

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

```
6A 00
E8 AC010000
                            PUSH 0
00401106
00401108
                                                                        FExitCode = 0
                                                                        ExitProcess
                            CALL (JMP.&kernel32.ExitProcess)
0040110D . C3
0040110E r$ 6A
                            RETN
                                                                         rStyle = MB_OK:MB_APPLMODAL
| Title = " Key File ReverseMe"
| Text = " You really did it! Congratz !!!"
                            PUSH 0
00401110
          . 68 00204000
                            PUSH ReverseM.00402000
00401115
          . 68 51204000
                            PUSH ReverseM.00402051
0040111A
          . 6A
                                                                          hOwner = NULL
                00
                            PUSH 0
          . E8 46020000
                            CALL (JMP.&user32.MessageBoxA)
CALL (JMP.&kernel32.ExitProcess)
                                                                        MessageBoxA
00401121 L. E8 93010000
00401126 . C3
                                                                        ExitProcess
                            RETN
004010D0
            .^EB EE
                                JMP SHORT ReverseM.004010C1
004010D3
            > E8 23000000
                                CALL ReverseM.004010FB
004010D8
            . 83FE 08
                                CMP ESI,8
                                JL SHORT ReverseM.004010E2
            .v7C 05
            . E8 20000000
                                CALL ReverseM.0040110E
            > 6A 00
                                PUSH 0
                                                                                   Style = MB_OK!MB_APPLMODAL
Title = " Key File ReverseMe"
              68 00204000
004010E4
                                PUSH ReverseM.00402000
              68 86204000
                                PUSH ReverseM.00402086
                                                                                    Text = "Keyfile is not valid. Sorry."
004010EE
              6A
                                PUSH 0
                                                                                    hOwner = NULL
                  72020000
              E8
                                                                                   MessageBoxA
                                CALL (JMP.&user32.MessageBoxA)
004010F5
            . E8 BF010000
                                CALL (JMP.&kernel32.ExitProcess)
                                                                                  -ExitProcess
004010FA
               C3
                                RETN
004010FB
           $ E8 D7010000
                                CALL (JMP.&kernel32.IsDebuggerPresent)
                                                                                 CIsDebuggerPresent
            . 83F8 01
00401100
00401103
                                CMP EAX, 1
            .^74 DD
                                JE SHORT ReverseM.004010E2
```

rExitCode = 0

ExitProcess

. сз

. 6A 00

. E8 AC010000

RETN

PUSH 0

CALL (JMP.&kernel32.ExitProcess)

00401105

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.

```
. E8 BF010000
 004010F5
                             -ExitProcess
 004010FA
           . C3
004010FB
           $ E8 D7010000
                             CALL <JMP.&kernel32.IsDebuggerPresent>
                                                                        CIsDebuggerPresent
                             CMP EAX,1
JE SHORT ReverseM.004010E2
 00401100
           . 83F8 01
           .^74 DD
 00401103
 00401105
           . C3
                             RETN
 00401106
                             PUSH 0
                                                                         rExitCode = 0
                             CALL (JMP.&kernel32.ExitProcess)
                                                                        ExitProcess
           . E8 AC010000
 00401108
             C3
 0040110D
                             RETN
             6A 00
                             PUSH 0
                                                                        Style = MB_OK:MB_F
0040110E FS
             68 00204000
                             PUSH ReverseM 00402000
304010E2
         > 6A 00
                         PUSH 0
                                                                  "Style = MB_OK!MB_APPLMODAL
| Title = " Key File ReverseMe"
304010E4
         . 68 00204000
. 68 86204000
                         PUSH ReverseM.00402000
                         PUSH ReverseM.00402086
                                                                  Text = "Keyfile is not valid. Sorry."
304010E9
304010EE
         . 6A 00
                         PUSH 0
                                                                  hOwner = NULL
         . E8 72020000
304010F0
                         CALL (JMP.&user32.MessageBoxA)

    MessageBoxA

                         CALL (JMP.&kernel32.ExitProcess)
           E8 BF010000
                                                                -ExitProcess
304010F5
304010FA
         $ E8 D7010000
                         CALL <JMP.&kernel32.IsDebuggerPresent>
304010FB
                                                                CIsDebuggerPresent
         . 83F8 01
30401103
         v74 09
                         JE SHORT ReverseM.0040110E
30401105 . C3
30401106 . 60 00
                         RETN
                        PUSH 0
                                                                cExitCode = 0
00401000
           > 43
           .^EB EE
                             JMP SHORT ReverseM.004010C1
           > E8 23000000
                             CALL ReverseM.004010FB
004010D8
           . 83FE 08
                            CMP ESI,8
JL SHORT ReverseM.004010E2
           .v7C 05
 004010DD
           . E8 2C000000
                             CALL ReverseM.0040110E
004010E2
           > 6A 00
                             PUSH 0
004010E4
           . 68 00204000
                             PUSH ReverseM.00402000
004010E9
           . 68 86204000
                             PUSH ReverseM.00402086
 004010EE
           . 6A 00
                             PUSH 0
           . E8 72020000
004010F0
                             CALL (JMP.&user32.MessageBoxA)
                             CALL (JMP.&kernel32.ExitProcess)
004010F5
           . E8 BF010000
004010FA
           . C3
                             RETN
004010FB
           $ E8 D7010000
                             CALL <JMP.&kernel32.IsDebuggerPresent>
00401100
             83F8 00
00401103
            ^74 DD
                             JE SHORT ReverseM.004010E2
00401105
             C3
004010EE
                                                                        hUwner = NULL
MessageBoxA
004010F0
             E8 72020000
                            CALL (JMP.&user32.MessageBoxA)
          . E8 BF010000
004010F5
                            CALL (JMP.&kernel32.ExitProcess)
                                                                        -ExitProcess
004010FA
                            RETN
          $ E8 D7010000
                            CALL (JMP.&kernel32.IsDebuggerPresent)
004010FB
                                                                       CIsDebuggerPresent
00401100
             83F8 01
                            CMP EAX, 1
00401103
                            NOP
             90
00401104
             90
                            NOP
00401105
           . C3
                            RETN
            6A 00
                            PUSH 0
00401106
                                                                        rExitCode = 0
00401108
             E8 AC010000
                            CALL (JMP.&kernel32.ExitProcess)
                                                                        -ExitProcess
             C3
0040110D
                            RETH
```

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 **0**으로 패치해 분기되지 않게 했다.

세번째 방법으로 분기되는 부분을 **NOP**으로 패치했다.