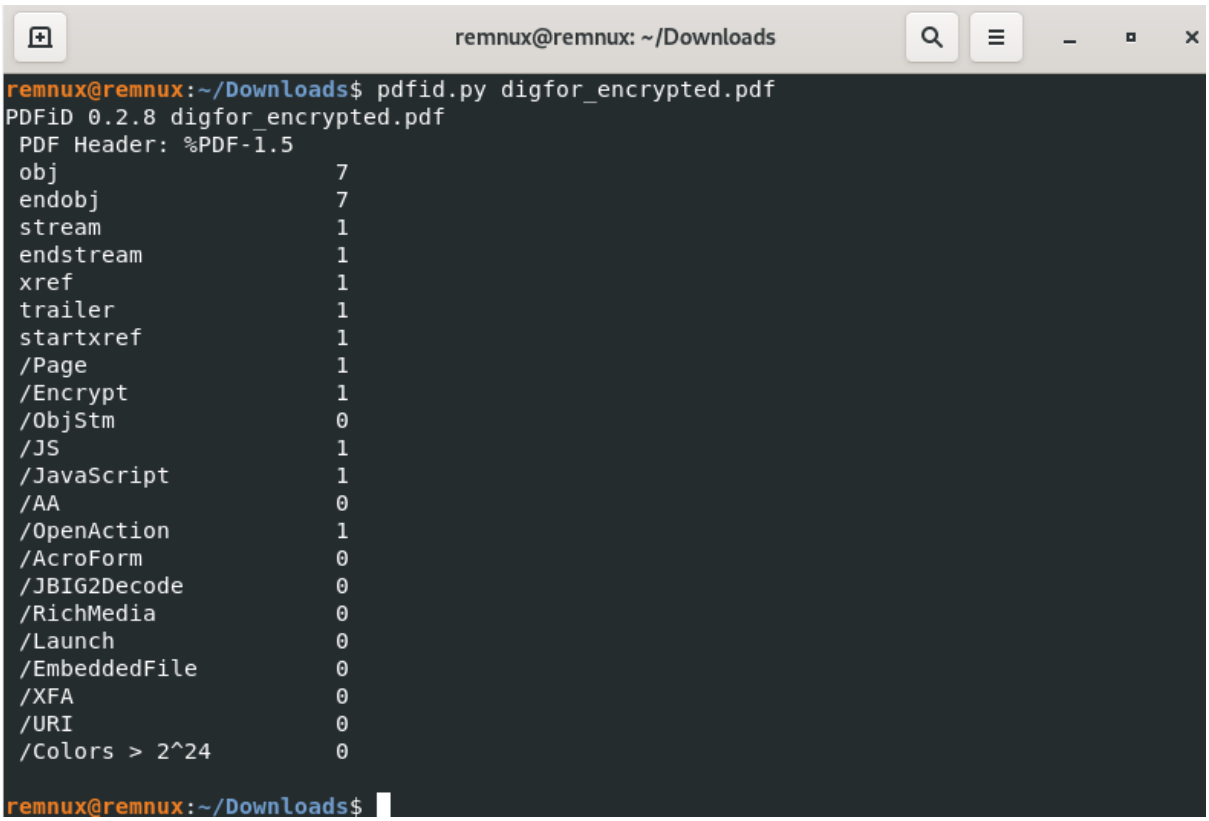
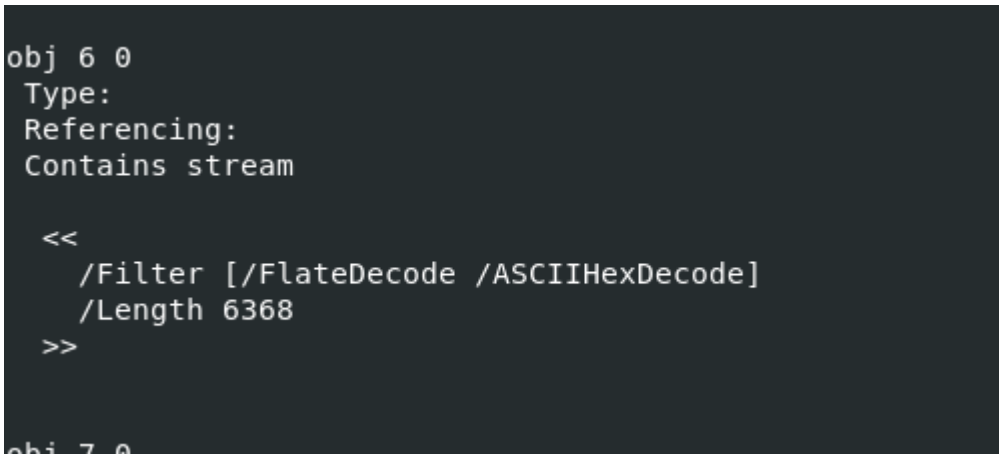
Malicious PDF File Analysis - No. 10

1.Number of objects:7



2.



3.

```
remnux@remnux:~/Downloads$ peepdf -s javascript  digfor_encrypted.pdf
Error: The script file "javascript" does not exist!!
remnux@remnux:~/Downloads$
```

```
remnux@remnux:~/Downloads$ peepdf  digfor_encrypted.pdf
Warning: PyV8 is not installed!!
Decryption error: Default user password not working here!!

File: digfor_encrypted.pdf
MD5: 66d64355ded5cd1e1967c309e9617fc2
SHA1: 984096952fc2ba01b0e081525ae7cd633b274585
SHA256: 04779932a647eb1575c63c1fff7628b44cd23e503c03396b7c69b34f7ed740c3
Size: 7365 bytes
Version: 1.5
Binary: True
Linearized: False
Encrypted: True (AES 128 bits)
Updates: 0
Objects: 7
Streams: 1
URIs: 0
Comments: 0
Errors: 1

Version 0:
  Catalog: 1
  Info: No
  Objects (7): [1, 2, 3, 4, 5, 6, 7]
  Streams (1): [6]
    Encoded (1): [6]
    Decoding errors (1): [6]
  Suspicious elements:
    /OpenAction (1): [1]
    /JS (1): [2]
    /JavaScript (1): [2]
```

4.

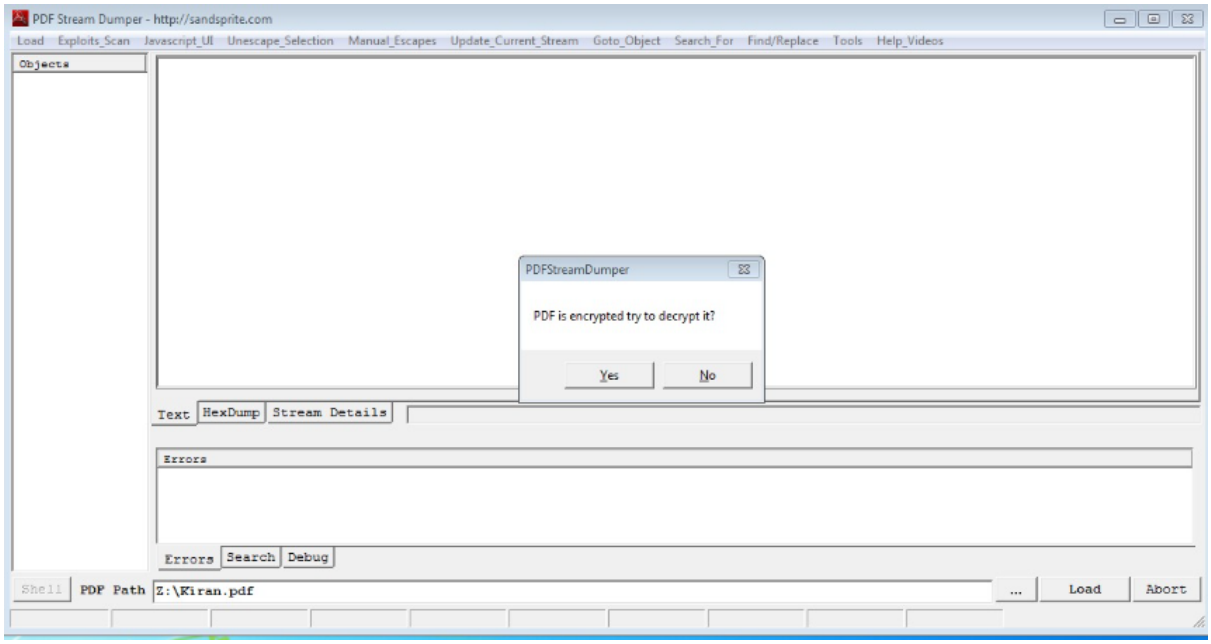
```
remnux@remnux:~/Downloads$ pdf-parser.py -o 2 digfor_encrypted.pdf
obj 2 0
 Type: /Action
 Referencing: 6 0 R

  <<
    /S /JavaScript
    /Type /Action
    /JS 6 0 R
  >>
```

```
remnux@remnux:~/Downloads$ pdf-parser.py --content digfor_encrypted.pdf
PDF Comment '%PDF-1.5\n'

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

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R, 4 0 R

  <<
    /OpenAction 2 0 R
    /Type /Catalog
    /Outlines 3 0 R
    /Pages 4 0 R
  >>



<<
/OpenAction 2 0 R
/Type /Catalog
/Outlines 3 0 R
```

```
remnux@remnux:~/Downloads$ pdfextract -s digfor_encrypted.pdf
Password: Extracted 1 PDF streams to 'digfor_encrypted.dump/streams'.
```

5.No need to de-obfuscate

6.Cannot extract the shell code as the contents is encrypted.

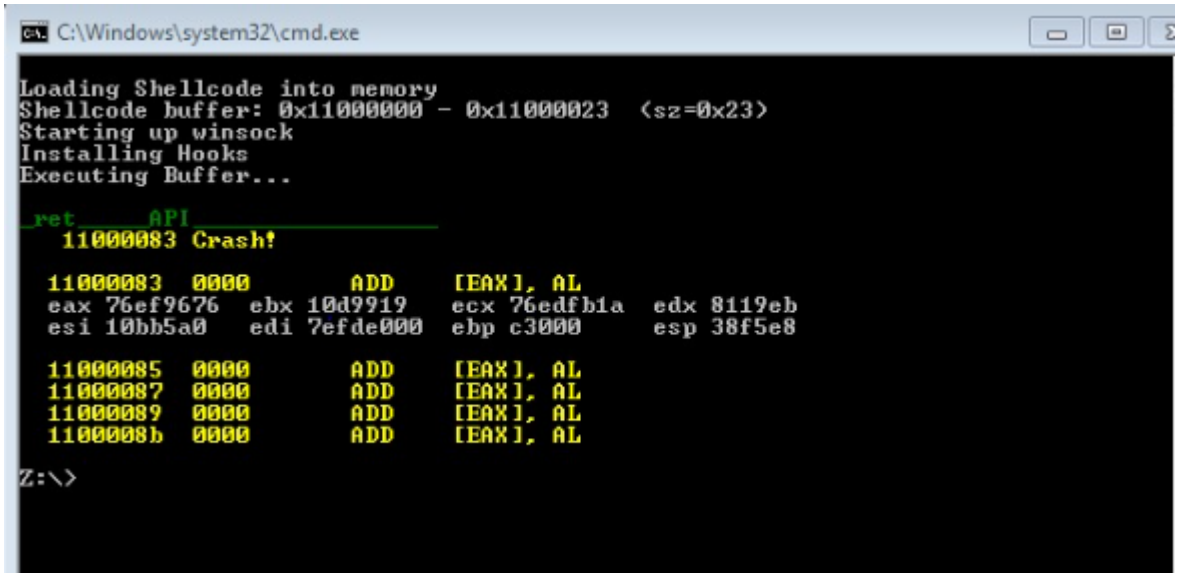


Decrypted file is getting created.

7.

```
remnux@remnux:~/Downloads$ pdf-parser.py -o 6 digfor_encrypted.pdf --raw > digobj6.raw
remnux@remnux:~/Downloads$ shellcode2exe.bat -s digobj6.raw > shellcode.exe
wine: created the configuration directory '/home/remnux/.wine'
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0012:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
0012:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0012:err:ole:get_local_server_stream Failed: 80004002
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0014:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
0014:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0014:err:ole:get_local_server_stream Failed: 80004002
Could not find Wine Gecko. HTML rendering will be disabled.
Could not find Wine Gecko. HTML rendering will be disabled.
wine: configuration in L"/home/remnux/.wine" has been updated.
remnux@remnux:~/Downloads$ ls
 27ec4974d4bd7b86efec586b0800f7a778b4442369195752e68b7841def5c363.dump   ni.dump        'Screenshot from 2022-10-11 10-19-43.png'
 27ec4974d4bd7b86efec586b0800f7a778b4442369195752e68b7841def5c363.pdf    ob6.dump        shellcode.exe
 digfor_encrypted.dump                                                  'obj6(1).dump'  'VirusShare_ce61bb19e57b75f43e5b476ee3698290(1).zip'
 digfor_encrypted.pdf                                                    obj6.dump       'VirusShare_ce61bb19e57b75f43e5b476ee3698290.zip'
 digobj6.raw                                                             obj6.raw
remnux@remnux:~/Downloads$
```

8.



Cannot run as the content are encrypted.

9.

No secret code in this file.