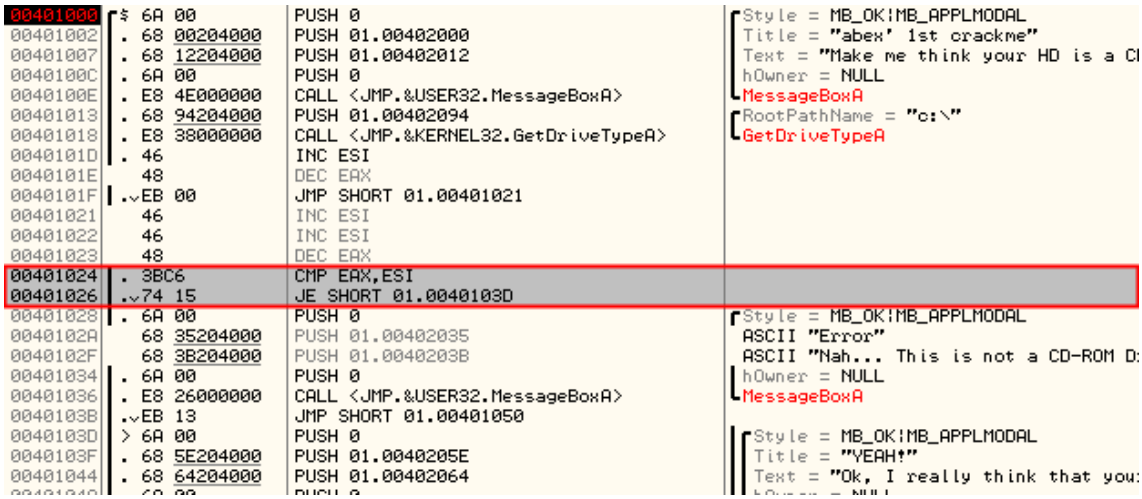
문제: HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

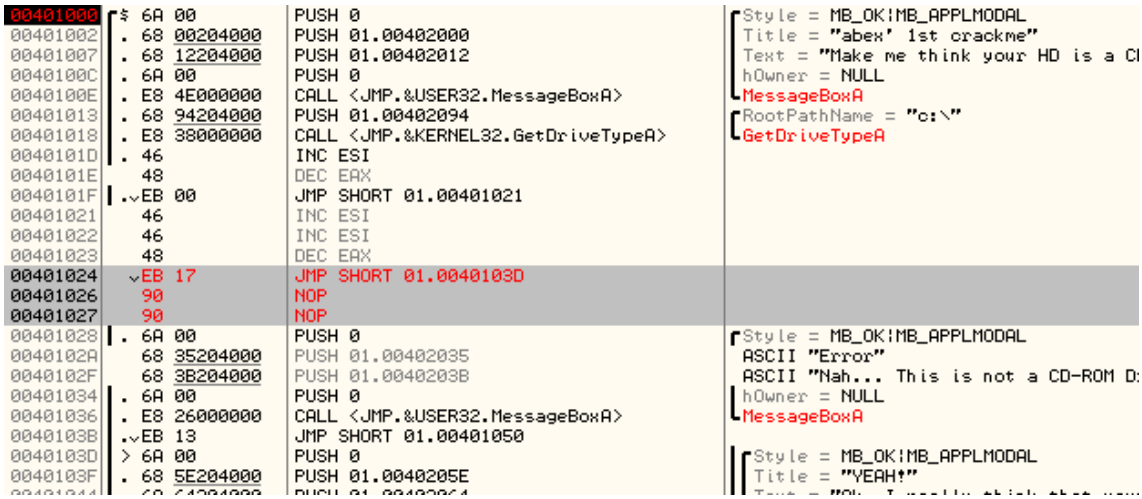


[그림 1. main 함수]

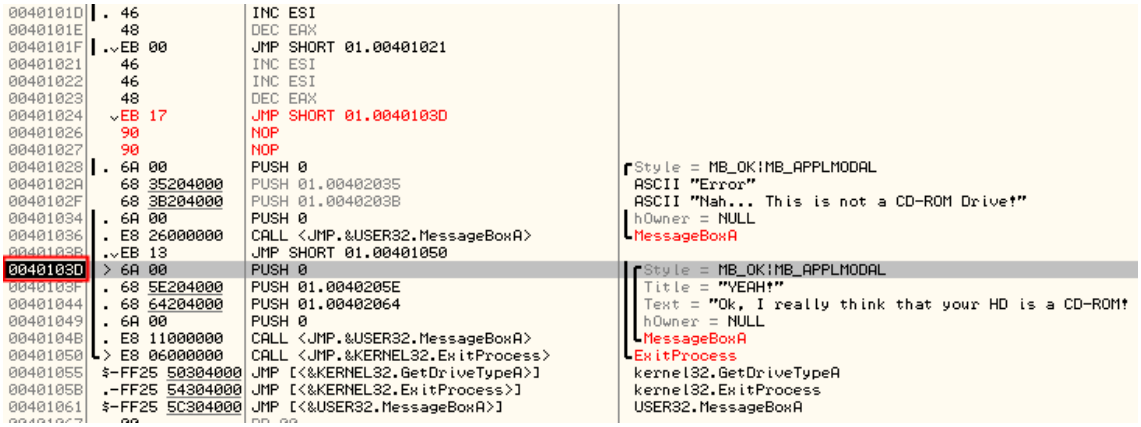
그림 1에서 빨간색 네모로 표시된 부분을 보면 EAX, ESI 레지스터의 값이 같을 경우 40103D 주소로 JMP한다. 그리고 그 곳에는 문제 해결을 알리는 메시지가 있다.

▸ **풀이 1. JMP를 이용한 주소 강제 이동**

어떻게든 40103D로 보내야 된다는 사고방식에서 나온 첫 번째 풀이방법. 중간에 코드 한 줄을 조건 없이 JMP 40103D로 바꿔주는 것이다.



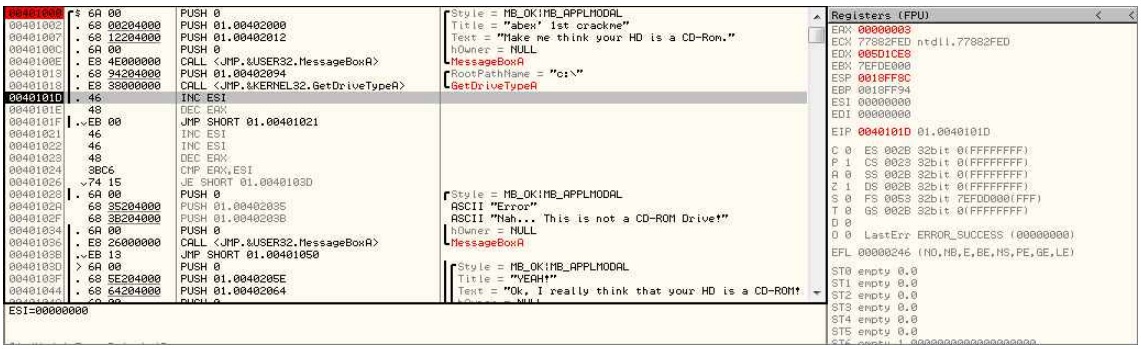
[그림 2. JMP 코드를 삽입한 모습]



[그림 3. 40103D 주소로 이동한 모습]

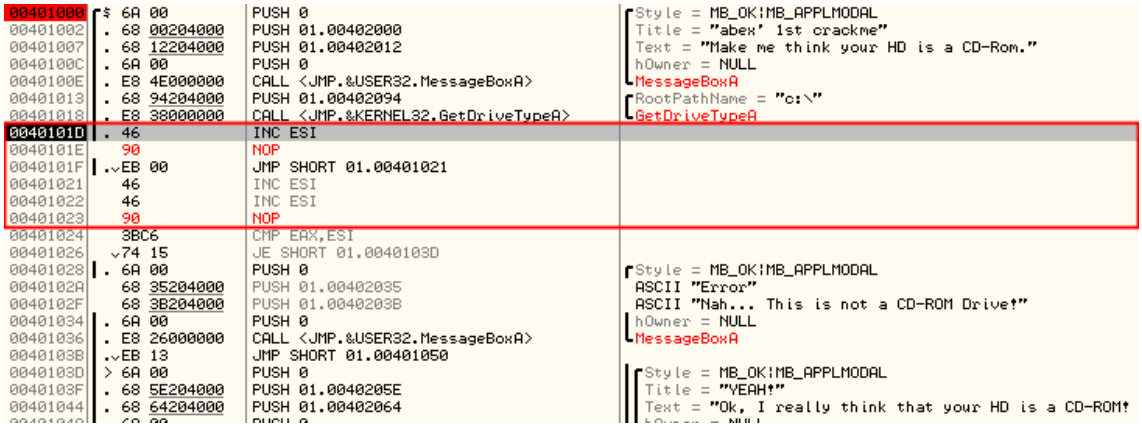
▸ **풀이 2. INC, DEC, NOP 활용**

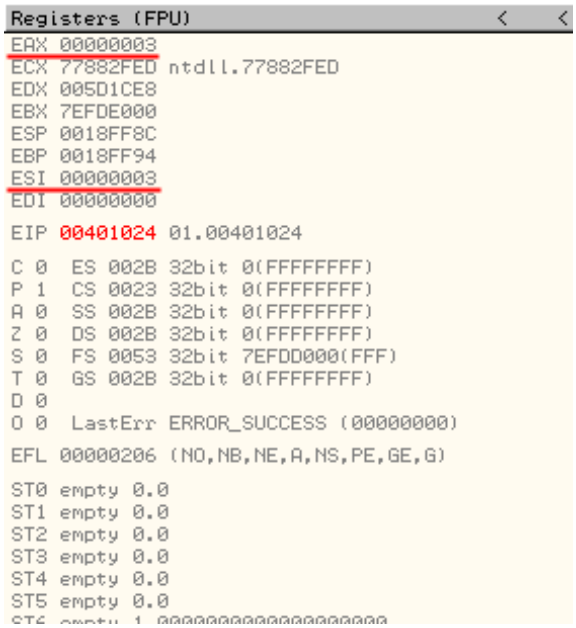
1번 풀이방법이 강제로 주소를 이동시켰다면, 이번엔 조건문에 의한 이동을 해보는 것이다. [그림 1]의 빨간 네모로 표시된 부분을 보면 EAX와 ESI의 값이 같을 경우 40103D로 이동하게 되어 있다. 아무 것도 건드리지 않고 CMP EAX ESI 명령을 실행할 경우, 값이 다르기 때문에 JE SHORT 01.0040103D를 만났을 때 40103D 주소로 이동하지 않는다.



[그림 4. GetDriveTypeA 함수를 빠져나온 직후의 모습]

GetDriveTypeA 함수를 빠져나왔을 때의 EAX의 값은 3이고 ESI의 값은 0이다. 그 밑의 INC와 DEC 명령을 다 실행하고 비교할 때쯤이면 EAX는 1, ESI는 3이 된다. 때문에, INC, DEC, NOP 명령을 적절히 활용해 EAX와 ESI의 값을 서로 같게 만들어준다.





[그림 5와 6. 코드 수정 후 실행]

EAX와 ESI의 값을 3으로 맞춰주고 성공 메시지가 있는 40103D 주소로 이동한다. 하지만 문제에선 GetDriveTypeA 함수에서 리턴값이 몇이 되어야 하냐고 물었다. [그림 4]를 보면 GetDriveTypeA 함수를 빠져나오고 나서 EAX의 값엔 -2를 하고, ESI의 값은 0인 상태에서 +3을 한다. EAX의 값을 3으로 만들어주기 위해선 GetDriveTypeA 함수의 리턴값은 5가 되어야 할 것이다. $(x-2=0+3)$