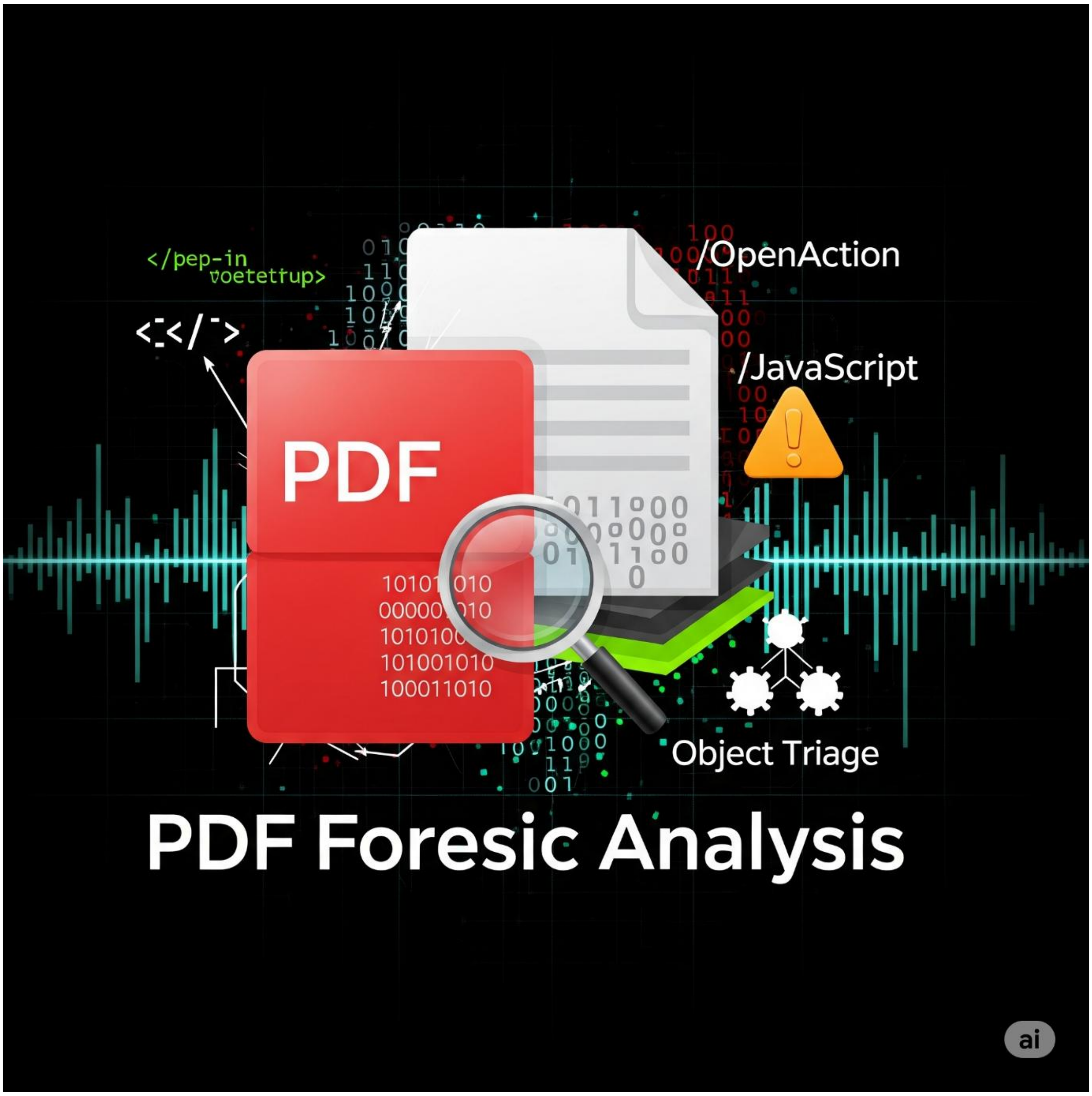
Day 12 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: PDF Forensic Tool



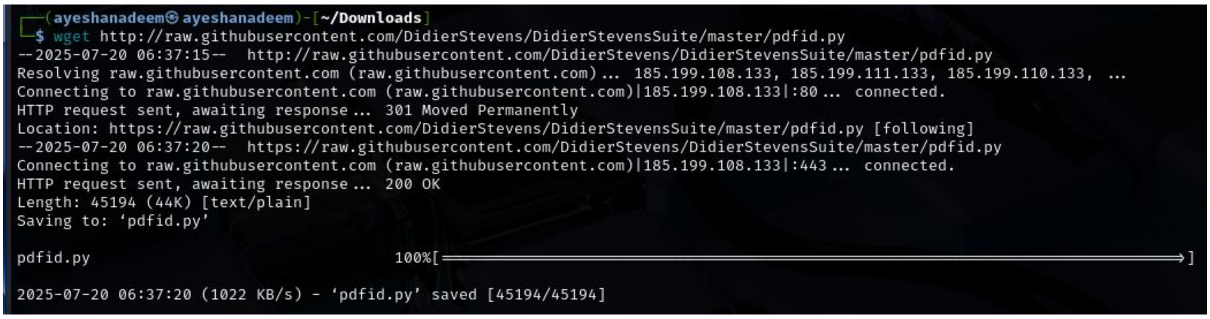
Contact Me: ayeshanm8@gmail.com

Date: 12th July, 2025

PDF Forensic Tools

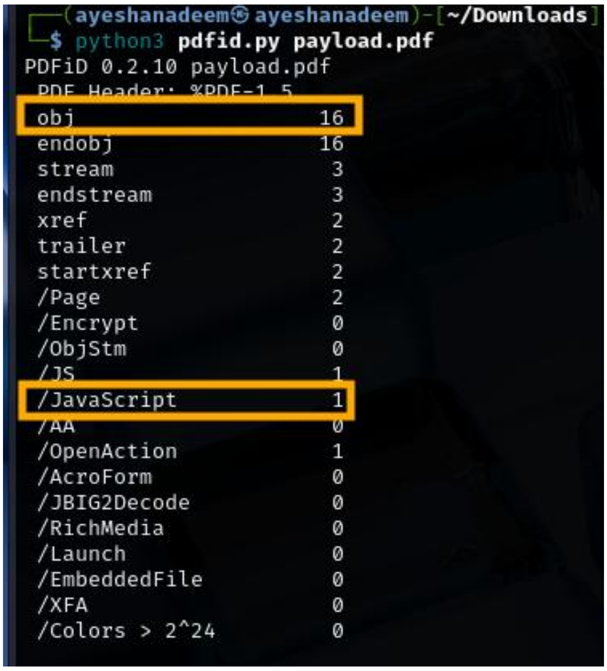
Tool 1 pdfid.py

Command 1:



```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ wget http://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/pdfid.py
--2025-07-20 06:37:15--  http://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/pdfid.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/pdfid.py [following]
--2025-07-20 06:37:20--  https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/pdfid.py
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45194 (44K) [text/plain]
Saving to: ‘pdfid.py’

pdfid.py                    100%[=====================================================================>]

2025-07-20 06:37:20 (1022 KB/s) - ‘pdfid.py’ saved [45194/45194]
```

Command 2:

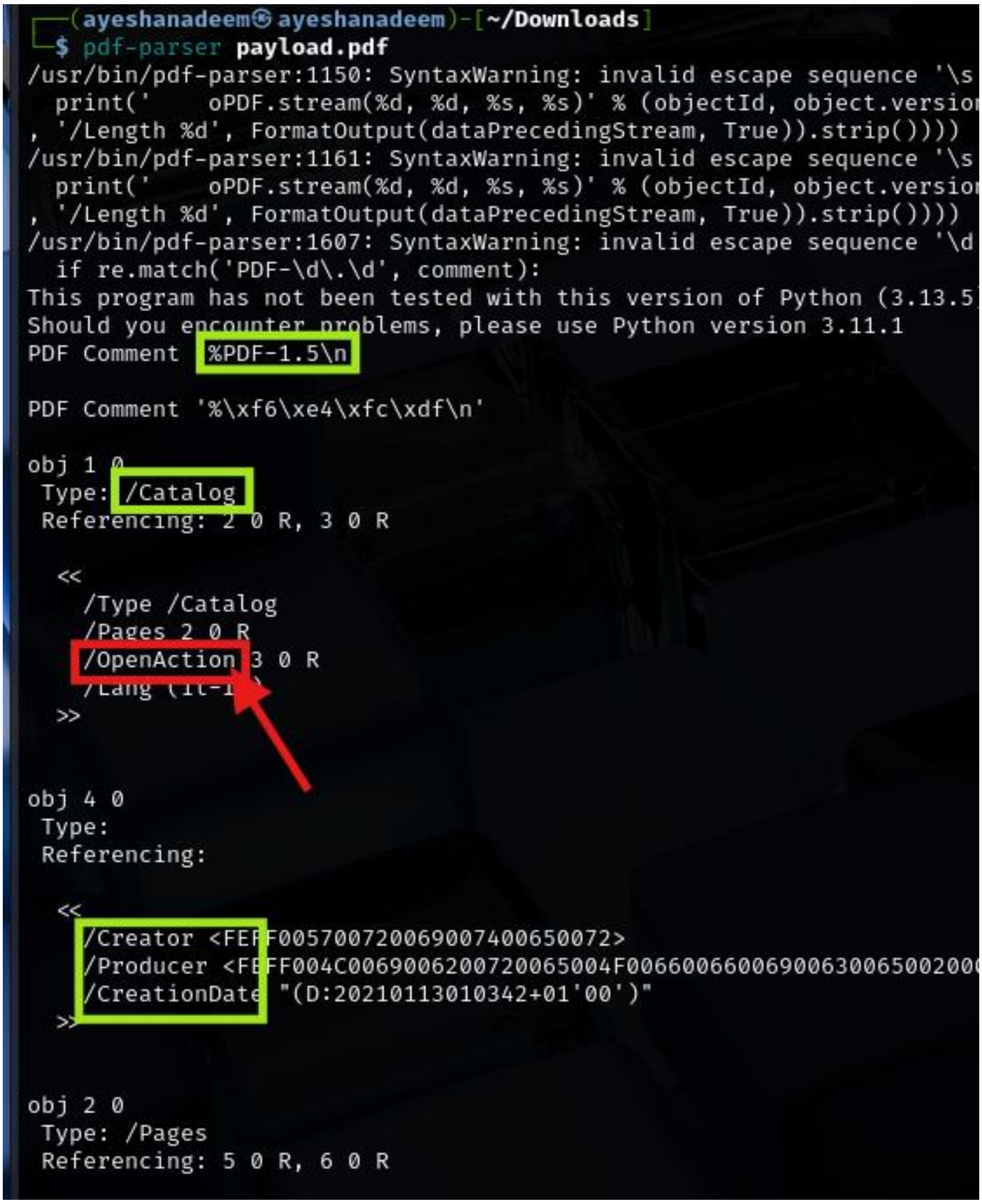


```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ python3 pdfid.py payload.pdf
PDFiD 0.2.10 payload.pdf
 PDF Header: %PDF-1.5
 obj                   16
 endobj                16
 stream                 3
 endstream              3
 xref                   2
 trailer                2
 startxref              2
 /Page                  2
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /Colors > 2^24         0
```

Here Javascript is detected in pdf file

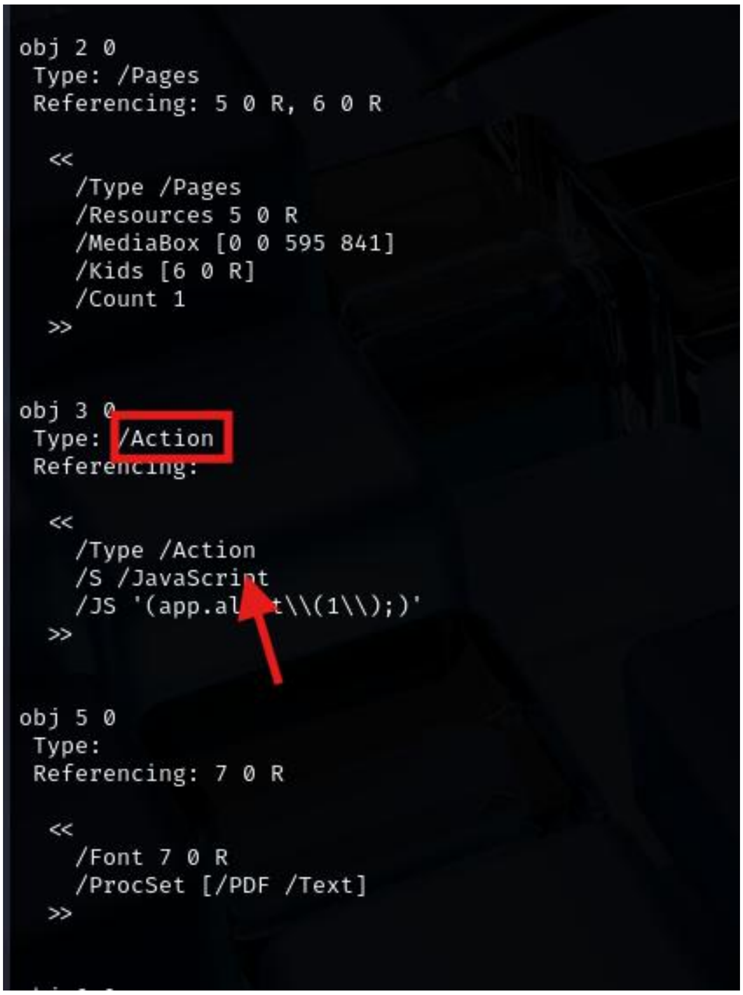
Tool 2 pdf-parser

Command 1:

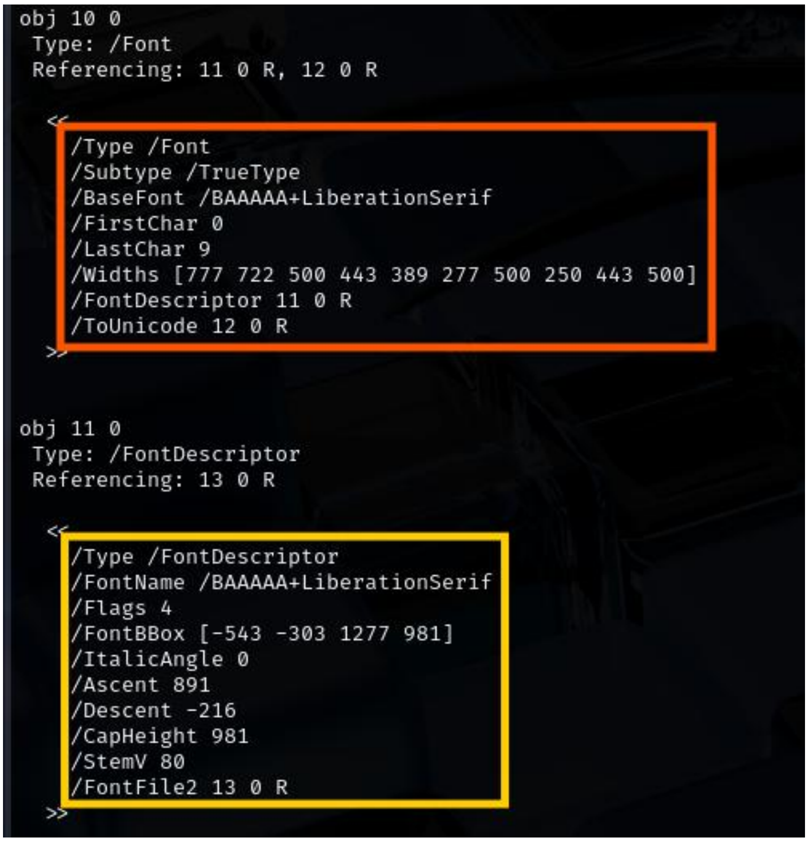


```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.versio
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.versio
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5
Should you encounter problems, please use Python version 3.11.1
PDF Comment  %PDF-1.5\n

PDF Comment '%\xf6\xe4\xfc\xdf\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R

  <<
    /Type /Catalog
    /Pages 2 0 R
    /OpenAction 3 0 R
    /Lang (it-I
  >>


obj 4 0
 Type:
 Referencing:

  <<
    /Creator <FEFF00570072006900740065072>
    /Producer <FEFF004C006900620072006500F0066006600690063006500200
    /CreationDate "(D:20210113010342+01'00')"
  >>


obj 2 0
 Type: /Pages
 Referencing: 5 0 R, 6 0 R
```

Here, objects like catalog, creator, producer, pages, lang, and type looks benign but Open Action look harmful (highlighted with red arrow). It might be start of javascript execution.

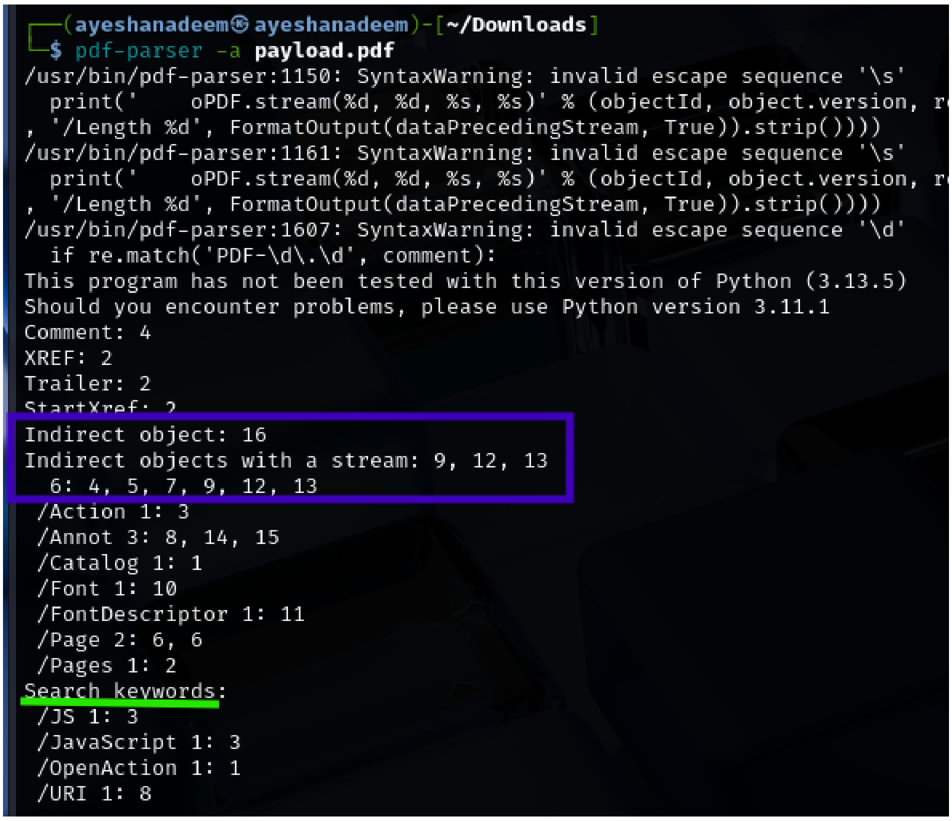


```
obj 2 0
 Type: /Pages
 Referencing: 5 0 R, 6 0 R

  <<
    /Type /Pages
    /Resources 5 0 R
    /MediaBox [0 0 595 841]
    /Kids [6 0 R]
    /Count 1
  >>


obj 3 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /JavaScript
    /JS '(app.alert\\(1\\);)'
  >>


obj 5 0
 Type:
 Referencing: 7 0 R

  <<
    /Font 7 0 R
    /ProcSet [/PDF /Text]
  >>
```



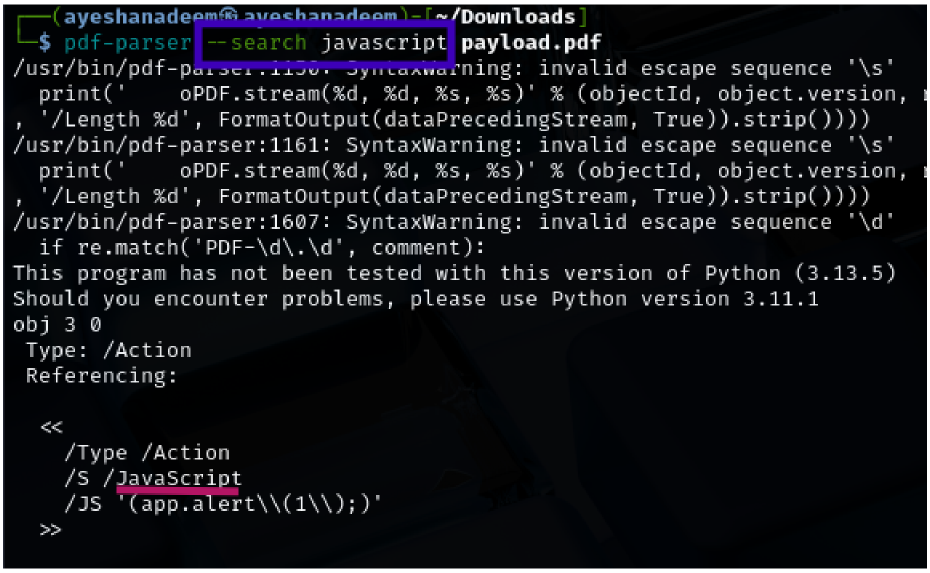
```
obj 10 0
 Type: /Font
 Referencing: 11 0 R, 12 0 R

  <<
    /Type /Font
    /Subtype /TrueType
    /BaseFont /BAAAAA+LiberationSerif
    /FirstChar 0
    /LastChar 9
    /Widths [777 722 500 443 389 277 500 250 443 500]
    /FontDescriptor 11 0 R
    /ToUnicode 12 0 R
  >>


obj 11 0
 Type: /FontDescriptor
 Referencing: 13 0 R

  <<
    /Type /FontDescriptor
    /FontName /BAAAAA+LiberationSerif
    /Flags 4
    /FontBBox [-543 -303 1277 981]
    /ItalicAngle 0
    /Ascent 891
    /Descent -216
    /CapHeight 981
    /StemV 80
    /FontFile2 13 0 R
  >>
```

Command 2:



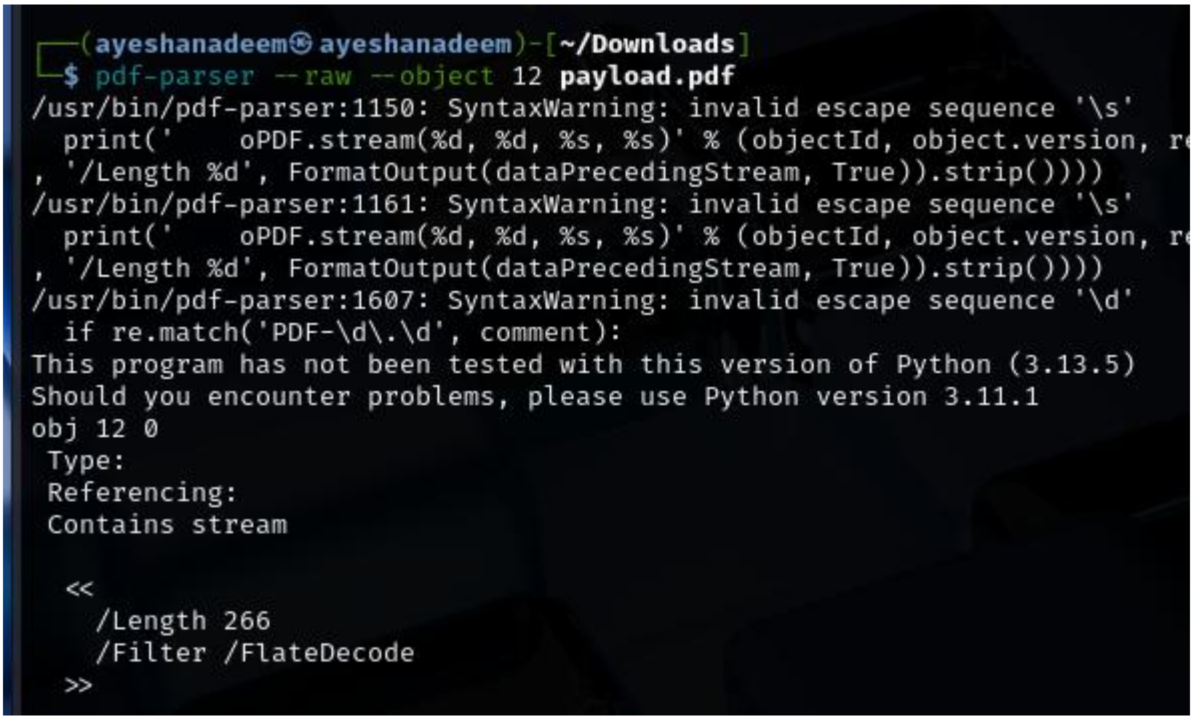
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser -a payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, r
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, r
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
Comment: 4
XREF: 2
Trailer: 2
StartXref: 2
Indirect object: 16
Indirect objects with a stream: 9, 12, 13
  6: 4, 5, 7, 9, 12, 13
 /Action 1: 3
 /Annot 3: 8, 14, 15
 /Catalog 1: 1
 /Font 1: 10
 /FontDescriptor 1: 11
 /Page 2: 6, 6
 /Pages 1: 2
Search keywords:
 /JS 1: 3
 /JavaScript 1: 3
 /OpenAction 1: 1
 /URI 1: 8
```

Command 3:



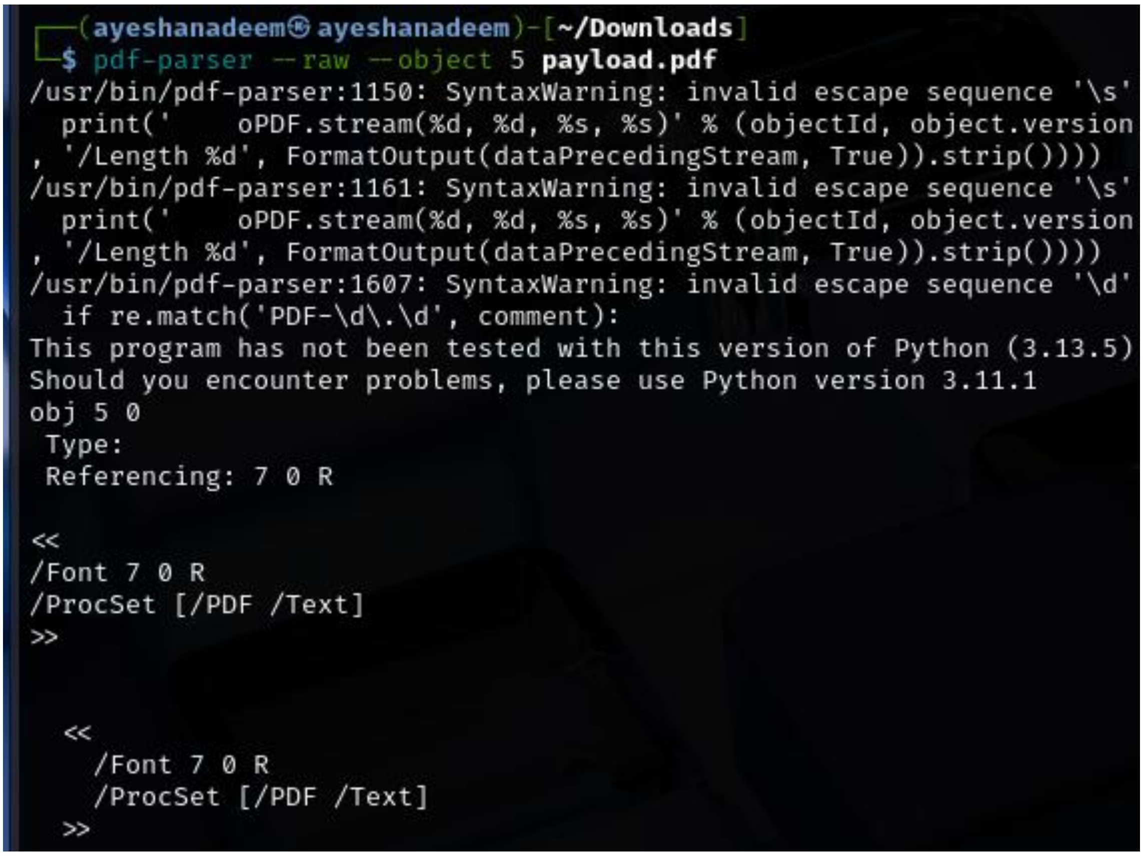
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser --search javascript payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version,
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version,
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
obj 3 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /JavaScript
    /JS '(app.alert\\(1\\);)'
  >>
```

Command 4:



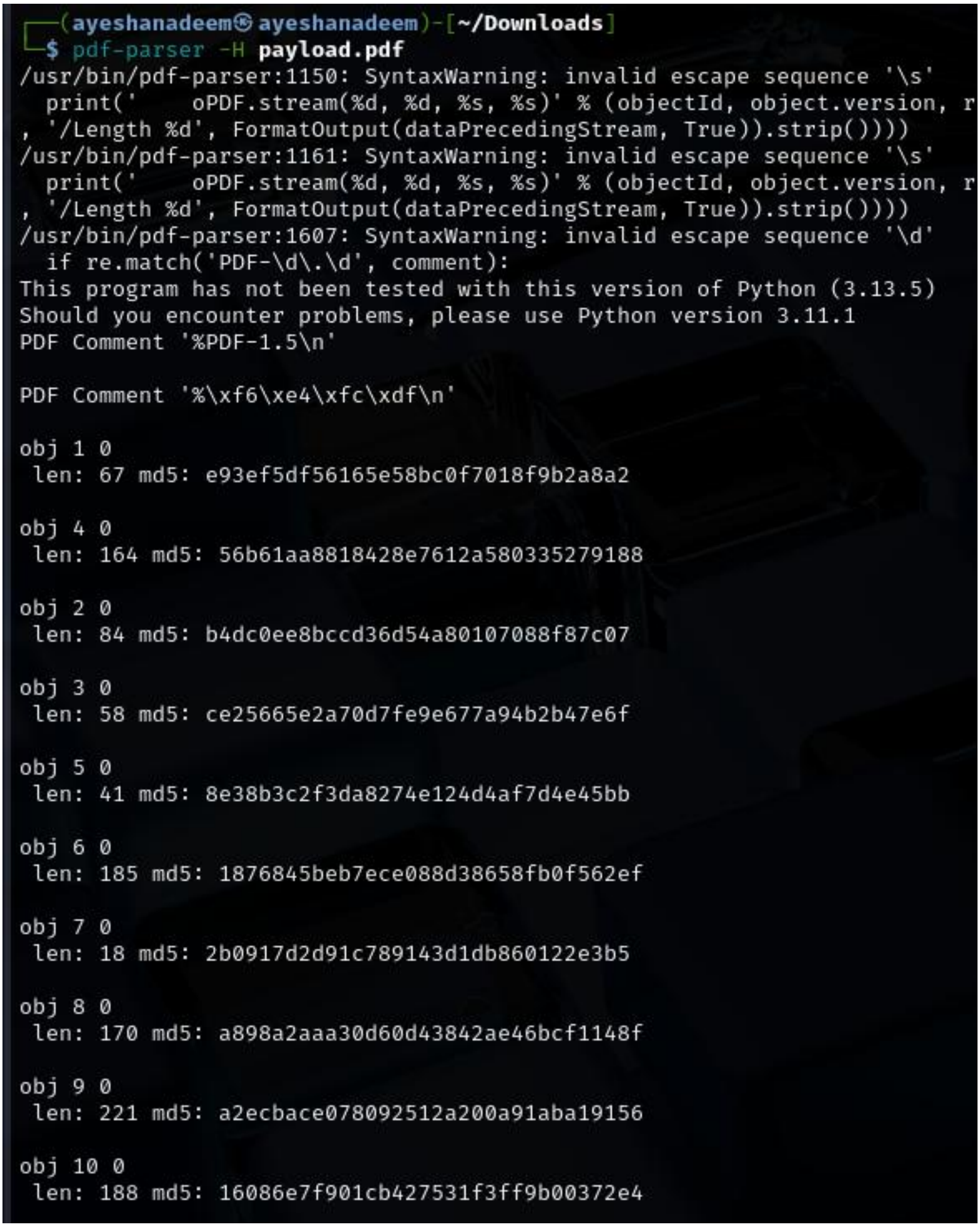
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser --raw --object 12 payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, re
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, re
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
obj 12 0
 Type:
 Referencing:
 Contains stream

  <<
    /Length 266
    /Filter /FlateDecode
  >>
```

Command 5:



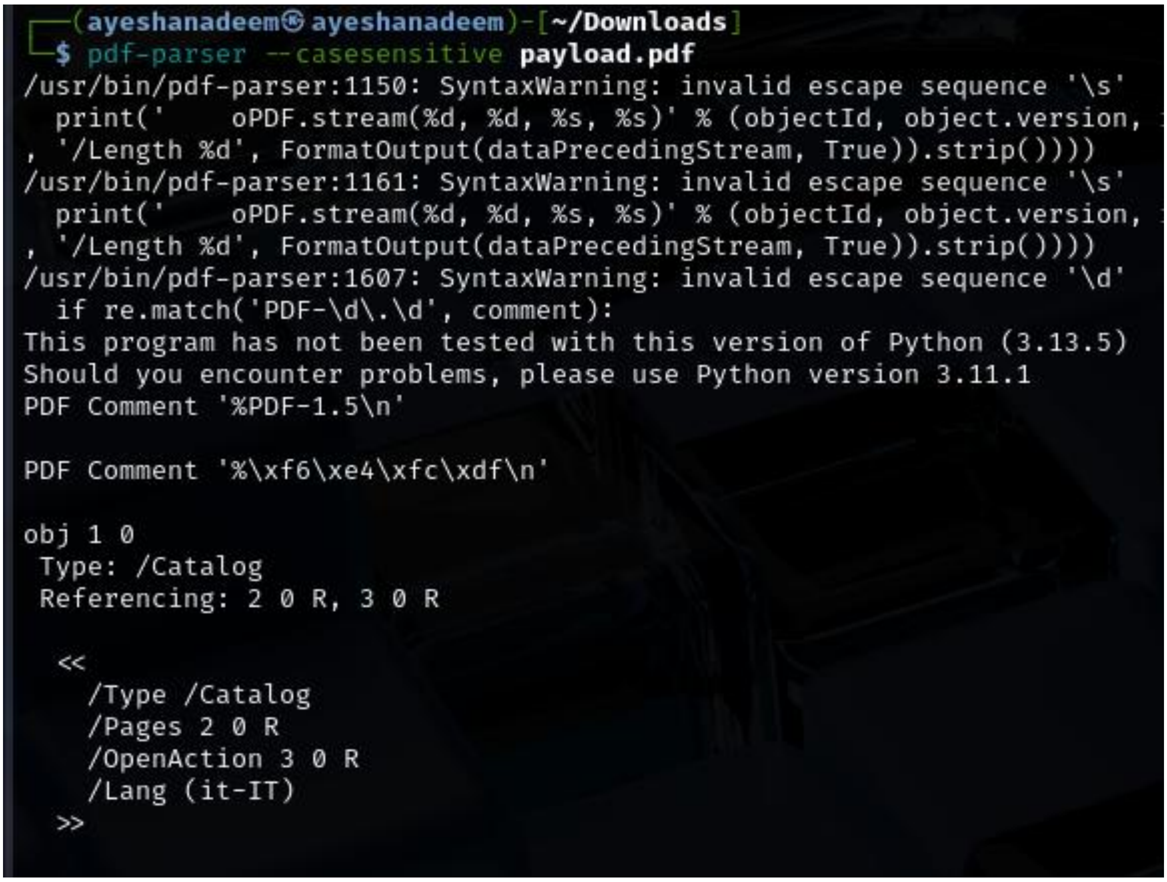
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser --raw --object 5 payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
obj 5 0
 Type:
 Referencing: 7 0 R

<<
/Font 7 0 R
/ProcSet [/PDF /Text]
>>


  <<
    /Font 7 0 R
    /ProcSet [/PDF /Text]
  >>
```

Command 6:



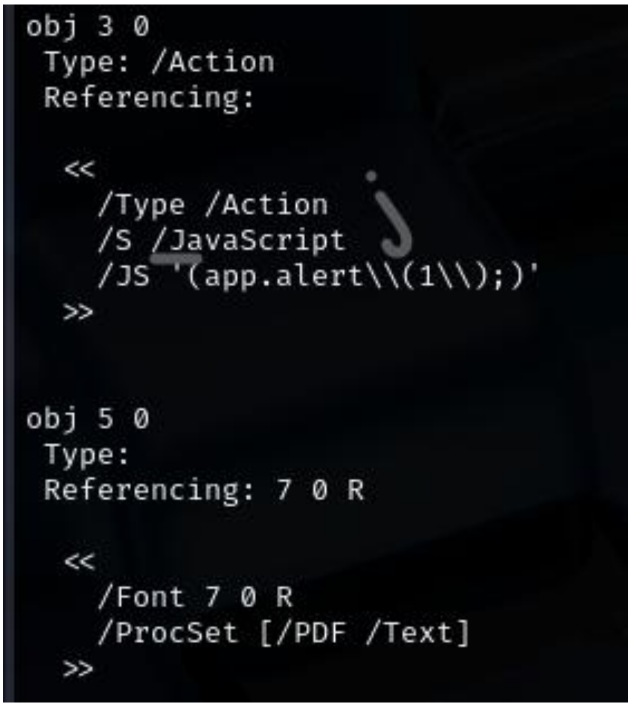
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser -H payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, r
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version, r
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
PDF Comment '%PDF-1.5\n'

PDF Comment '%\xf6\xe4\xfc\xdf\n'

obj 1 0
 len: 67 md5: e93ef5df56165e58bc0f7018f9b2a8a2

obj 4 0
 len: 164 md5: 56b61aa8818428e7612a580335279188

obj 2 0
 len: 84 md5: b4dc0ee8bccd36d54a80107088f87c07

obj 3 0
 len: 58 md5: ce25665e2a70d7fe9e677a94b2b47e6f

obj 5 0
 len: 41 md5: 8e38b3c2f3da8274e124d4af7d4e45bb

obj 6 0
 len: 185 md5: 1876845beb7ece088d38658fb0f562ef

obj 7 0
 len: 18 md5: 2b0917d2d91c789143d1db860122e3b5

obj 8 0
 len: 170 md5: a898a2aaa30d60d43842ae46bcf1148f

obj 9 0
 len: 221 md5: a2ecbace078092512a200a91aba19156

obj 10 0
 len: 188 md5: 16086e7f901cb427531f3ff9b00372e4
```

Command 7:



```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/Downloads]
└─$ pdf-parser --casesensitive payload.pdf
/usr/bin/pdf-parser:1150: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version,
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1161: SyntaxWarning: invalid escape sequence '\s'
  print('    oPDF.stream(%d, %d, %s, %s)' % (objectId, object.version,
, '/Length %d', FormatOutput(dataPrecedingStream, True)).strip())))
/usr/bin/pdf-parser:1607: SyntaxWarning: invalid escape sequence '\d'
  if re.match('PDF-\d\.\d', comment):
This program has not been tested with this version of Python (3.13.5)
Should you encounter problems, please use Python version 3.11.1
PDF Comment '%PDF-1.5\n'

PDF Comment '%\xf6\xe4\xfc\xdf\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R

  <<
    /Type /Catalog
    /Pages 2 0 R
    /OpenAction 3 0 R
    /Lang (it-IT)
  >>
```

Looks inside the PDF only for exact matches of a word or code (.exe virus), where uppercase and lowercase matters (e.g., "JavaScript" ≠ "javascript").



```
obj 3 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /JavaScript
    /JS '(app.alert\\(1\\);)'
  >>


obj 5 0
 Type:
 Referencing: 7 0 R

  <<
    /Font 7 0 R
    /ProcSet [/PDF /Text]
  >>
```