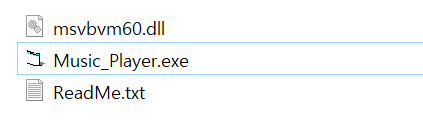
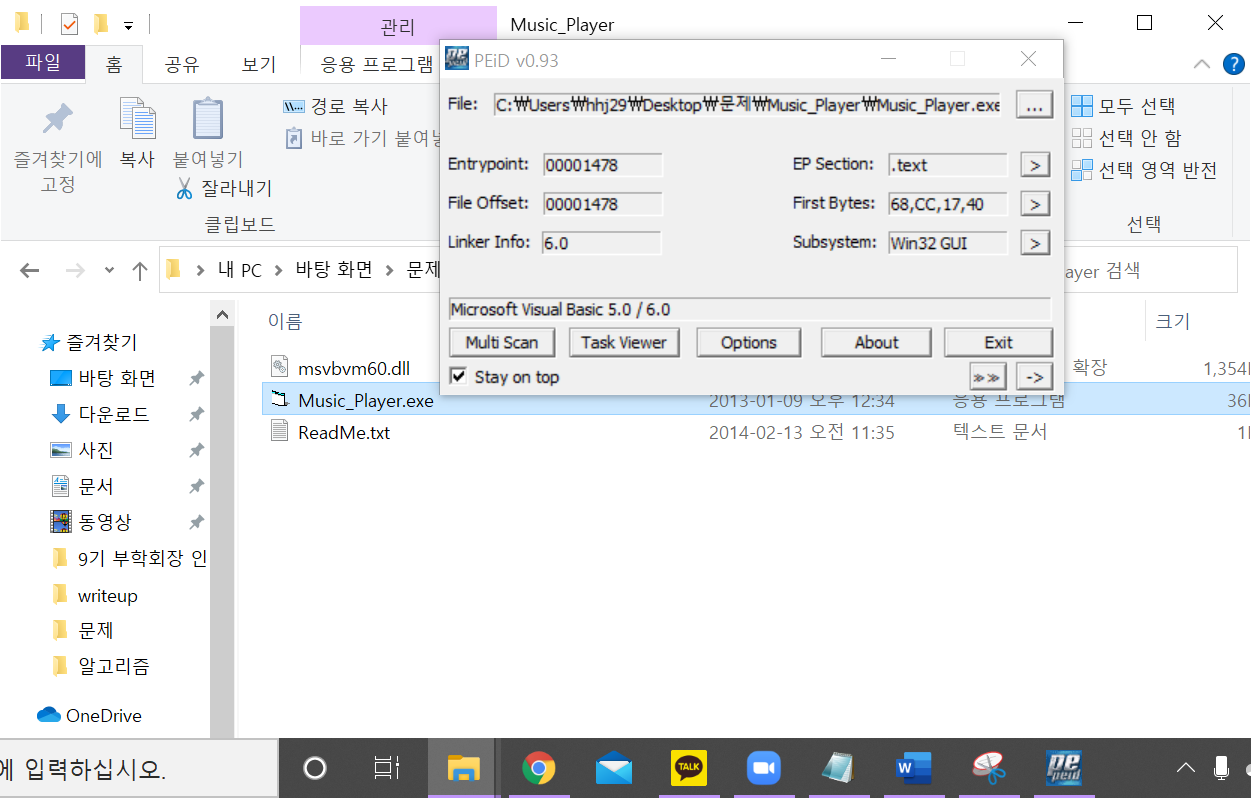
1. 문제 확인



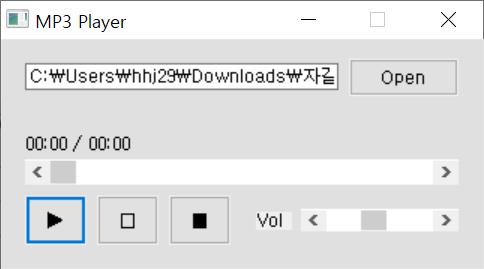
2. 과정

패킹 여부를 확인해보았다.

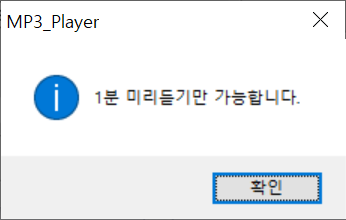


별다른 이상이 없어 파일을 열어보았다.

파일은 뮤직 플레이어였고, 음악 파일을 넣고 재생시키면 1분간 음악을 재생하는 기능이 있다.



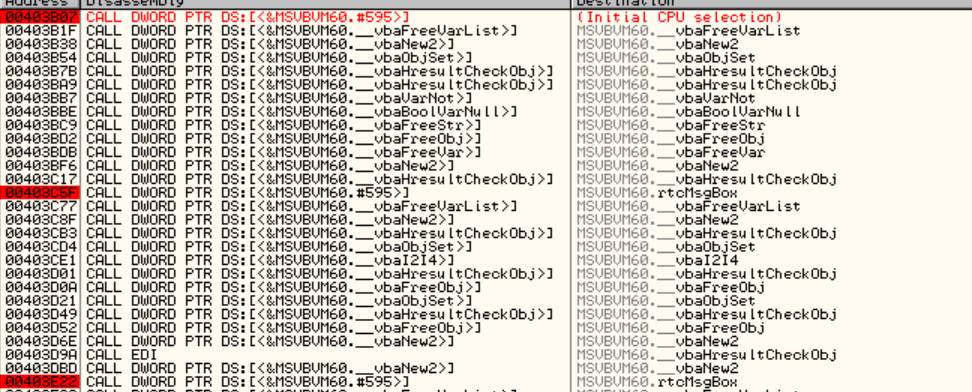
여기서 1분을 초과하게 되면 다음과 같은 메시지창이 뜨면서 음악이 종료된다.

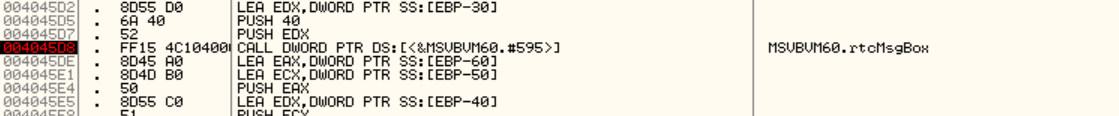


올리디버거를 켜서 확인해보았다.

우선 메시지창이 뜨는 곳을 알아내기 위해 문자열 검색을 확인하다가 발견할 수 없었다. 그래서 함수를 확인해보았다.

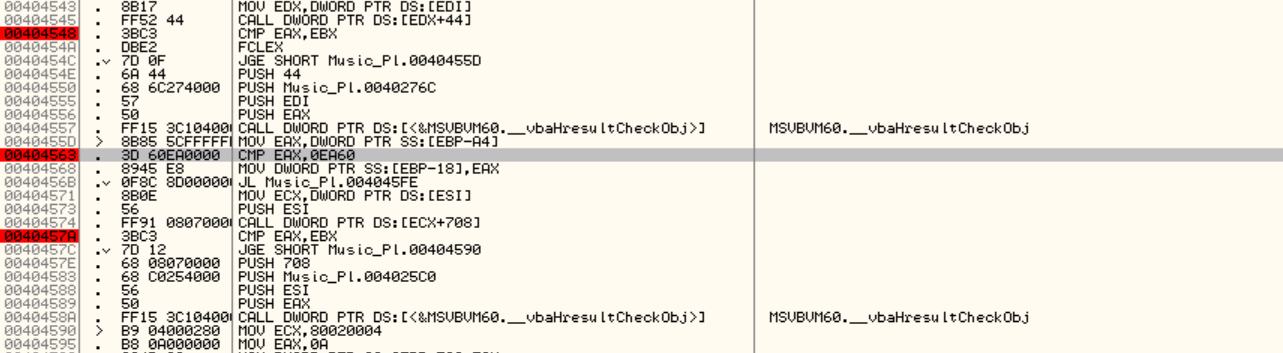
다음과 같이 함수에 MsgBox를 불러오는 곳에 bp를 걸고 문제를 실행해보도록 한다.



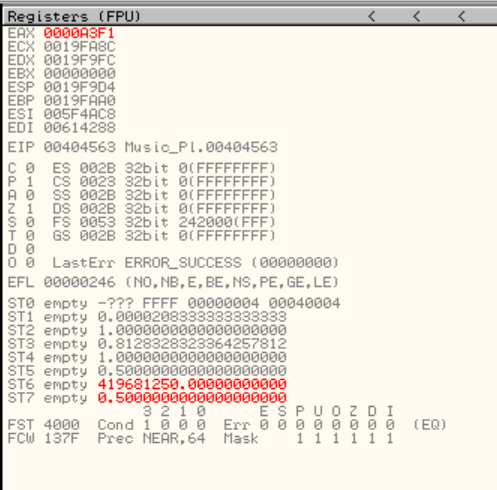


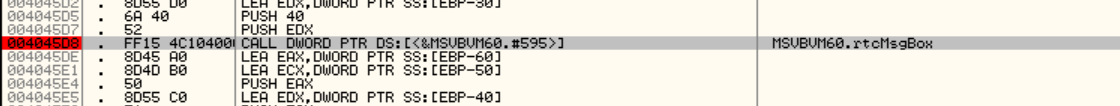
디버깅을 해보니까 이 위치에서 걸리게 되는데 1초마다 걸리게 된다. 이걸 보아 이곳에서 1초

CMP로 검사하는 부분이라는 것을 알 수 있다.

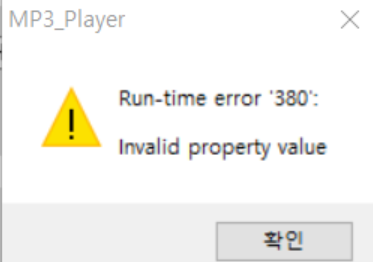


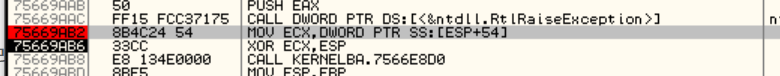
여기선 EAX와 0EA60(60000)를 비교한다. 60000이 60초인 것 같아 이걸 더 큰 값으로 고쳐주면 60초를 넘겨서도 음악이 재생될 것 같다.





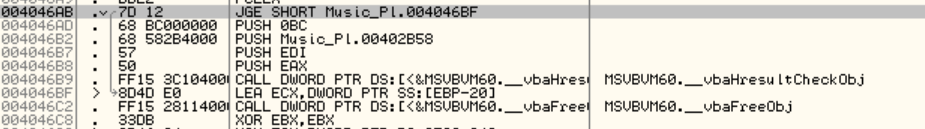
변경 후 문제를 실행했는데 이상하게 런타임오류 창이 뜨면서 다음과 같은 위치로 이동했다.





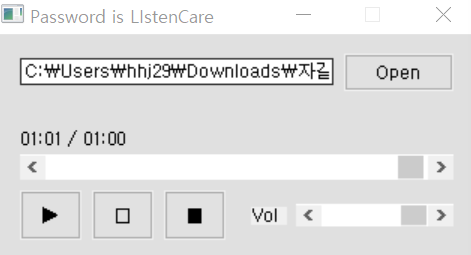
뭔가 싶어서 어느 부분에서 오류를 띄우는지 확인해본 결과

4046B9에서 호출한다는 것을 발견했다.



따라서 그 위에 있는 점프문을 이용해 이 부분을 거치지 않도록 수정해보았다.

JGE -> JMP로



다음과 같이 1분이 넘어도 에러창이 뜨지 않고 실행되면서 패스워드를 발견할 수 있었다.