손상된 파일에서 .text의 Point to Raw Data 값이 0x00000400이고 손상된 파일의 .txet의 raw시작 주소는 0x00000350이다
0xB0값의 데이터를 복원해줌, 아래 코드는 PE 1000에 맞춤 pe헤더 아래 부분 0x40 삭제

수정본

```
1   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
    B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
    BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90
    54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73
    74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57
    69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    50 45 00 00 4C 01 04 00 00 00 00 00 00 00 00 00
    00 00 00 00 E0 00 0F 01 0B 01 02 19 00 02 00 00
    00 0A 00 00 00 00 00 00 00 10 00 00 00 10 00 00
    00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00
    04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
```

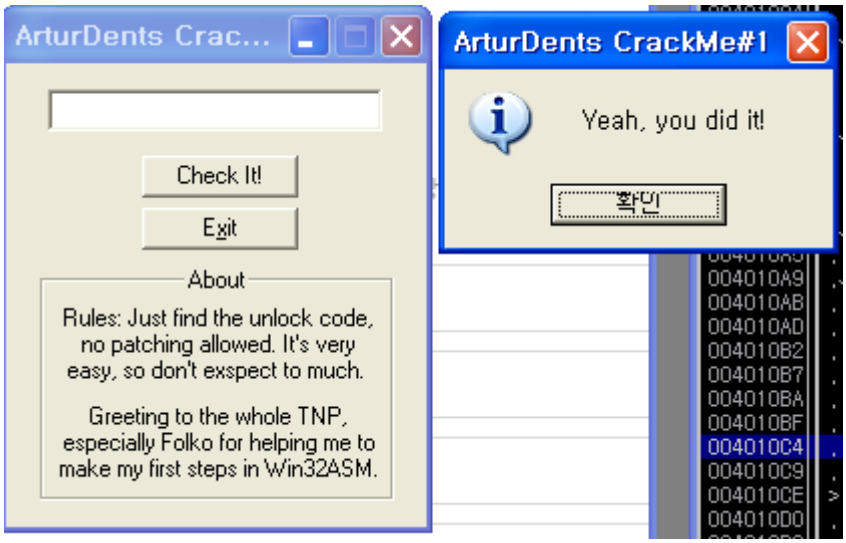
원본

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,........@.......
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 0A 00 00 00 00 00 00 00 10 00 00 00 10 00 00  ................
00000040   00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00  . ....@.........
00000050   04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ................
00000060   00 50 00 00 00 04 00 00 00 00 00 00 02 00 00 00  .P..............
00000070   00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00000080   00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000090   2C 20 00 00 3C 00 00 00 00 40 00 00 18 03 00 00  , ..<....@......
000000A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0   00 00 00 00 00 00 00 00 00 20 00 00 2C 00 00 00  ......... ..,...
000000F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100   00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00  .........text...
```

복원 후 실행

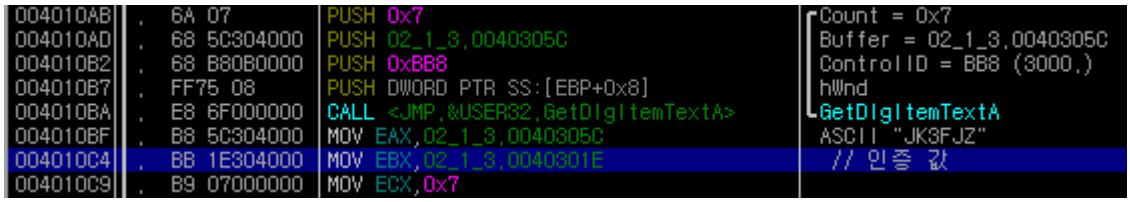
키 입력 없이 실행 가능

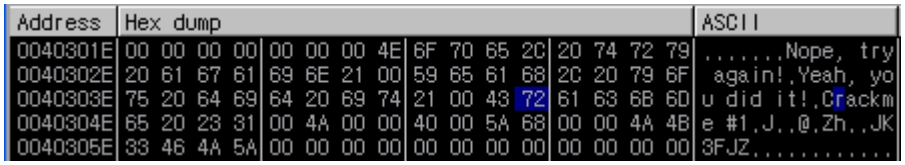


- 인증 루틴

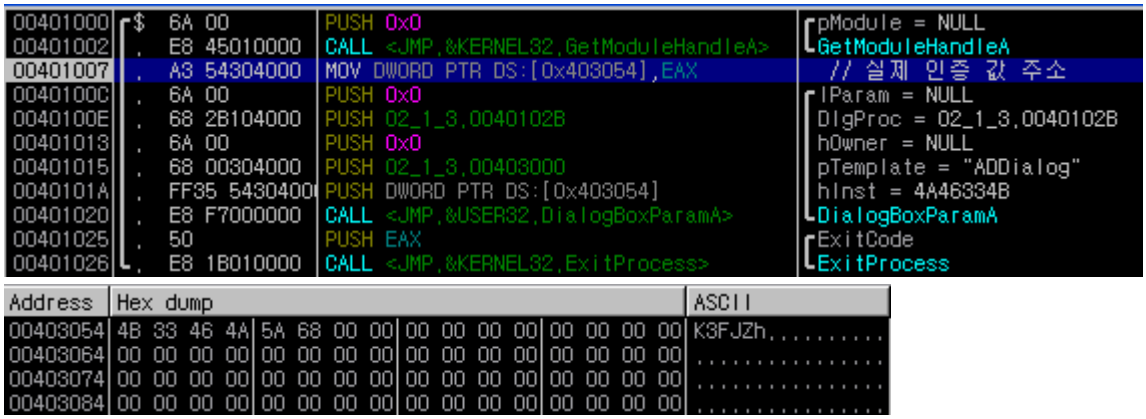
입력 받은 값 7byte를 0040301e값과 비교한다. 실제 0040301e값에는 00 00 00 00 00 00 00값으로

인증 값 입력 없이 인증이 가능 하다





복원된 파일 실행 시 실제 인증 값(웹에서 정답)으로 사용되는 JK3FJZh 값을 덮어 쓰게 된다



00403054 주소 값의 4b 33 46 4a값에 핸들 값을 씀으로 아래와 같이 00 00 40 00 으로 수정되어다.