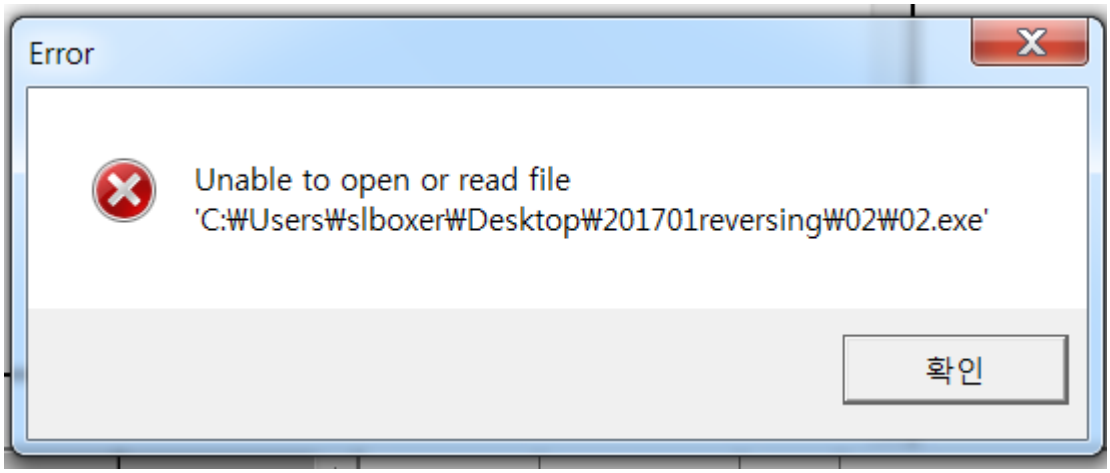
Korean :

패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :

The program that verifies the password got messed up and ceases to execute. Find out what the password is.

파일을 살리고 패스워드를 분석하는 문제같다.



흐음..손상되었다더니 진짜 에러가 난다.

실행 파일이 손상되었다면 뭔가 시그니처같은게 잘렸거나 하지 않았을까 싶어서 HxD를 틀었다.

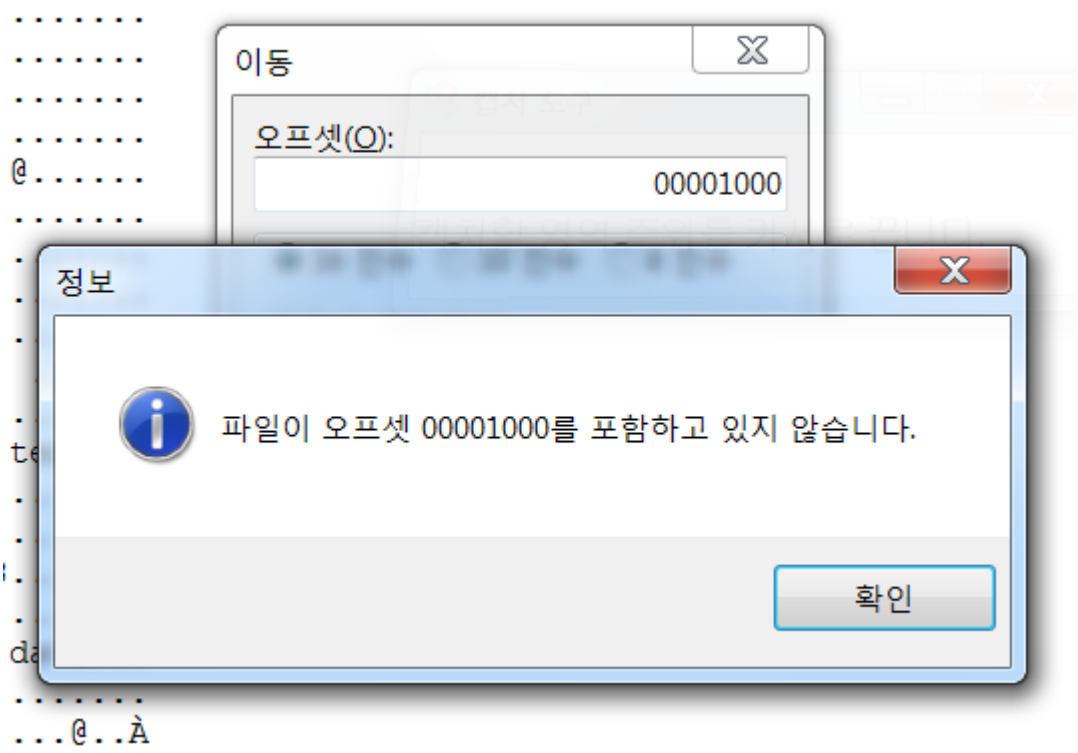
```
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 0A 00 00 00 00 00 00 00 10 00 00 00 10 00 00  ................
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  ................
```

pe파일이다.

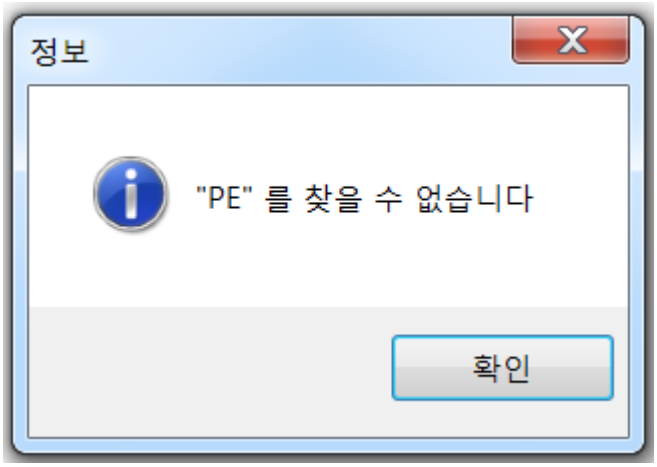
헤더를보면

```
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  ................
```

일단 dos header. e_magic인 MZ가 있고, 맨 끝에 4바이트는 e_lfanew의 것이다. 00 10 00 00은 리틀엔디안 표기이므로 제대로 읽으면 00 00 10 00. 그 위치로 가면NT header가 나올것이다.

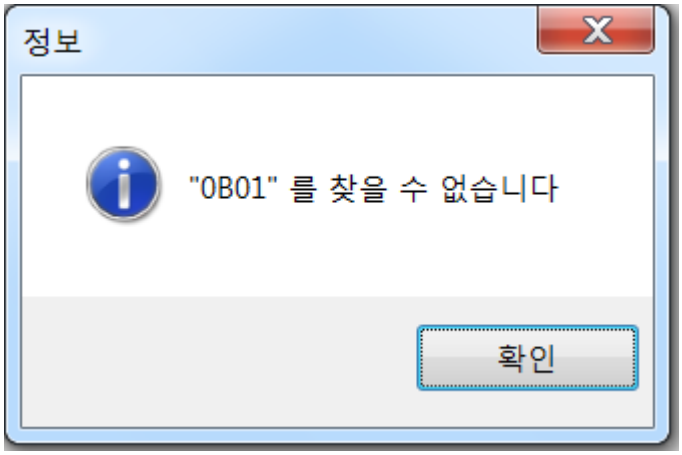


앗 근데 갈수 없다. 잘린 부분은 여기려나?



문자?텍스트?검색을 해봤는데 PE도 찾을 수 없었다. NT헤더도 소실되었다는 것.

그러면 넣어줘야 되려나...? 근데 파일마다 정보가 다르지 않을까....흠...



아니 없는게 왜이리 많아..!

Image Iptional Header 구조체의 시작부분도 없음을 볼 수 있다.

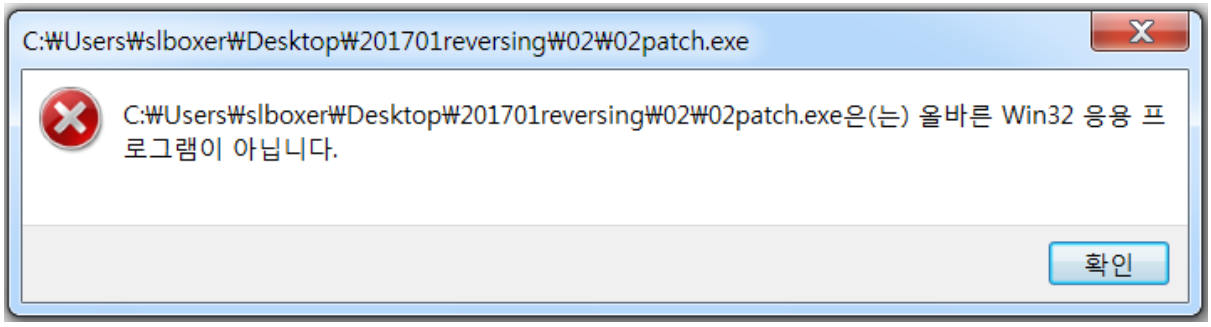
```
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 0A 00 00 00 00 00 00 00 10 00 00 00 10 00 00  ................
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  ................
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

전체 상태를 보면 이렇게 생겼는데, 싹다 0이고 .text랑 .data 그리고 .rsrc...이 나타나는걸 보면 여긴 섹션 헤더이다. 그러니까 이 앞에 있는 e_lfanew부터 NT헤더까지 다 잘렸다는 것이다. 아...

일단 긴가민가 하면서 notepad.exe를 열어 소실된 부분을 붙여넣기 해봤다.

```
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 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00  ............à...
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  50 45 00 00 4C 01 03 00 87 52 02 48 00 00 00 00  PE..L...‡R.H....
000000F0  00 00 00 00 E0 00 0F 01 0B 01 07 0A 00 78 00 00  ....à........x..
00000100  00 8C 00 00 00 00 00 00 9D 73 00 00 00 10 00 00  .Œ.......s......
00000110  00 90 00 00 00 00 00 01 00 10 00 00 00 02 00 00  ................
00000120  05 00 01 00 05 00 01 00 04 00 00 00 00 00 00 00  ................
00000130  00 40 01 00 00 04 00 00 CE 26 01 00 02 00 00 80  .@......Î&.....€
00000140  00 00 04 00 00 10 01 00 00 00 10 00 00 10 00 00  ................
00000150  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  04 76 00 00 C8 00 00 00 00 B0 00 00 04 83 00 00  .v..È....°...ƒ..
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 50 13 00 00 1C 00 00 00  ........P.......
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 A8 18 00 00 40 00 00 00  ........¨...@...
000001B0  50 02 00 00 D0 00 00 00 00 10 00 00 48 03 00 00  P...Ð.......H...
000001C0  00 00 00 00 00 00 00 20 00 00 2C 00 00 00 00 00  ....... ..,.....
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 2E 74 65 78 74 00 00 00 52 01  .......text...R.
000001F0  00 00 00 10 00 00 00 02 00 00 00 04 00 00 00 00  ................
```

그리고 저장후 실행....



아앗 잘못되었다

아니면 아까 붙여넣을 때 파일크기가 변경된댔는데 그것때문인가?

그래서 붙여넣을 때 변경된 파일크기만큼 padding영역을 지워봤다.

그러나 소용없었다고 한다...

대체 왜그러는거지...orz

조금 내려가다 보니 이런 데이터 영역이 나타났다.

```
000005C0  00 00 00 00 C0 20 00 00 B2 20 00 00 F0 20 00 00  ....À ..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  ................
000006A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000700  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000710  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000720  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000730  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
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
```

비밀번호 알아내면 Yeah 부분이 나올것으로 예상된다. 그 비밀번호는 음...옆에 보니까 비밀번호스러운 문자인 JK3FJZh같은데....뭐지 이런식으로 풀릴 리가 없는데...?ㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋㅋ

비밀번호는 JK3FJZh 로 예상, 그러나 파일을 살려서 검증하는건 하지 못했다고 한다..