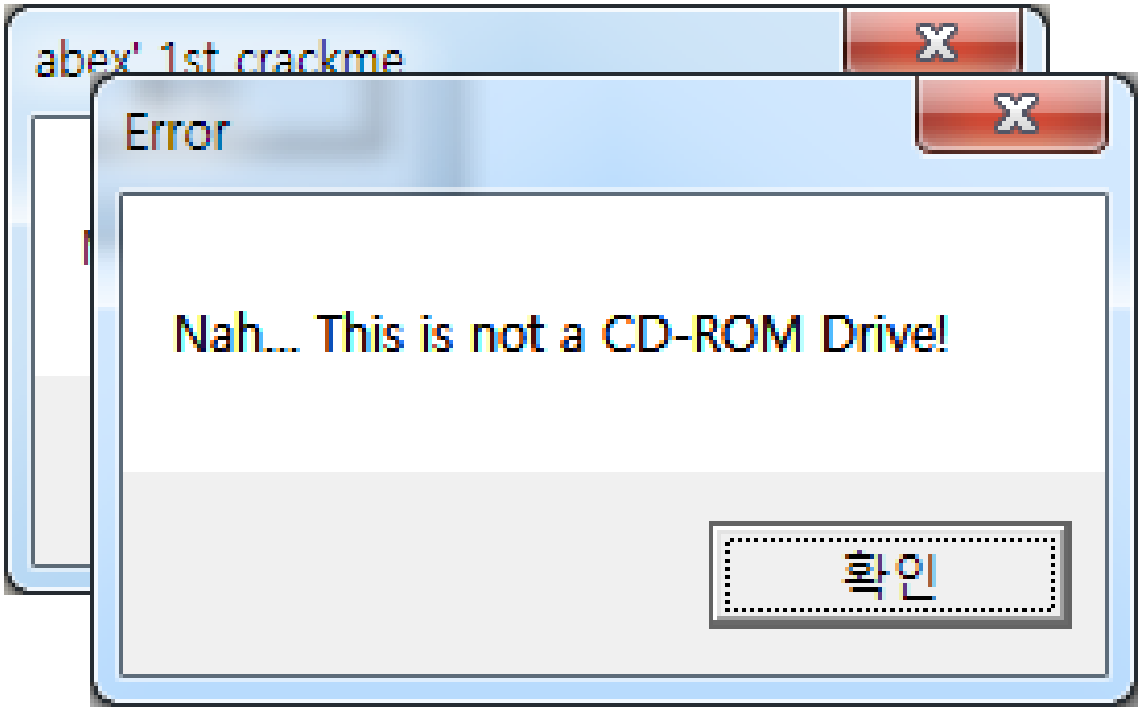
Challenges : Basic 01

Author : abex

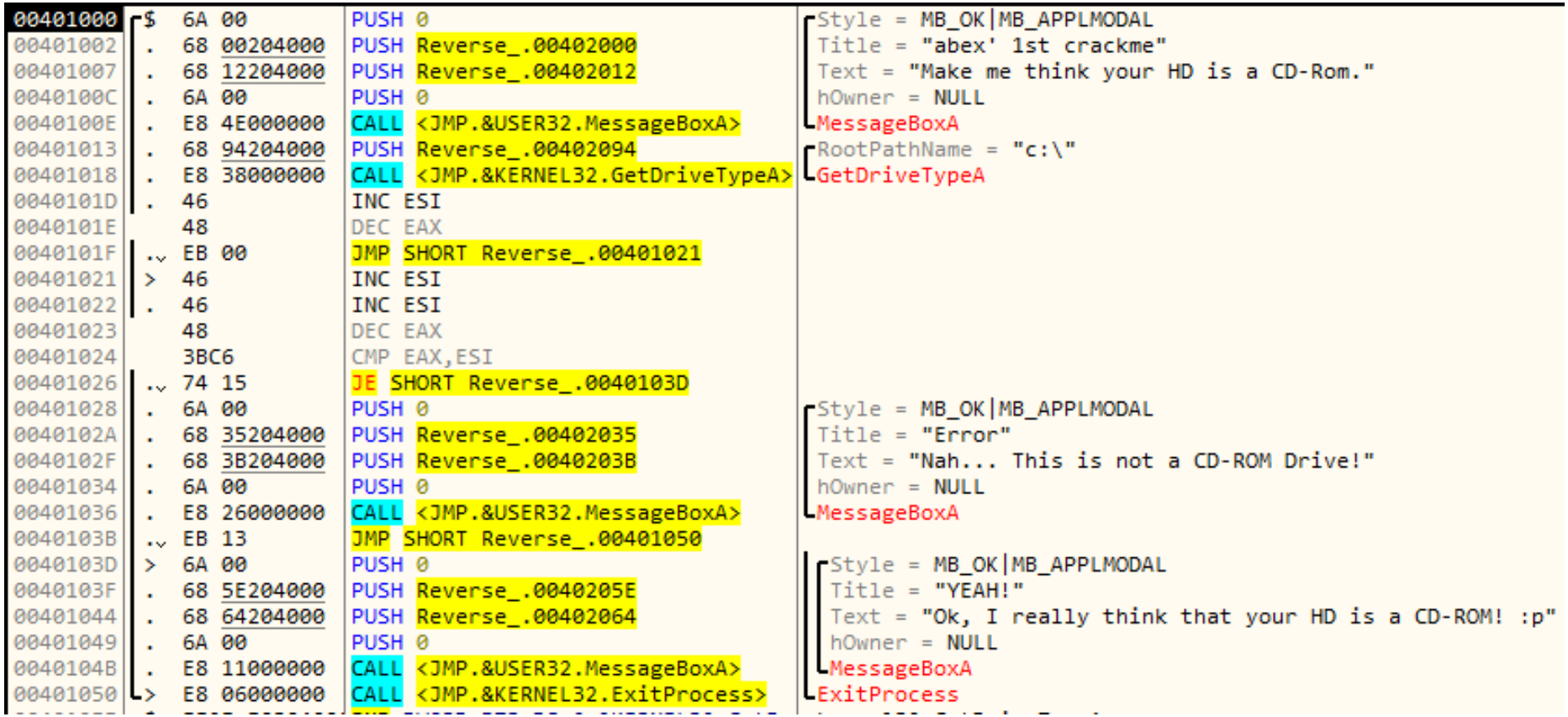
Korean :
HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

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

문제 실행 시

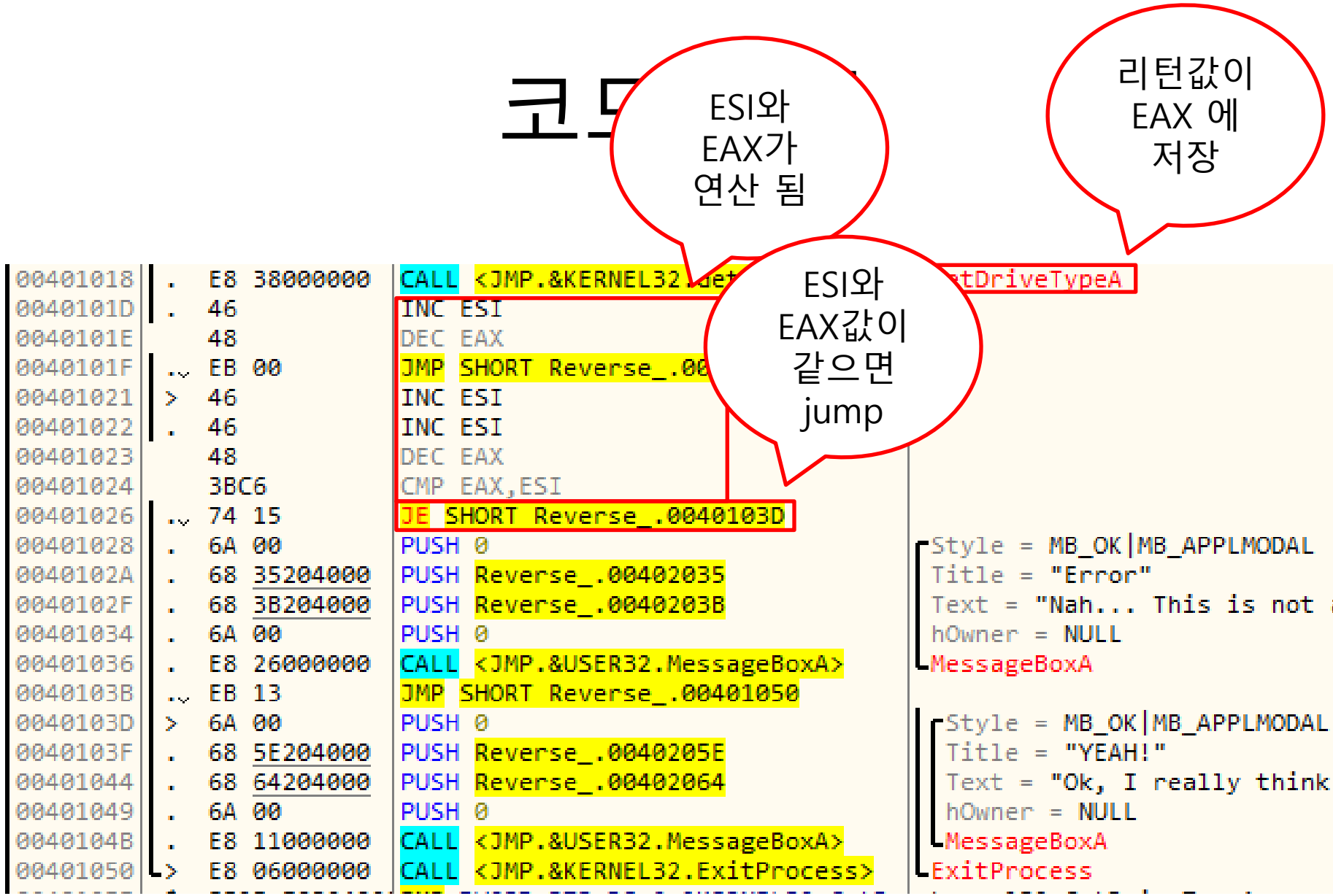


문제 코드

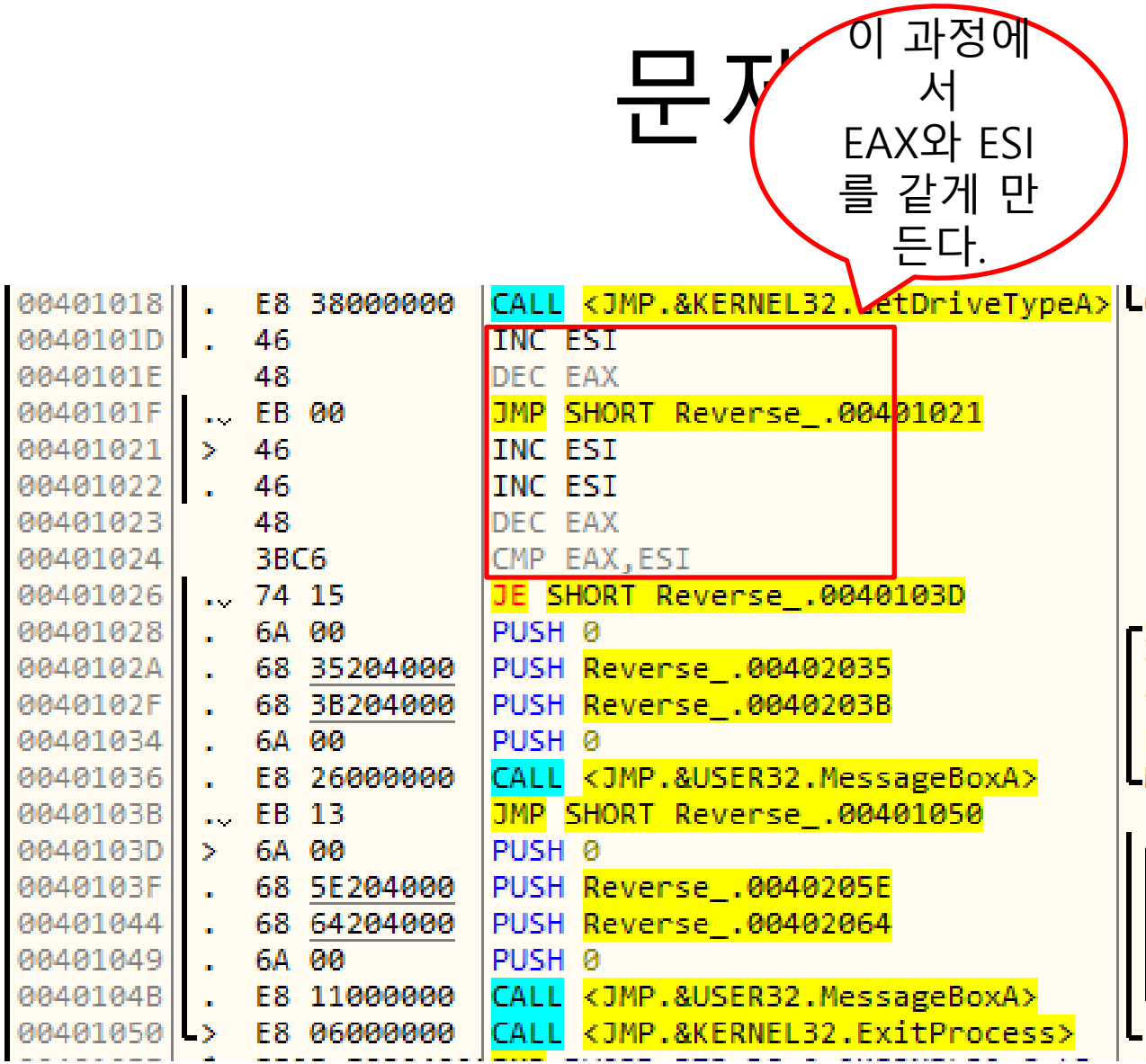


```
00401000 $  6A 00         PUSH 0                          Style = MB_OK|MB_APPLMODAL
00401002 .  68 00204000   PUSH Reverse_.00402000         Title = "abex' 1st crackme"
00401007 .  68 12204000   PUSH Reverse_.00402012         Text = "Make me think your HD is a CD-Rom."
0040100C .  6A 00        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

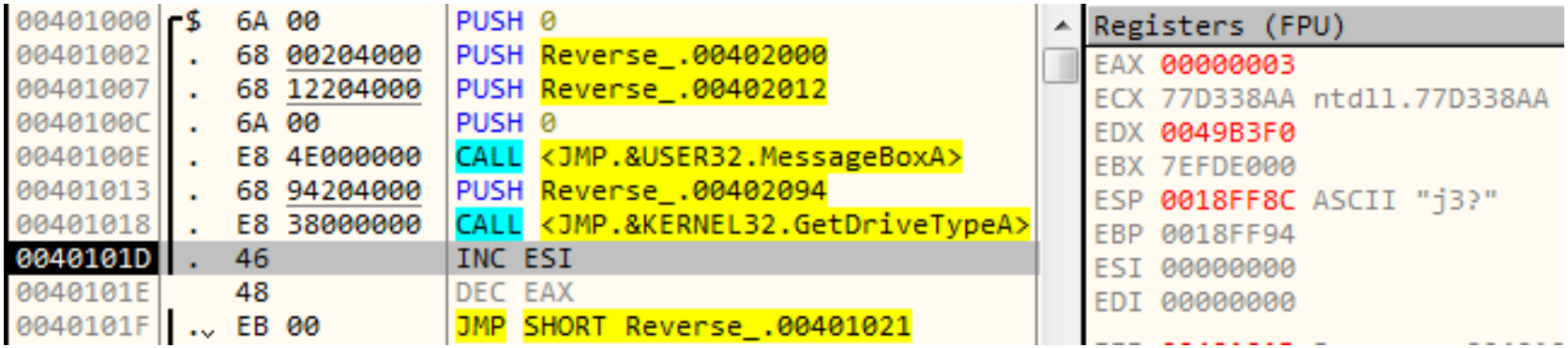
코드


ESI와
EAX가
연산 됨
ESI와
EAX값이
같으면
jump
리턴값이
EAX 에
저장
00401018 . E8 38000000 CALL <JMP.&KERNEL32.Get
tDriveTypeA
0040101D . 46 INC ESI
0040101E 48 DEC EAX
0040101F .v EB 00 JMP SHORT Reverse_.00
00401021 > 46 INC ESI
00401022 . 46 INC ESI
00401023 48 DEC EAX
00401024 3BC6 CMP EAX,ESI
00401026 .v 74 15 JE SHORT Reverse_.0040103D
00401028 . 6A 00 PUSH 0
0040102A . 68 35204000 PUSH Reverse_.00402035
0040102F . 68 3B204000 PUSH Reverse_.0040203B
00401034 . 6A 00 PUSH 0
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>
0040103B .v EB 13 JMP SHORT Reverse_.00401050
0040103D > 6A 00 PUSH 0
0040103F . 68 5E204000 PUSH Reverse_.0040205E
00401044 . 68 64204000 PUSH Reverse_.00402064
00401049 . 6A 00 PUSH 0
0040104B . E8 11000000 CALL <JMP.&USER32.MessageBoxA>
00401050 > E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>
Style = MB_OK|MB_APPLMODAL
Title = "Error"
Text = "Nah... This is not a CD
hOwner = NULL
MessageBoxA
Style = MB_OK|MB_APPLMODAL
Title = "YEAH!"
Text = "Ok, I really think tha
hOwner = NULL
MessageBoxA
ExitProcess

문제

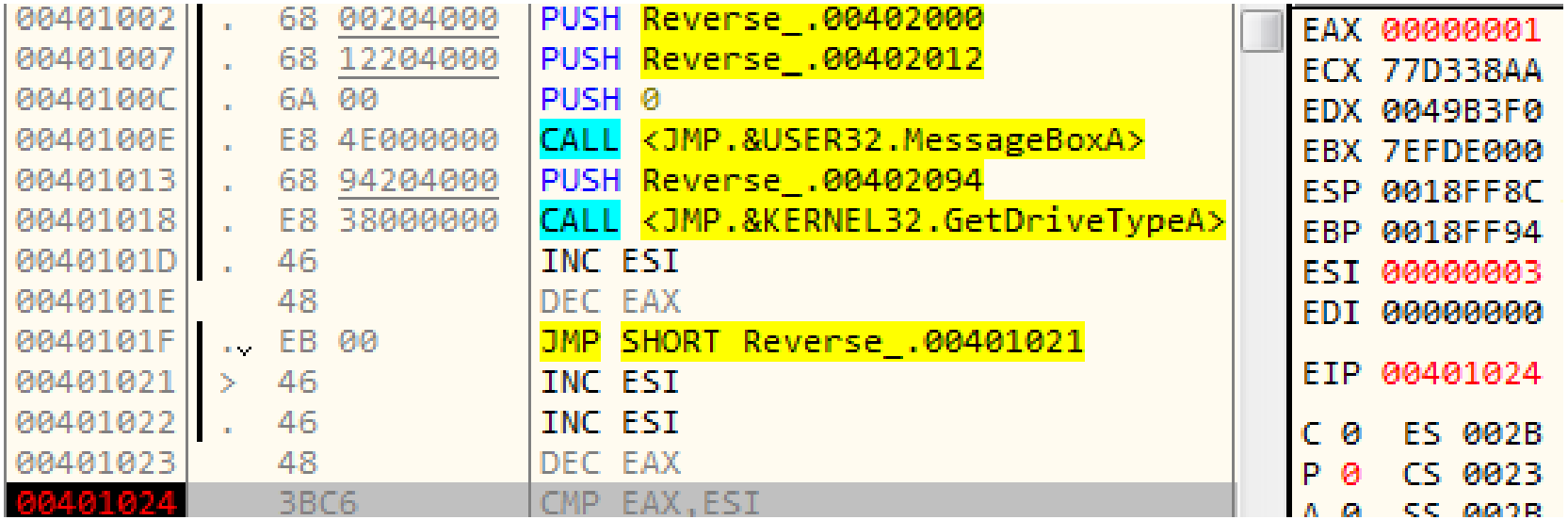

이 과정에서 EAX와 ESI를 같게 만든다.
00401018 . E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>
GetDriveTypeA
0040101D . 46 INC ESI
0040101E 48 DEC EAX
0040101F .v EB 00 JMP SHORT Reverse_.00401021
00401021 > 46 INC ESI
00401022 . 46 INC ESI
00401023 48 DEC EAX
00401024 3BC6 CMP EAX,ESI
00401026 .v 74 15 JE SHORT Reverse_.0040103D
00401028 . 6A 00 PUSH 0
Style = MB_OK|MB_APPLMODAL
0040102A . 68 35204000 PUSH Reverse_.00402035
Title = "Error"
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 .v EB 13 JMP SHORT Reverse_.00401050
0040103D > 6A 00 PUSH 0
Style = MB_OK|MB_APPLMODAL
0040103F . 68 5E204000 PUSH Reverse_.0040205E
Title = "YEAH!"
00401044 . 68 64204000 PUSH Reverse_.00402064
Text = "Ok, I really think tha
00401049 . 6A 00 PUSH 0
hOwner = NULL
0040104B . E8 11000000 CALL <JMP.&USER32.MessageBoxA>
MessageBoxA
00401050 > E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>
ExitProcess

문제 풀이



GetDriveTypeA의 리턴값(EAX에 저장되는 값)은 3

문제 풀이



CMP EAX, ESI가 일어나기 전, 연산과정 이후
- EAX: 1(**3->1**)
- ESI: 3

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