

CCCY432 – Reverse Engineering and Malware Analysis

Lab 2 – Basic Static Analysis

Lara Sami Alofi
2110886
Y

Due Date: 8 September 2024 11:00PM

Task 1: Static Properties Analysis of Windows Executable:

Step A: Analyze Executables with Flare VM Tools

1. Detect It Easy (DIE):

- Open **Detect It Easy** on Flare VM.
- **Drag & drop** brbbot.exe and then sample_packed.exe into the tool.
- **Capture a screenshot** of the results.
- This tool helps detect packing and compilers.

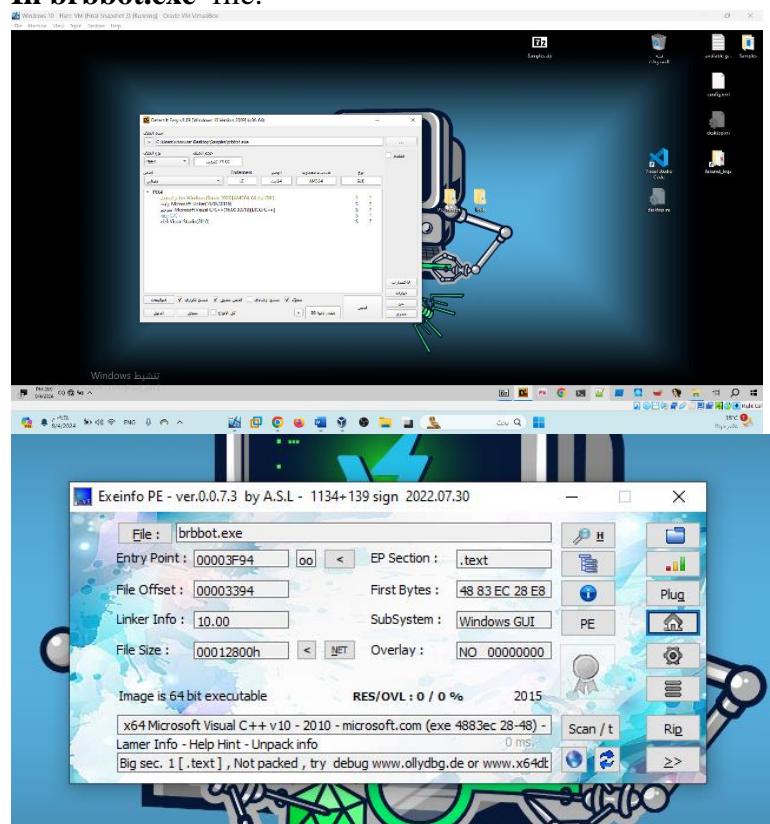
2. ExeInfoPE:

- Open **ExeInfoPE**.
- **Drag & drop** both brbbot.exe and sample_packed.exe into the tool.
- **Capture a screenshot** showing detailed file structure and packing information.

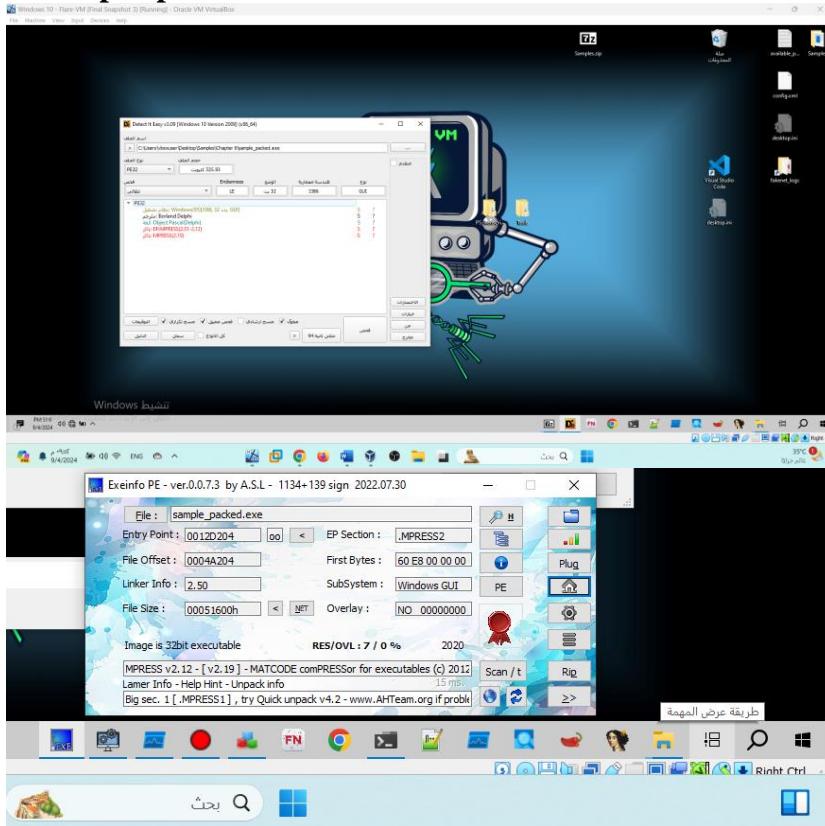
brbbot.exe: Architecture: AMD64, Compiler: Microsoft Visual C/C++.

sample_packed.exe: Architecture: I386, Packed with MPRESS.

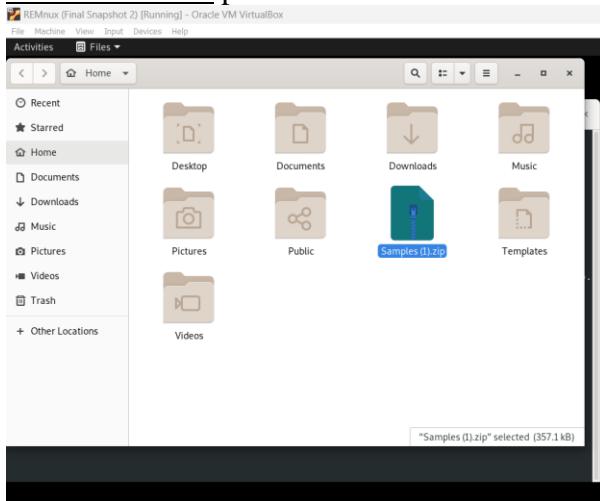
In brbbot.exe file:



In sample_packed.exe file:



REMnux Tools: peframe



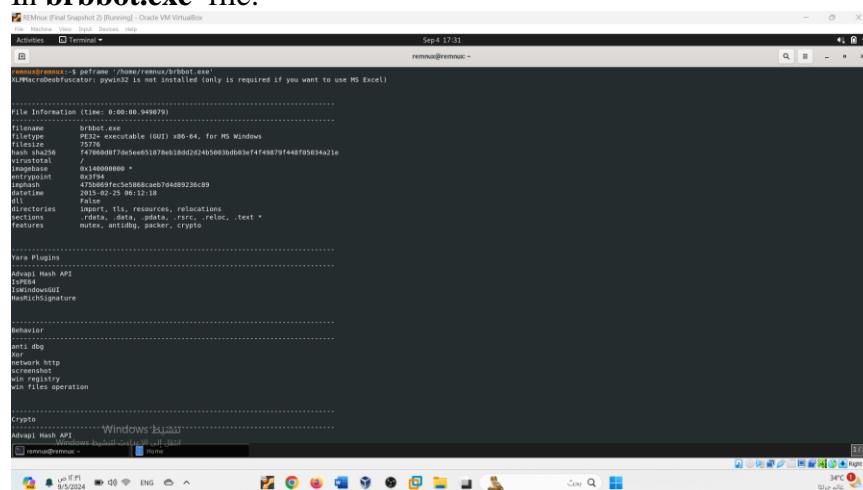
B. Unzipping Files and Using peframe in REMnux

1. Unzip the files within the REMnux environment.

```
remnux@remnux:~$ unzip '/home/remnux/Samples (1)/Samples;brbbot.zip'
Archive: /home/remnux/Samples (1)/Samples;brbbot.zip
[/home/remnux/Samples (1)/Samples;brbbot.zip] brbbot.exe password:
  inflating: brbbot.exe
remnux@remnux:~$ unzip '/home/remnux/Samples (1) (1)/Samples/Sample_packed.zip'
Archive: /home/remnux/Samples (1) (1)/Samples/Sample_packed.zip
[/home/remnux/Samples (1) (1)/Samples/Sample_packed.zip] Chapter 8/.DS_Store password:
replace Chapter 8/.DS_Store? [y]es, [n]o, [A]ll, [N]one, [r]ename:
error: invalid response [{ENTER}]
replace Chapter 8/.DS_Store? [y]es, [n]o, [A]ll, [N]one, [r]ename:
error: invalid response [{ENTER}]
replace Chapter 8/.DS_Store? [y]es, [n]o, [A]ll, [N]one, [r]ename:
error: invalid response [{ENTER}]
replace Chapter 8/.DS_Store? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
replace Chapter 8/emolet.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
replace Chapter 8/sample_packed.exe? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
```

2. Use the peframe command to gather static information about the executable, including metadata, section details, and imports.

In brbbot.exe file:



```
remnux@remnux:~$ peframe '/home/remnux/brbbot.exe'
XLMMacroDefuzzer: pxwin32 is not installed (only is required if you want to use MS Excel)

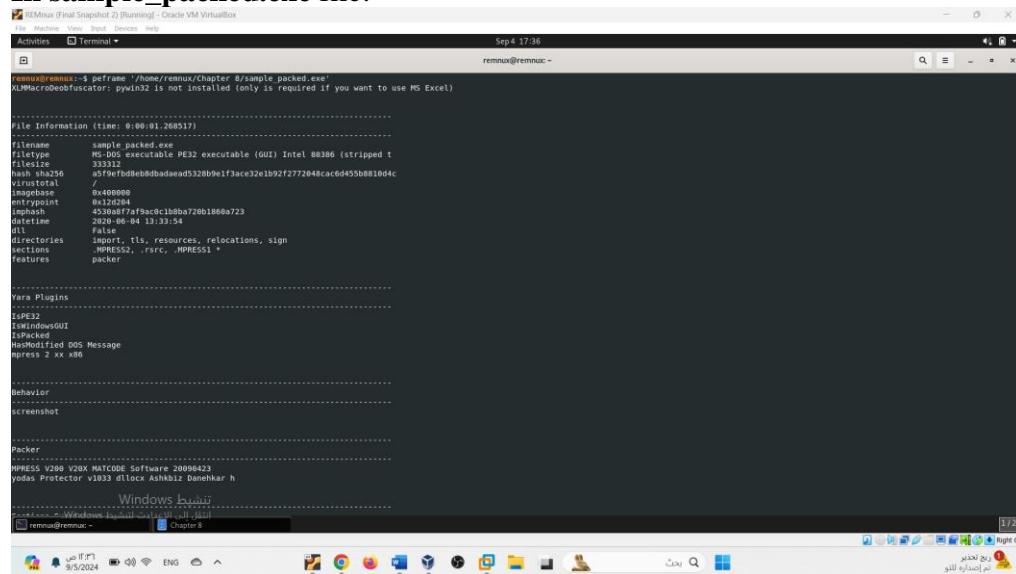
File Information (time: 00:00:00.000000)
-----
filename: brbbot.exe
filetype: PE32+ executable (GUI) x86-64, for MS Windows
filesize: 7576
hash sha256: f314088f7d74e65187eb1bd2d24059803b03ef4f49879f440f05834a21e
virusTotal: 0/1409999000 +
entrypoint: 0x3794
impHash: 4793c5cd58664c807d4d89236c89
datetime: 2013-02-25 04:12:18+0000
dlls: False
directories: import, tls, resources, relocations
sections: .data, .data., .pdata, .rsrc, .reloc, .text *
features: ntext, antidbg, packer, crypto

Yara Plugins:
Adwapi Hash API
Dumper
IsWindows64
HashSignature

Behavior:
anti dbg
vir
network http
screenshot
sign
win file
win files operation

Crypto:
Adwapi Hash API
```

In sample_packed.exe file:



```
remnux@remnux:~$ peframe '/home/remnux/Chapter 8/sample_packed.exe'
XLMMacroDefuzzer: pxwin32 is not installed (only is required if you want to use MS Excel)

File Information (time: 00:00:01.268517)
-----
filename: sample_packed.exe
filetype: MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped !)
filesize: 333312
hash sha256: a519efbd8e8ddbaddead5320bbe1f3ac3e32e1b92f2772048cac6d455b8810d4c
virusTotal: 0/1409999000 +
imagebase: 0x400000
entrypoint: 0x126284
impHash: 42301a7af9ac0c1bb0728b01866a723
datetime: 2020-06-04 13:33:54
dlls: False
directories: import, tls, resources, relocations, sign
sections: _HPRESS2, _rsrc, _HPRESS1 *
features: packer

Yara Plugins:
isPE32
IsWindowsGUI
IsPacked
HasModified DOS Message
ppress 2 xx x86

Behavior:
screenshot

Packer:
HPRESS V200 V20X MATCODE Software 20090623
yodas Protector V1033 d1lock Ahmals2 Banehkar h

Windows تثبيت
Windows تثبيت - Windows تثبيت
remnux@remnux:~$ Chapter 8
```

	brbbot.exe	sample_packed.exe
Architecture	AMD64	I386
Compiler	Microsoft visual C/C++(16.00.30.3019)[LTCG/C++]	Pobject pascal (Delphi)
Packed?	Not packed (from exeinfo PE tool)	Yes
Type of Packer		Packer: EP:MPRESS(2.01-2.12) Packer: MPRESS(2.19)

C. Getting Strings from Both Executables

- Extract strings from the executables using Flare VM and REMnux tools:
 - Flare VM: Use PeStudio and BinText.

In brbbot.exe file:

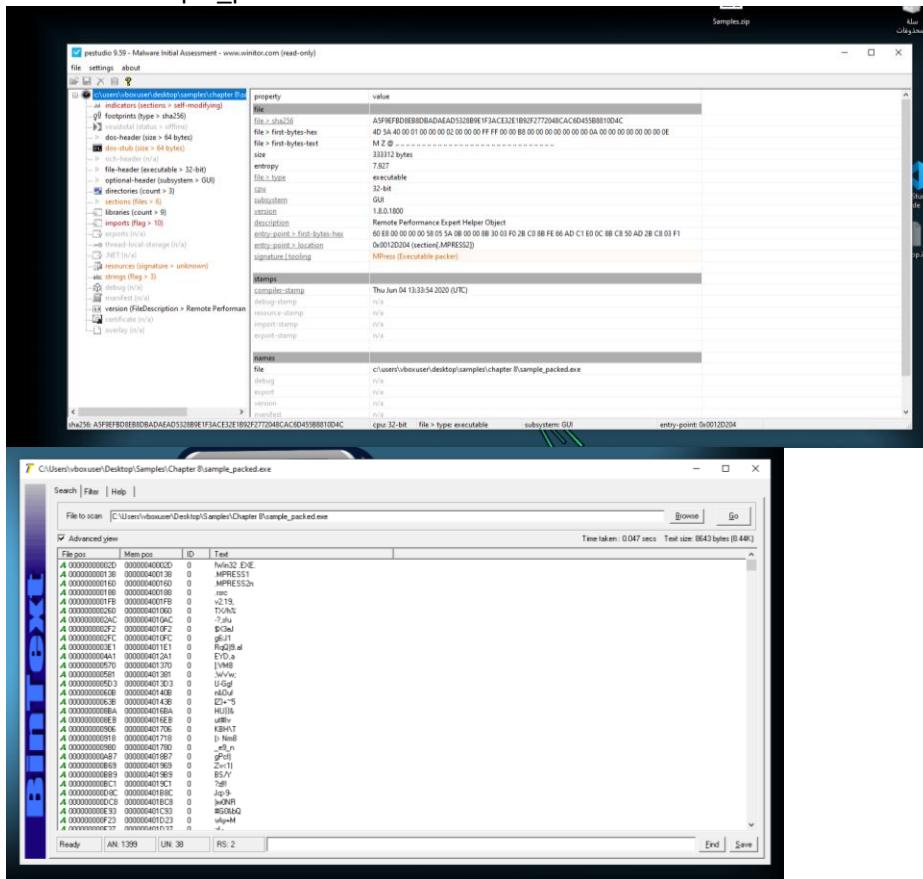
The screenshot shows the Flare VM interface with the file structure of brbbot.exe. The imports section lists several DLLs and their functions:

library (S)	duplicate (0)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	type (I)	imports (115)	group (0)	description
ADVAPI32.dll	-	*	0x00010C90	0x0000E340	implicit	9	refcheck	Advanced Windows 32 Base API
WININET.dll	-	*	0x00010F20	0x0000E340	implicit	5	refcheck	Internet Extensions for Win32 Library
WS2_32.dll	-	*	0x00011020	0x0000E360	implicit	5	refcheck	Windows Socket Library
KERNEL32.dll	-	*	0x00010D98	0x0000E078	implicit	86	-	Windows NT BASE API Client
USER32.dll	-	*	0x00010FC0	0x0000E330	implicit	1	-	Multi-User Windows USER API Client Library

The screenshot shows the BinText application displaying the extracted strings from brbbot.exe. The strings include various API names and error messages. Some strings are highlighted in red, such as 'The program cannot be run in DOS mode.' and 'This program cannot be run in DOS mode.'

File	Line	Mem pos	ID	Text
brbbot.exe	0	0x0000000000000004E	0	!The program cannot be run in DOS mode.
brbbot.exe	1	0x00000000000000170	0	!exit
brbbot.exe	2	0x000000000000001A5	0	!read
brbbot.exe	3	0x0000000000000023F	0	!write
brbbot.exe	4	0x00000000000000268	0	!read&data
brbbot.exe	5	0x000000000000001F5	0	!pdetect
brbbot.exe	6	0x0000000000000021C	0	!mem
brbbot.exe	7	0x00000000000000277	0	!mem&abc
brbbot.exe	8	0x00000000000000294	0	!abc
brbbot.exe	9	0x0000000000000029C	0	!WATAUH
brbbot.exe	10	0x000000000000002A0	0	!AVAWAWH
brbbot.exe	11	0x000000000000002E5	0	!USVATH
brbbot.exe	12	0x00000000000000B02	0	!UJAVAWAWH
brbbot.exe	13	0x00000000000000C40	0	!UJAVAWAWH
brbbot.exe	14	0x00000000000000C5F	0	!UJAVAWAWH
brbbot.exe	15	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	16	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	17	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	18	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	19	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	20	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	21	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	22	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	23	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	24	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	25	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	26	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	27	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	28	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	29	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	30	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	31	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	32	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	33	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	34	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	35	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	36	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	37	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	38	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	39	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	40	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	41	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	42	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	43	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	44	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	45	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	46	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	47	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	48	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	49	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	50	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	51	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	52	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	53	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	54	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	55	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	56	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	57	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	58	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	59	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	60	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	61	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	62	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	63	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	64	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	65	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	66	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	67	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	68	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	69	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	70	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	71	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	72	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	73	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	74	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	75	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	76	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	77	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	78	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	79	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	80	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	81	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	82	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	83	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	84	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	85	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	86	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	87	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	88	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	89	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	90	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	91	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	92	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	93	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	94	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	95	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	96	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	97	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	98	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	99	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	100	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	101	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	102	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	103	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	104	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	105	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	106	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	107	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	108	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	109	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	110	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	111	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	112	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	113	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	114	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	115	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	116	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	117	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	118	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	119	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	120	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	121	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	122	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	123	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	124	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	125	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	126	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	127	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	128	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	129	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	130	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	131	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	132	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	133	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	134	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	135	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	136	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	137	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	138	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	139	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	140	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	141	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	142	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	143	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	144	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	145	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	146	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	147	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	148	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	149	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	150	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	151	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	152	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	153	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	154	0x00000000000000C90	0	!UJAVAWAWH
brbbot.exe	155	0x00000000000000C94	0	!UJAVAWAWH
brbbot.exe	156	0x00000000000000C9F	0	!UJAVAWAWH
brbbot.exe	157	0x00000000000000D00	0	!UJAVAWAWH
brbbot.exe	158	0x00000000000000C77	0	!UJAVAWAWH
brbbot.exe	159	0x00000000000000C90</		

In sample_packed.exe file:



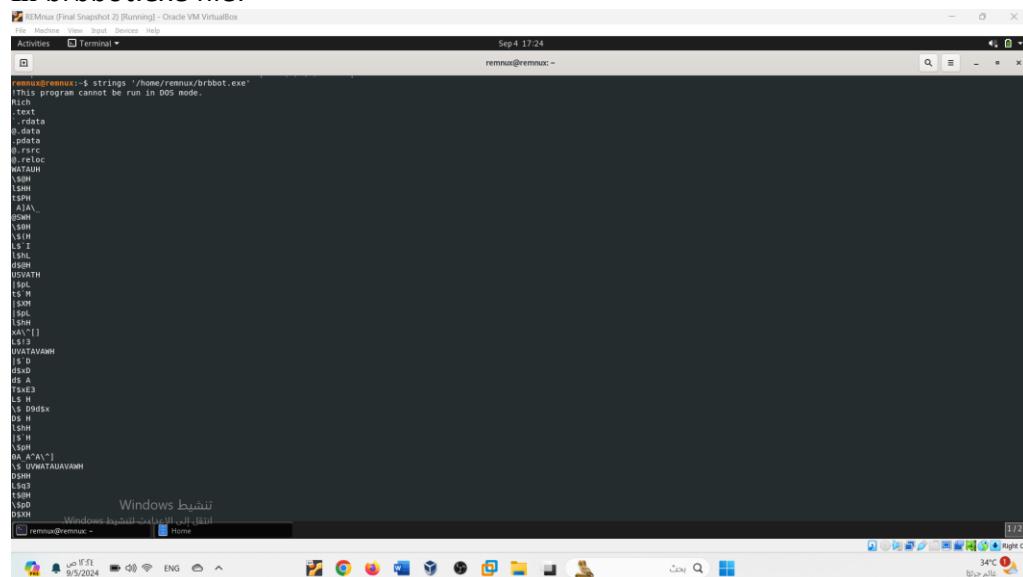
- o **REMnux:** Use strings and pestr.

Use strings command:

In sample_packed.exe file:

```
remnux@remnux:~$ strings '/home/remnux/Chapter 8/sample_packed.exe'
\W1032 .EXE
.MPRESS
.MPRESS2n
.TX/n
V2.19
TX/n
.E99
.u_
.Z3.tu
.S3d
.d6.11
.mqQ19.aI
.w_
.vD.a
.lwlp
.;.VM8
;wv;
;75#
U.Gg!
.KtL
.rS0U!
;Z>-5
.smp
.HU)i6
.u#tV
.RmN
(> N8
;v1s
;e9.n
;r7o
;u;d9
;gPcf!
;Pm9
;Lb(9
;Zv<1|
;Zz|11
;Dl;y
;I*k
;Jq9-
;JwNR
;g9
;G6d2o
Windows تقطيع
remnux@remnux:~$ Chapter 8
```

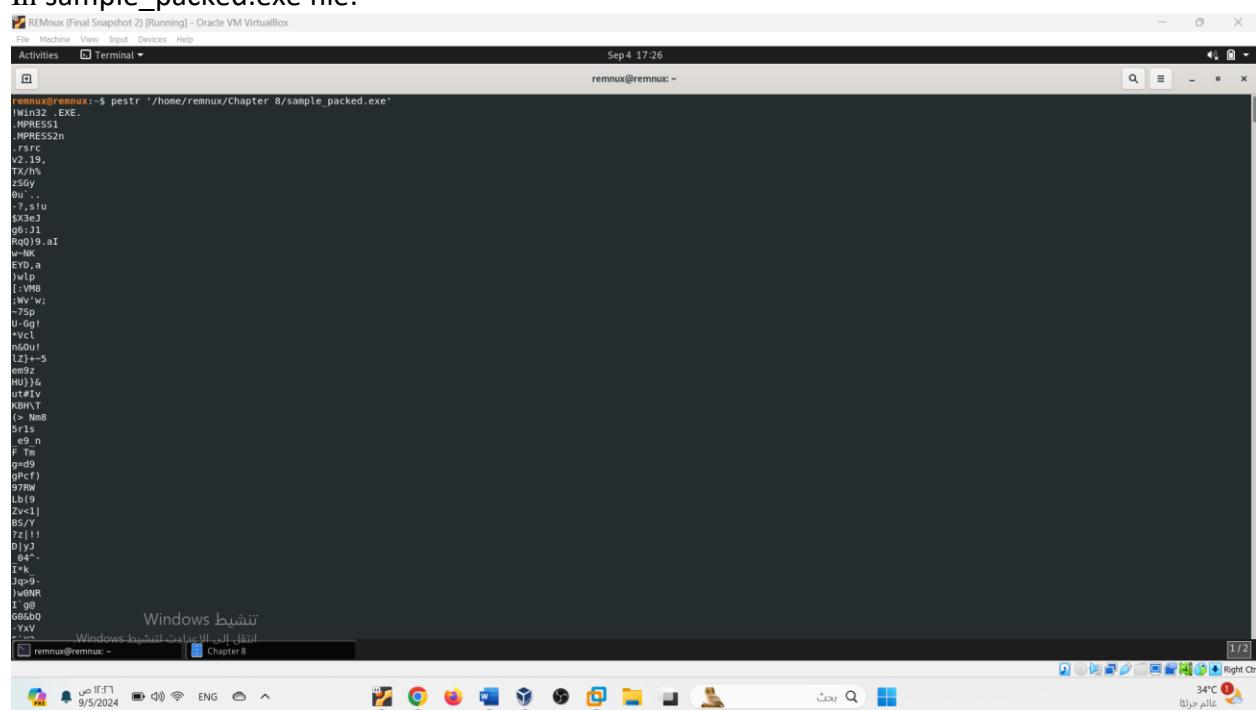
In brbbot.exe file:



```
remnux@remnux:~$ strings '/home/remnux/brbbot.exe'
!This program cannot be run in DOS mode.
Rich
Text
.rdata
.g.data
.pdata
.g.rsrc
.g.reloc
.WORD
.SHM
.LSH
.TSPY
.AIA\
.BSWH
.VSH
.LSH
.LS T
.TSH
.dSH
.USVATH
.IPL
.TS X
.ISXH
.IPL
.ISH
.xA" []
.LS I
.DISTAVAH
.IE D
.dxD
.RA A
.TSx3
.LS H
.VS 90DX
.DS H
.LSH
.TSH
.TSPY
.BA "A" "
.EI .DISTAVAH
.DSH
.Lsq3
.TSPY
.VSH
.DSXH
Windows تنشيط
Windows -> إلخ -> إلخ -> إلخ
remnux@remnux:~
```

Use pestr command :

In sample_packed.exe file:



```
remnux@remnux:~$ pestr '/home/remnux/Chapter 8/sample_packed.exe'
!Win32 .EXE.
.MPRESS1
.MPRESS2n
.FFC
.v2.19.
.TX/h%
zSgY
0u
.P
.E3eJ
.Q6.JI
RqQj9.aI
w-NK
EYD.a
.JM
.LvMB
:W/W;
-U7sp
U-GgJ
+Vcl
.R000
(LZ)---$ em9z
HU)j6 ut#IV
KBHT
(> Nm8
x3
.e9.n
F Tm
g=d9
gPcf)
9790
LWl9
2v1]
BS/Y
Tz!!!
0|yJ
.04
T*k
Jqp9-
)w0NR
I g@0
06500
.YXV
Windows تنشيط
انتقل الى الاعداد لتنشيط
Windows -> إلخ -> إلخ -> إلخ
remnux@remnux:~
```

In brbbot.exe file:

```

remnux@remnux: ~$ pestr '/home/remnux/brbbot.exe'
!This program cannot be run in DOS mode.

Rich
.text
.rdata
.data
.pdata
.rsrc
.reloc
WATAUH
USVATH
[...]
Windows تنشيط
Windows إختراق الأجهزة
Windows Home
[...]
remnux@remnux: ~

```

	brbbot.exe	sample_packed.exe	Why ?																		
List 5 interesting strings in the exe	<p>library (5) duplicate (0) fl</p> <table border="1"> <tr><td>ADVAPI32.dll</td><td>-</td></tr> <tr><td>WININET.dll</td><td>-</td></tr> <tr><td>WS2_32.dll</td><td>-</td></tr> <tr><td>KERNEL32.dll</td><td>-</td></tr> <tr><td>USER32.dll</td><td>-</td></tr> </table> ADVAPI32.dll WININET.dll WS2_32.dll KERNEL32.dll USER32.dll	ADVAPI32.dll	-	WININET.dll	-	WS2_32.dll	-	KERNEL32.dll	-	USER32.dll	-	<p>section:MPR... utility</p> <table border="1"> <tr><td>ascii 6</td><td>x</td></tr> <tr><td>ascii 12</td><td>x dos-message</td></tr> <tr><td>bitmap PREVIEWGLYPH bitmap</td><td>IMPRESS1:0x00039... 232</td></tr> <tr><td>rcdata TDIAFRAME unknown</td><td>IMPRESS1:0x00044... 337</td></tr> </table> Bitmap Rcdata OleRun !Win32.EXE FreeSid	ascii 6	x	ascii 12	x dos-message	bitmap PREVIEWGLYPH bitmap	IMPRESS1:0x00039... 232	rcdata TDIAFRAME unknown	IMPRESS1:0x00044... 337	<p>brbbot.exe - Interesting Strings:</p> <p>ADVAPI32.dll: This is a DLL file that provides access to advanced Windows API functions, particularly related to security and registry management. Malware often interacts with this library to manipulate system services or access sensitive data.</p> <p>WININET.dll: This library is used for network</p>
ADVAPI32.dll	-																				
WININET.dll	-																				
WS2_32.dll	-																				
KERNEL32.dll	-																				
USER32.dll	-																				
ascii 6	x																				
ascii 12	x dos-message																				
bitmap PREVIEWGLYPH bitmap	IMPRESS1:0x00039... 232																				
rcdata TDIAFRAME unknown	IMPRESS1:0x00044... 337																				

		<p>communication, particularly with HTTP and FTP protocols. Malware might use it for downloading additional payloads or exfiltrating data over the internet.</p> <p>WS2_32.dll: This is a Windows Sockets library used for network communication, indicating that the executable may attempt to communicate over a network, possibly to send/receive commands or data.</p> <p>KERNEL32.dll: This fundamental Windows library contains core system functions for memory management, file handling, and system services. Many malware samples use this library to interact with the system at a low level.</p> <p>USER32.dll: This DLL manages user interface components like windows, messages, and</p>
--	--	--

		<p>controls. Malware may utilize this to display fake windows or manipulate user inputs.</p> <p>sample_packed.exe - Interesting Strings:</p> <p>Bitmap: This indicates that the executable may contain images or use graphics in its operation. Malware can use this for deceptive user interfaces or even to hide malicious code within images.</p> <p>Rodata: This is a resource data string, potentially indicating that the malware has embedded resources (e.g., configuration files, scripts, or other binary data).</p> <p>OleRun: A reference to the Object Linking and Embedding (OLE) API, which could suggest that the executable interacts with embedded objects, possibly for file</p>
--	--	--

		<p>manipulation or running embedded scripts.</p> <p>!Win32.EXE: This string could indicate the executable is identifying itself as a 32-bit Windows executable, potentially to bypass certain protections or target specific systems.</p> <p>FreeSid: A reference to a function that frees security identifiers (SIDs). This could indicate manipulation of user credentials or security tokens, which is a common tactic in privilege escalation.</p>
--	--	--

- A. In imports section, the API calls that marked with **X** and strings should be investigated first in your code analysis.

In sample_packed.exe file:

pestudio 9.59 - Malware Initial Assessment - www.wimtor.com (read-only)

File settings about

Imports (Flag: 10)

flag (2)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (0)	technique (1)	type (1)
X	0x00120103	0x00120106	0 (0x0000)	security	-	implicit
	0x00120108	0x00120108	0 (0x0000)	dynamic-library	T1106 Execution through API	implicit
	0x00120133	0x00120133	0 (0x0000)	dynamic-library	-	implicit
	0x0012015C	0x0012015C	0 (0x0000)	-	-	implicit
	0x0012016E	0x0012016E	0 (0x0000)	-	-	implicit
	0x00120181	0x00120181	0 (0x0000)	-	-	implicit
	0x001201B0	0x001201B0	0 (0x0000)	-	-	implicit
	0x001201C7	0x001201C7	0 (0x0000)	-	-	implicit
	0x001201D0	0x001201D0	0 (0x0000)	-	-	implicit
	0x001201F4	0x001201F4	0 (0x0000)	-	-	implicit

File: Machine: View: Input: Devices: Help

Windows 10 - Flare-VM (Final Snapshot 3) [Running] - Oracle VM VirtualBox

cpu: 32-bit file > type: executable subsystem: GUI entry-point: 0x00120204

...Detect It Easy v3.09 [Windows 1]

Windows 10 - Flare-VM (Final Snapshot 3) [Running] - Oracle VM VirtualBox

PM 25:10 9/4/2024 ENG 35°C عالم جرنا Right Ctrl

In brbbot.exe file:

pestudio 9.59 - Malware Initial Assessment - www.wimtor.com (read-only)

File settings about

Imports (Flag: 115)

flag (35)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (0)	technique (10)	type (5)
X	0x00000000001106	0x00000000001068	608 (0x0260)	registry	-	implicit
	0x00000000001107	0x00000000001072	503 (0x0147)	registry	T1405 Data Destruction	implicit
	0x00000000001108	0x00000000001082	560 (0x0230)	registry	T1112 Modify Registry	implicit
	0x00000000001109	0x00000000001092	0x00000000001092	reconnaissance	T1092 System Information Discovery	implicit
	0x0000000000110A	0x00000000001094	402 (0x0192)	reconnaissance	T1081 File and Directory Discovery	implicit
	0x0000000000110B	0x00000000001108	644 (0x0254)	reconnaissance	-	implicit
	0x0000000000110C	0x00000000001106	630 (0x0276)	reconnaissance	-	implicit
	0x0000000000110D	0x00000000001104	618 (0x025A)	reconnaissance	-	implicit
	0x0000000000110E	0x00000000001104	770 (0x0302)	reconnaissance	T1082 System Information Discovery	implicit
	0x0000000000110F	0x00000000001104	677 (0x02A9)	reconnaissance	-	implicit
	0x00000000001110	0x00000000001178	666 (0x02B8)	reconnaissance	T1034 System Time Discovery	implicit
	0x00000000001111	0x00000000001128	415 (0x01C7)	reconnaissance	T1057 Process Discovery	implicit
	0x00000000001112	0x00000000001108	97 (0x0038)	network	-	implicit
	0x00000000001113	0x00000000001108	133 (0x008B)	network	-	implicit
	0x00000000001114	0x00000000001174	159 (0x009F)	network	-	implicit
	0x00000000001115	0x00000000001108	107 (0x006B)	network	-	implicit
	0x00000000001116	0x00000000001108	89 (0x0059)	network	-	implicit
	0x00000000001117	0x00000000001108	770 (0x0302)	network	-	implicit
	0x00000000001118	0x00000000001108	731 (0x0307)	network	-	implicit
	0x00000000001119	0x00000000001108	87 (0x0037)	network	-	implicit
	0x0000000000111A	0x00000000001108	172 (0x00AC)	network	-	implicit
	0x0000000000111B	0x00000000001108	0 (0x0000)	network	-	implicit
	0x0000000000111C	0x00000000001108	0 (0x0000)	network	-	implicit
	0x0000000000111D	0x00000000001108	0 (0x0000)	network	-	implicit
	0x0000000000111E	0x00000000001108	0 (0x0000)	network	-	implicit
	0x0000000000111F	0x00000000001108	0 (0x0000)	network	-	implicit
	0x00000000001120	0x00000000001108	0 (0x0000)	network	-	implicit
	0x00000000001121	0x00000000001108	624 (0x0270)	memory	-	implicit
	0x00000000001122	0x00000000001108	723 (0x0303)	memory	-	implicit
	0x00000000001123	0x00000000001108	727 (0x037)	memory	-	implicit

File: Machine: View: Input: Devices: Help

Windows 10 - Flare-VM (Final Snapshot 3) [Running] - Oracle VM VirtualBox

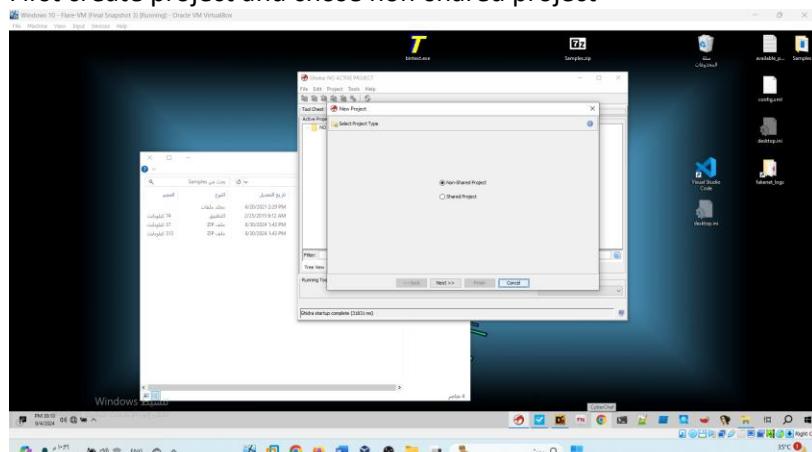
PM 26:10 9/4/2024 ENG 35°C عالم جرنا Right Ctrl

B. Investigating Imports

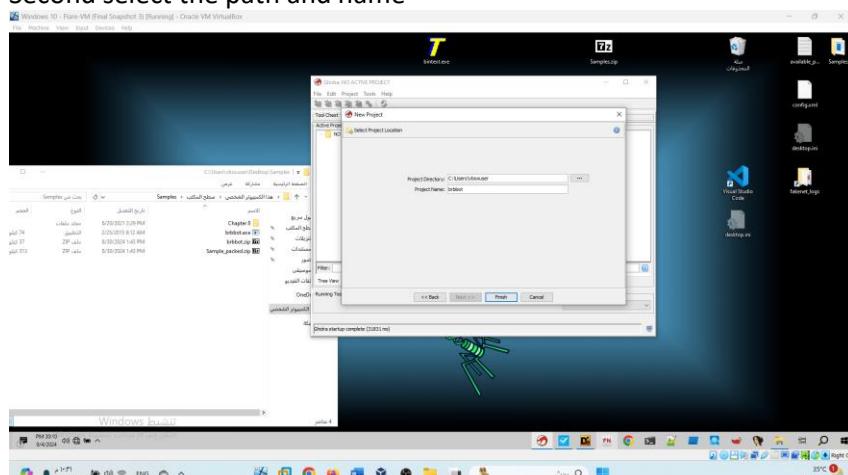
1. Analyze the **imports** section of the executables. Focus on API calls marked with an x, as these should be investigated further during code analysis.
2. Use **Ghidra** to display strings longer than 10 characters from each executable,

In brbbot.exe file:

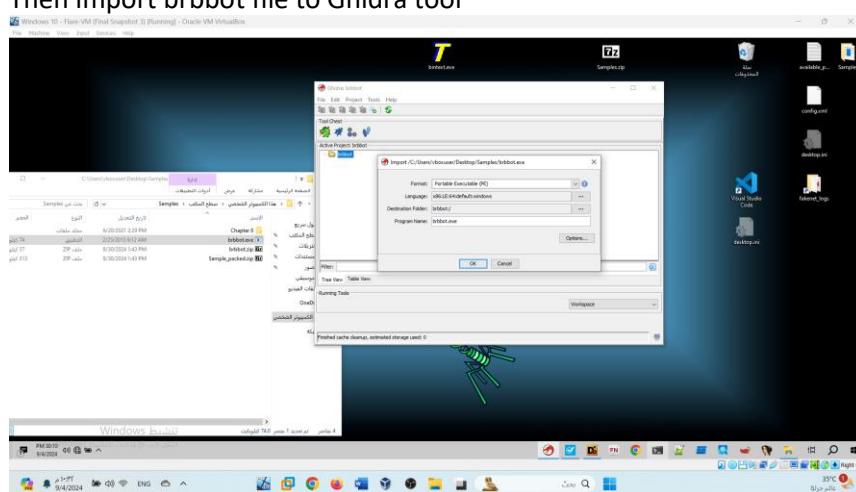
First create project and chose non-shared project



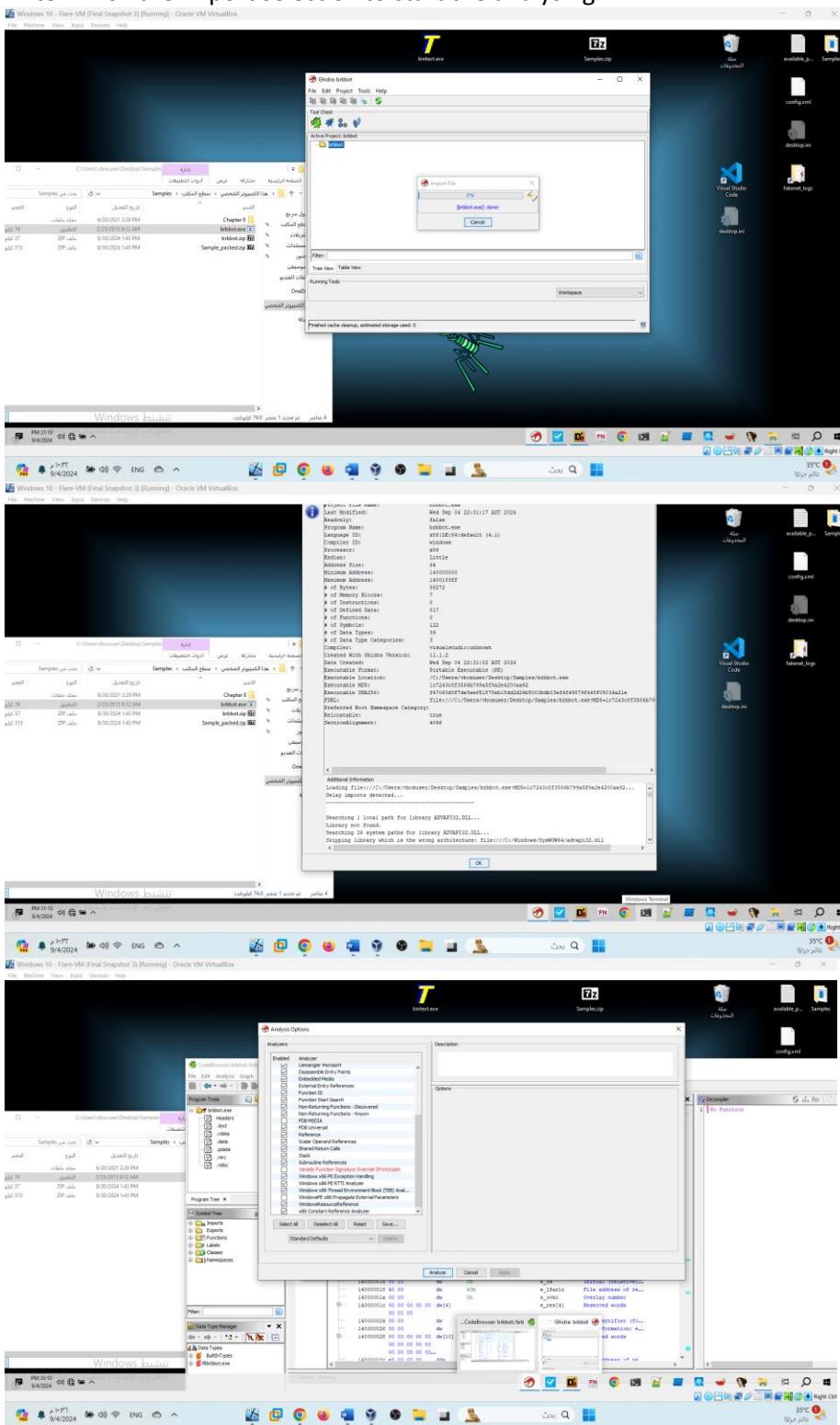
Second select the path and name

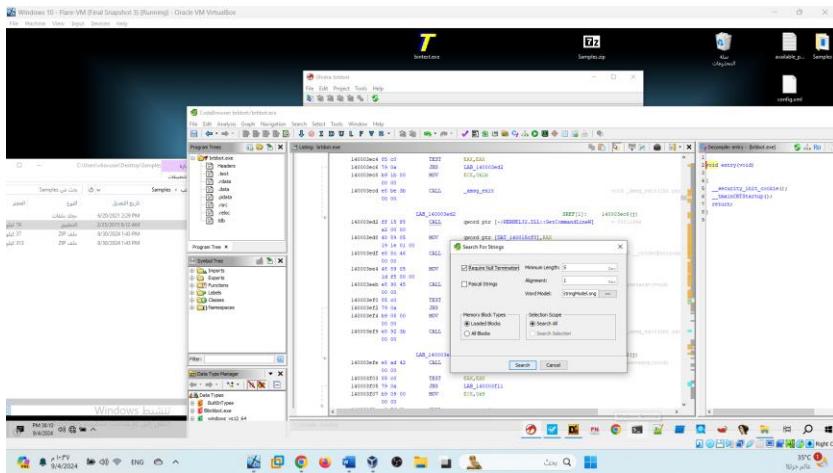


Then import brbbot file to Ghidra tool

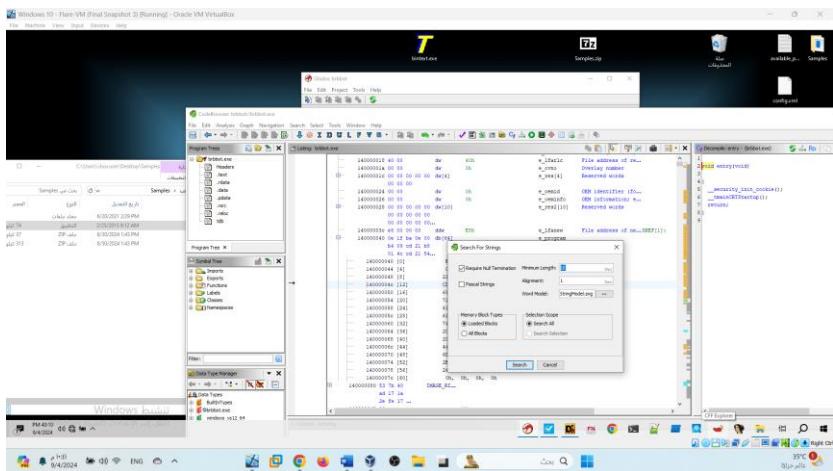


After finish the import select ok to start the analysing

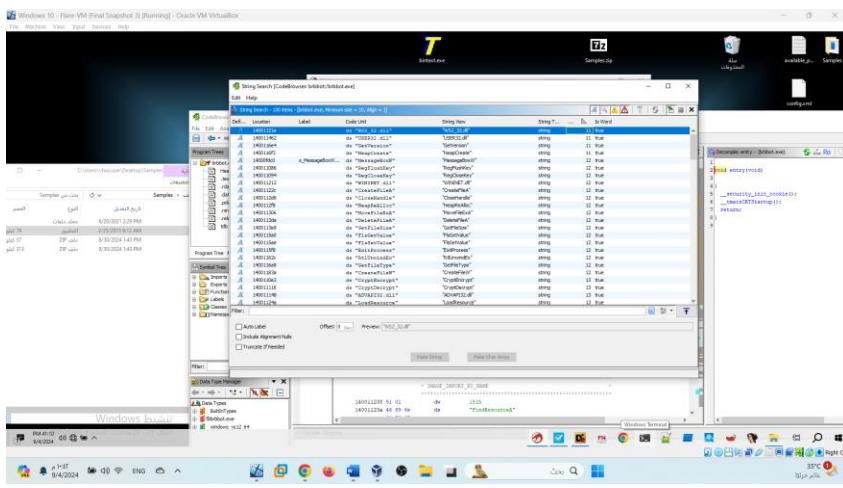




Here enter the length 10

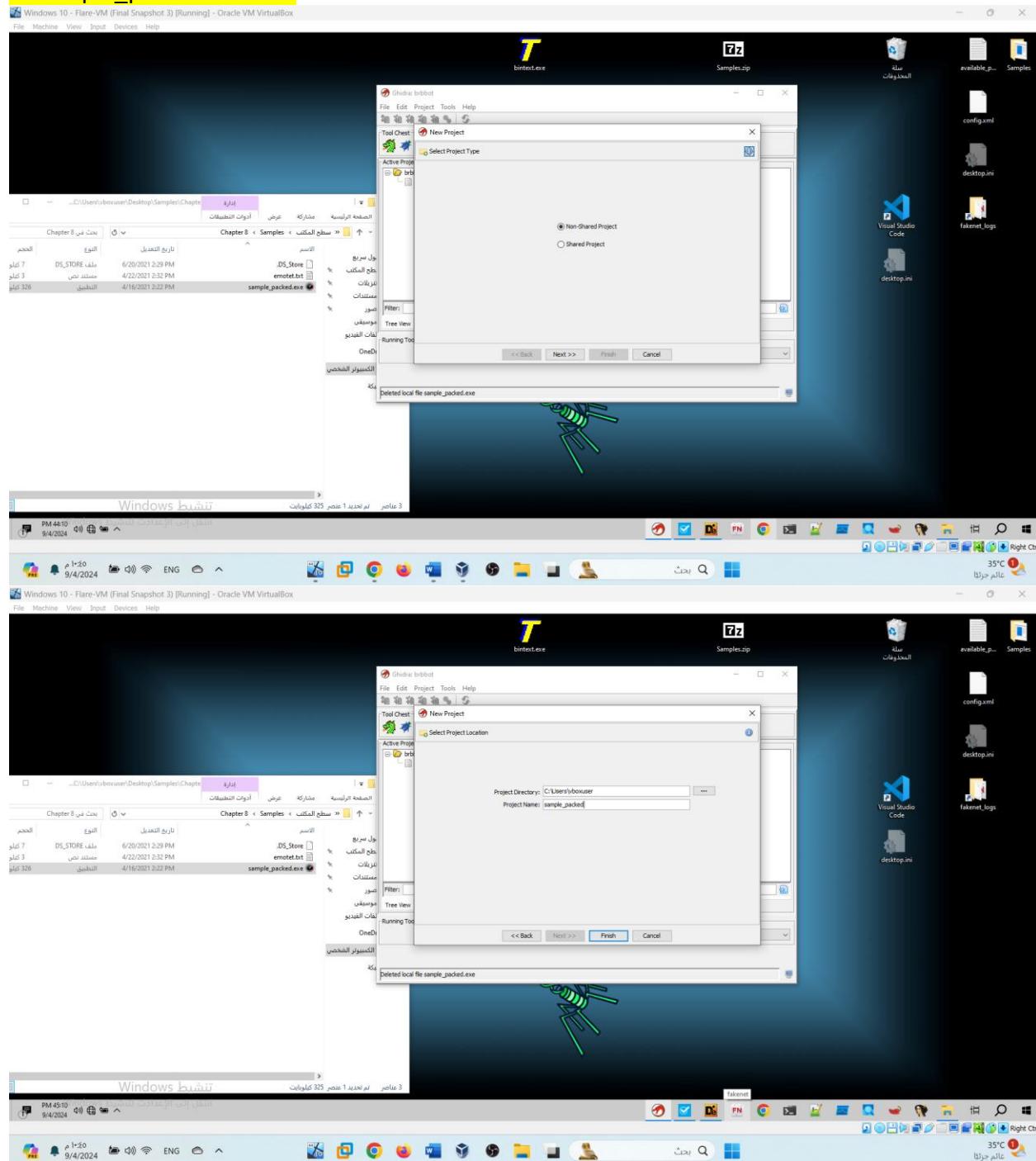


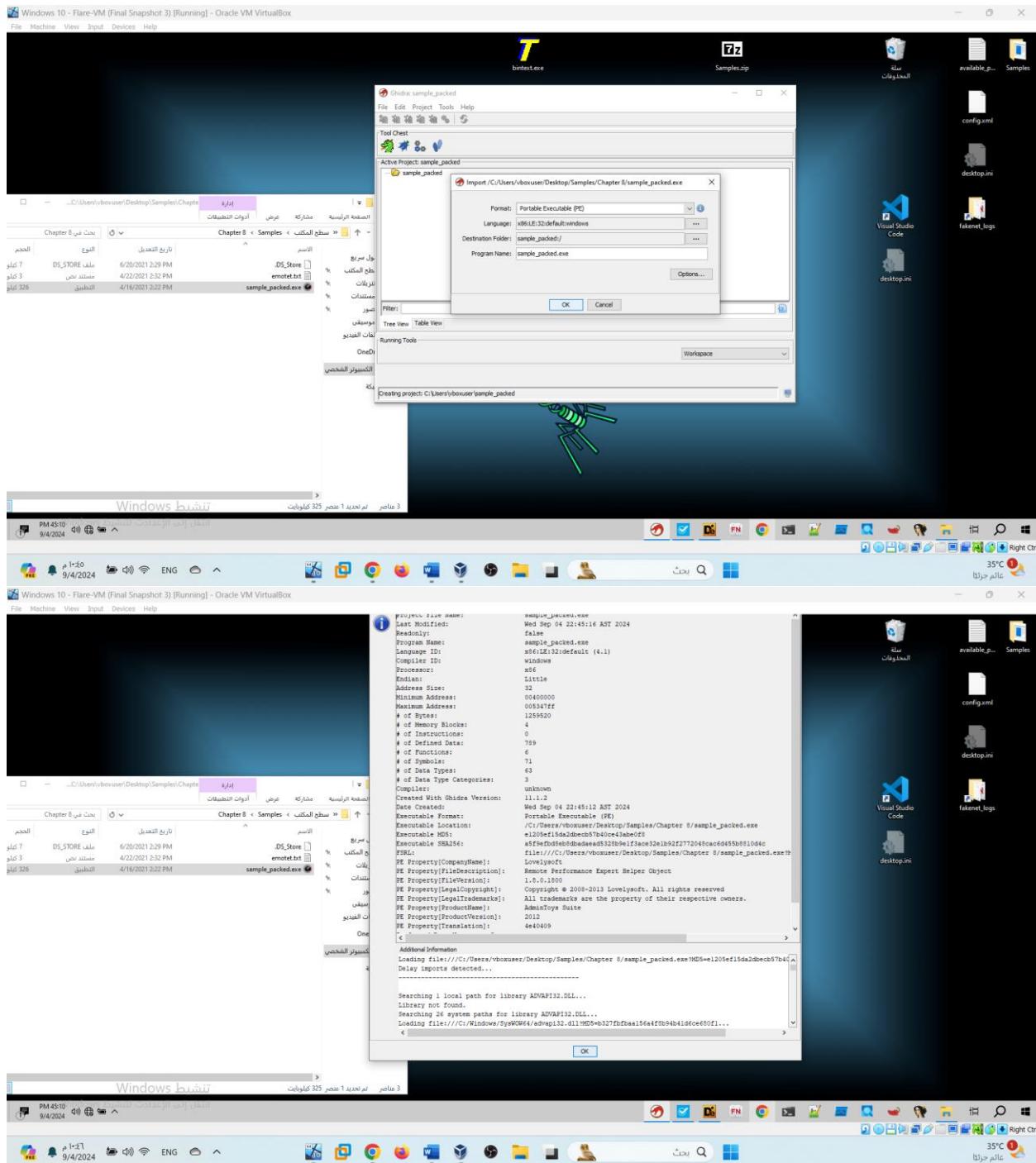
Display more than 10 characters

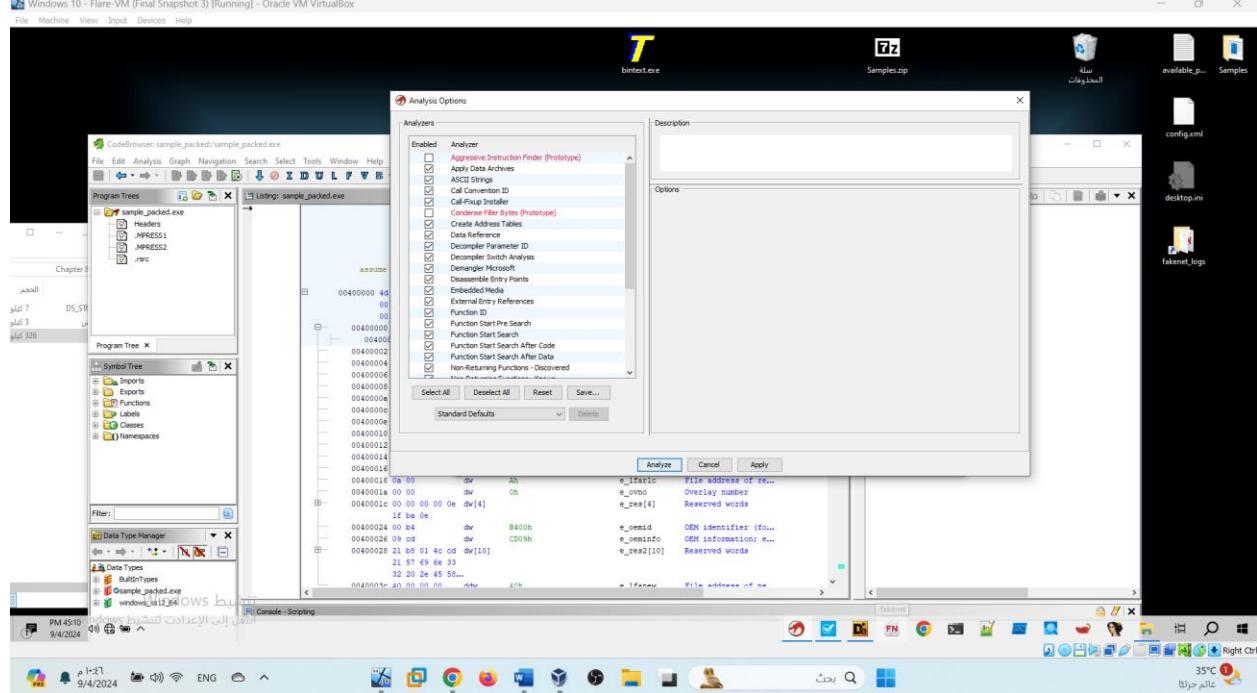
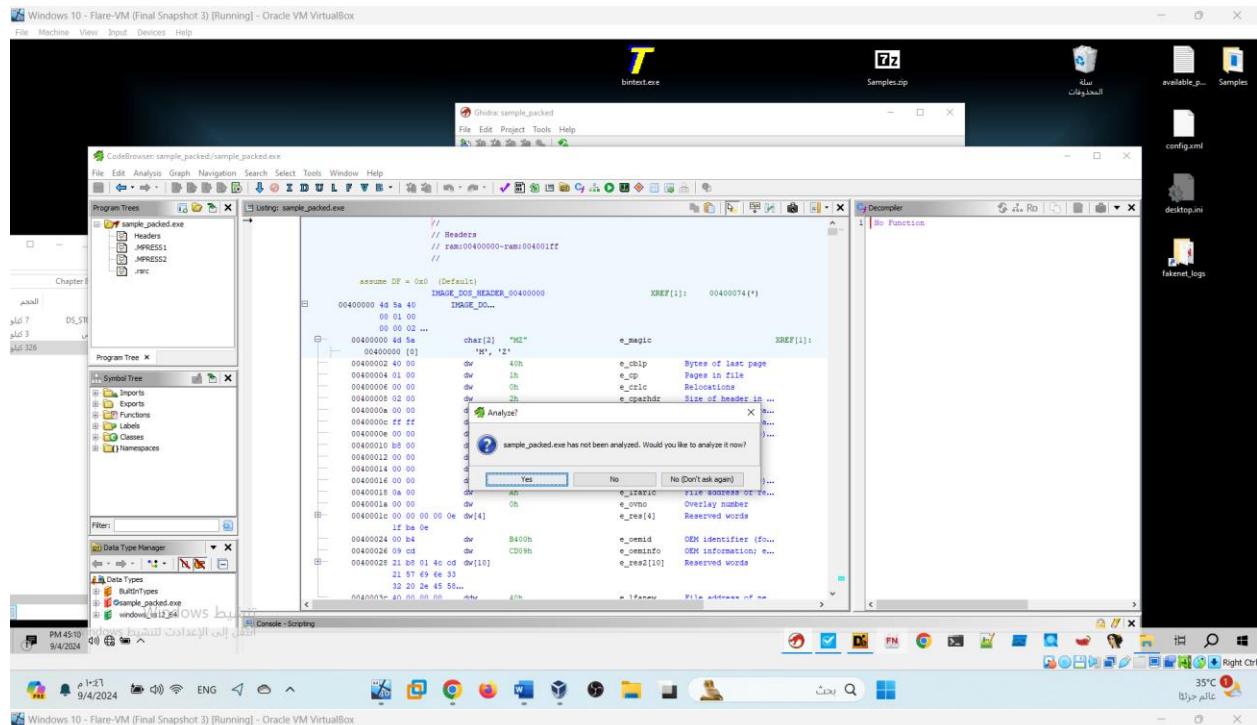


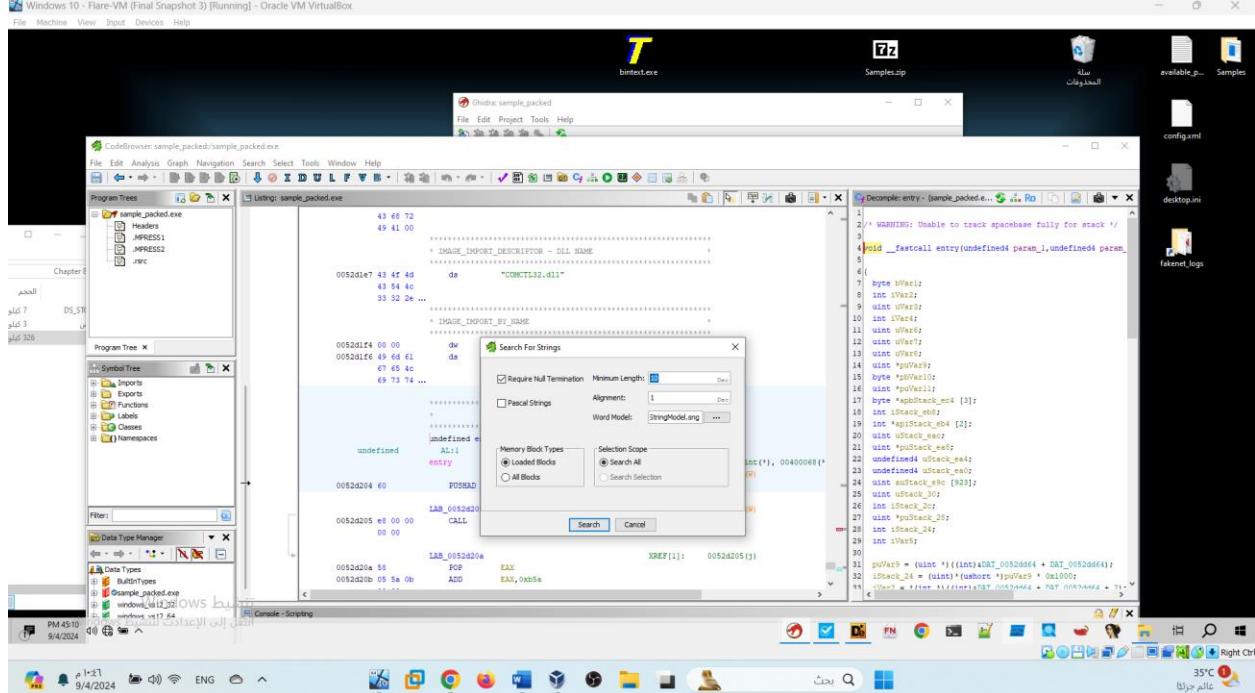
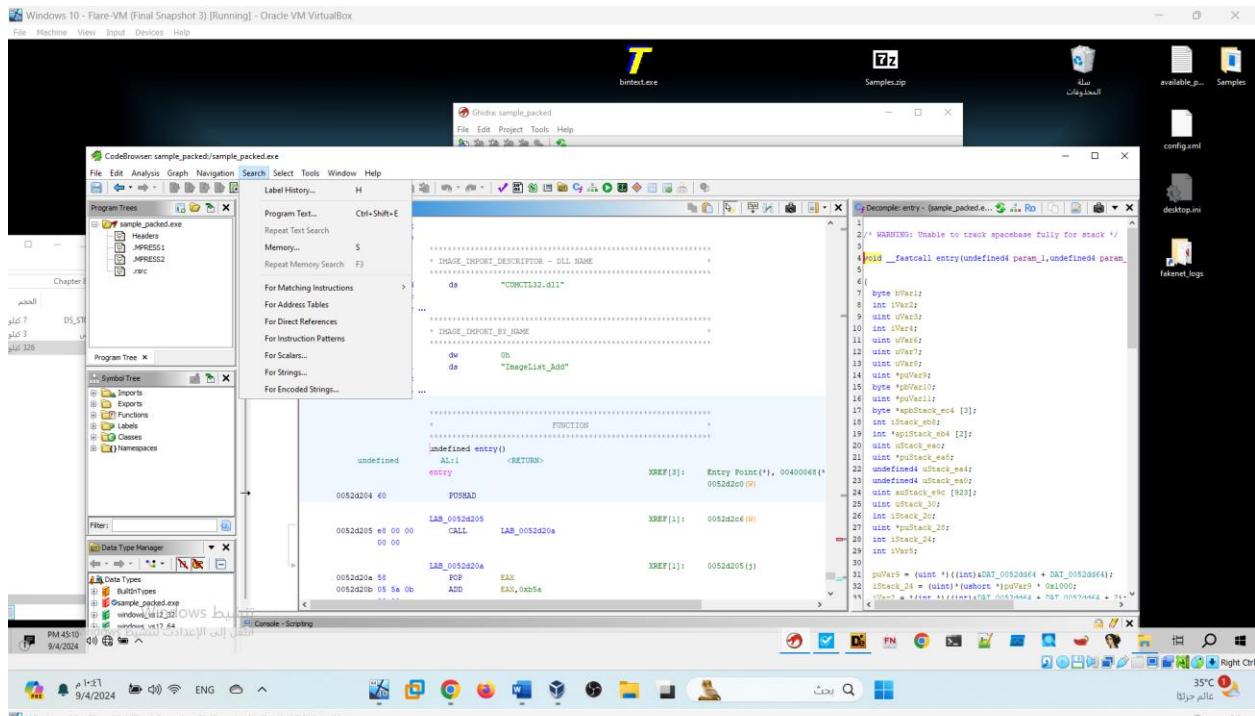
Repeat the steps

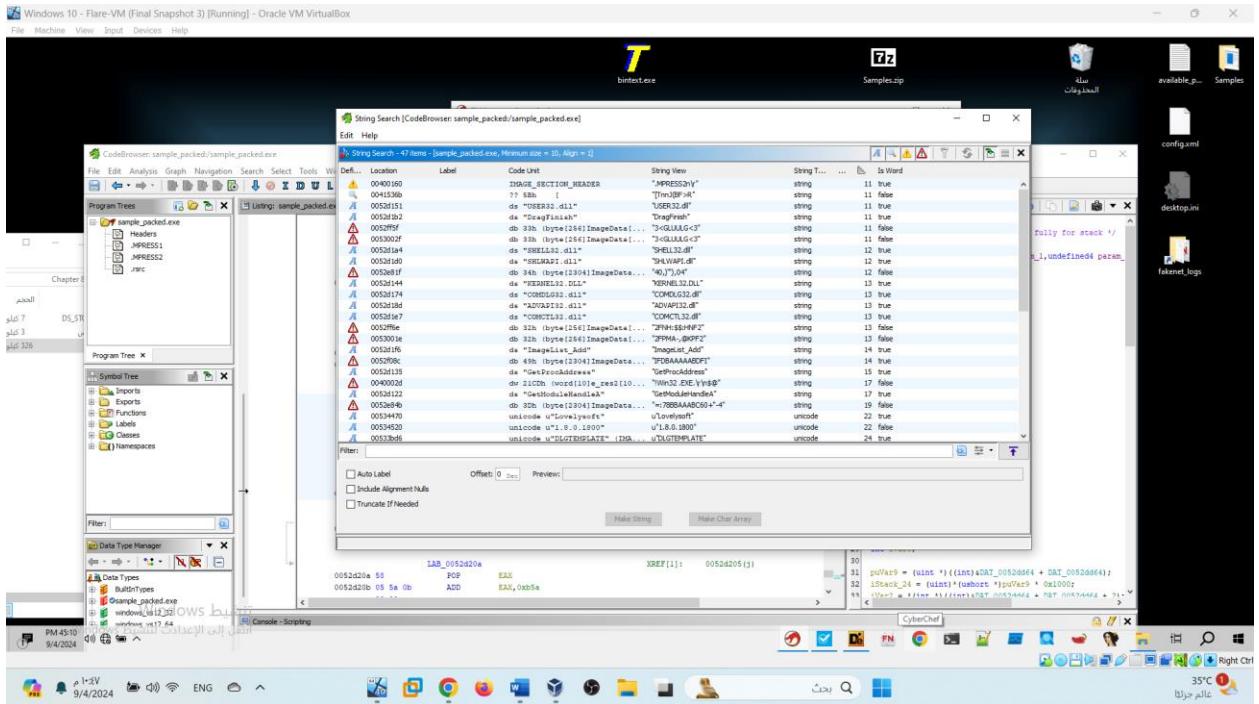
In sample_packed.exe file:





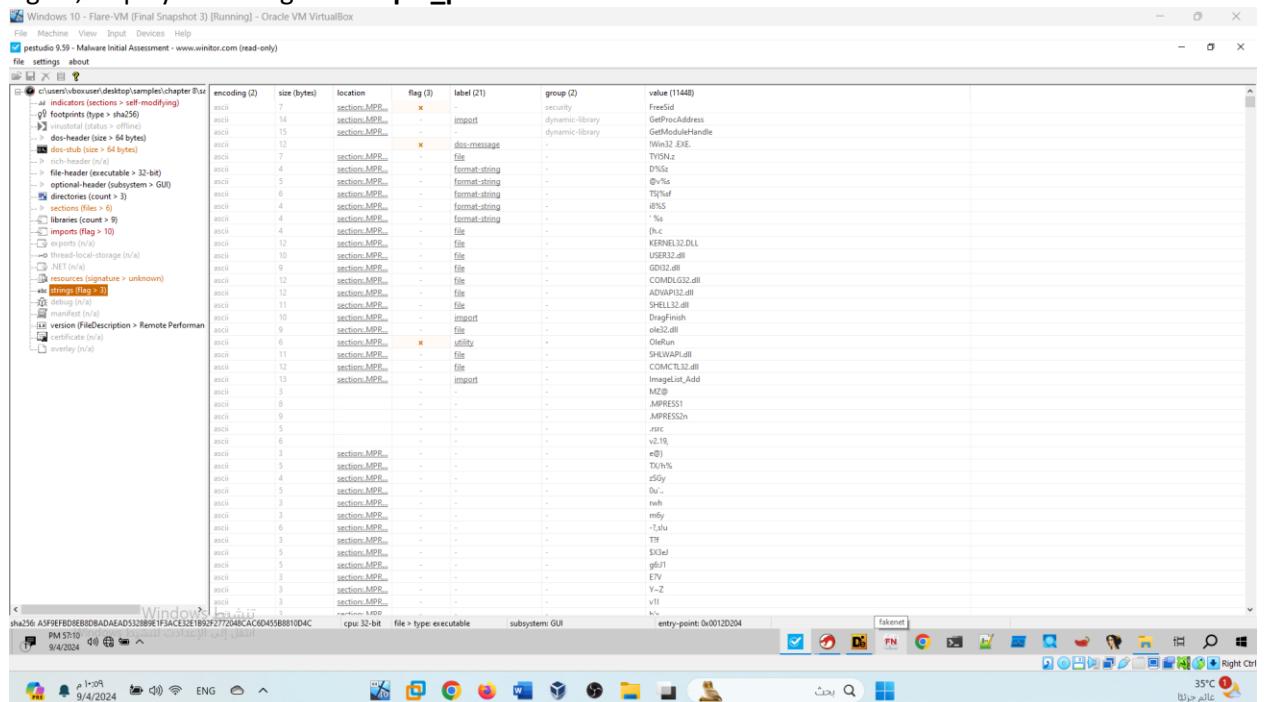






Task 2: Process hacker brbbot.exe:

A. Again, display the strings of sample_packed.exe in PeStudio

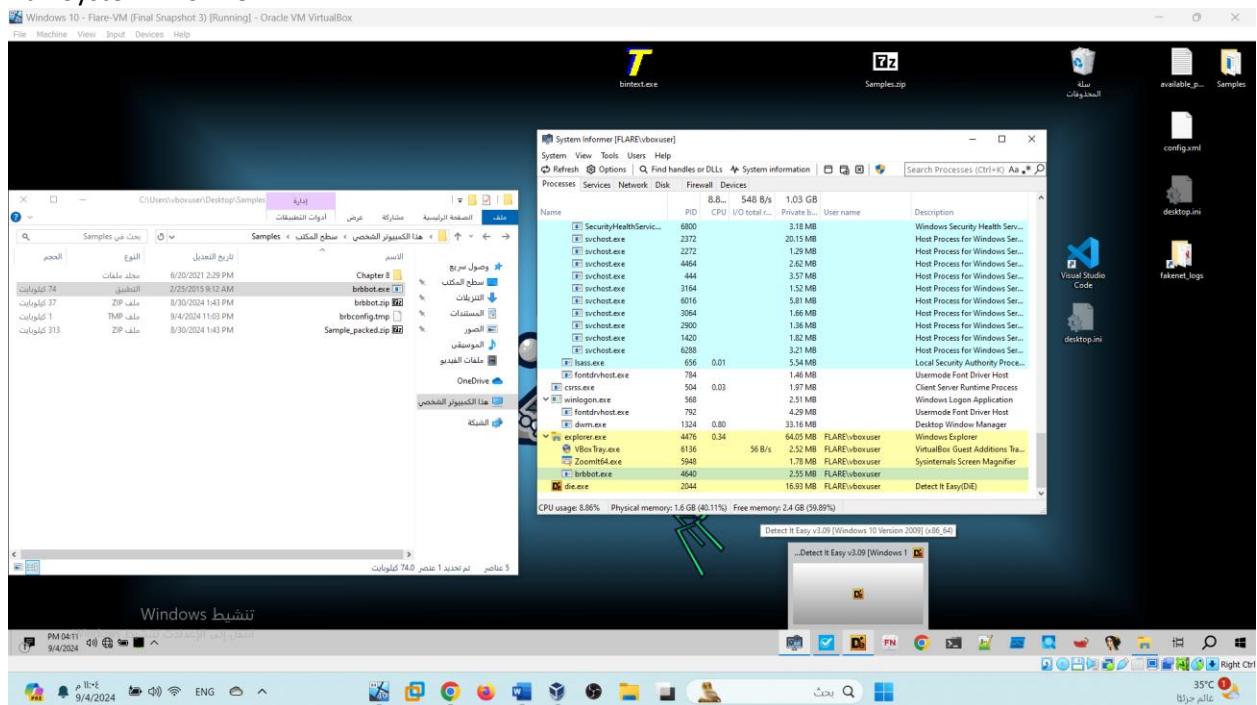


B. Can you see readable strings? Why?

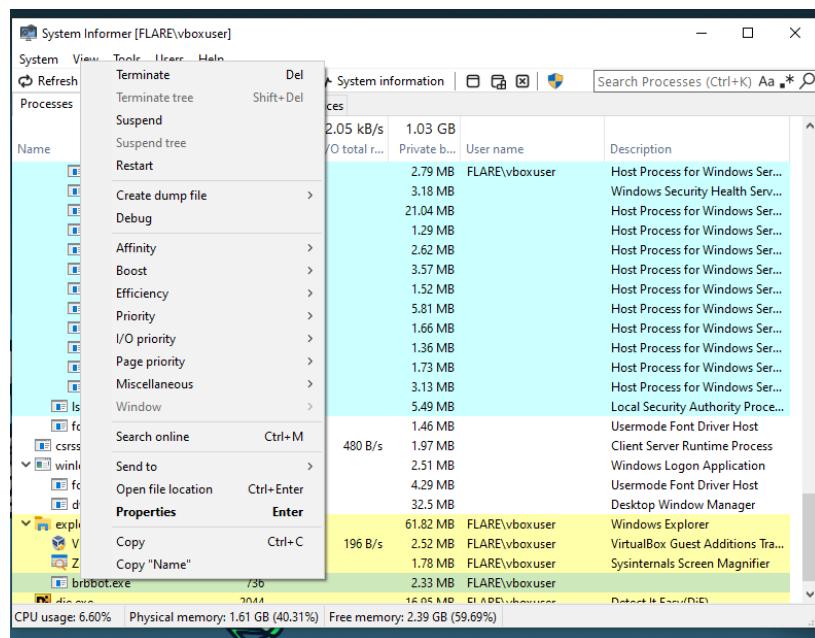
Yes, I can see readable strings such as "HttpSendRequestA," which is a function from the Windows API used to send HTTP requests. This function is commonly found in malware that communicates with a Command and Control (C2) server, exfiltrates data, or downloads additional malicious payloads.

C. Execute (double-click) **brbbot.exe**

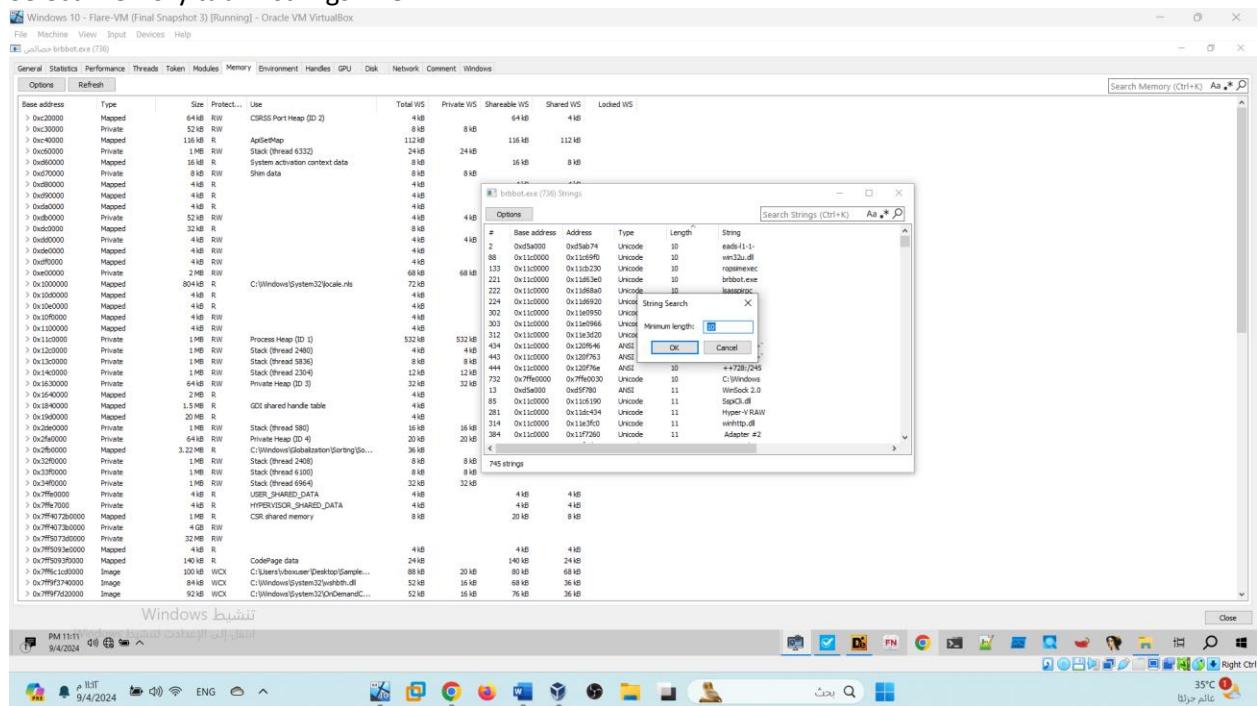
D. Run System informer



E. In system informer -> right-click on **brbbot.exe**

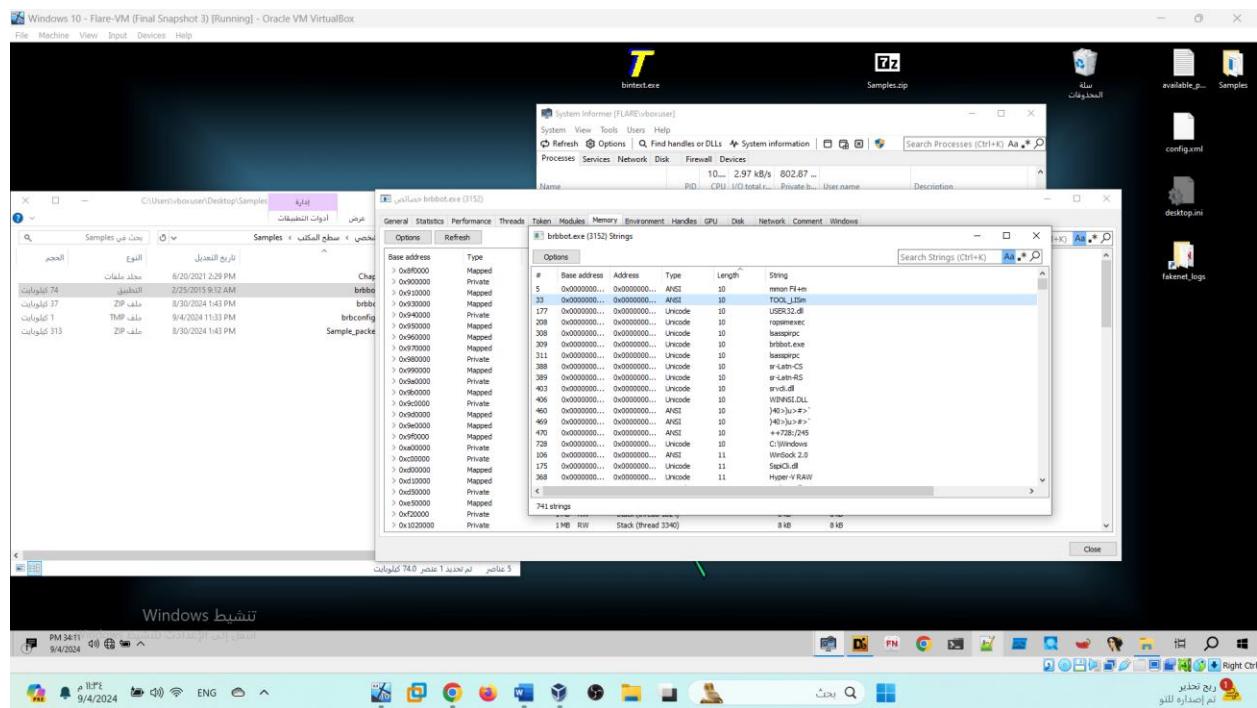


F. Select Memory tab -> strings -> OK



G. Can you see the strings? Why?

Yes, I can see the imported functions from the DLL, which are considered important strings in this malware, along with other notable strings that are part of the malware's behavior.

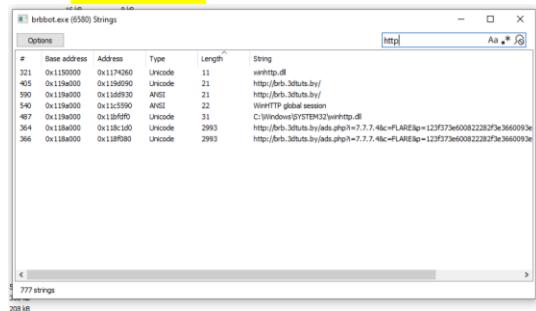


H. Click on Filter -> select Contains (case-insensitive)..

I. Search for **http**



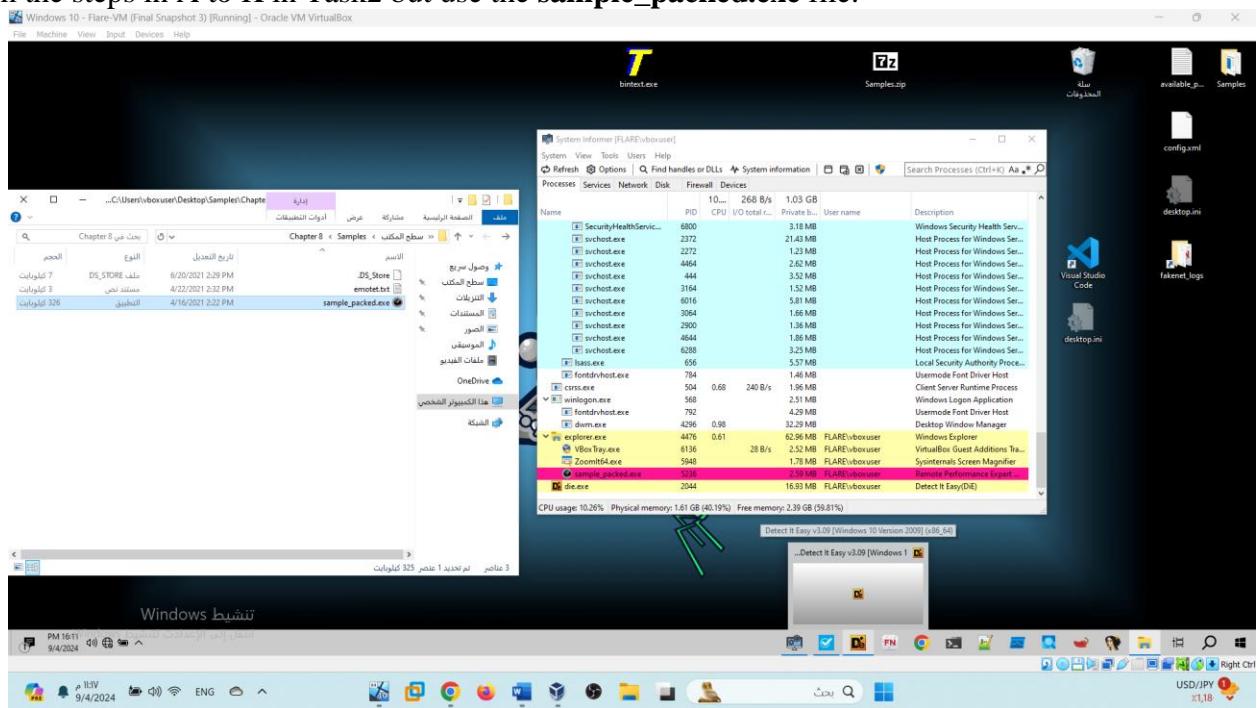
J. Take screenshot of the result

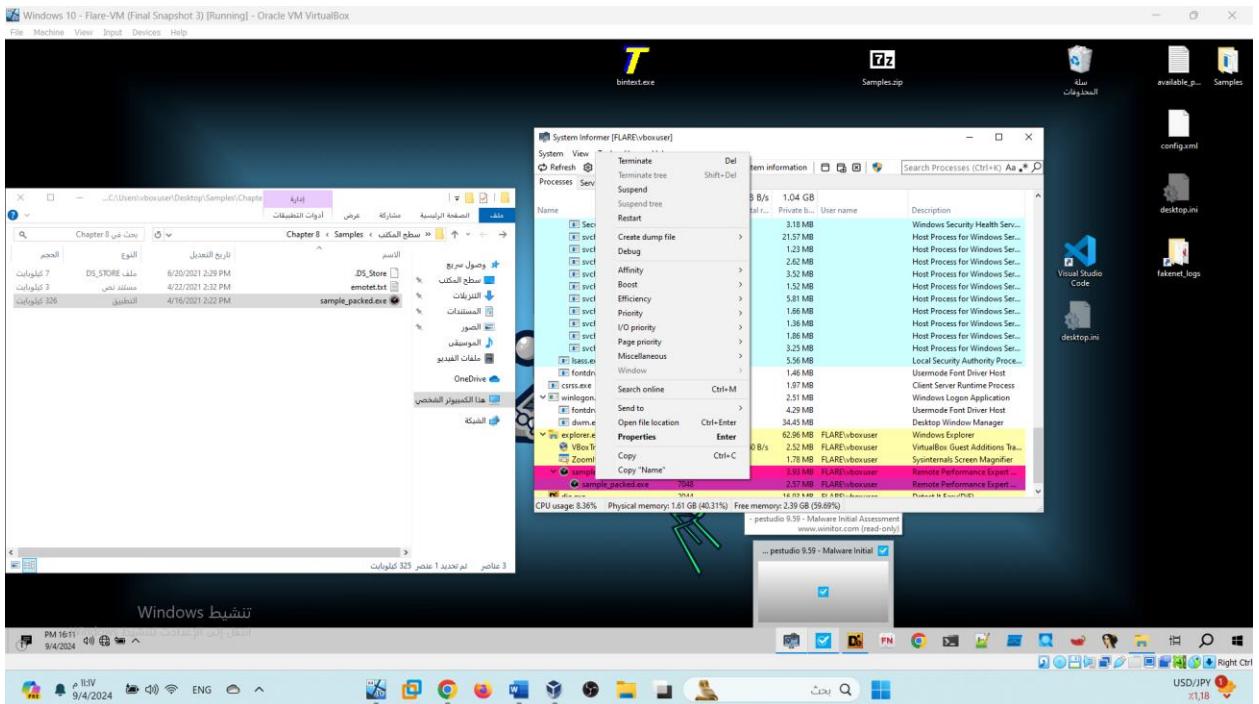


Task 3: Process Hacker (sample_packed.exe):

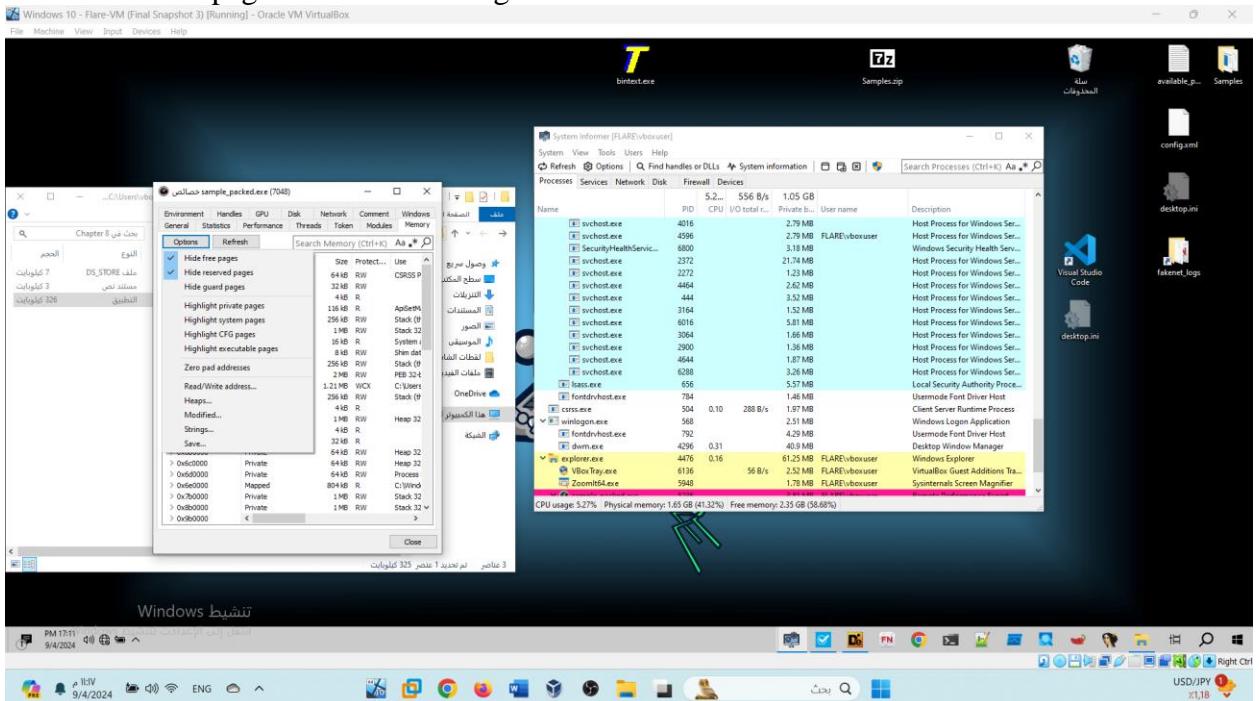
- Repeat steps A to K from Task 2 but for the packed executable (`sample_packed.exe`).
- Analyze strings from the memory of `sample_packed.exe` using Process Hacker

Perform the steps in A to K in Task2 but use the `sample_packed.exe` file.

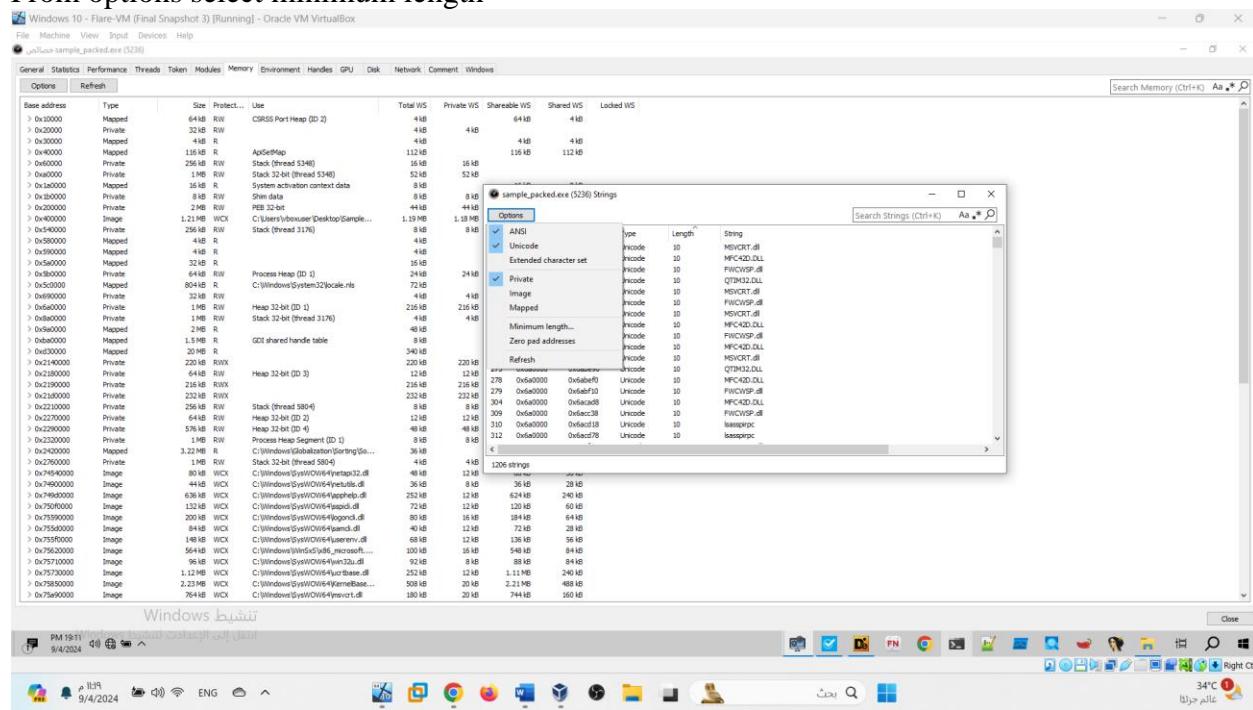




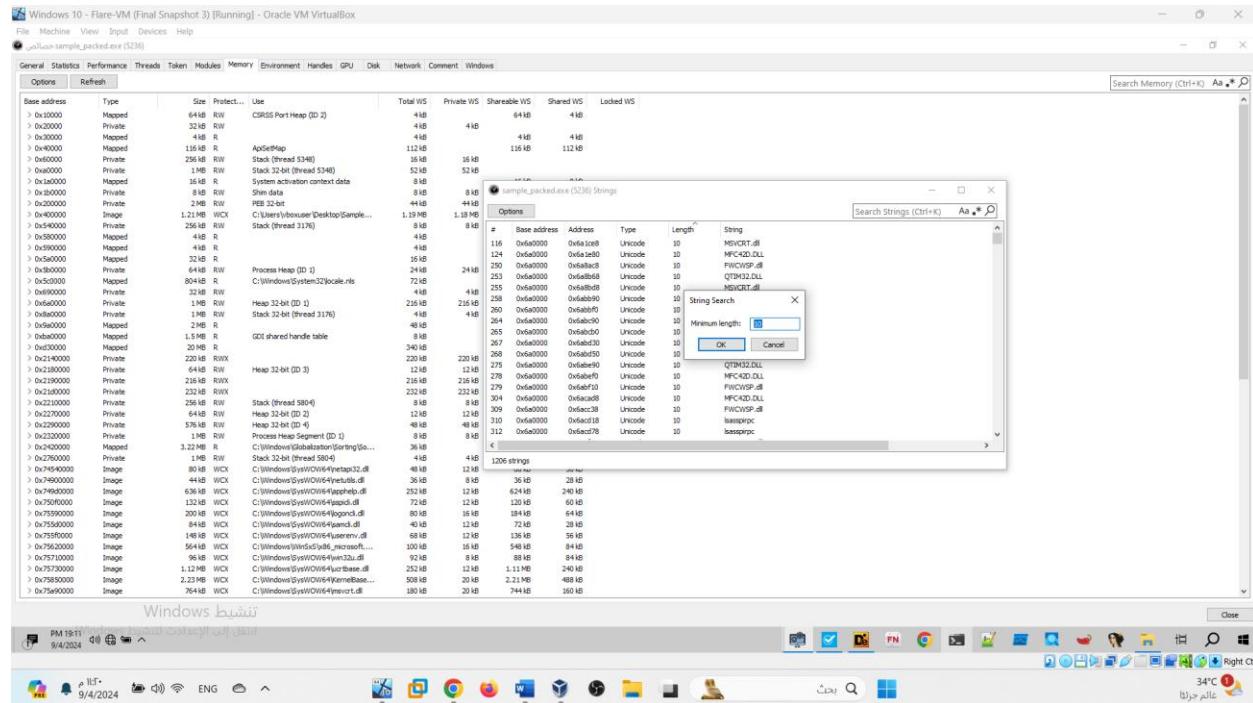
Select hide free pages then select strings

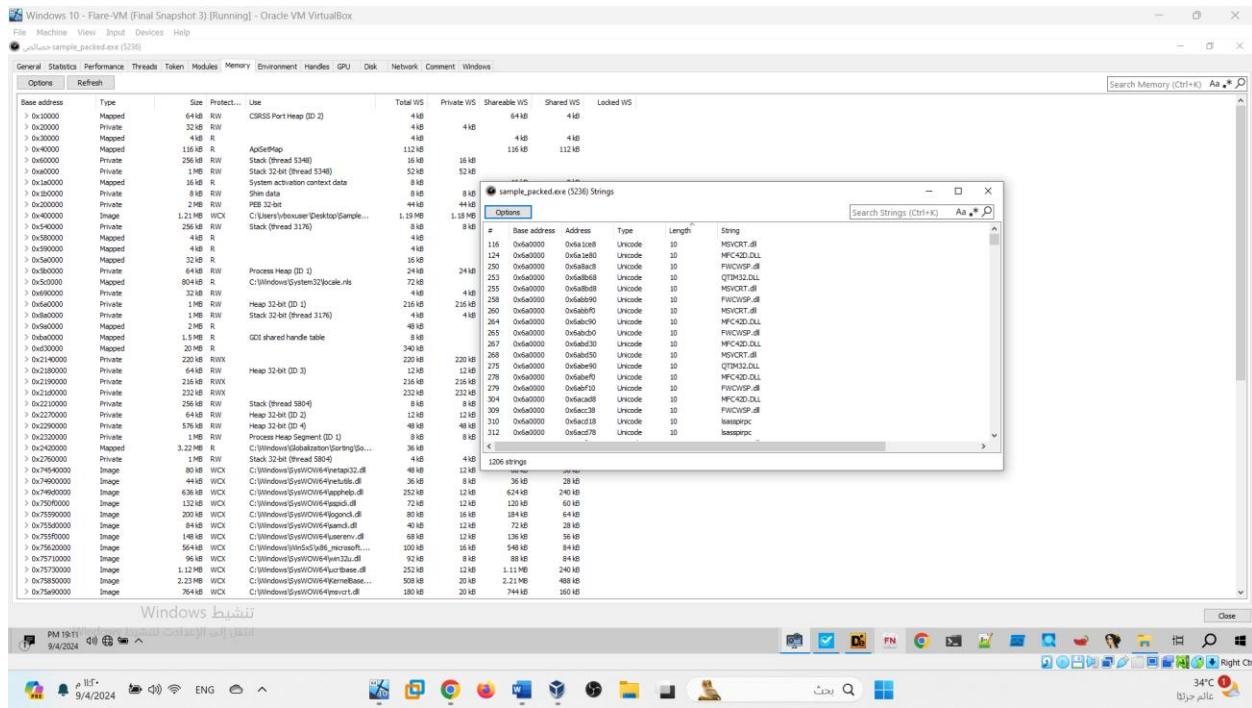


From options select minimum length



Enter 10

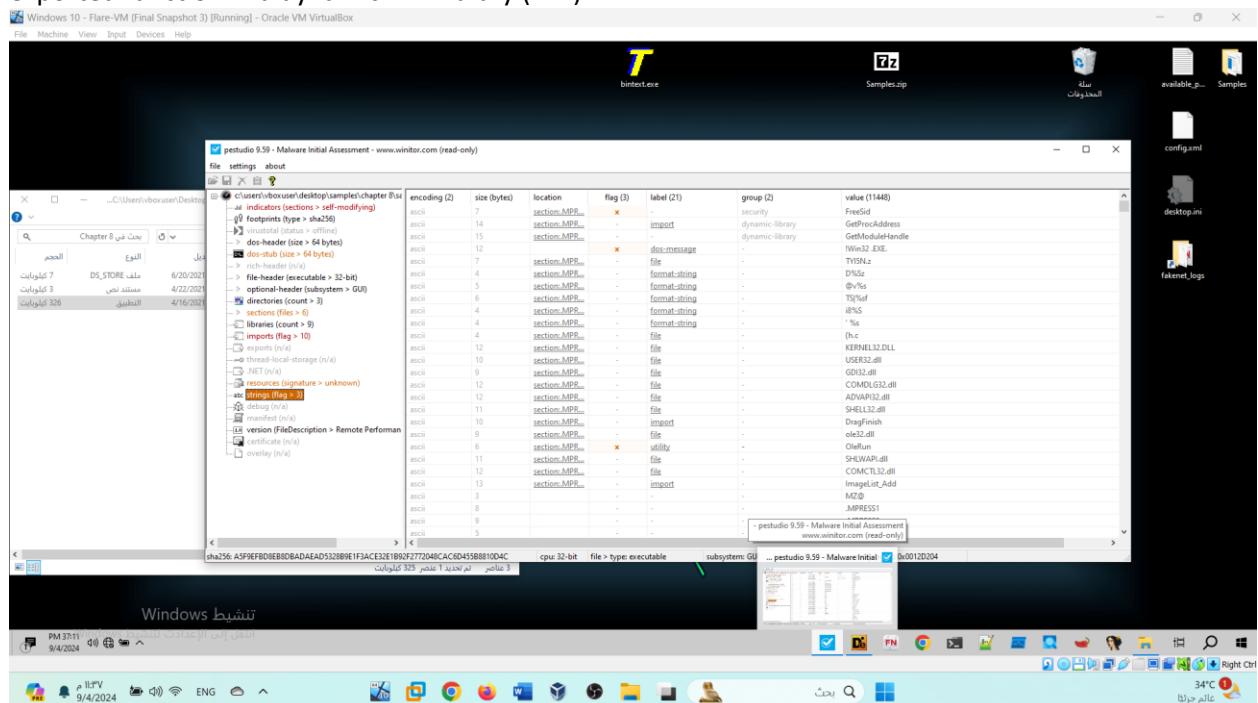




A. Answer the questions B & G for sample_packed.exe

B. Can you see readable strings? Why? From PEstudio

Yes, I can see some readable strings, such as the imported function FreeSid from the ADVAPI32.dll, which may indicate specific functions or methods being used by the malware. Another example is GetProcAddress, a common function used to obtain the address of an exported function in a dynamic-link library (DLL).



Can you see the strings? Why?

Yes, after executing the file, the imported functions from the DLLs become visible, and they are considered important strings in this malware, offering insights into its behavior.

#	Base address	Address	Type	Length	String
116	0x1e0000	0x1e108f	Unicode	10	MSVCR7.dll
124	0x1e0000	0x1e120f	Unicode	10	MFC42D.dll
250	0x1e0000	0x1e132f	Unicode	10	FVCVISP.dll
253	0x1e0000	0x1e136f	Unicode	10	QTIM32.DLL
255	0x1e0000	0x1e138f	Unicode	10	MSVCR7.dll
258	0x1e0000	0x1e13bf	Unicode	10	FVCVISP.dll
260	0x1e0000	0x1e149f	Unicode	10	MSVCR7.dll
264	0x1e0000	0x1e151f	Unicode	10	MSVCR7.dll
265	0x1e0000	0x1e1abf	Unicode	10	FVCVISP.dll
267	0x1e0000	0x1e1af0	Unicode	10	MFC42D.dll
268	0x1e0000	0x1e1af5	Unicode	10	MSVCR7.dll
273	0x1e0000	0x1e1b1f	Unicode	10	QTIM32.DLL
278	0x1e0000	0x1e1b3f	Unicode	10	MFC42D.dll
279	0x1e0000	0x1e1b7f	Unicode	10	FVCVISP.dll
304	0x1e0000	0x1eac3f	Unicode	10	MFC42D.dll
309	0x1e0000	0x1eac38	Unicode	10	FVCVISP.dll
310	0x1e0000	0x1eac39	Unicode	10	MSVCR7.dll
312	0x1e0000	0x1edc7f	Unicode	10	lessprivc
324	0x1e0000	0x1fac1f	Unicode	10	FVCVISP.dll
326	0x1e0000	0x1fac2f	Unicode	10	MSVCR7.dll
327	0x1e0000	0x1fac3f	Unicode	10	MFC42D.dll
328	0x1e0000	0x1fac38	Unicode	10	MFC42D.dll
329	0x1e0000	0x1fad3f	Unicode	10	FVCVISP.dll
330	0x1e0000	0x1fad5f	Unicode	10	MSVCR7.dll
336	0x1e0000	0x1fad58	Unicode	10	MSVCR7.dll
379	0x1e0000	0x1fb1ff	Unicode	10	user32.dll
383	0x1e0000	0x1fb1ef	Unicode	10	sr_Latin-CS
384	0x1e0000	0x1fb21e	Unicode	10	sr_Latin-RS
414	0x1e0000	0x1fb35f	Unicode	10	ed.exe^C
592	0x1e0000	0x1ecc3f	Unicode	10	USER32.dll
593	0x1e0000	0x1ecc39	Unicode	10	lessprivc
594	0x1e0000	0x1ecc40	Unicode	10	msvcr7.dll
595	0x1e0000	0x1ecc5d	Unicode	10	C:\Windows
597	0x1e0000	0x1ecc5f	Unicode	10	user32.dll
598	0x1e0000	0x1ecc60	Unicode	10	C:\Windows
599	0x1e0000	0x1ecc61	Unicode	10	C:\Windows
600	0x1e0000	0x1ecc60	Unicode	10	EXTRACTOPT
602	0x1e0000	0x1ecc6f	Unicode	10	C:\Windows
603	0x1e0000	0x1ecc7f	Unicode	10	user32.dll
641	0x1e0000	0x2198ef	Unicode	10	MSVCR7.dll
681	0x21e000	0x2198ef	ANSI	10	W:\>O_>O_>O
682	0x21e000	0x2198fb	ANSI	10	h^~K~d~^O
683	0x21e000	0x2196df	ANSI	10	X\ip_Urg#
760	0x21e000	0x2194ef	ANSI	10	user32.dll
789	0x21e000	0x2194f0	ANSI	10	SysAllocMem
774	0x21e000	0x2194ef	ANSI	10	NTUSER.DAT
777	0x21e000	0x219df7	ANSI	10	ROOOTCIMV2