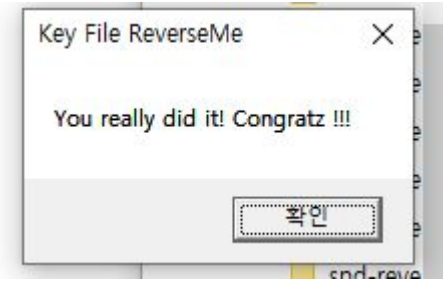
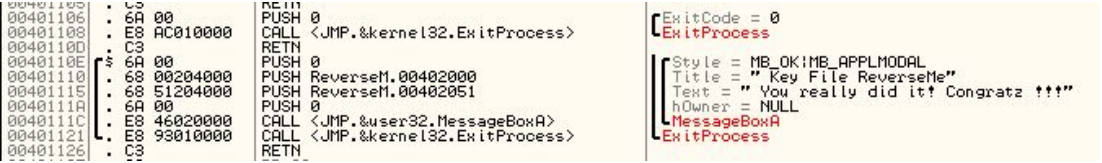
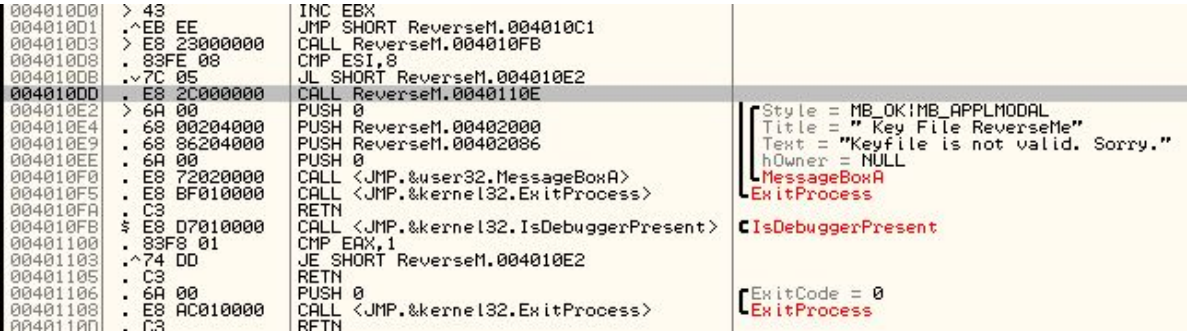


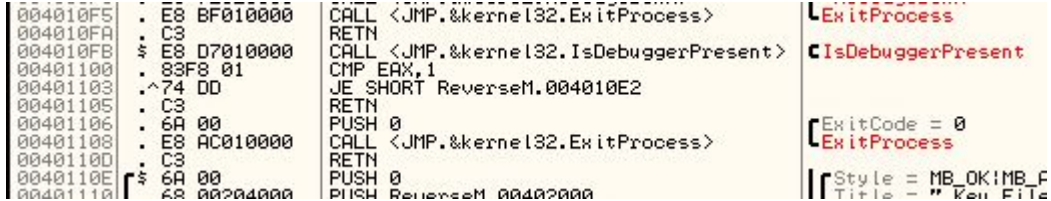

프로그램 실행 시 성공 메시지가 뜬다. 이번엔 어떤 튜토리얼인지 디버거로 분석해본다.



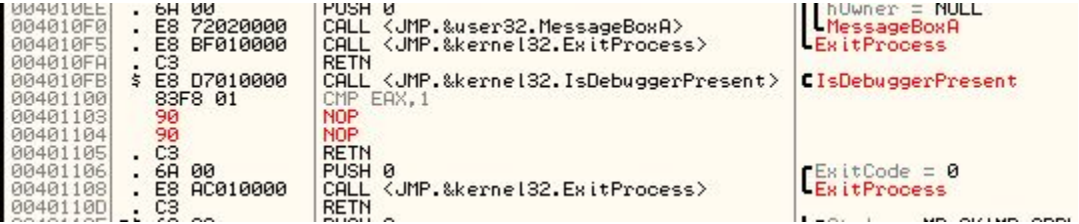




문자열로 검색해보니 아까 성공 메시지가 보이고, 해당 부분을 어디서 호출하는지 하나 하나 따라가보니 4010DD에서 호출한다.

해당 주소 위에 또 함수를 호출하고, 분기문이 있어서 보니 IsDebuggerPresent 결과에 따라 실행 결과가 달라진다.
IsDebuggerPresent의 결과를 충족하면, 4010E2로 분기하는데, 보이는것과 같이 여기는 오류메시지가 뜨는 부분이다.






IsDebuggerPresent는 디버깅 중이면 1 아니면 0을 반환한다. 현재 디버깅중이니 1을 반환할거고, 그럼 오류메시지를 반환할 것이다.

첫번째 방법으로 안티 디버깅에 걸리면 오류메시지로 분기하는 부분을 성공메시지로 분기하게 패치했다.

두번째 방법으로 디버깅 반환값과 비교하는 부분을 0으로 패치해 분기되지 않게 했다.

세번째 방법으로 분기되는 부분을 NOP으로 패치했다.