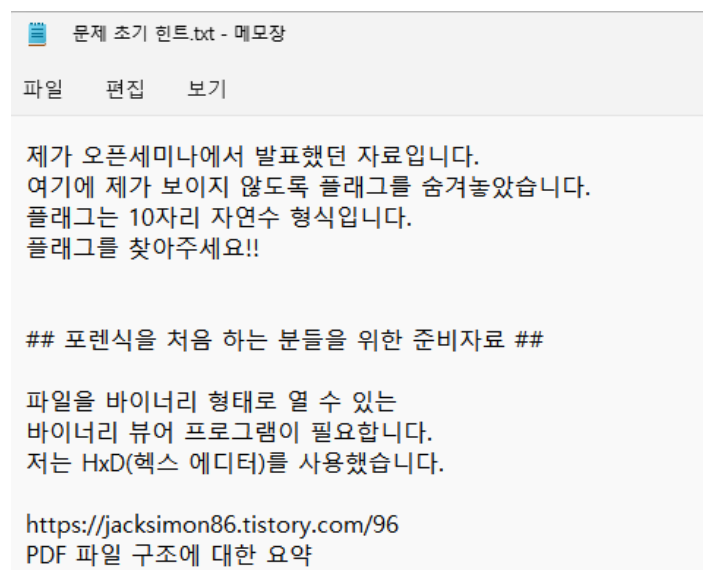


About KEEPER 문제

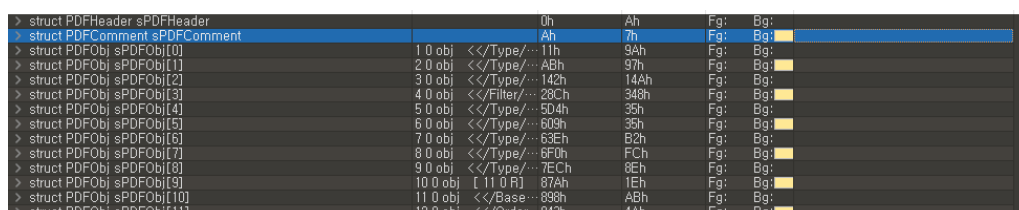
2021-03-30 강승민



파일을 확인했을 때 사진과 같이 일반적인 pdf 파일로 정상적으로 읽히고 보이는 것을 확인할 수 있다. 이를 봤을 때 flag를 어떻게 찾아야 할지 감이 안 잡혀서 힌트를 봤더니



이와 같이 바이너리 뷰어를 이용하라는 힌트를 주셨다. 그래서 010Editor로 보았다.



010Editor의 기능으로 pdf파일이 자동으로 분석되어 보여진다.

```

> struct PDFTrailer sPDFTrailer[1]
CF889h Bh Fg: Bg:
> struct PDFUnknown sPDFUnknown
CF894h E1D8h Fg: Bg:

```

이중 위 그림과 같이 PDF파일의 구조가 아니라서 Unknown으로 표기되는 부분이 마지막에 포함되어 있어 보았더니

```

C:F880h: 0A 38 34 39 38 37 37 0D 0A 25 25 45 4F 46 89 50 .849877...%EOF%P
C:F890h: 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 NG...|....IHDR..
C:F8A0h: 02 55 00 00 01 76 08 02 00 00 00 C8 B4 FA E0 00 U...v...E'ú

```

이와 같이 PNG파일의 헤더부분이 보였다.

```

0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
0010h: 00 00 02 55 00 00 01 76 08 02 00 00 00 C8 B4 FA ...U...v...E'ú
0020h: E0 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 à....sRGB.sI.e..
0030h: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..úa|..
0040h: 00 09 70 4B 59 73 00 00 12 74 00 00 12 74 01 DE ..pHYs...t...t.B
0050h: 66 1F 78 00 00 E1 73 49 44 41 54 78 5E EC BD 85 E.x...ásIDATx^i%
0060h: 63 54 C7 FB F6 FD FC 0B EF FB 3E BF DF F7 5B 88 cTÇûöýü.iû>¿ß÷[^
0070h: EC 6E 3C EB 1B C1 A9 BB BB 2B 2D AE 71 F7 E0 6E ìn<ë.Á@»»+-@q÷àn
0080h: 2D 6D 29 35 A8 52 A5 50 DA 42 85 2A 2D 45 8B BB -m) 5`R¥PÚB...*-E<»
0090h: 3B D1 F5 CD BC D7 3D 73 76 B3 59 4B 02 69 0B C9 ;Ñõí¼×=sv³YK.i.É
00A0h: 7C 3A 0D 67 CF 19 3F C9 7D ED 3D 67 66 CE FF 61 |:.gI.?É)i=gfiÿa
00B0h: 12 89 44 22 91 F4 3C A4 FE 49 24 12 89 A4 27 22 .%D" 'ô<xpI$.%#'"
00C0h: F5 4F 22 91 48 24 3D 11 A9 7F 12 89 44 22 E9 89 ÕO" 'H$=.©...%D"é%
00D0h: 48 FD 93 48 24 12 49 4F 44 FA 9F 44 22 91 48 7A Hý"HS.TODâÿD" 'Hz

```

그래서 그림과 같이 아래 부분을 다 복사하여 PNG 파일로 만들어보았더니



이러한 FLAG를 얻을 수 있었다.