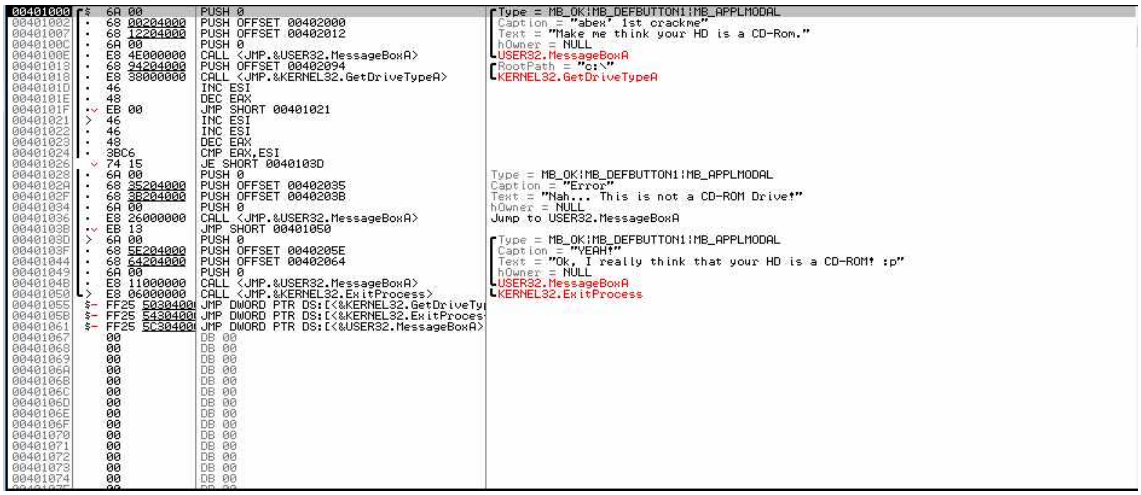
CodeEngn Reversing
Basic 1
문제풀이 보고서

ID : Haren
http//heibondk.tistory.com

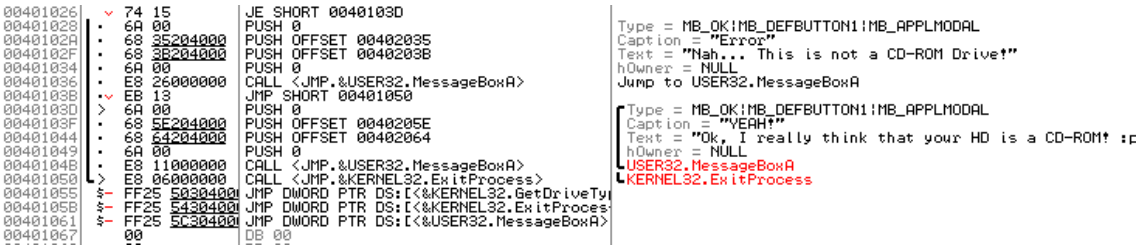
Basic 1

코드엔진은 처음이라 가장 처음 문제를 푸려 Basic 1문제를 받았습니다. 리버싱을 공부하면서 접하게 되는 서적 중 이승원 지음의 리버싱 핵심원리를 공부하며 초반부에서 실습을 했던 abex crackme 1 문제였음을 알게 되었고 디버깅에 착수했습니다.

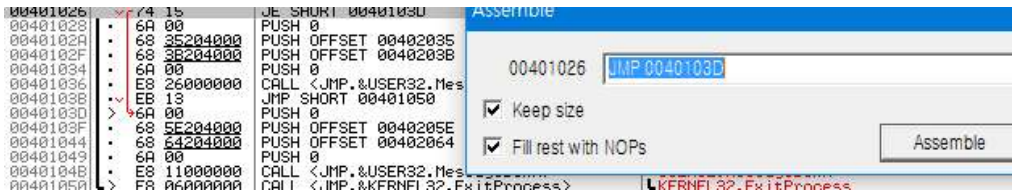
파일의 실행과 그 결과는 첨부하지 않고, 문제 풀이 과정만 첨부하도록 하겠습니다.



Ollydbg로 해당 문제 파일을 열은 뒤 어셈블리 코드를 보면 굉장히 짧고, 한 눈에 구조 파악이 가능한 것을 알 수 있습니다.



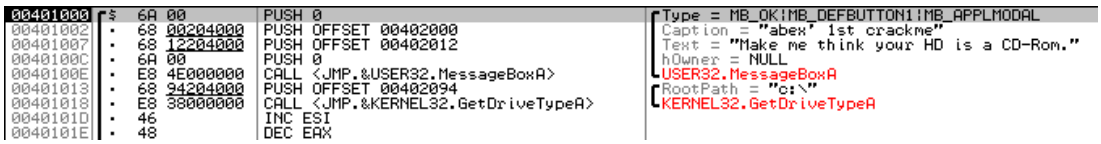
401026 주소의 JE SHORT 0040103D라는 조건 분기문의 참/거짓에 따라 에러와 성공문을 결정하게 됩니다.



해당 조건분기문을 무조건 분기문으로 패치를 시킨 뒤 실행하게 되면

사진처럼 크랙이 완료됨을 볼 수 있습니다.

하지만 이 문제의 flag는 이 프로그램이 CD-ROM으로 인식할 수 있게 해주는 리턴값입니다.
그런 이유로 코드를 다시 분석해보았습니다.



KERNEL32.GetDriveTypeA가 왠지 의심스러워 GetDriveTypeA를 검색해보았습니다.

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.

MSDN에서 발견한 표입니다. CD-ROM으로 인식시킬 수 있는 리턴값은 DRIVE_CDROM의 5임을 알 수 있었습니다.

Flag : 5