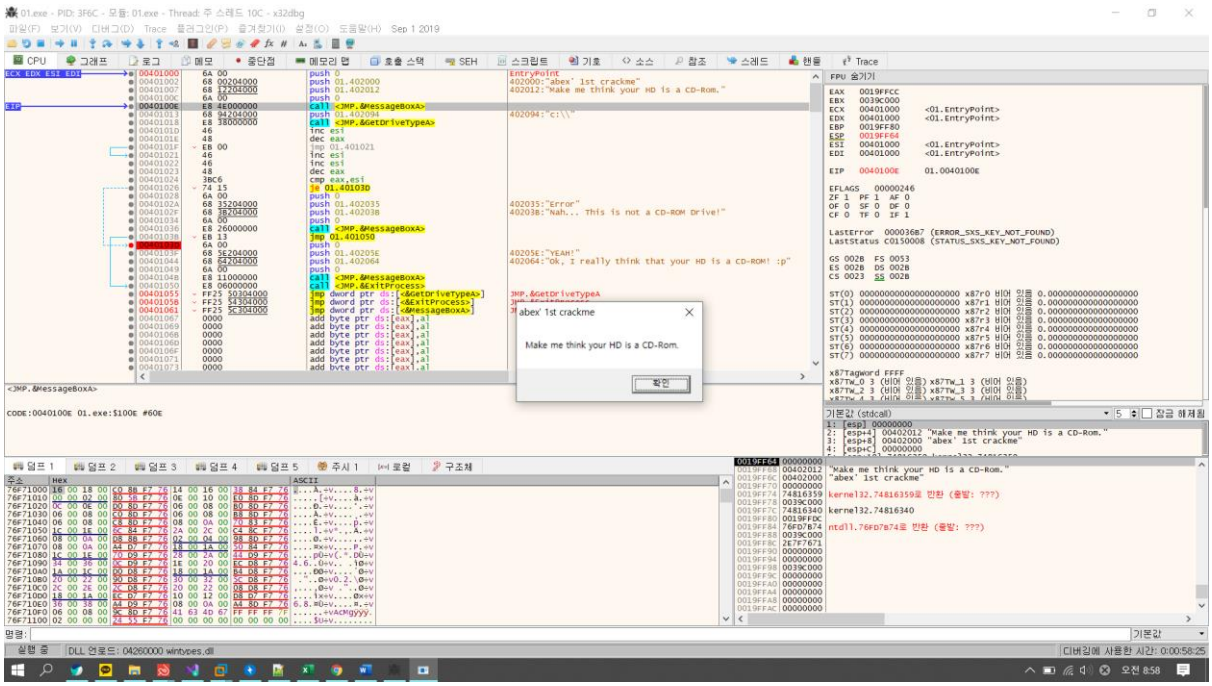
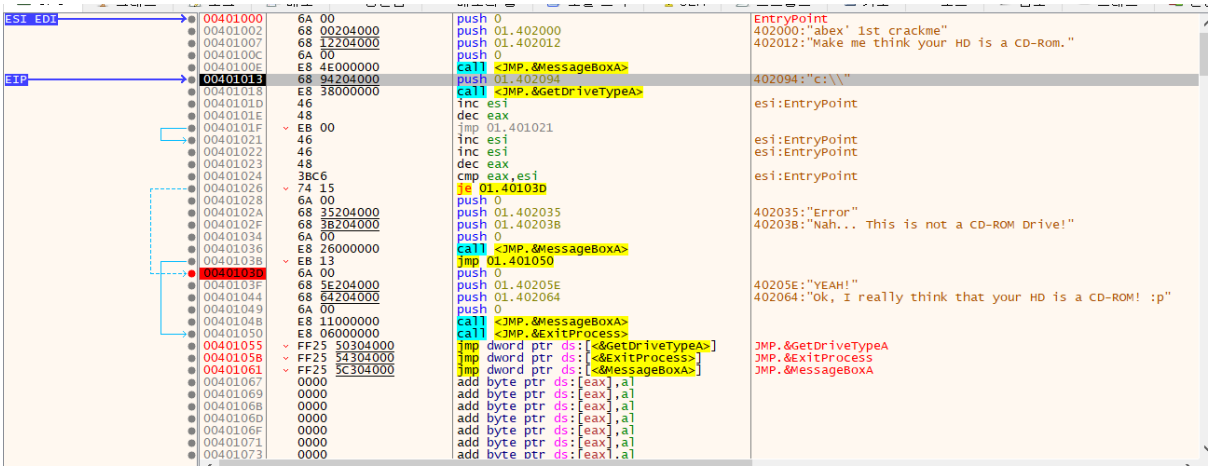
01.exe 풀이 해설



일단 프로그램을 구동 한 다음 구조를 살펴본다.



구조를 살펴보니 GetDriveTypeA를 실행 한 다음 리턴 값을 받고 비교를 하여 CD-Rom인지 아닌지를 확인 하는 프로그램 이다.

일단 작동이 시작 되면 메시지 박스를 출력한 다음 GetDriveTypeA API를 통해 리턴값을 eax에 저장을 하게 되는데 이때 인터넷 검색을 통해 어떤 리턴 값이 Cd-Rom 인지를 찾아 보았다.

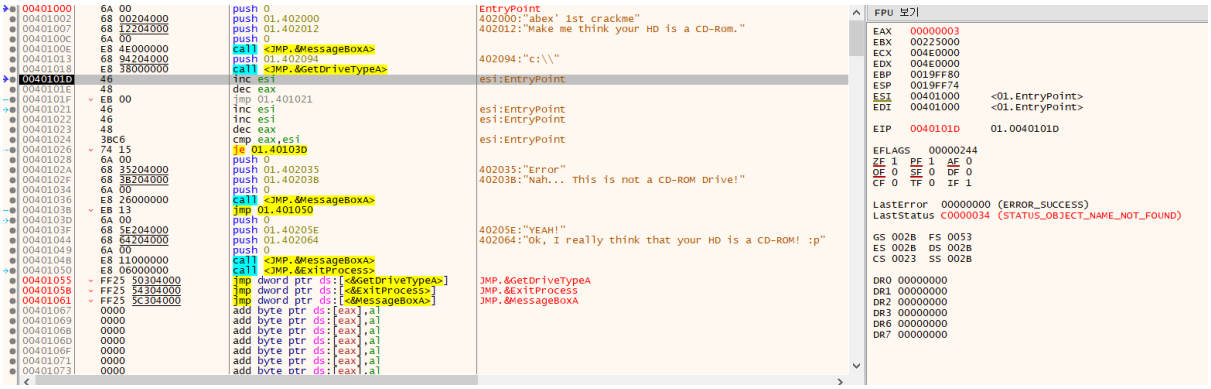
Return Value

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.

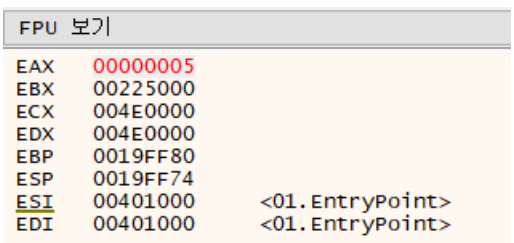
CD-ROM은 eax에 5를 리턴 받아야 한다는 사실을 알게 되었다.

그런 다음 GetDriveTypeA API를 실행 한다음의 레지스터값과 그다음에 실행되는 어셈블리어를 분석하였다.



GetDriveTypeA API의 리턴값은 3으로 반환을 받았다.

이때 CD-ROM의 리턴값은 5를 받아야 하기 때문에 EAX의 레지스터를 5로 수정 한다.



그다음 ESI를 1 증가시켜 401000 → 401001로 변경이 되었고

EAX를 1 다운 시켜 5 → 4로 변경이 되었다.

그 다음 JMP 401021로 이동한다.

그다음 ESI를 1씩 증가 두번을 하여 401001 → 401003으로 변경이 되었다.

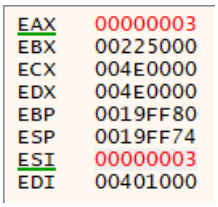
그리고 EAX를 1를 다운 시켜 4 → 3으로 변경이 되었다.

이때 CMP를 하여 EAX와 ESI를 비교 하게 되는데

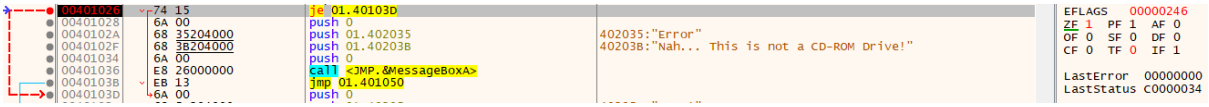
401003 과 3를 비교 하기 때문에 ZF는 0를 얻게 되고 CD-ROM이 아니라는 메시지가 출력 될것을 예상 하게 되었다.

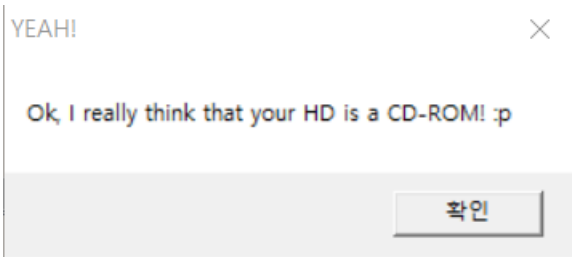
ESI의 초기값이 401000이라는 값이 오기 때문에 결국은 실제 "C:₩₩"이 CD-ROM이여도 오작동 한다는 것을 알게 되었다.

고로 해결 방법은 여러가지 방법이 나오게 되는데 ESI또는EAX 둘중 하나를 같게 수정 하는 방법과



또는 CMP를 한다음 ZF를 1로 변경하여 JMP를 작동하게 만든다.



그러면 최종적으로 

이라는 화면을 볼수 있게 된다.

일단 이 문제를 제작자가 원하는 GetDriveTypeA의 리턴값은 5 이지만, 실제로 동작하도록 하는 리턴값은 401005이다.