

National Forensic Sciences University

School of Cyber security and Digital Forensics



Subject: CTMSCS S2 P3 Malware Analysis

(TA-II Assignment)

Submitted to: Mr. Dharmesh Dave and Mr. Parag Rughani

Submitted by: Disha Sharma (2401030020014)

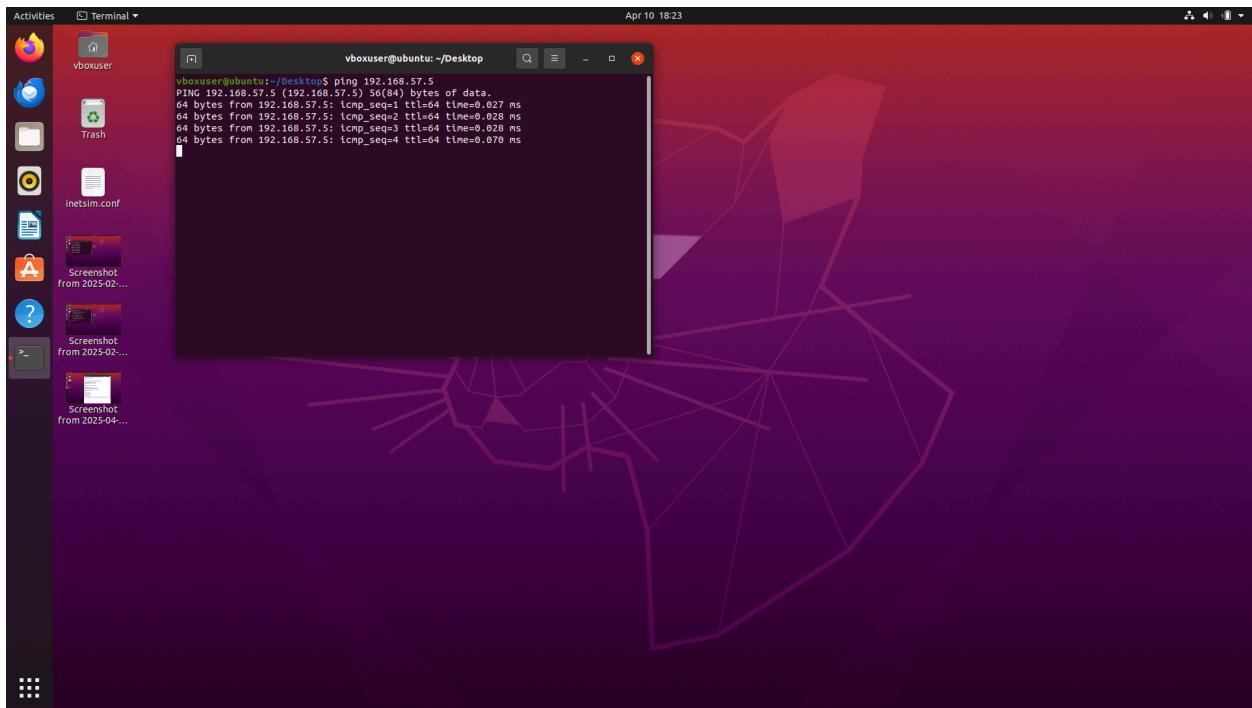
Submission Date: 03/04/2025

INDEX

Dynamic Analysis Lab set-up and analysis.

1. 02 VMs (Windows+Linux)
2. Both shall be pingable
3. Connected with Host only network adapter (connect with internet whenever required but not during analysis)
4. Install minimum requirements for normal operations in both the VMs. (i.e. browser, office, pdf reader, etc.)
5. Install sysinternals and Apate DNS in windows VM
6. Install and configure inetsim in Linux
7. Simulate the fake internet in windows as mentioned in the chapter-03 of the Practical Malware Analysis Book.
8. Complete the analysis of all the PE files of Lab 03 as mentioned at the end of the chapter -03 of the said book.

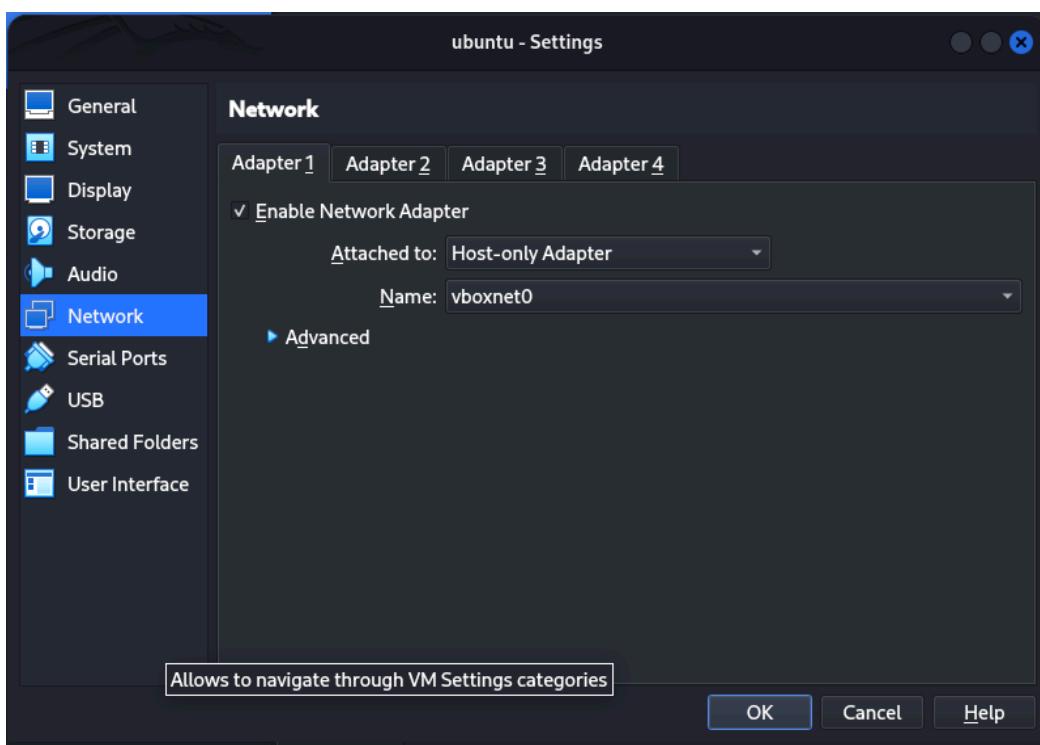
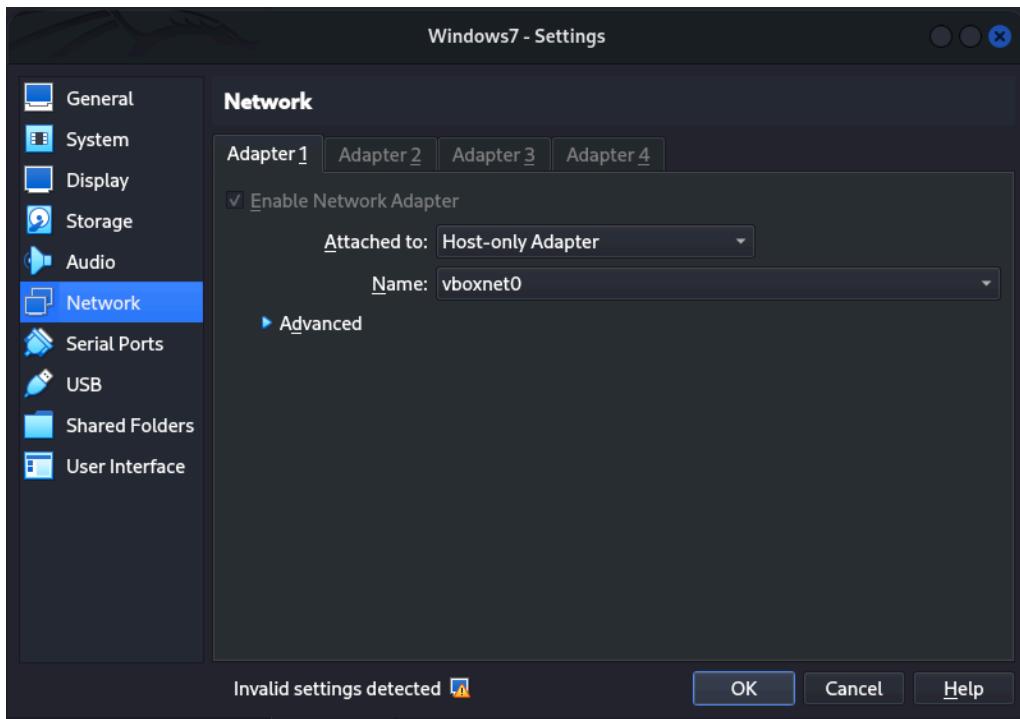
1. 02 VMs (Windows+Linux)



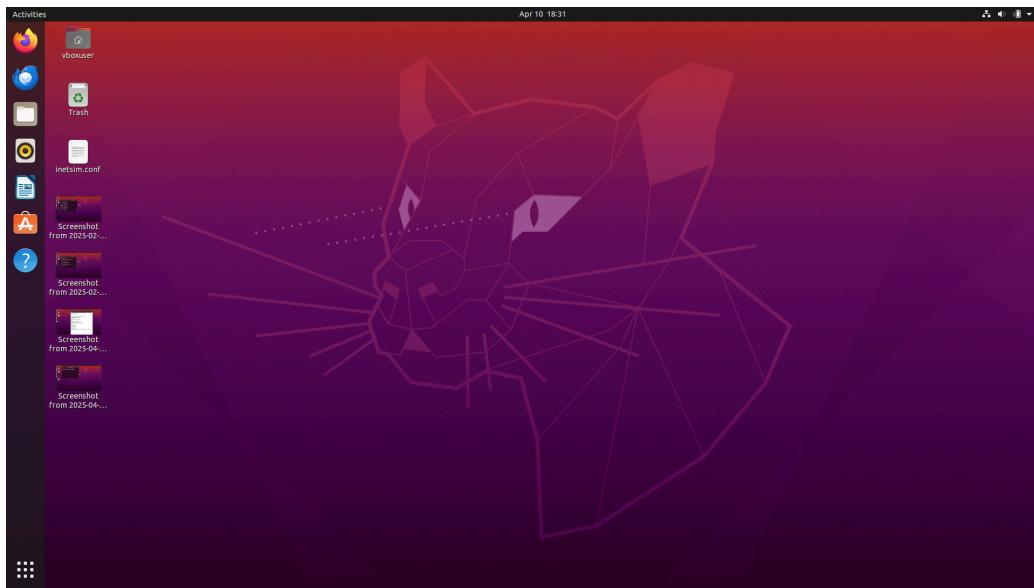
A screenshot of a Windows cmd.exe terminal window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays the following text:

```
Default Gateway . . . . . :  
Tunnel adapter isatap.{DBDABFD5-F587-4EE3-9CD0-1D1D474860BC} :  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . . . :  
C:\Users\Jafar>clear  
'clear' is not recognized as an internal or external command,  
operable program or batch file.  
C:\Users\Jafar>ping 192.168.56.107  
Pinging 192.168.56.107 with 32 bytes of data:  
Reply from 192.168.56.107: bytes=32 time<1ms TTL=128  
Ping statistics for 192.168.56.107:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
C:\Users\Jafar>
```

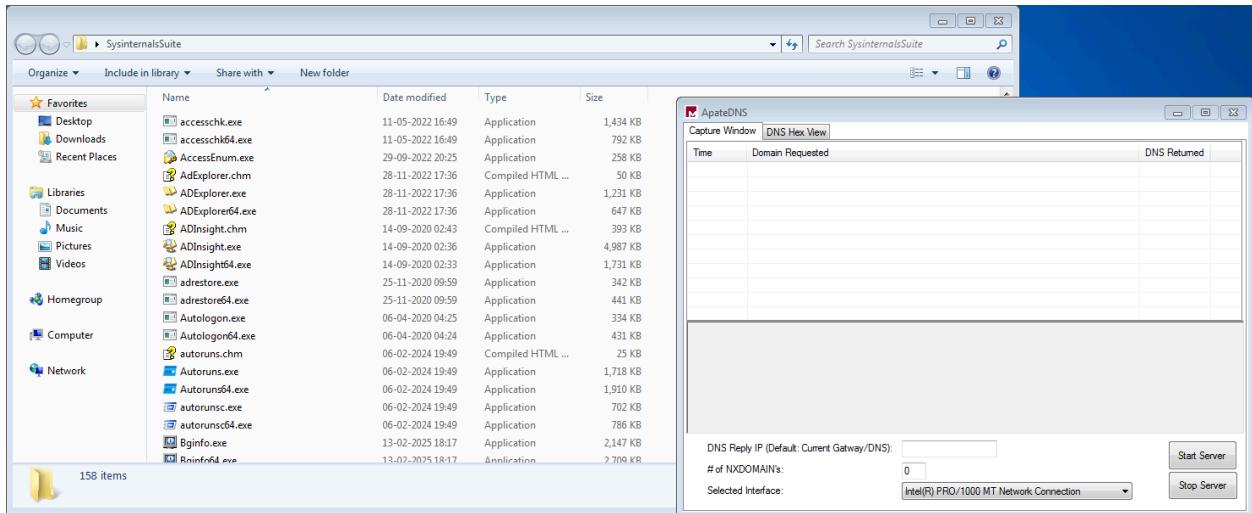
3. Connected with Host only network adapter (connect with internet whenever required but not during analysis)



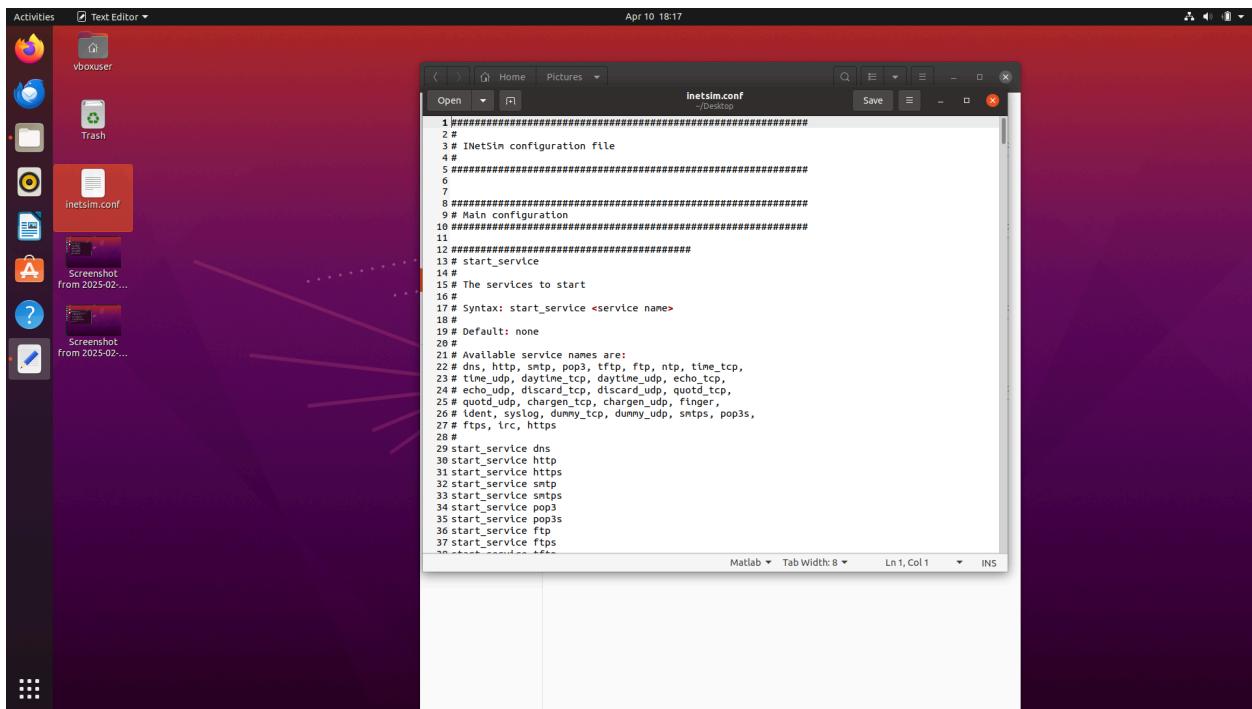
4. Install minimum requirements for normal operations in both the VMs. (i.e. browser, office, pdf reader, etc.)



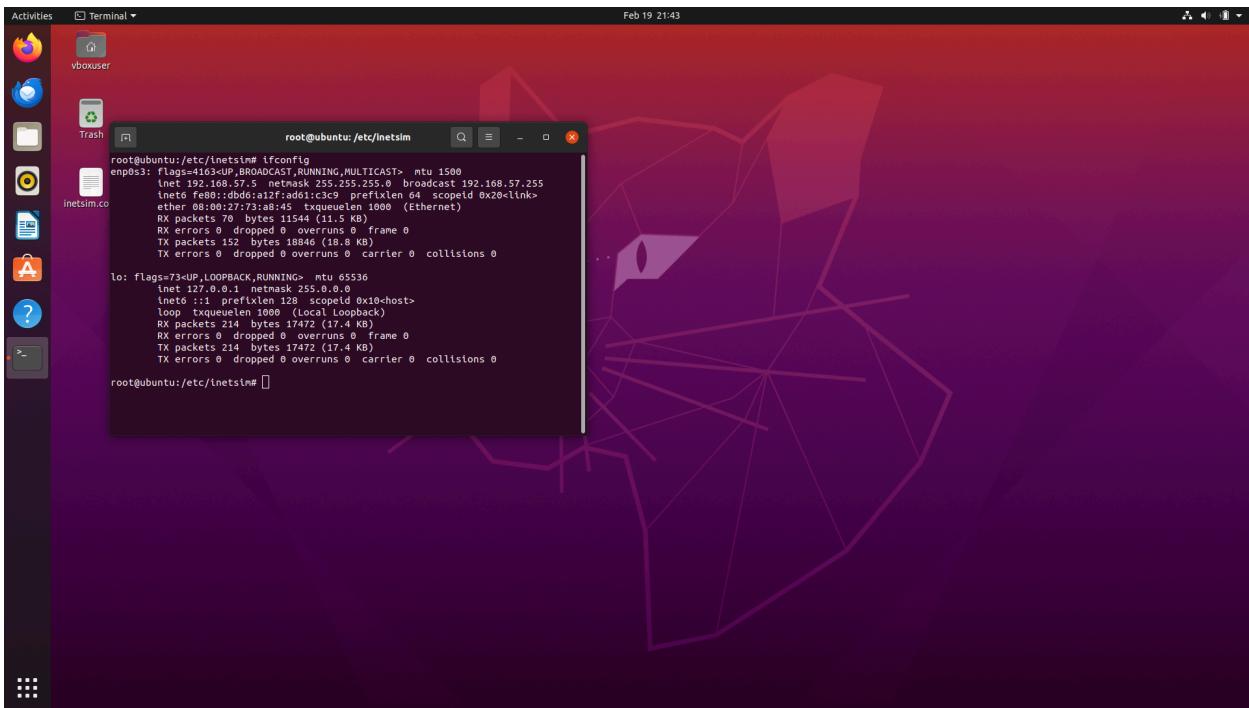
5. Install sysinternals and Apate DNS in windows VM



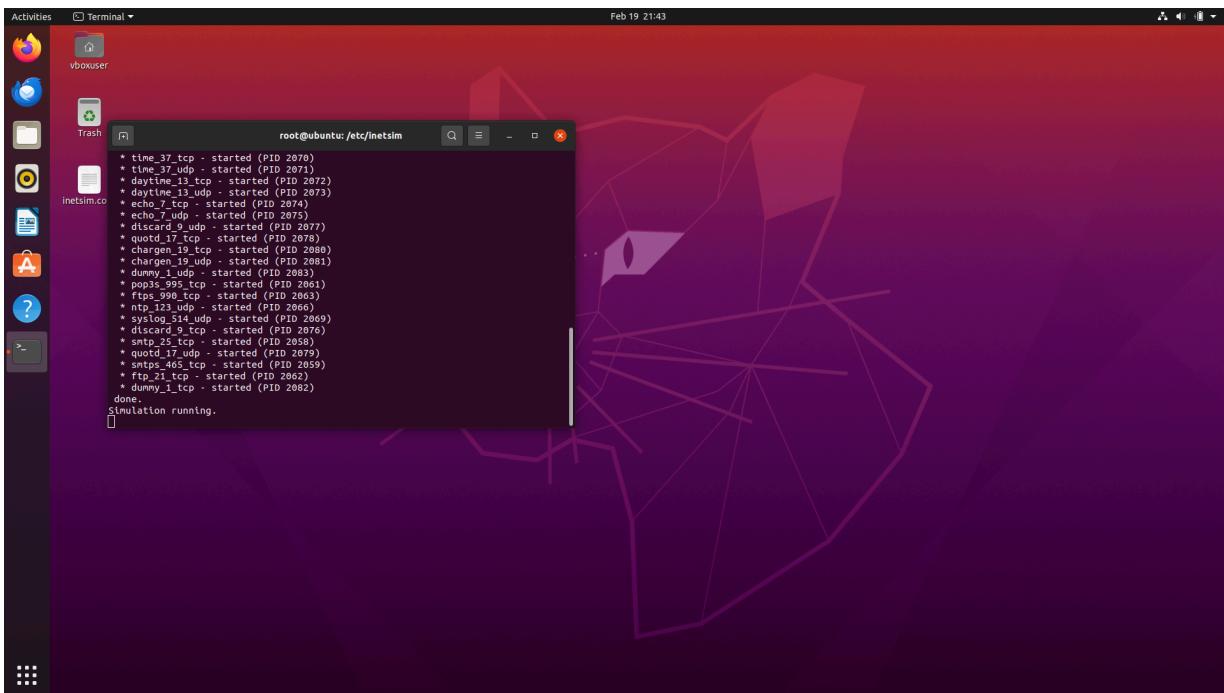
6. Install and configure inetsim in Linux



7. Simulate the fake internet in windows as mentioned in the chapter-03 of the Practical Malware Analysis Book.



Configuring inetsim using IP Address of Linux VM



Running the Inetsim simulation

ApateDNS

Capture Window DNS Hex View

Time	Domain Requested	DNS Returned
21:44:28	optimizationguide-pa.googleapis.com	FOUND
21:44:37	www.gstatic.com	NXDOMAIN
21:44:37	www.gstatic.com	NXDOMAIN
21:44:38	www.gstatic.com	FOUND
21:45:12	update.googleapis.com	FOUND
21:45:18	www.google.com	FOUND
21:45:18	www.google.com	FOUND

```
[+] Using 192.168.57.5 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.
[+] Sending 2 NXDOMAIN replies to clients
[+] Server started at 21:43:38 successfully.
```

DNS Reply IP (Default: Current Gateway/DNS):

of NXDOMAIN's:

Selected Interface:

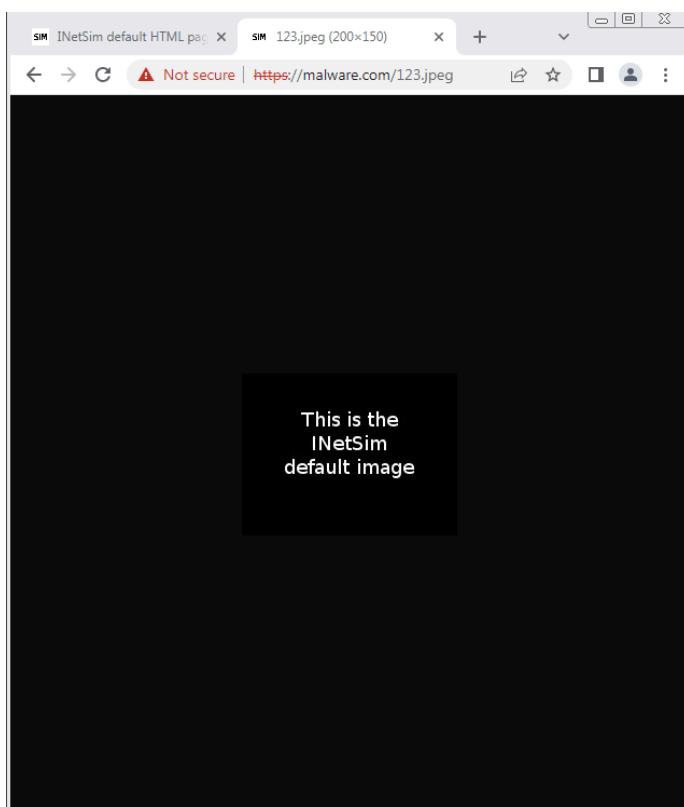
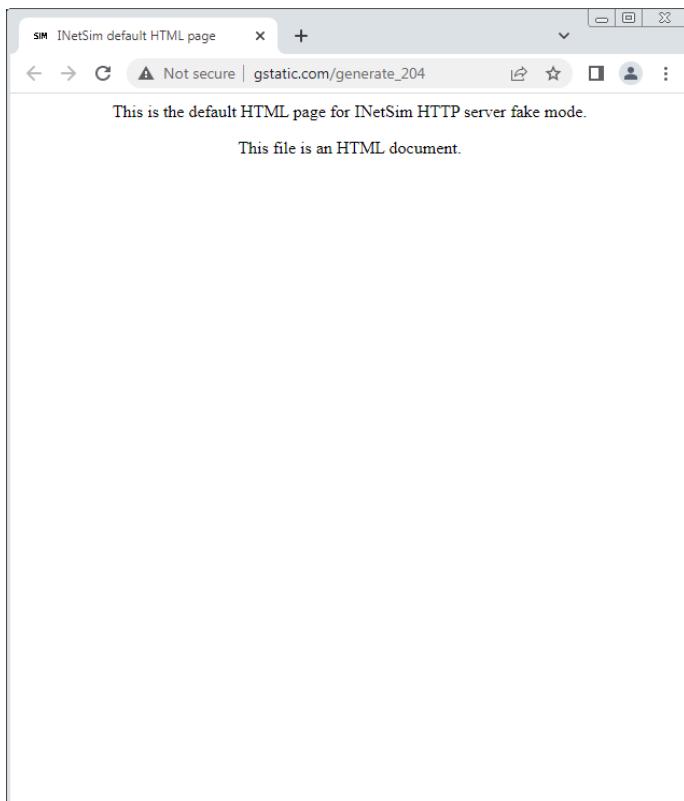
Starting the server at ApateDNS.

```
[+] Using 192.168.57.5 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.
[+] Sending 2 NXDOMAIN replies to clients
[+] Server started at 21:43:38 successfully.
[+] Stopping Server...
[+] DHCP detected, setting DNS back to DHCP.
[+] DNS Restored.
[+] Interfaces list has been refreshed.
```

DNS Reply IP (Default: Current Gateway/DNS):

of NXDOMAIN's:

Selected Interface:



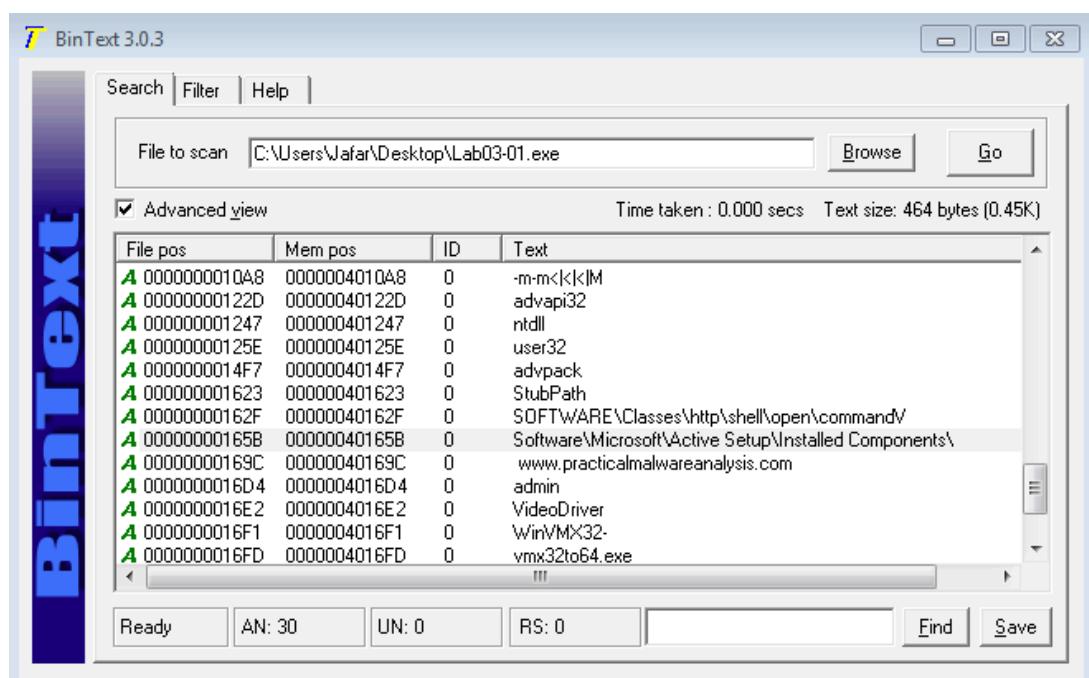
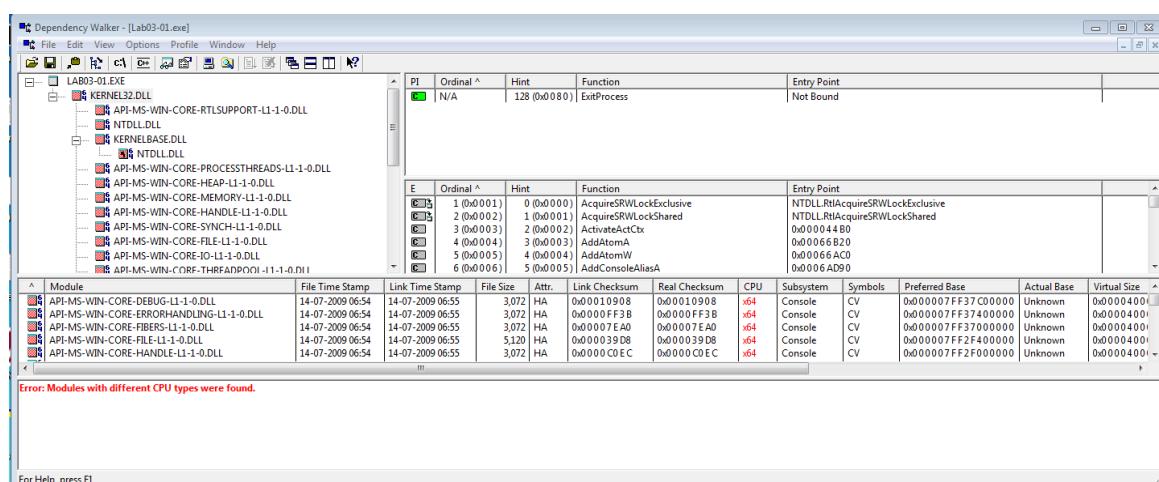
Successfully configured Inetsim

8. Complete the analysis of all the PE files of Lab 03 as mentioned at the end of the chapter -03 of the said book.

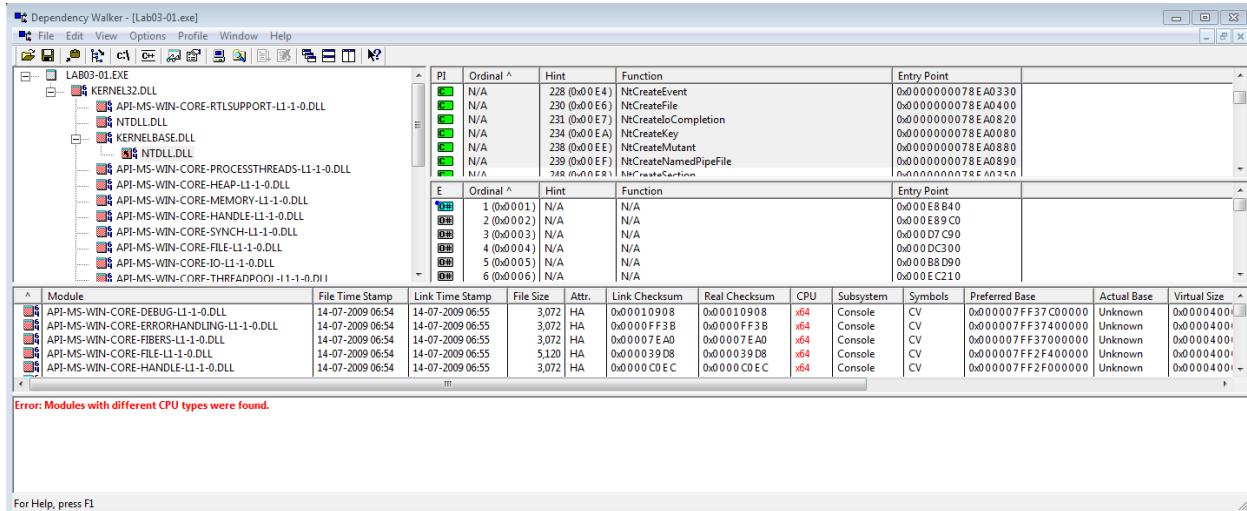
3-1

Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools.

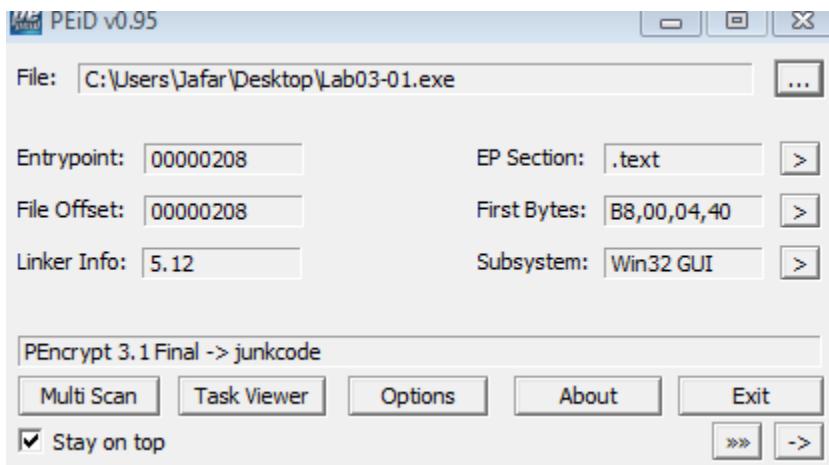
1.What are this malware's imports and strings?



2.What are the malware's host-based indicators?

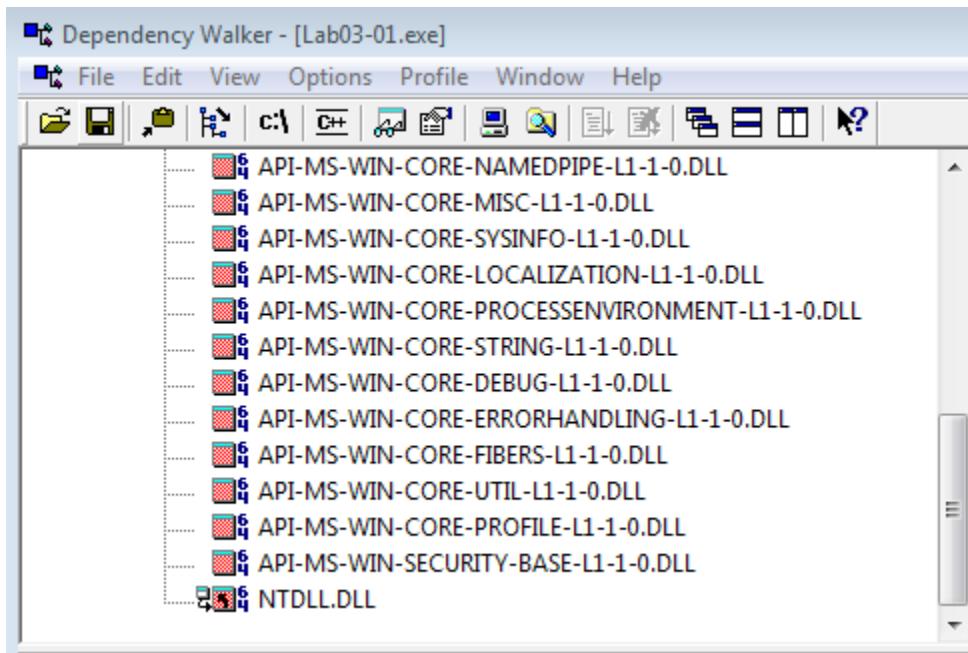


The NTdll.dll imports functions related to creating and modifying files, events and keys.



The file has also been packed using the PEncrypt packer

3. Are there any useful network-based signatures for this malware? If so, what are they?



No network based indicators were found since no presence of DLLs were seen like Ws2_32.dll or Wininet.dll

3-2

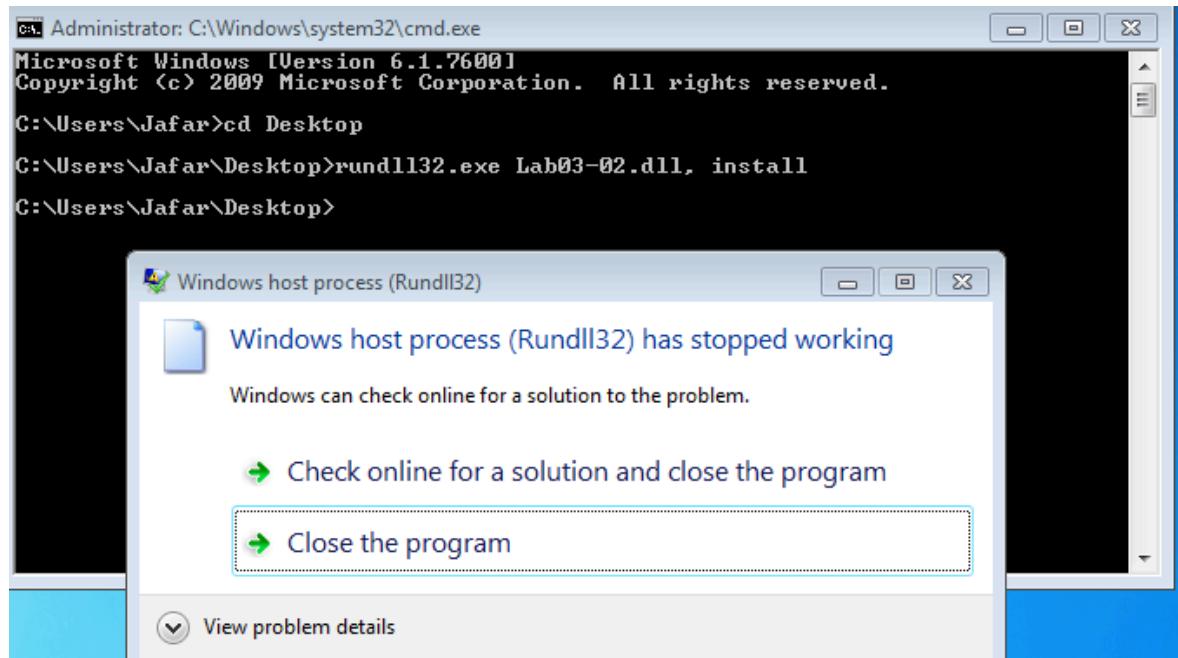
Analyze the malware found in the file Lab03-02.dll using basic dynamic analysis tools.

1. How can you get this malware to install itself?

pFile	Data	Description	Value
00004400	0000568C	HintName RVA	0147 OpenServiceA
00004404	0000567C	HintName RVA	0170 SetServiceStatus
00004408	00005680	HintName RVA	0172 RegOpenKeyExA
0000440C	00005559	HintName RVA	017B RegQueryValueExA
00004410	0000564A	HintName RVA	0159 RegCloseKey
00004414	00005638	HintName RVA	0145 OpenSCManagerA
00004418	00005626	HintName RVA	004C CreateServiceA
00004420	00005610	HintName RVA	0034 CloseServiceHandle
00004424	00005604	HintName RVA	0163 RegSetValueExA
00004428	000056EE	HintName RVA	0195 RegisterServiceA
0000442C	000056D0	HintName RVA	018E RegisterServiceCtrlHandlerA
0000442C	0000569C	HintName RVA	01AE SetServiceStatus
00004430	00000000	End of Import	ADVAPI32.dll
00004434	00005548	HintName RVA	0150 GetShortPathA
00004438	00005540	HintName RVA	0043 GetShortPathW
0000443C	00005568	HintName RVA	0045 GetCurrentDirectoryA
00004440	00005536	HintName RVA	0044 CreateProcessA
00004444	00005590	HintName RVA	0308 IsInFile
00004448	0000559C	HintName RVA	0271 SetLastError
0000444C	000055AC	HintName RVA	01F5 OutputDebugStringA
00004450	000055A0	HintName RVA	0010 CreateModule
00004454	0000551C	HintName RVA	0210 LoadFile
00004458	0000550C	HintName RVA	0165 GetTempPathA
0000445C	000054F8	HintName RVA	0121 GetLongPathNameA
00004460	000054E8	HintName RVA	01C2 LoadLibraryA
00004464	000054D8	HintName RVA	013E GetProcAddress
00004468	000054C6	HintName RVA	004A CreateThread

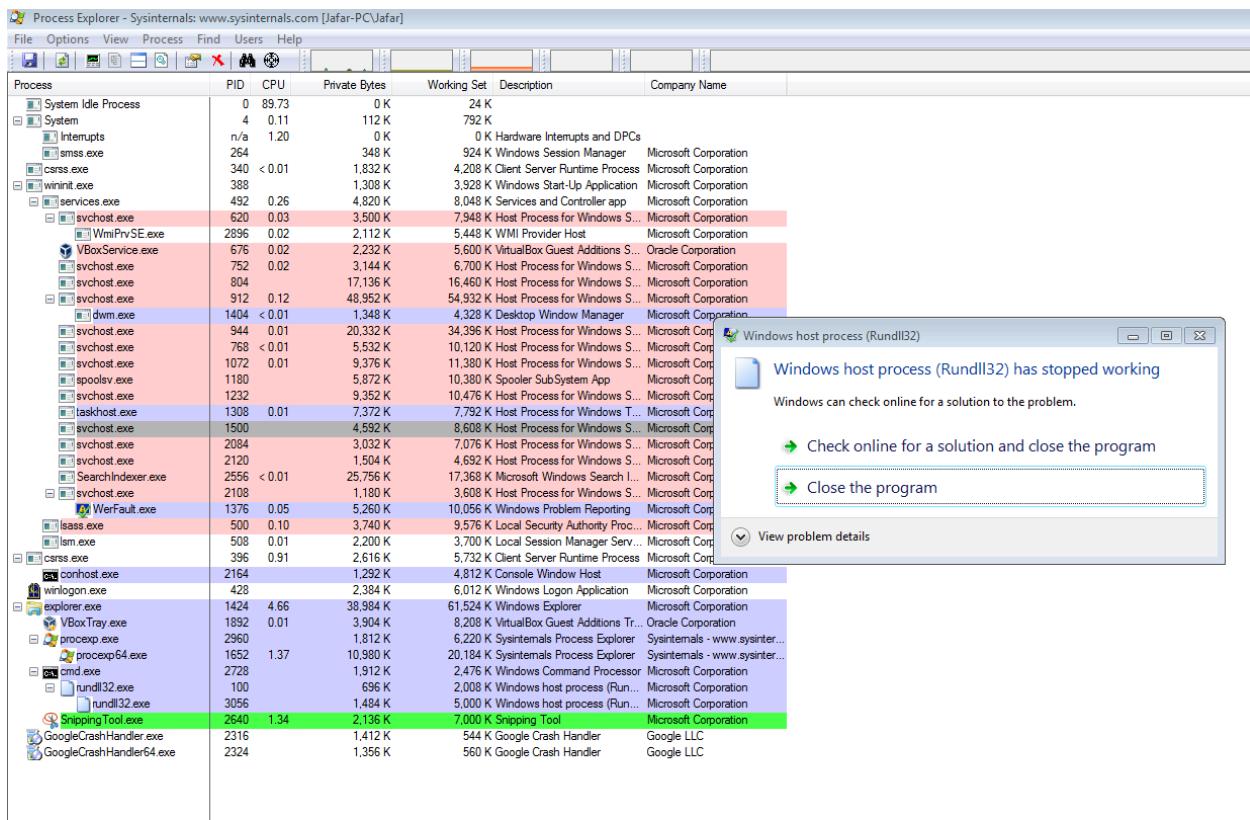
The malware runs as a service and thus installs itself.

2. How would you get this malware to run after installation?



Program can be run using the CLI rundll32.exe

3. How can you find the process under which this malware is running?



The system crashes on running the respective dll.

4. Which filters could you set in order to use procmon to glean Information?

Because there's likely to be multiple svchost processes, we can filter by the Process ID to glean information only on the svchost process responsible for running this malware.

5.What are the malware's host-based indicators?

PI	Ordinal ^	Hint	Function	Entry Point
N/A	52 (0x034)	N/A	CloseServiceHandle	Not Bound
N/A	76 (0x04C)	N/A	CreateServiceA	Not Bound
N/A	120 (0x078)	N/A	DeleteService	Not Bound
N/A	325 (0x145)	N/A	OpenSCManagerA	Not Bound
N/A	327 (0x147)	N/A	OpenServiceA	Not Bound
N/A	347 (0x15E)	N/A	ReClassKey	Not Bound
N/A	350 (0x15F)	N/A	RegCreateKeyA	Not Bound
N/A	370 (0x172)	N/A	RegOpenKeyExA	Not Bound
N/A	379 (0x17B)	N/A	RegQueryValueExA	Not Bound
N/A	390 (0x186)	N/A	RegSetValueExA	Not Bound
N/A	398 (0x18E)	N/A	RegisterServiceCtrlHandlerA	Not Bound
N/A	430 (0x1AE)	N/A	SetServiceStatus	Not Bound

Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
IESHIM.DLL	Error opening file. The system cannot find the file specified (2).											
ADVAPI32.DLL	14-07-2009 07:10	14-07-2009 06:54	877,056	A	0x000E415A	0x000E415A	x64	Console	CV	0x00007FF7FF10000	Unknown	0x0000DB00
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x0000C943	0x0000C943	x64	Console	CV	0x0000000004000000	Unknown	0x00003000	
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x0000DD30	0x0000DD30	x64	Console	CV	0x00007FF38000000	Unknown	0x00004000	
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x00007FF37C00000	Unknown	0x00004000	

For Help, press F1

Dependency walker shows the creation, modification of registry keys, files and service handles which are potential host based indicators.

6.Are there any useful network-based signatures for this malware?

PI	Ordinal ^	Hint	Function	Entry Point
N/A	69 (0x045)	N/A	HttpOpenRequestA	Not Bound
N/A	71 (0x047)	N/A	HttpQueryInfoA	Not Bound
N/A	73 (0x049)	N/A	HttpSendRequestA	Not Bound
N/A	86 (0x056)	N/A	InternetCloseHandle	Not Bound
N/A	90 (0x05A)	N/A	InternetConnectA	Not Bound
N/A	111 (0x06F)	N/A	InternetOpenA	Not Bound
N/A	119 (0x077)	N/A	InternetReadFile	Not Bound

Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
IESHIM.DLL	Error opening file. The system cannot find the file specified (2).											
ADVAPI32.DLL	14-07-2009 07:40	14-07-2009 06:54	877,056	A	0x000E415A	0x000E415A	x64	Console	CV	0x00007FF7FF10000	Unknown	0x0000DB00
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x0000C943	0x0000C943	x64	Console	CV	0x0000000004000000	Unknown	0x00003000	
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x0000DD30	0x0000DD30	x64	Console	CV	0x00007FF38000000	Unknown	0x00004000	
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x00007FF37C00000	Unknown	0x00004000	
API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL	14-07-2009 06:54	3,072	HA	0x0000D1A2	0x0000D1A2	x64	Console	CV	0x00007FF37B00000	Unknown	0x00004000	

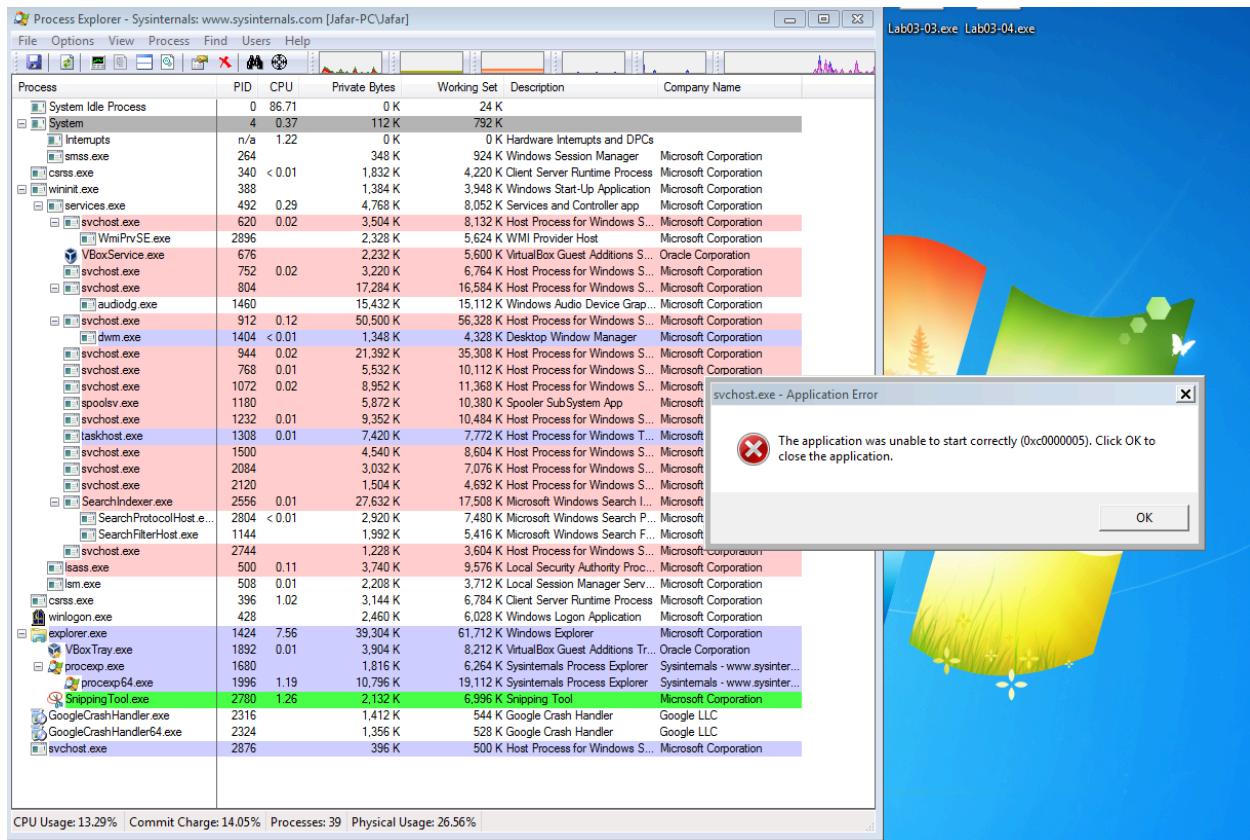
For Help, press F1

The file shows the presence of network based dlls as well as network based functions as network based indicators.

3-3

Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment.

1.What do you notice when monitoring this malware with Process Explorer?



The executable crashes while running even with admin privileges

2.Can you identify any live memory modifications?

To look for memory analysis we need to examine the svchost service but since the executable crashes, further analysis not possible.

3.What are the malware's host-based indicators?

The screenshot shows the Dependency Walker interface for the file LAB03-03.exe. The left pane displays the module structure of LAB03-03.EXE, which includes KERNEL32.DLL, NTDLL.DLL, and KERNELBASE.DLL. The right pane shows a table of API calls with columns for PI, Ordinal, Hint, Function, and Entry Point. Below this is another table for memory dump information with columns for Module, File Time Stamp, Link Time Stamp, File Size, Attr., Link Checksum, Real Checksum, CPU, Subsystem, Symbols, Preferred Base, Actual Base, and Virtual Size.

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x00004000
API-MS-WIN-CORE-BUFFERHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x00004000
API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x00004000
API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknown	0x00004000
API-MS-WIN-CORE-HANDLE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000C0EC	0x0000C0EC	x64	Console	CV	0x000007FF2F000000	Unknown	0x00004000

These functions show the files and memory are being written to or modified thus being potential host based indicators

4.What is the purpose of this program?

The program seems like a keylogger as it communicates with files and registry keys as well as modifies them and stores the logs in a file.

3-4

Analyze the malware found in the file Lab03-04.exe using basic dynamic analysis tools. (This program is analyzed further in the Chapter 9 labs.)

1. What happens when you run this file?

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	88.98	0 K	24 K		
System	4	0.14	112 K	792 K		
Interrupts	n/a	1.02	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	264		348 K	924 K	Windows Session Manager	Microsoft Corporation
css.exe	340	< 0.01	1,832 K	4,220 K	Client Server Runtime Process	Microsoft Corporation
wininit.exe	388		1,384 K	3,948 K	Windows Start-Up Application	Microsoft Corporation
services.exe	492	0.28	4,820 K	8,056 K	K Services and Controller app	Microsoft Corporation
svchost.exe	620	0.02	3,504 K	8,136 K	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	2896		2,208 K	5,528 K	WMI Provider Host	Microsoft Corporation
VBoxService.exe	676	0.30	2,340 K	5,620 K	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe	752	0.02	3,220 K	6,760 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	804	0.01	17,092 K	16,488 K	Host Process for Windows S...	Microsoft Corporation
audiogd.exe	1460		15,348 K	15,044 K	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe	912	0.13	51,556 K	57,300 K	Host Process for Windows S...	Microsoft Corporation
dwm.exe	1404	< 0.01	1,348 K	4,328 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	944	0.01	24,776 K	36,564 K	Host Process for Windows S...	Microsoft Corporation
taskeng.exe	2012		1,428 K	4,476 K	Task Scheduler Engine	Microsoft Corporation
svchost.exe	768	0.01	5,532 K	10,140 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1072	0.01	9,240 K	11,572 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1180		5,924 K	10,396 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1232	0.02	9,352 K	10,480 K	Host Process for Windows S...	Microsoft Corporation
taskhost.exe	1308	0.01	7,656 K	8,020 K	Host Process for Windows T...	Microsoft Corporation
svchost.exe	1500		4,680 K	8,676 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2084		3,032 K	7,076 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	2120		1,504 K	4,692 K	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	2556	0.01	27,824 K	17,480 K	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.e...	1624	< 0.01	2,928 K	7,504 K	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe	3036		1,996 K	5,392 K	Microsoft Windows Search F...	Microsoft Corporation
lsass.exe	500	0.19	3,740 K	9,576 K	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	508	0.02	2,220 K	3,728 K	Local Session Manager Serv...	Microsoft Corporation
css.exe	396	0.69	3,144 K	6,784 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	428		2,460 K	6,028 K	Windows Logon Application	Microsoft Corporation
explorer.exe	1424	5.32	39,008 K	61,200 K	Windows Explorer	Microsoft Corporation
VBoxTray.exe	1892	0.06	3,908 K	8,212 K	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe	140		1,820 K	6,232 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	2656	1.49	10,396 K	18,756 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	2632	1.27	2,136 K	7,032 K	Snipping Tool	Microsoft Corporation
GoogleCrashHandler.exe	2316		1,412 K	940 K	Google Crash Handler	Google LLC
GoogleCrashHandler64.exe	2324		1,356 K	528 K	Google Crash Handler	Google LLC

The program crashes

2.What is causing the roadblock in dynamic analysis?

When the file is run it deletes itself immediately. This could be caused by command line parameters needing to be passed to the program, it needing to fetch a particular file from a remote location, it detecting it is in a sandbox, it only targeting a particular timezone, or it only running on a specific domain. Some clues can be found by looking at the program strings.

3.Are there other ways to run this program?

We can try opening the file in CFF explorer and then examining details as well as modifying them whenever required thus performing basic static and basic dynamic analysis techniques.