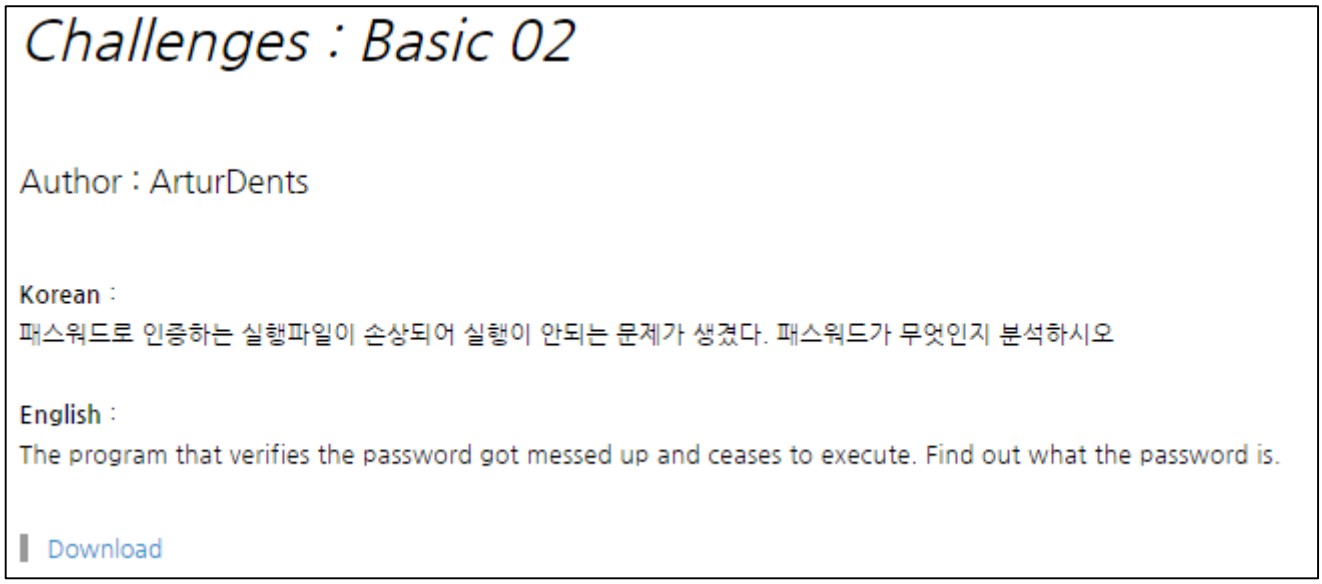
Code Engn Challenges : Basic 02 풀이 보고서

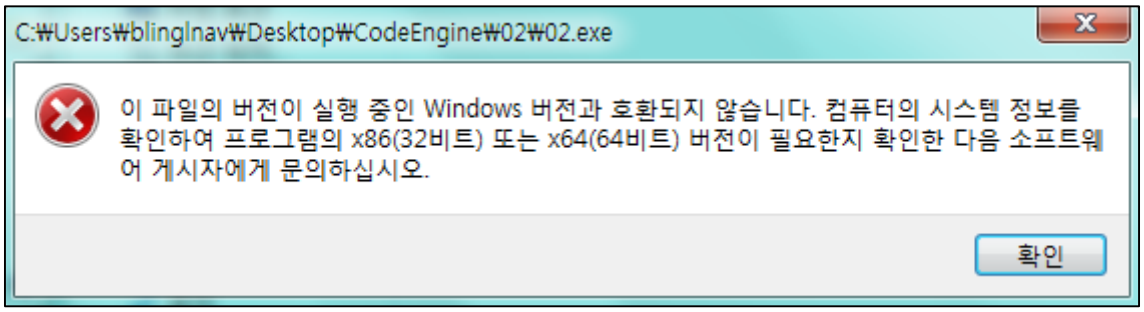
blinglnav

문제



풀이

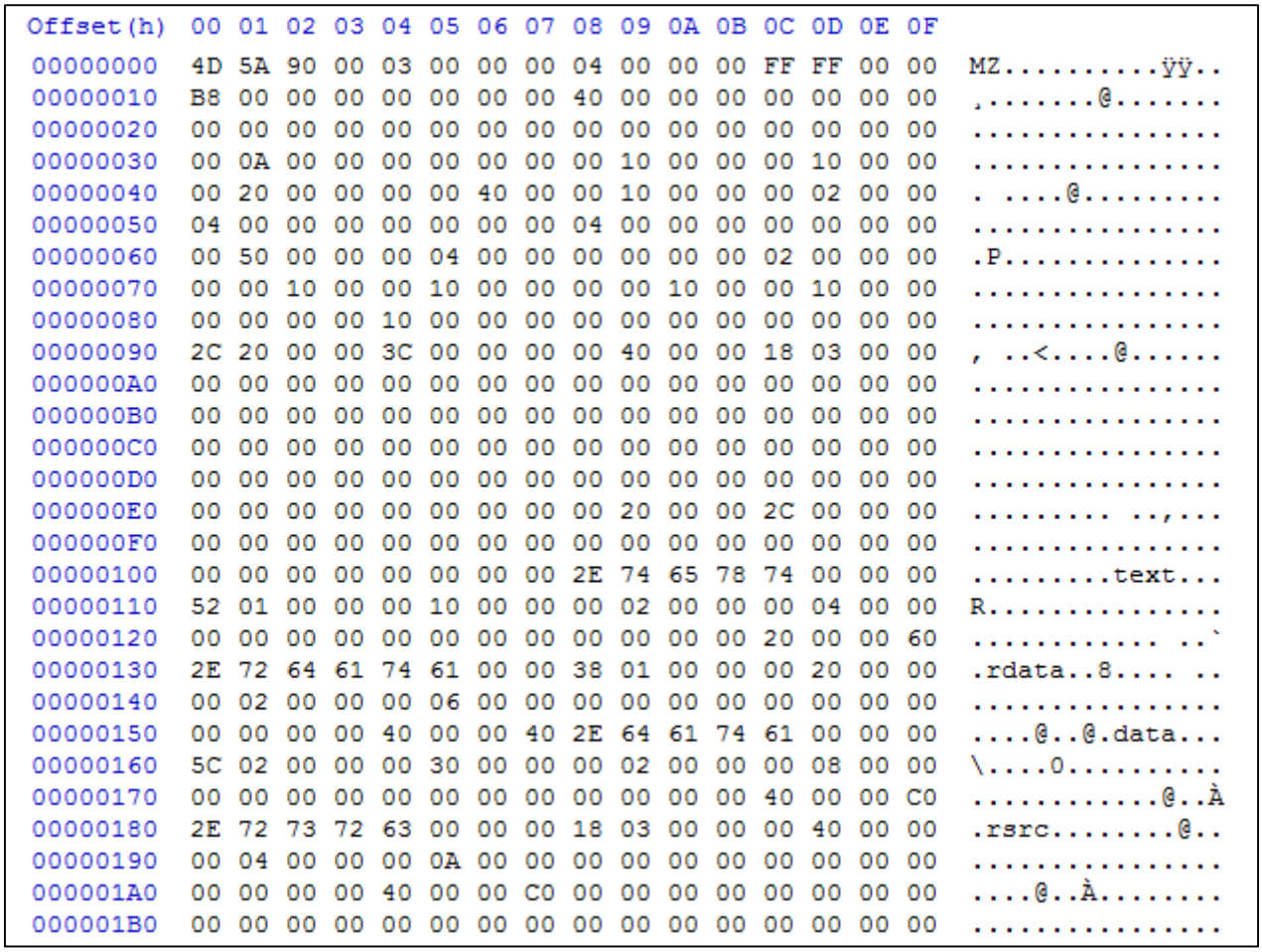
역시 실행해보자. (문제에서 실행파일이 손상되었다고 했기 때문에 아마도 실행이 안될 것이다.)



<역시 안된다>

실행 문제는 PE Header 손상일 가능성이 크다. 하지만 난이도가 Basic인데 설마 PE Header를 복구하라고 하진 않을 듯하기도 하고, 한다 하더라도 자신이 없으므로 노가다로 찾아보자.

HxD와 같은 Hex Editor로 실행파일을 연다.



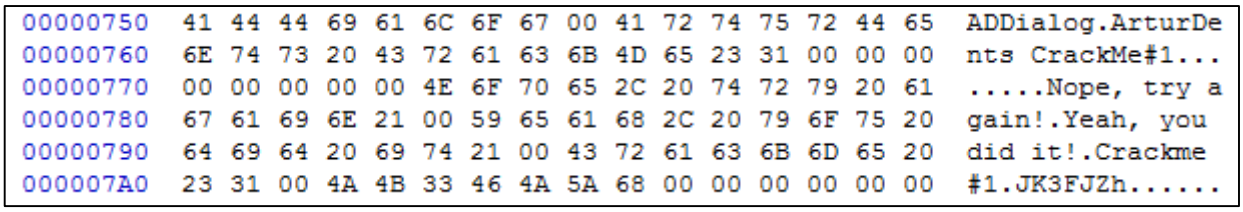
```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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...
00000110   52 01 00 00 00 10 00 00 00 02 00 00 00 04 00 00  R...............
00000120   00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
00000130   2E 72 64 61 74 61 00 00 38 01 00 00 00 20 00 00  .rdata..8.... ..
00000140   00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00  ................
00000150   00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00  ....@..@.data...
00000160   5C 02 00 00 00 30 00 00 00 02 00 00 00 08 00 00  \....0..........
00000170   00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  ............@..À
00000180   2E 72 73 72 63 00 00 00 18 03 00 00 00 40 00 00  .rsrc........@..
00000190   00 04 00 00 00 0A 00 00 00 00 00 00 00 00 00 00  ................
000001A0   00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00  ....@..À........
000001B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

DOS Header, PE Header, Section Header가 보인다. 이미지에서 'P"E"₩0"₩0'이 보이지 않는 것으로 보아 아마도 PE Signature 쪽을 손상시킨 것 같다.

어쨌든, 실행파일에 특별한 조작을 가하지 않았다면 Password는 .rsrc 섹션에서 찾을 수 있을 것이다.

쭉 스크롤을 내리면 프로그램에서 출력될 것으로 추정되는 문자열들이 보입니다.



```
00000750   41 44 44 69 61 6C 6F 67 00 41 72 74 75 72 44 65  ADDialog.ArturDe
00000760   6E 74 73 20 43 72 61 63 6B 4D 65 23 31 00 00 00  nts CrackMe#1...
00000770   00 00 00 00 00 4E 6F 70 65 2C 20 74 72 79 20 61  .....Nope, try a
00000780   67 61 69 6E 21 00 59 65 61 68 2C 20 79 6F 75 20  gain!.Yeah, you
00000790   64 69 64 20 69 74 21 00 43 72 61 63 6B 6D 65 20  did it!.Crackme
000007A0   23 31 00 4A 4B 33 46 4A 5A 68 00 00 00 00 00 00  #1.JK3FJZh......
```

여기에서 특별한 의미를 갖지 않는 JK3FJZh가 Auth Key로 추정됩니다.

Auth 창에서 넣고 submit하면 성공

Auth Key JK3FJZh