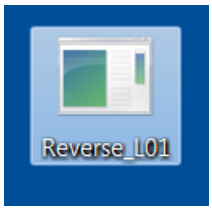
Basic REC level 1 풀이

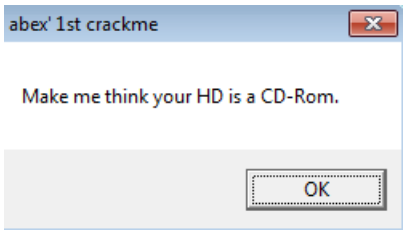
Turtledove

rlgus0626@gmail.com



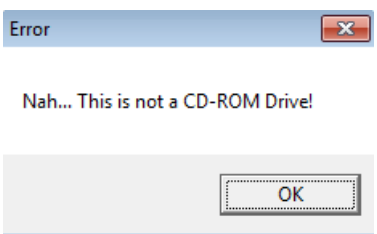
Reverse_L01 이라는 이름의 파일입니다.

한번 실행해보겠습니다.



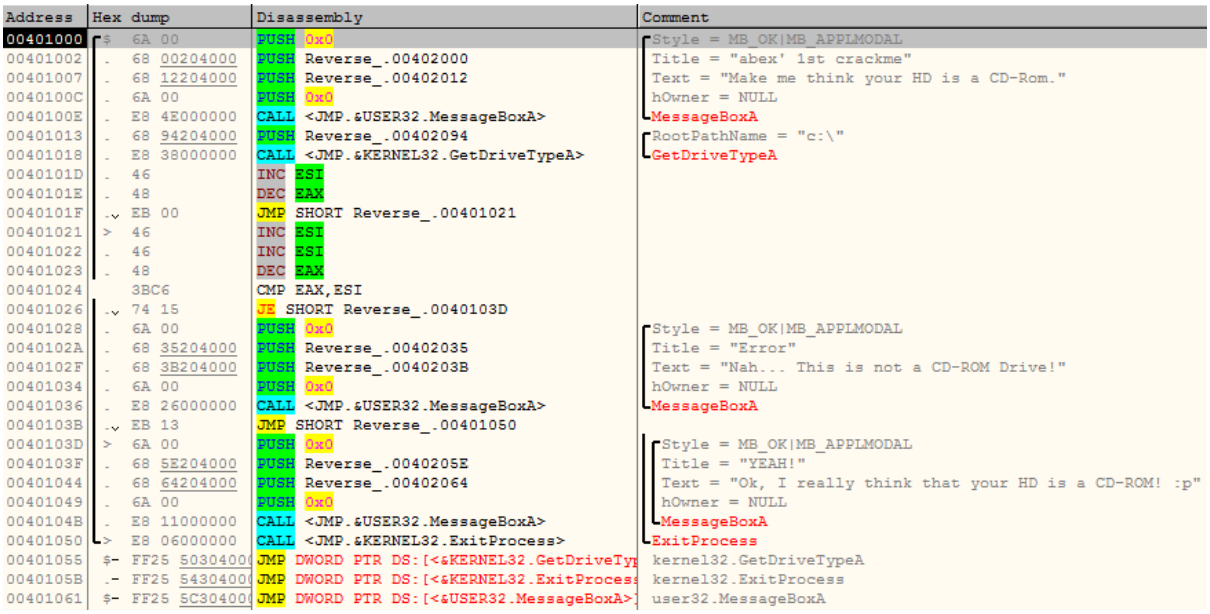
"너의 하드를 나의 CD-Rom으로 생각하게 만들어라"라는 문구가 나오네요.

OK를 눌러보면,



"어쨌든... 이것은 CD-Rom이 아니다!"라고 뜨네요.

파일을 올리디버거로 열어보겠습니다.



```
Address   Hex dump     Disassembly                          Comment
00401000  $  6A 00     PUSH 0x0                             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 0x0                             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 0x0                             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 0x0                             hOwner = NULL
00401036  .  E8 26000000 CALL <JMP.&USER32.MessageBoxA>     MessageBoxA
0040103B  .v EB 13     JMP SHORT Reverse_.00401050
0040103D  >  6A 00     PUSH 0x0                             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 0x0                             hOwner = NULL
0040104B  .  E8 11000000 CALL <JMP.&USER32.MessageBoxA>     MessageBoxA
00401050  L> E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>   ExitProcess
00401055  $- FF25 5030400( JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy kernel32.GetDriveTypeA
0040105B  .- FF25 5430400( JMP DWORD PTR DS:[<&KERNEL32.ExitProces kernel32.ExitProcess
00401061  $- FF25 5C30400( JMP DWORD PTR DS:[<&USER32.MessageBoxA> user32.MessageBoxA
```

먼저 MessageBoxA 함수부터 살펴보겠습니다. MessageBoxA 함수란 이름 그대로 메시지 박스를 띄워주는 함수입니다. 내용을 보면 아까 파일을 실행했을 때 나왔던 문구들이 보이네요.

그런데 아까 확인하지 못한 문구가 하나 있네요.

바로 "OK, I really think your HD is a CD-ROM! :p"라는 문구입니다.

드라이브가 CD-ROM일 때 나타나는 성공 문구 인 것 같네요.

우리는 HDD를 CD-ROM으로 인식시키기 위해서 GetDriveTypeA의 리턴값을 구해야 하므로 성공 문자열이 뜨게 해야한다는 개념이네요.

먼저 GetDriveTypeA의 리턴값을 보기 위해서 GetDriveTypeA 함수까지만 실행해보겠습니다.

```
00401018  .  E8 38000000   CALL <JMP.&KERNEL32.GetDriveTypeA>   GetDriveTypeA
0040101D  .  46            INC ESI                              Reverse_.<Modu
```

함수가 호출되고 종료되었습니다. 이제 레지스터창에서 리턴값을 확인해보겠습니다.

```
EAX 00000003
```

EAX 레지스터는 리턴값을 담는 레지스터입니다.

그러므로 GetDriveTypeA의 리턴값은 3입니다.

```
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
```

계속 실행하다보면 EAX는 2번 감소하고, ESI는 3번 증가합니다.

그래서 비교문까지 오게되면 EAX는 1, ESI는 3이 됩니다.

EAX와 ESI가 다르므로 ZeroFlag의 값이 0이 되어 JE 명령문에서 점프를 하지않고 실행 되어 실패 문구를 띄우므로 우리는 EAX와 ESI의 값을 맞춰줘야 합니다.

그러면 EAX가 2가 더 커야 하므로 우리는 GetDriveTypeA의 리턴값인 EAX를 +2 시켜주어 5로 만들어야합니다.

```
EAX 00000005
```

더블클릭해서 5로 수정해주고 실행을 해보면

```
EAX 00000003
ECX 77636570
EDX 00282AE8
EBX 7FFDD000
ESP 0012FF8C
EBP 0012FF94
ESI 00000003
EDI 00000000
```

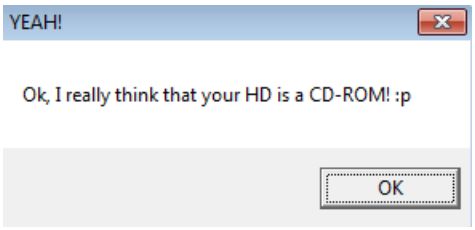
EAX와 ESI의 값의 각각 3이 되어 일치가 됩니다.

```
00401026  .v 74 15        JE SHORT Reverse_.0040103D
00401028  .  6A 00        PUSH 0x0                    ; 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
00401034  .  6A 00        PUSH 0x0                    ; hOwner = NULL
00401036  .  E8 26000000  CALL <JMP.&USER32.MessageBoxA>  ; MessageBoxA
0040103B  .v EB 13        JMP SHORT Reverse_.00401050
0040103D  >  6A 00        PUSH 0x0                    ; Style = MB_OK|MB_APPLMODAL
```

EAX와 ESI의 값이 일치하므로 JE문에서 점프를 하여 0040103D로 오게 됩니다.

```
00401026  .v 74 15        JE SHORT Reverse_.0040103D
00401028  .  6A 00        PUSH 0x0                    ; 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 0x0                    ; hOwner = NULL
00401036  .  E8 26000000  CALL <JMP.&USER32.MessageBoxA>  ; MessageBoxA
0040103B  .v EB 13        JMP SHORT Reverse_.00401050
0040103D  >  6A 00        PUSH 0x0                    ; 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 0x0                    ; hOwner = NULL
0040104B  .  E8 11000000  CALL <JMP.&USER32.MessageBoxA>  ; MessageBoxA
00401050  >  E8 06000000  CALL <JMP.&KERNEL32.ExitProcess>  ; ExitProcess
```

계속 실행시켜주다 보면 성공 문구를 띄우게 됩니다.



그러므로 GetDriveTypeA의 리턴값은 5가 되어야 합니다.