PDF markers

Problem: Is a file hidden in this pdf file?

Hint: file or File?

Given: french-rev.pdf

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

Steps:
1) The given pdf file seems to be just an ordinary pdf. It opens and displays just like any other pdf. We run "foremost" on the file and don't have anything.

2) Because the problem mentions "a file hidden" and the hint also mentioned "file or File", it appears that there is a file in the given pdf. So, we may need to extract a file embedded inside the given pdf. There are several tools to parse the structure and embedded objects of the given pdf file. We use "pdf-parser" downloaded from https://blog.didierstevens.com/programs/pdf-tools/. Run the tool with the given pdf file is below. It shows a long list of object in the pdf file.

```
[qijun@glap forensics]$ ./pdf-parser.py french-rev.pdf
PDF Comment '%PDF-1.6\r'

PDF Comment '%\xe2\xe3\xcf\xd3\r\n'

obj 637 0
 Type: /ObjStm
 Referencing:
 Contains stream

  <<
    /Filter /FlateDecode
    /First 717
    /Length 1030
    /N 82
    /Type /ObjStm
  >>
```

(3) Now, we need to narrow down our search. Since "file" is mentioned a lot of times in the problem, we search "file" in the parsed result. The command is "./pdf-parser.py french-rev.pdf | grep -i file".

```
    /FontFile 330 0 R
    /FontFile 335 0 R
    /FontFile 340 0 R
    /FontFile 344 0 R
    /FontFile 347 0 R
    /FontFile 351 0 R
    /FontFile 341 0 R
    /FontFile 358 0 R
    /Creator (Adobe Acrobat 8.1 Combine Files)
    /Embeddedfiles 631 0 R
    /Names '[(ADBE::FileAttachmentsCompatibility\x00)633 0 R]'
    /JS '(var v = app.viewerVersion;\\nif \\(v < 7\\)\\n{\\n\tv
```

(4) In the screenshot, we can see an interesting “Embeddedfiles” word. It appears to indicate there is an embedded file in the given pdf. But, we need to figure out the reason why we cannot see the file. So, we search Embeddedfiles and are pointed to the PDF reference at http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf
Then, we search “embeddedfiles” in the reference and get the following result.

EmbeddedFiles	name tree	*(Optional; PDF 1.4)* A name tree mapping name strings to file specifications for embedded file streams (see Section 3.10.3, “Embedded File Streams”).

(5) We notice the difference of “Embeddedfiles” in the given pdf and “EmbeddedFiles” in the pdf reference. Surely, PDF reader cannot recognize “Embeddedfiles”. That is the reason why the embedded file is not shown in PDF reader. Hence, we use hex editor “bless” to change “Embeddedfiles” to “EmbeddedFiles” to get the flag…