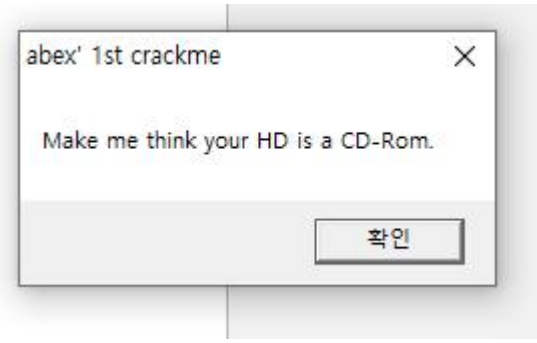
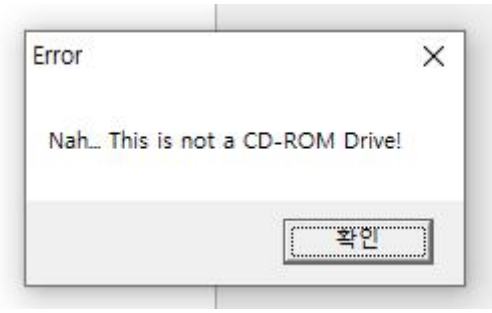
[CodeEngn-basic RCE-01]

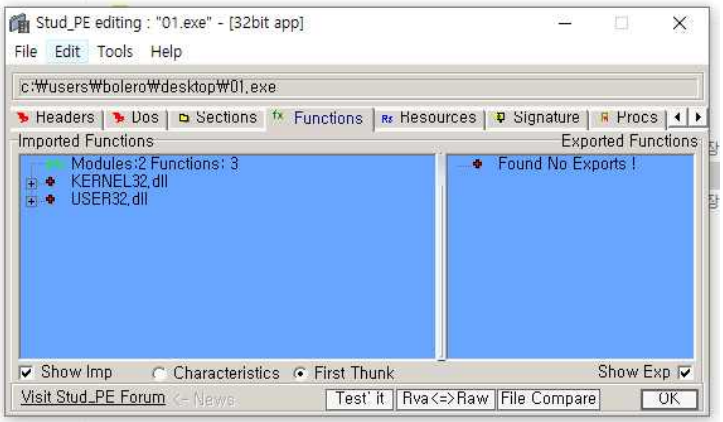
C 드라이브를 CD롬으로 인식시키기



1. 그냥 돌리면 Nah...하면서 인식 안해줌.



이걸 이제 어떻게?
Olly Dbg로 열어본다.
그전에, 이 파일이 32bit 파일인지 64bit 파일인지 체크해야함 -> STUD PE 프로그램으로 체크
ntdll 없으면 32bit로 보자



32bit 맞는 듯.

olly dbg 로 열면

이렇게 나옴.

함수들 보니까

1. MessageBoxA 2. GetDriveTypeA 3. 다시 MessageBoxA 4. ExitProcess

1번은 그냥 문제제시인 것 같고, 2번이 HDD인식 과정? 3번이 결과 메시지 4번이 프로그램 종료

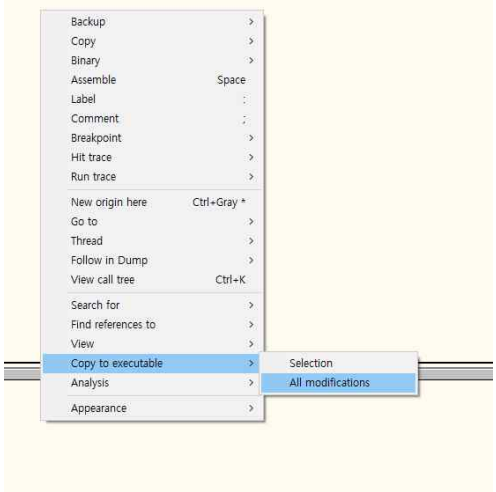
돌려보니까 00401021부터 00401024까지 ESI 두 번 증가(INC)시키고 EAX 한 번 감소(DEC)시킨다. 그리고 나중에 ESI랑 EAX랑 비교해서 같으면 점프(JE) 어디로? 0040103D -> 정답입니다! 메시지 출력 부분.

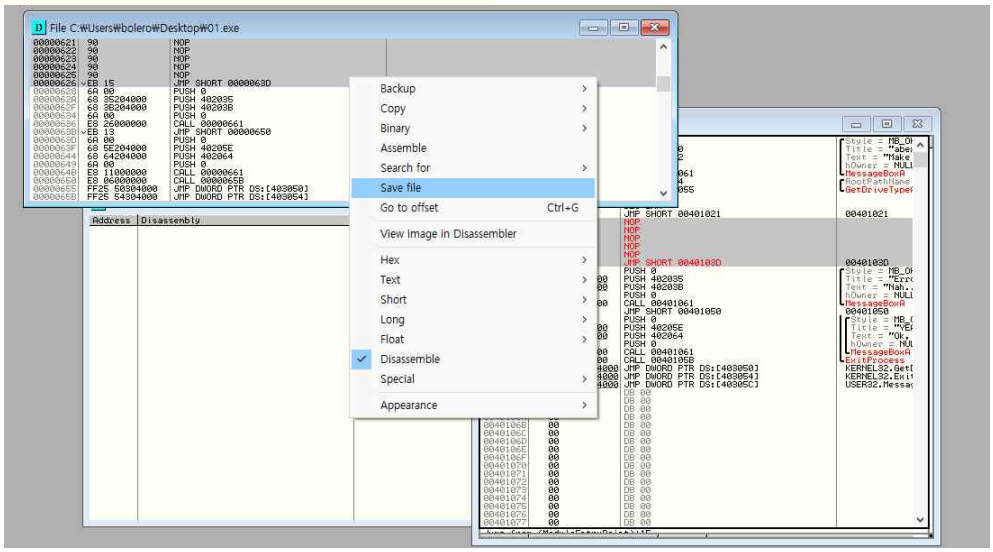
난 그냥 저부분 다 NOP으로 때렸다. 그리고 JE가 아니라 JMP로 바꿈(무조건분기)

이렇게!

패치하는 법

우클릭 -> copy to executable -> All modifications -> Copy All 클릭

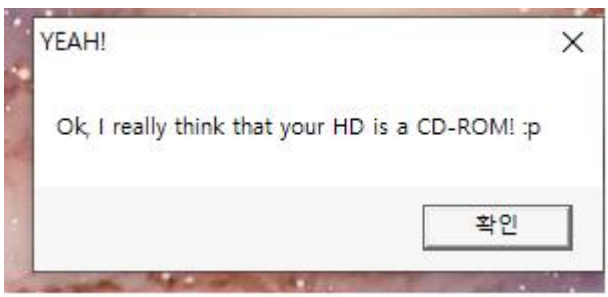




우클릭 후 Save file 클릭(창이 보면 좌측 상단 File~이 있고 우측 하단 CPU - 가 있다. 여기서 좌측 상단에 우클릭 해야함.)

이후 file name 적고 save하면 됨. 난 01_patch.exe 로 저장.

그러면...

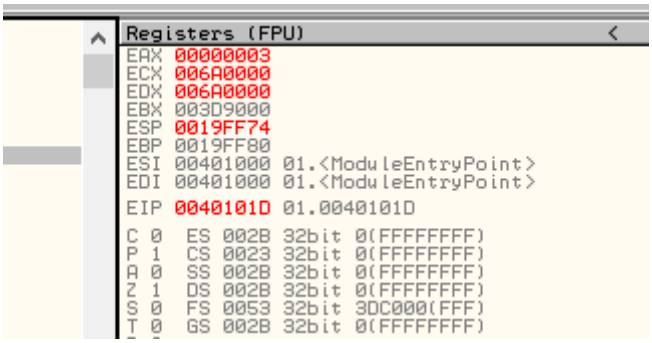


성공!

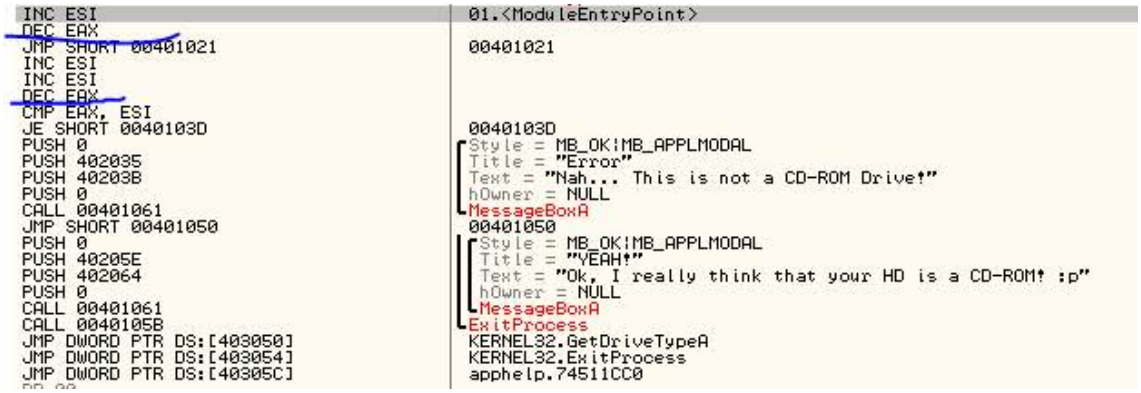
문제는 GetDriveTypeA의 리턴값이 뭐가 되어야 정상 실행되는가? 인데

리턴값 -> EAX로 들어감.

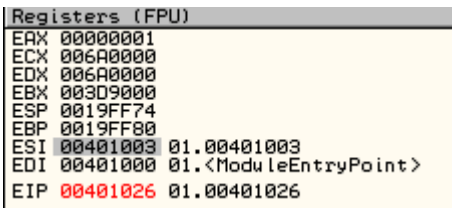
그럼 GetDriveTypeA 함수 실행된 이후 EAX 값을 봐야 함.



EAX = 3 나왔네?
이후 어셈코드를 보면



DEC EAX가 2번있음.
계속 실행해보자. 소스 보니까 CMP EAX, ESI 비교인데, 저기 코드라인까지 갔을 때 ESI 값도 봐야함.



ESI = 3나왔네
EAX = 1이니까... 두 개가 같으면(JE) 정상문구 출력 -> EAX + 2해야 함.
즉, GetDriveTypeA 리턴값이 3이 아니라 5가 된다면...
DEC EAX, DEC EAX 했을 때 3이 나온다.

답 : 5