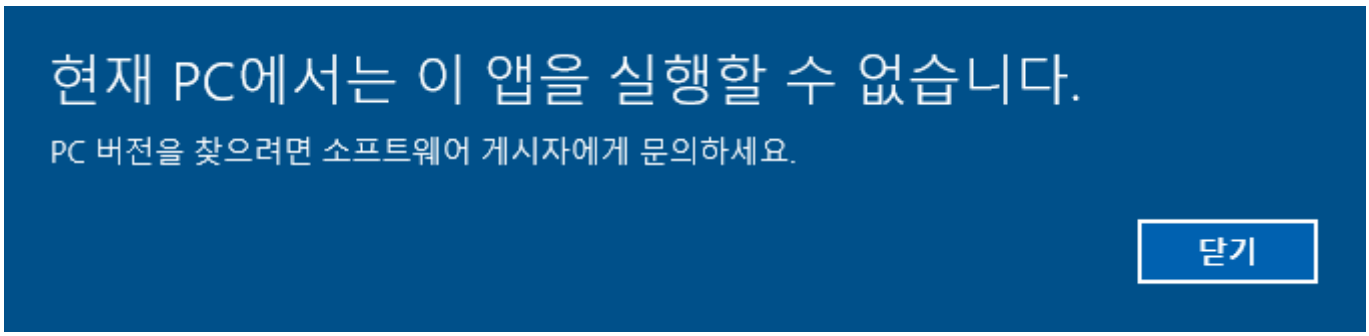
codeengn-basic-L02 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 11. 09:48

문제를 시작하기 전, 되새김질을 하겠습니다.

디버거로 파일을 열어야한다는 고정관념을 버릴 필요가 있음
계속 왜 파일이 열리지 않는지를 고칠 생각을 했음
풀이를 보고 HxD로 봐야 한다는 것을 알았음

문제를 받고 디버거로 열어보려 하니,



문제가 열리지 않는다. 나는 이게 왜 열리지 않는지를 고치기 위해 구글링을 했었다...

HxD로 까보면,

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

4D 5A가 반겨주는데, 4D와 5A는 이것이 PE구조의 프로그램인 것을 나타내면서,

MS-DOS의 개발자였던 Mark Zbikowski의 머리글자를 딴 것이라고 한다.

더 아래로 내리다보면,

```
000005C0   00 00 00 00 C0 20 00 00 B2 20 00 00 F0 20 00 00  ....A ..² ..ð ..
000005D0   A6 20 00 00 D2 20 00 00 94 20 00 00 E0 20 00 00  ¦ ..Ò ..” ..à ..
000005E0   00 00 00 00 92 00 44 69 61 6C 6F 67 42 6F 78 50  ....’.DialogBoxP
000005F0   61 72 61 6D 41 00 B8 00 45 6E 64 44 69 61 6C 6F  aramA.¸.EndDialo
00000600   67 00 00 01 47 65 74 44 6C 67 49 74 65 6D 00 00  g...GetDlgItem..
00000610   02 01 47 65 74 44 6C 67 49 74 65 6D 54 65 78 74  ..GetDlgItemText
00000620   41 00 BB 01 4D 65 73 73 61 67 65 42 6F 78 41 00  A.».MessageBoxA.
00000630   10 02 53 65 6E 64 4D 65 73 73 61 67 65 41 00 00  ..SendMessageA..
00000640   2B 02 53 65 74 46 6F 63 75 73 00 00 55 53 45 52  +.SetFocus..USER
00000650   33 32 2E 64 6C 6C 00 00 75 00 45 78 69 74 50 72  32.dll..u.ExitPr
00000660   6F 63 65 73 73 00 11 01 47 65 74 4D 6F 64 75 6C  ocess...GetModul
00000670   65 48 61 6E 64 6C 65 41 00 00 4B 45 52 4E 45 4C  eHandleA..KERNEL
00000680   33 32 2E 64 6C 6C 00 00 00 00 00 00 00 00 00 00  32.dll..........
00000690   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

중간중간 메시지박스 형태가 보인다. 더 내려보겠다.

```
00000740   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
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......
000007B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

플래그가 발견되었다. {JK3FJZh}

처음에 뭘 어떻게 해야 할 지 몰라서 풀이를 보고야 말았다

위에 말했던 것처럼 고정관념을 버려야 할 필요가 있겠다.

이렇게 배워나가는 것이라 생각한다 . 😁