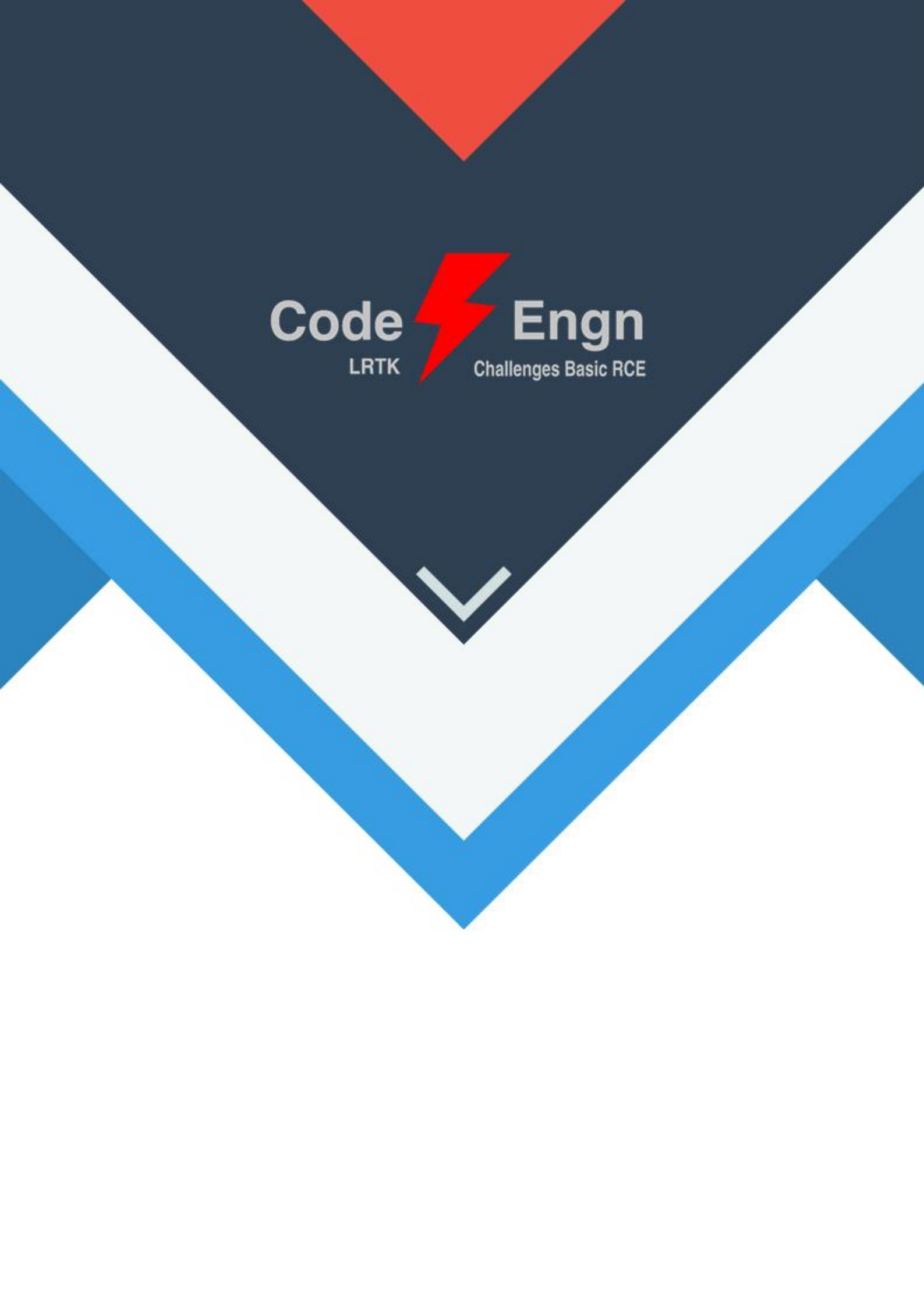
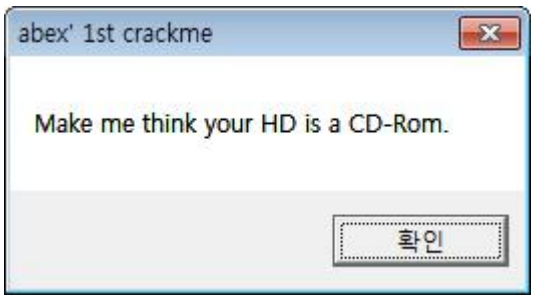

Code
Engn
LRTK
Challenges Basic RCE

01. HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

실행 화면



[첫 번째 실행 사진]

[두 번째 실행 사진]

프로그램을 실행 시키면 “HDD가 CD-ROM이라고 생각하도록 하십시오.” 라는 문구가 나온다. 그 후 확인 버튼을 클릭하면 CD-ROM 드라이브가 아니라는 문구가 나온다.

일단 IDA로 까보기 전에 생각할 수 있는 시나리오는 첫 번째 메시지 창을 띄우고 드라이브들을 확인하는 함수를 통하여 CD-ROM인지 아닌지를 검사를 하여 확인 버튼을 클릭 했을 때 각 결과에 따른 메시지 창을 띄우게 하는 시나리오를 생각 해 볼 수 있다.

```
public start
start proc near
push    0               ; uType
push    offset Caption  ; "abex' 1st crackme"
push    offset Text     ; "Make me think your HD is a CD-Rom."
push    0               ; hWnd
call    MessageBoxA
push    offset RootPathName ; "c:\\"
call    GetDriveTypeA
inc     esi
dec     eax
jmp     short $+2
```

IDA 디버거를 통하여 확인을 해봤더니 일단 “C:\\”가 Push 되고 “GetDriveTypeA” 라는 함수가 Call이 되는 것을 볼 수 있다.
Google에 “GetDriveTypeA” 함수를 검색하여 역할과 각 결과에 따른 리턴 값이 무엇인지 확

인을 했다.

GetDriveTypeA function

10/12/2018 • 2 minutes to read

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.

Return Value

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

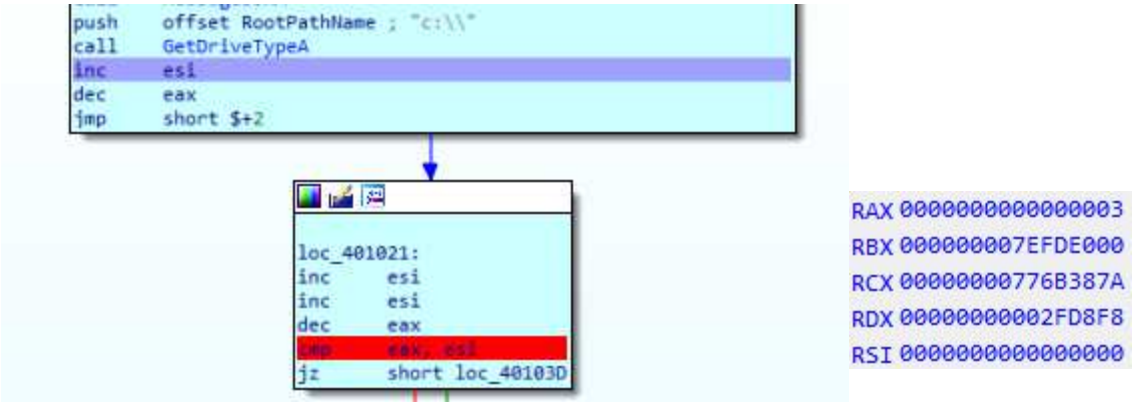
Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
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.

역할
디스크 드라이브가 이동식, 고정, CD-ROM, RAM 디스크 또는 네트워크 드라이브인지 확인합니다.
드라이브가 USB 유형의 드라이브인지 확인하려면 SetupDiGetDeviceRegistryProperty에 전화를 걸어 SPDRP_REMOVAL_POLICY 속성을 지정합니다.

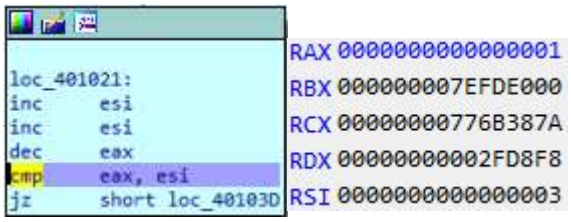
리턴 값을 살펴보면 Drive_CDROM의 리턴 값은 5인 것을 알 수 있다.

이미 답은 나왔지만 디버거를 통하여 좀 더 확실하게 답을 찾아보겠다.

IDA의 기능을 사용하여 프로그램의 전체적인 모습을 확인 하였다.
GetDriveTypeA 함수를 실행 후 총 esi가 3 증가, eax가 2 감소되는 것을 확인 할 수 있다.
그 후 JZ 어셈을 통하여 결과 메시지 창을 출력하는 것을 알 수 있었다.



GetDriveTypeA 함수가 실행 후 나오는 리턴 값 즉, RAX를 확인을 했더니 3이 나왔다.
해당 컴퓨터의 C 드라이브는 HDD이기 때문에 리턴 값이 나왔다.
그 후, esi는 3이 증가하였고, eax는 2가 감소하였다.



그 후, 비교를 하여 틀리면 0이 되기 때문에 JZ 어셈을 통하여 CD-ROM이 아니라는 문구가 생겨진 메시지 창이 출력된다.

즉, GetDriveTypeA 함수의 리턴 값은 5가 되어야 CD-ROM이 맞다는 문구가 생겨진 메시지

창이 출력되게 된다.

정답 : 5
GetDriveTypeA의 정보 사이트 - https://docs.microsoft.com/en-us/windows/desktop/api/fileapi/nf-fileapi-getdrivetypea#syntax