Basic1

2018년 4월 8일 일요일 오후 11:16

Code Engn

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

Download

우선 GetDriveTypeA 란 함수는 무엇인가?

MSDN에 접속해 알아보았다.
영어지만 우리에게 구글에서 지원해주는 번역기가 존재한다.
하지만 나는 영어 공부가 필요한 미생이라 한번 미번역으로 보자면

Determines whether a disk drive is a removable, fixed, CD-ROM, RAM disk, or network drive.

To determine whether a drive is a USB-type drive, call SetupDiGetDeviceRegistryProperty and specify the **SPDRP_REMOVAL_POLICY** property.

Syntax

```
C++

UINT WINAPI GetDriveType(
  _In_opt_ LPCTSTR lpRootPathName
);
```

Parameters

lpRootPathName [in, optional]
The root directory for the drive.

A trailing backslash is required. If this parameter is **NULL**, the function uses the root of the current directory.

Disk가 이동형(usb), 고정형, CD-ROM, RAM , 혹은 네트워크 드라이브인지 아닌지 확인이 가능한 함수인 것 같다.
단 USB타입의 드라이브인지 확인하려면 SetupDigetDeviceRegistryPropert함수를 호출하여 SPDRP_REMOVAL_POLICY를 지정해줘야 한다고 한다.

함수 호출인자로는 ipRootPathName [옵션] -> 매개 변수 type : LPCTSTR : const char *
the root directory for the drive 를 지정해 줘야 한다고 한다.
만약 매개변수가 NULL 이면 현재 디렉토리의 루트를 사용한다고 한다.
자 이제 함수의 반환 값을 알아보자.

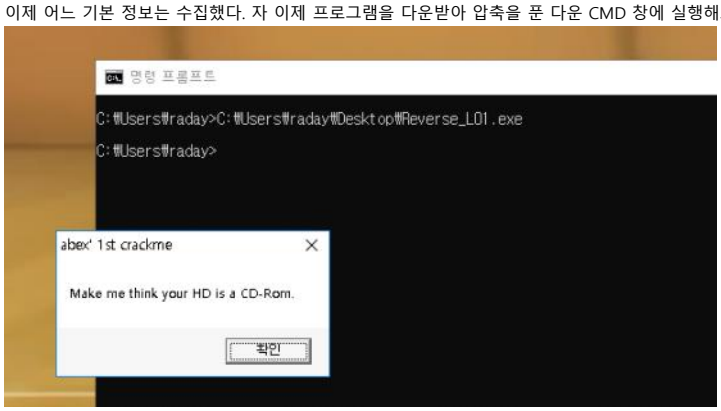
Return value

The return value specifies the type of drive, which can be one of the following values.

Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
DRIVE_FIXED 3	The drive has fixed media; for example, a hard disk drive or flash drive.
DRIVE_REMOTE 4	The drive is a remote (network) drive.
DRIVE_CDROM 5	The drive is a CD-ROM drive.
DRIVE_RAMDISK 6	The drive is a RAM disk.

보아하니 영어다.. 싫다.
하지만 대충 보니 0~6까지 값 중 하나가 출력된다고 한다.
0 : DRIVE_UNKNOWN : 드라이브 타입을 결정할 수 없다
1 : DRIVE_NO_ROOT_DIR : 루트의 경로가 무효(유효하지 않다.), 예를 들어, 지정된 경로에 마운트 된 볼륨이 없다,?
2 : DRIVE_REMOVABLE : 이 드라이브는 이동형 미디어이다. 예를 들어, 플로피 드라이브, 플래시 카드리더기, 엄지 드라이브?
3 : DRIVE_FIXED : 이 드라이브는 고정형이다. 포함, 예를 들어 ,하드 디스크, 플래시 드라이브
4 : DRVIE_REMOTE : 이 드라이브는 네트워크 드라이브이다.
5 : DRVIE_CDROM : 이 드라이브는 CD-ROM이다.
6 : DRVIE_RAMDISK : 이 드라이브는 RAM 디스크이다.

이제 어느 기본 정보는 수집했다. 자 이제 프로그램을 다운받아 압축을 푼 다운 CMD 창에 실행해보자.



Make methink yout HD is a CD-Rom 메시지 박스를 출력
MessageBox 함수를 사용
확인을 클릭하면

Nah... This is not a CD-ROM Drive! 라는 메시지 박스(MessageBox 함수 사용)를 출력
자 x32dbg 로 열어보자!

```
00401000    6A 00           push 0                                  EntryPoint
00401002    68 00 20 40 00  push reverse_l01.402000                 402000:"abex' 1st crackme"
00401007    68 12 20 40 00  push reverse_l01.402012                 402012:"Make me think your HD is a CD-Rom."
0040100C    6A 00           push 0
0040100E    E8 4E 00 00 00  call <reverse_l01.MessageBoxA>
00401013    68 94 20 40 00  push reverse_l01.402094                 402094:"c:\\"
00401018    E8 38 00 00 00  call <reverse_l01.GetDriveTypeA>
0040101D    46              inc esi                                 esi:EntryPoint
0040101E    48              dec eax
0040101F    EB 00           jmp reverse_l01.401021
00401021    46              inc esi                                 esi:EntryPoint
00401022    46              inc esi                                 esi:EntryPoint
00401023    48              dec eax
00401024    3B C6           cmp eax,esi                             esi:EntryPoint
00401026    74 15           je reverse_l01.40103D
00401028    6A 00           push 0
0040102A    68 35 20 40 00  push reverse_l01.402035                 402035:"Error"
0040102F    68 3B 20 40 00  push reverse_l01.40203B                 40203B:"Nah... This is not a CD-ROM Drive!"
00401034    6A 00           push 0
00401036    E8 26 00 00 00  call <reverse_l01.MessageBoxA>
0040103B    EB 13           jmp reverse_l01.401050
0040103D    6A 00           push 0
0040103F    68 5E 20 40 00  push reverse_l01.40205E                 40205E:"YEAH!"
00401044    68 64 20 40 00  push reverse_l01.402064                 402064:"Ok, I really think that your HD is a CD-ROM! :p"
00401049    6A 00           push 0
0040104B    E8 11 00 00 00  call <reverse_l01.MessageBoxA>
00401050    E8 06 00 00 00  call <reverse_l01.ExitProcess>
00401055    FF 25 50 30 40 00 jmp dword ptr ds:[<&GetDriveTypeA>]   GetDriveTypeA
0040105B    FF 25 54 30 40 00 jmp dword ptr ds:[<&ExitProcess>]     ExitProcess
00401061    FF 25 5C 30 40 00 jmp dword ptr ds:[<&MessageBoxA>]     MessageBoxA
00401067    00 00           add byte ptr ds:[eax],al
00401069    00 00           add byte ptr ds:[eax],al
```

실행 창으로 왔다. 자 이제 우리를 에러 문장이 보이는 messagebox 로 보내는 분기문이 어디지 체크해 보자

우선 실행 메시지를 출력한 다음 GetDriveTypeA이라는 함수의 매개인자로는 C:₩₩를 보냈다.

```
EAX   00000001
EBX   002AD000
ECX   2E5C6AE2
EDX   026FD000
EBP   0019FF94
ESP   0019FF80     &"c:\\"
ESI   00401000     <reverse_l01.EntryPoint>
EDI   00401000     <reverse_l01.EntryPoint>

EIP   00401018     reverse_l01.00401018

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

```
EAX   00000003
EBX   002AD000
ECX   2E5C6AD2
EDX   026FB100
EBP   0019FF94
ESP   0019FF84
ESI   00401000     <reverse_l01.EntryPoint>
EDI   00401000     <reverse_l01.EntryPoint>

EIP   0040101D     reverse_l01.0040101D

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

Get Drive Type 함수를 출력 후 나온 결과 값이다.

그 다음 실행 되는 것은

```
0040101D    46              inc esi                                 esi:EntryPoint
0040101E    48              dec eax
0040101F    EB 00           jmp reverse_l01.401021
00401021    46              inc esi                                 esi:EntryPoint
00401022    46              inc esi                                 esi:EntryPoint
00401023    48              dec eax
```

이 부분으로 dec eax 까지 실행 시키면

```
EAX   00000001
EBX   00395000
ECX   2FB35527
EDX   024BB200
EBP   0019FF94
ESP   0019FF84
ESI   00401003     &"abex' 1st crackme"
EDI   00401000     <reverse_l01.EntryPoint>

EIP   00401024     reverse_l01.00401024

EFLAGS   00000300
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1
```

EAX = 1

ESI = 401003

그 다음 문장!

```
00401023    48              dec eax
00401024    3B C6           cmp eax,esi
00401026    74 15           je reverse_l01.40103D
```

Cmp eax,esi

즉 eax - esi 인데

Eax 값이 더 크면 ZF 0 , CF 0

Esi 값이 더 크면 ZF 0 , CF 1

값이 두 개다 같으면 ZF 1, CF 0 이다.

Cmp를 실행 시키고 봤더니?!

JE reverse_101.40103D -> ZF가 1이라면 40103D로 점프!

하지만 현재 내 플래그들은

```
EAX   00000001
EBX   003C3000
ECX   E51851A4
EDX   025FB200
EBP   0019FF94
ESP   0019FF84
ESI   00401003     &"abex' 1st crackme"
EDI   00401000     <reverse_l01.EntryPoint>

EIP   00401026     reverse_l01.00401026

EFLAGS   00000293
ZF 0  PF 0  AF 1
OF 0  SF 1  DF 0
CF 1  TF 0  IF 1
```

ZF 0가 이므로.. 다음 코드인 401028 코드로 이동해보니.....

```
00401028    6A 00           push 0
0040102A    68 35 20 40 00  push reverse_l01.402035                 402035:"Error"
0040102F    68 3B 20 40 00  push reverse_l01.40203B                 40203B:"Nah... This is not a CD-ROM Drive!"
00401034    6A 00           push 0
00401036    E8 26 00 00 00  call <reverse_l01.MessageBoxA>
0040103B    EB 13           jmp reverse_l01.401050
```

너는 나에게 에러를 줬어 그럼 만약 ZF가 1이라면 가는 코드를 보자

```
0040103B    EB 13           jmp reverse_l01.401050
0040103D    6A 00           push 0
0040103F    68 5E 20 40 00  push reverse_l01.40205E                  40205E:"YEAH!"
00401044    68 64 20 40 00  push reverse_l01.402064                  402064:"Ok, I really think that your HD is a CD-ROM! :p"
00401049    6A 00           push 0
0040104B    E8 11 00 00 00  call <reverse_l01.MessageBoxA>
00401050    E8 06 00 00 00  call <reverse_l01.ExitProcess>
```

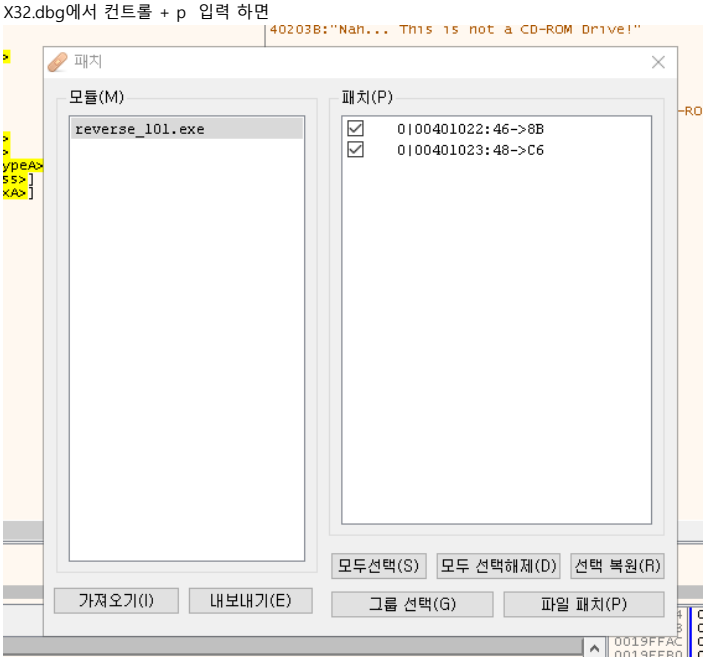
응 저쪽은 잘 되었다고 하네?
그럼 JE를 만족하게 하는 방법들을 생각해보자 가장 간단한 것은 비교문에서 EAX 값이 ESI 값과 같으면 된다.
하지만 이 방법은 지속적이지 않다. 그럼 코드를 변경해보자
그 앞에 EAX값과 ESI 값 을 1씩 더하거나 빼는 코드 중 CMP 바로 앞에
MOV EAX,ESI로 수정해 저장 후 실행해보자

```
00401022    46              inc esi
00401023    48              dec eax
```

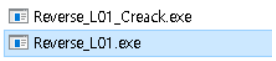
장난 칠 코드 : 그런데 왜 두 줄이 필요한가?
Mov eax,esi 로 할 경우 필요한 바이트 수는 2바이트 하지만 만약 401023 쪽을 건들려 버린다면 밑에 있는 cmp 문이 이상해 질 수 있으므로
1바이트 씩 사용하고 있는 두개의 코드를 대상으로 mov eax,esi 로 변경 해보면

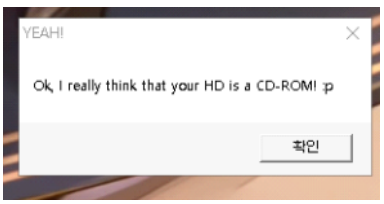
```
00401021    46              inc esi
00401022    8B C6           mov eax,esi
```

응 깔끔하게 잘 변경 되었다. 이것을 패치 해 실행 해 보자.
X32.dbg에서 컨트롤 + p 입력 하면



여기서 파일 패치 클릭 후 원하는 경로에 파일 저장 후 실행 해보자





성공입니다.
이제 코드를 복원해보죠!

```
#include<stdio.h>
#include<windows.h>
LRESULT CALLBACK WndProc(HWND,UINT,WPARAM,LPARAM);
int APIENTRY WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance
          ,LPSTR lpszCmdParam,int nCmdShow)
{
__int32 Eax=0;
__int32 Esi=0;
MessageBox(0,"Make me think your HD is a CD-ROM","abex' 1st crackme",0);
Eax=GetDriveTypeA("C:\\");
Esi++;
Eax--;
Esi++;
Esi++;
Eax--;
if(Eax==Esi)
{
MessageBox(0,"OK, I really think that your HD is a CD-ROM! :p","YHAH!",0);
}else{
```

```
MessageBox(0,"Nah...This is not a CD-ROM","Error",0);
}
return 0;
}
LRESULT CALLBACK WndProc(HWND hWnd,UINT iMessage,WPARAM wParam,LPARAM lParam)
{
    switch(iMessage) {
    case WM_DESTROY:
        PostQuitMessage(0);
        return 0;
    }
    return(DefWindowProc(hWnd,iMessage,wParam,lParam));
}
```

자 이제 코드 크랙과 코드 복원을 해보았고 이제 우리의 문제가 뭐였는지 보자.

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

Download

CD-ROM으로 인식시키기 위해서 GetDriveTypeA의 리턴값은?
FIXED으로 실험했을때 3을 리턴값으로 줬다.
EAX-2 == ESI+3
할 때 EAX-ESI=5
5가 0이 되려면 EAX값에 5가 들어와야 한다.