Challenges : Basic 01

Author : abex

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

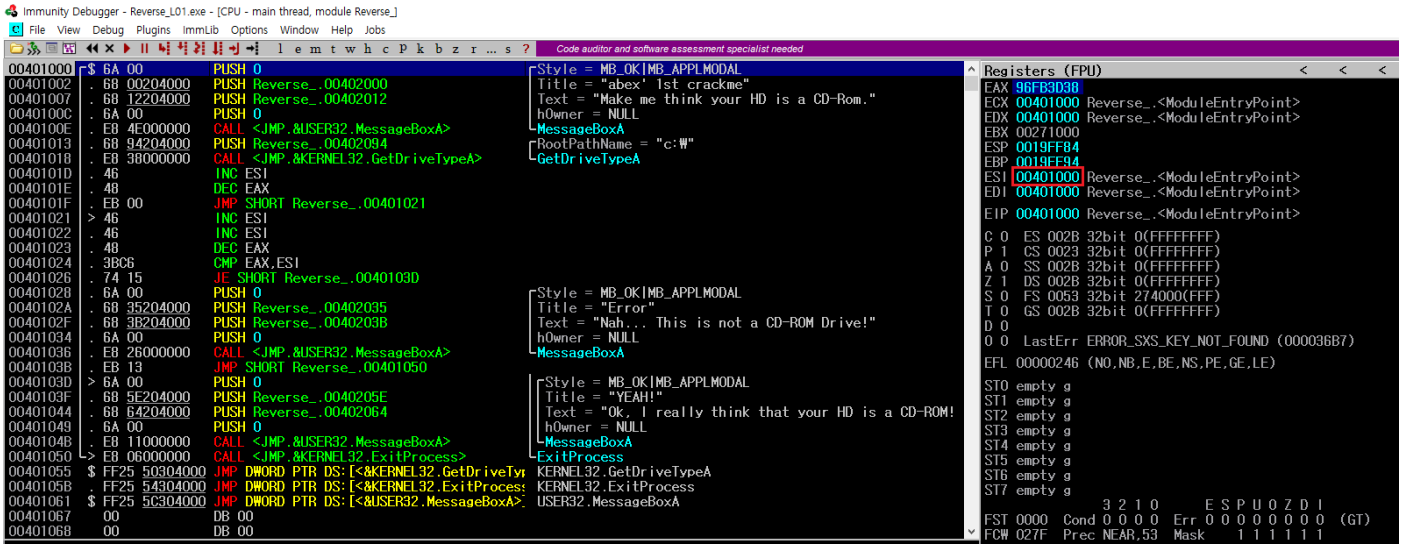
문제에 따라 CD-ROM으로 인식하는 Return Value는 5이다.

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.

출처: https://msdn.microsoft.com/ko-kr/library/windows/desktop/aa364939(v=vs.85).aspx

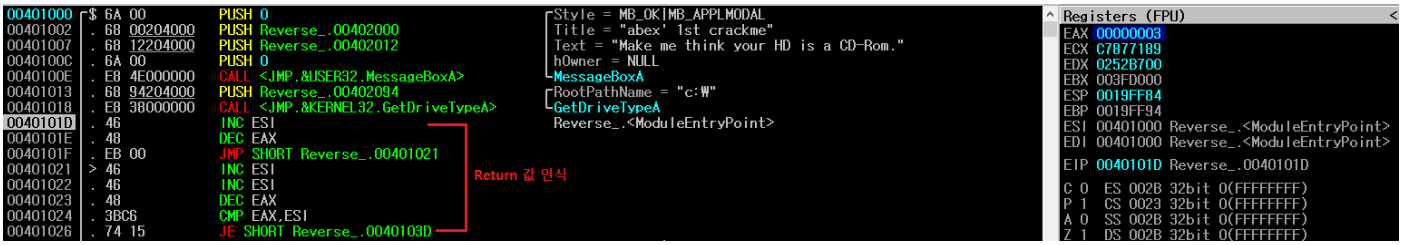


<Entry Point>

"Ok, I really think that your HD is a CD-ROM! :p"라는 성공 문구로 보이는 곳이 있고 시작 부분이 0040103D임을 알 수 있다.

0040103D로 이동되는 곳은 00401026 JE SHORT Reverse_.0040103D

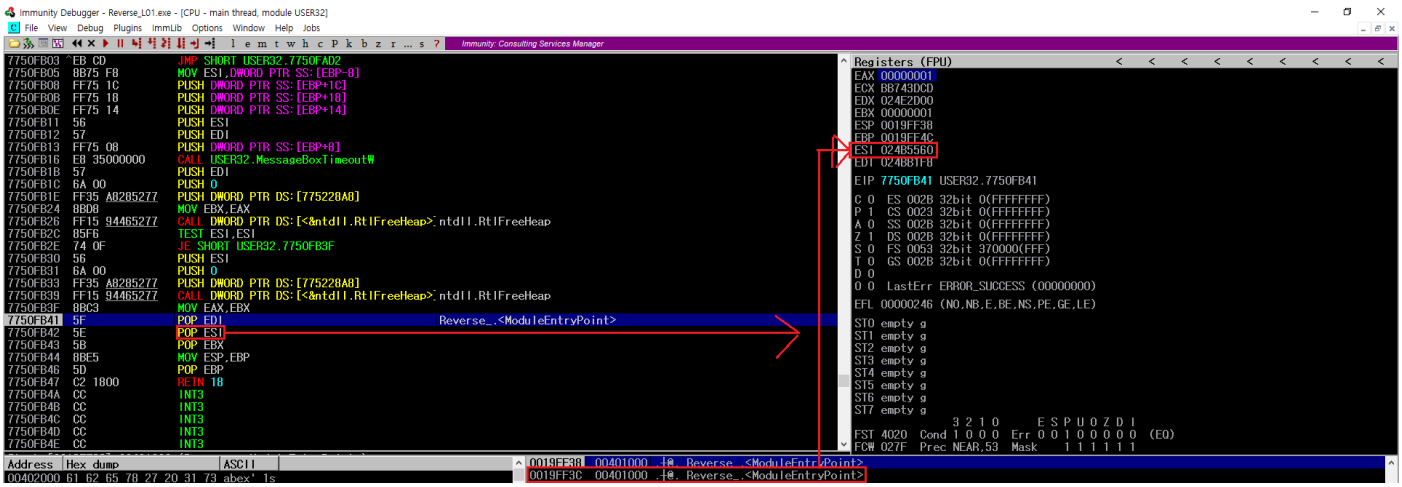
그렇다면 바로 위 CMP EAX,ESI를 보고 EAX가 ESI와 같아야 성공이라는 것을 알게 된다.



Return 값을 측정하는 부분을 보면 ESI는 총 +3을 하고 EAX는 -2를 연산하여 CMP연산을 한다.

CD-ROM으로 인식하는 값인 5를 넣으면 맞아 떨어져야 하지만

시작하는 부분을 살펴보면 EAX는 00000003이고 ESI는 00401000이다.



0040100E CALL <JMP.&USER32.MessageBoxA>를 살펴보면 위와 같이 ESI에 00401000을 채워지는 것을 볼 수 있다.

그래서 다시 돌아가 Return값을 측정하기 시작하는 부분에 EAX값을 00401005를 넣으면 CD-ROM으로 인식한다.