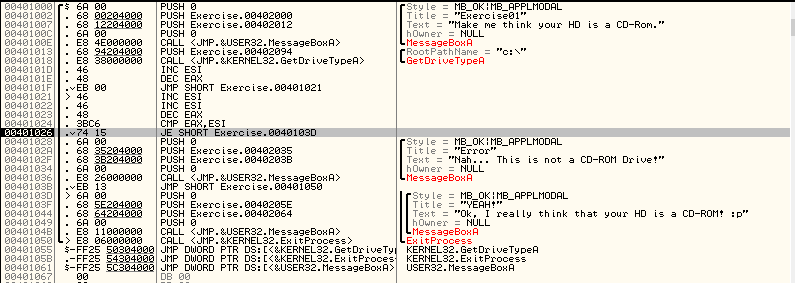
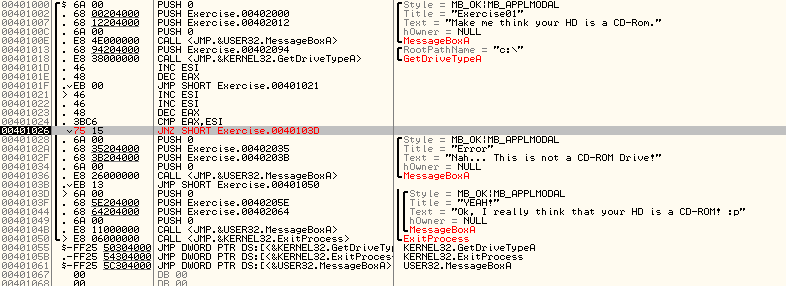
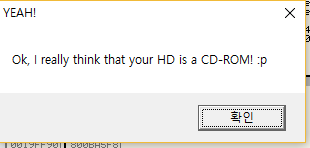
Exercise01



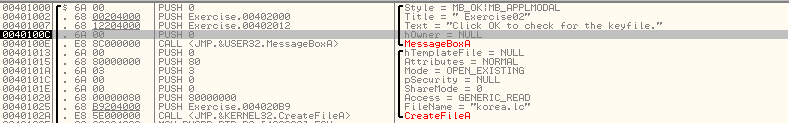
저 부분에서 ZF에 따라 Fail로 갈 수도 있고, Success로 갈 수도 있다. 그러니까 JE를 단순하게 JNZ로 바꿔버리면 된다.

JNZ로 고쳤더니 제대로 넘어간다.

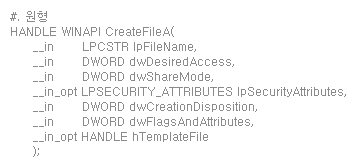


Exercise01 Clear!

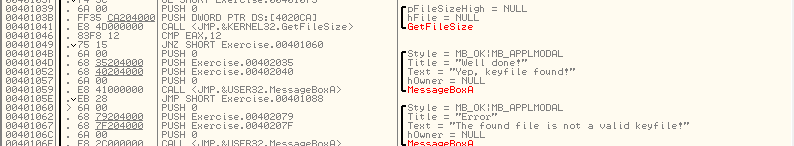
Exercise02



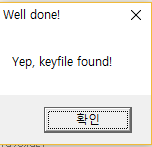
MessageBoxA를 실행한 다음 CreateFileA를 실행한다.



CreateFileA 함수의 구조이다. 여기서 dwCreationDisposition의 값을 보면, push 3이라고 되어있다. Mode=OPEN\_EXISTING을 보니 이미 있는 파일을 여는 작동을 하고, 파일이 없으면 에러를 출력하는 것 같다. 따라서 FileName부분에 있는 “korea.lc” 파일을 생성해준다.

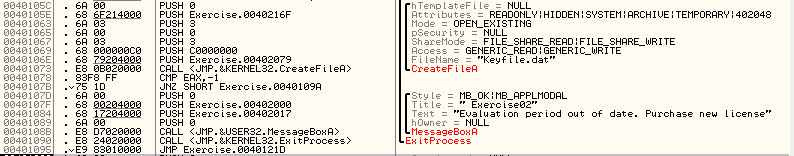


GetFileSize를 하여 CMP EAX,12를 한다. 따라서 파일 size를 12로 맞추면 해결되는 문제인 것 같다. 그냥 0으로 12문자 채운 뒤 저장하고 파일을 실행하자.



Exercise2 Clear!

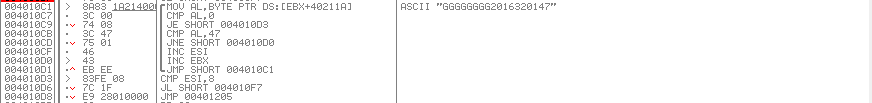
Exercise3



여기서 CreatFileA을 통해 “keyfile.dat”파일을 찾는다. 2번과 같이 keyfile.dat 파일을 만들어주자.



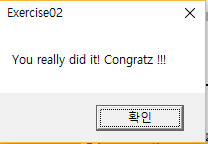
CMP DWRD PTR DS:[402173],10 에서 JL 구문으로 파일 크기가 10보다 크지 않으면 Fail을 띄우는 것 같다. 402173번째 주소를 보니 크기가 들어있는 것을 보니 맞는 것 같다.



여기서 반복구문으로 AL에 문자 하나씩을 넣은 뒤, CMP AL, 47(‘G’)를 통해 G라는 문자가 있으면 ESI를 증가시키고, CMP AL,0 를 통해 문자열의 끝을 검사한다.

CMP ESI,8을 가지고 JL SHORT 004010F7(Fail)을 검사하고, 그 밑에 JMP 00401205(Success)로 넘어가는 구문이 있는 것을 보니 G가 8개 이상 있으면 통과한다.

따라서 key 파일에 G를 8개를 넣고, 대충 아무거나(학번 등)을 넣은 뒤 통과시켜보니 되었다.



Exercise03 Clear! (오타가…)