PDF message

Problem: The pdf file signatures seem odd in this

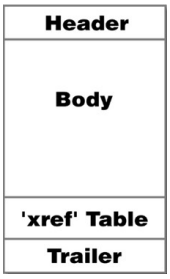
Hint: Hex edit

Given: Fall-of-Roman-Empire.pdf

Note: Recommended hex editor ‘Bless Hex Editor’
http://home.gna.org/bless/

Add link for magic number
‘file’ command

Steps:
1) Given a pdf that seems to be just an ordinary pdf. It opens and displays just like any other pdf. Pdf files have the structure shown bellow.



The header is the first line of a pdf and identifies the type of file. For a pdf the beginning marker is ‘%PDF-1.4’ The trailer contains the end of file marker, for this file it is ‘%%EOF’

2) So, we load the pdf into the editor tool “bless”. When looking at only the very beginning and very end of the document inside of the hex editor, we find the normal header “%PDF-1.4”, but the trailer is missing.

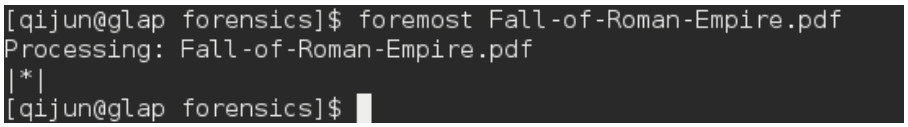
```
00000000 25 50 44 46 2D 31 2E 34 0A 25 C3 A4 C3 BC C3 B6 C3 9F 0A 32 20 30 %PDF-1.4.%.........2 0
00000016 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68 20 33 20 30 20 52 2F 46  obj.<</Length 3 0 R/F

0004d210 DF EE 8D 9F 55 86 89 93 81 F8 7F 69 2B B9 4B 8E 5D AA 62 FA 30 23 ....U......i+.K.].b.0#
0004d226 6C F1 05 0E 13 61 98 A4 87 D0 55 25 81 26 40 A8 A4 9F F7 07 FF D9 l....a....U%.&@.......
0004d23c
```

3) So, we search the trailer “%%EOF”, and find it somewhere in the middle of the file.

```
0004a508 0A 33 30 32 30 39 37 0A 25 25 45 4F 46 0A FF D8 FF E0 00 10 4A 46 .302097.%%EOF.......JF
0004a51e 49 46 00 01 01 01 00 48 00 48 00 00 FF FE 00 13 43 72 65 61 74 65 IF.....H.H......Create
```

4) But, we find “JFIF” after the trailer. Hence, it could be another file simply appended to the end of the original pdf file. The appended file could be an image JPEG. Here is a list of file signatures at https://en.wikipedia.org/wiki/List_of_file_signatures. A JPEG file starts with “FFD8”. So, we copy all data starting from “FFD8” to the end to another file to get the flag…

Alternative solutions:
1) There are many handful forensic tools to detect hidden files. One is “foremost”. Simply run “foremost given_file”, and it will try to find files with known signatures inside the given file.



2) Then, we look into the folder “output” produced by “foremost” in default to get the flag…