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.)

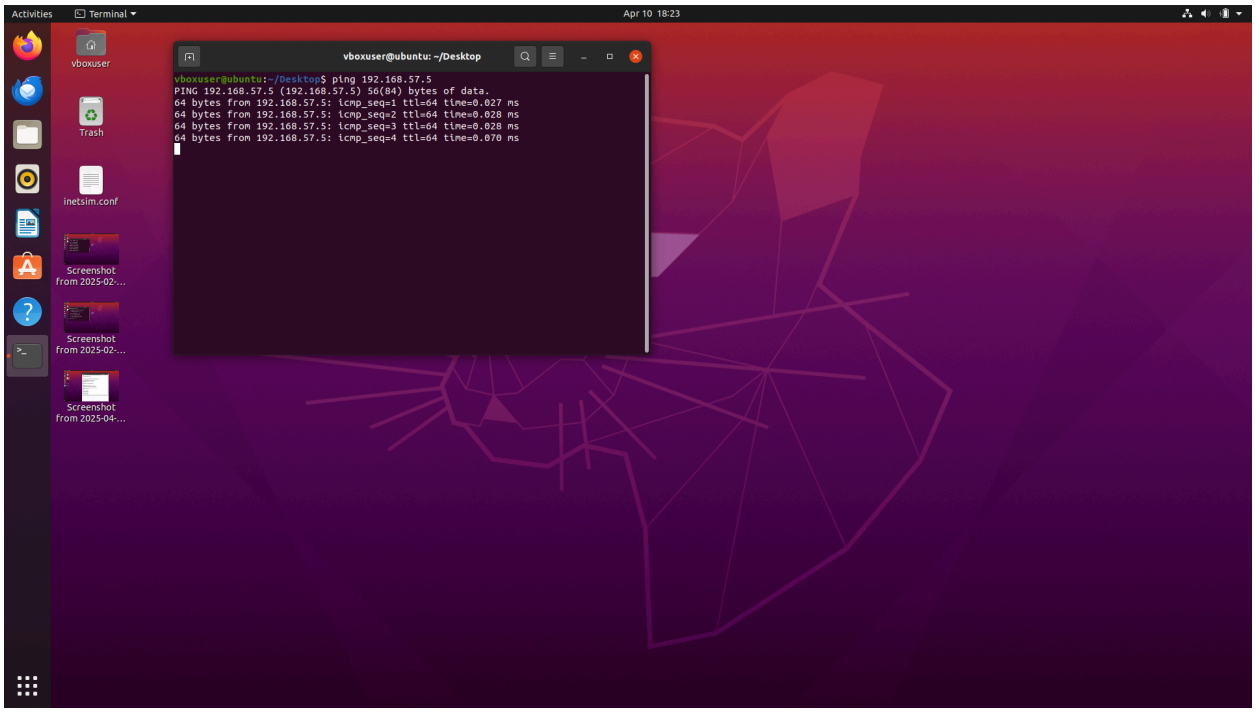
5. Install sysinternals and Apate DNS in windows VM

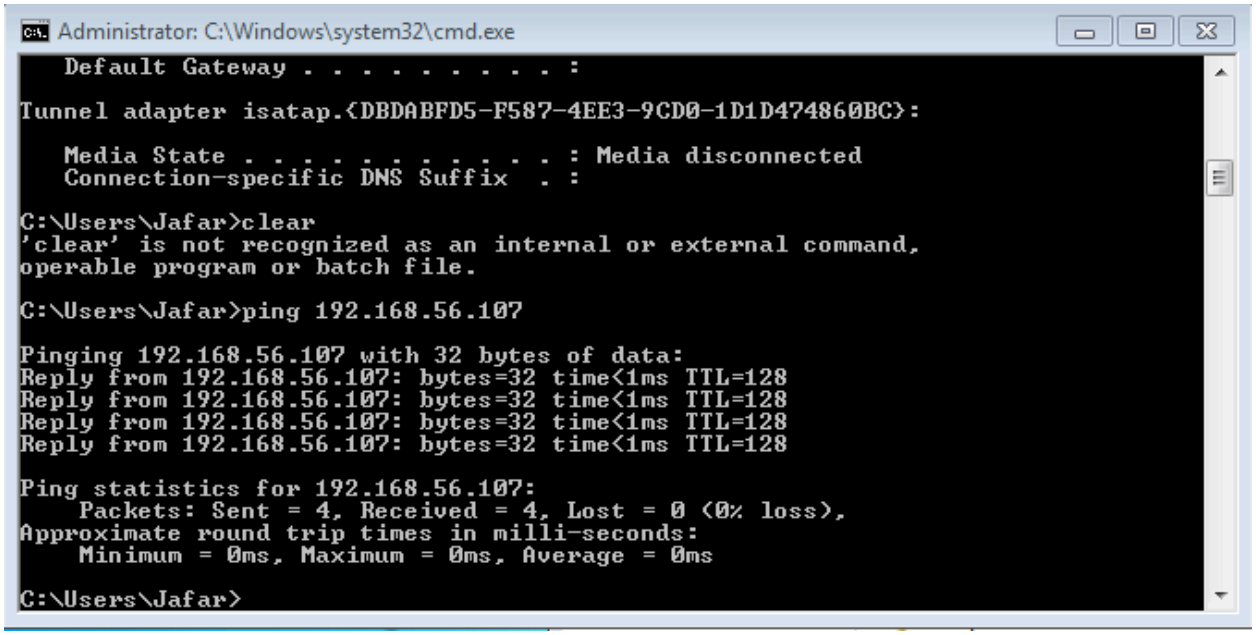
6. Install and configure inetsim in Linux

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

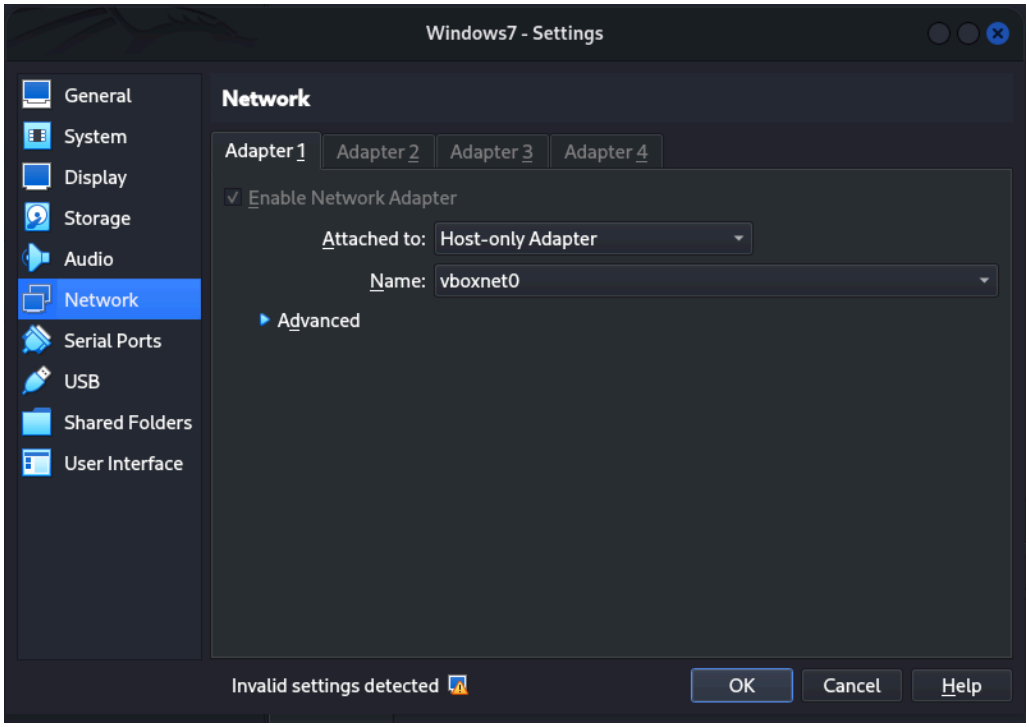
8. Complete the analysis of all the PE files of Lab 03 as mentioned at the end of the chapter -03 of the said book.

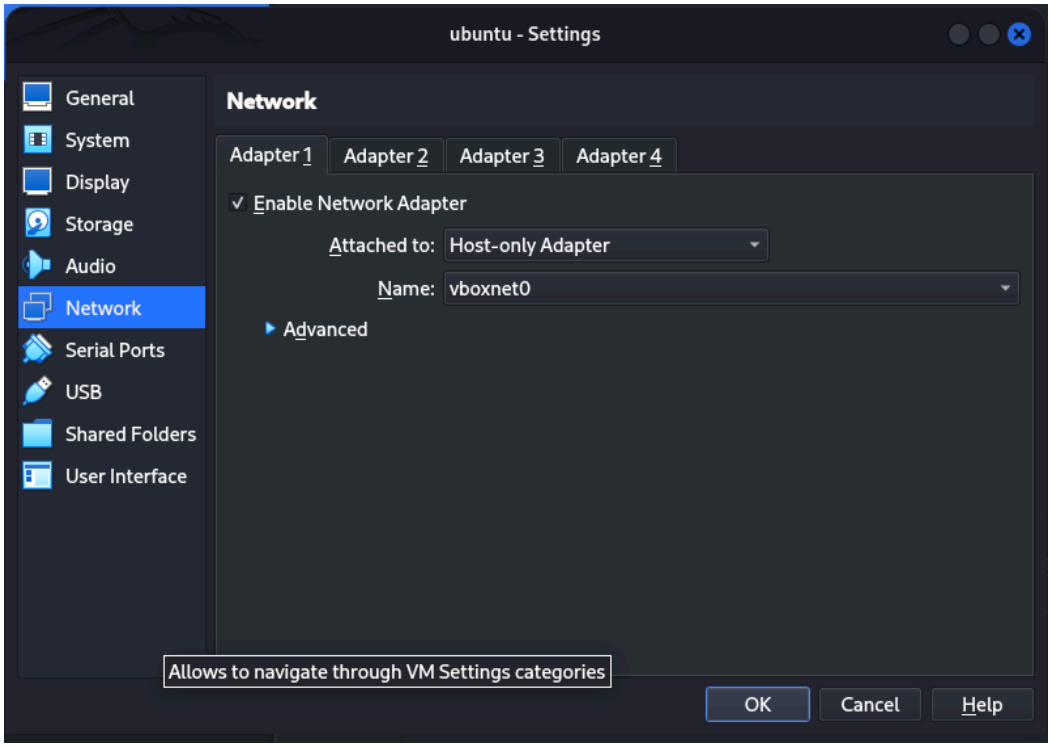
1. 02 VMs (Windows+Linux)



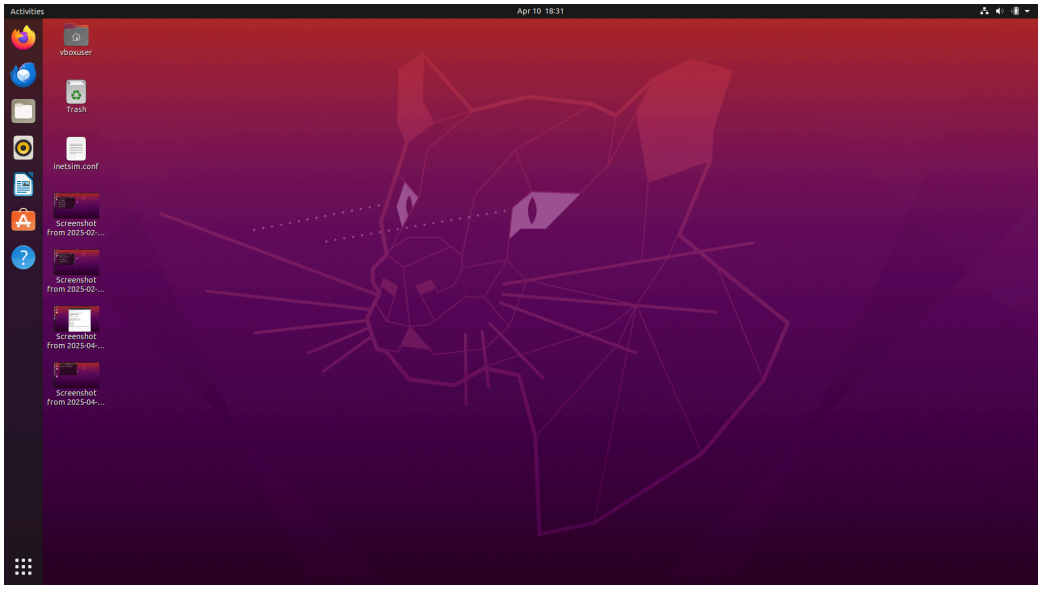


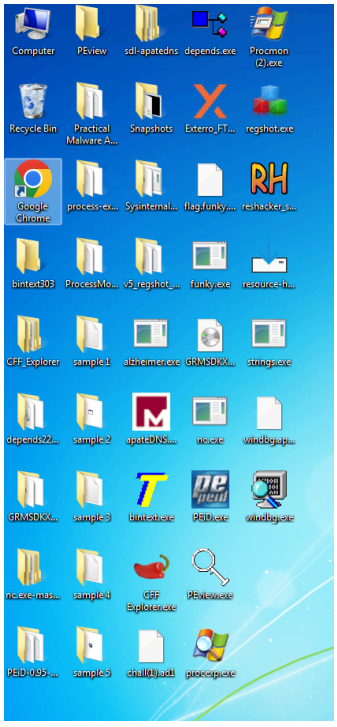
3. Connected with Host only network adapter (connect with internet whenever required but not during analysis)



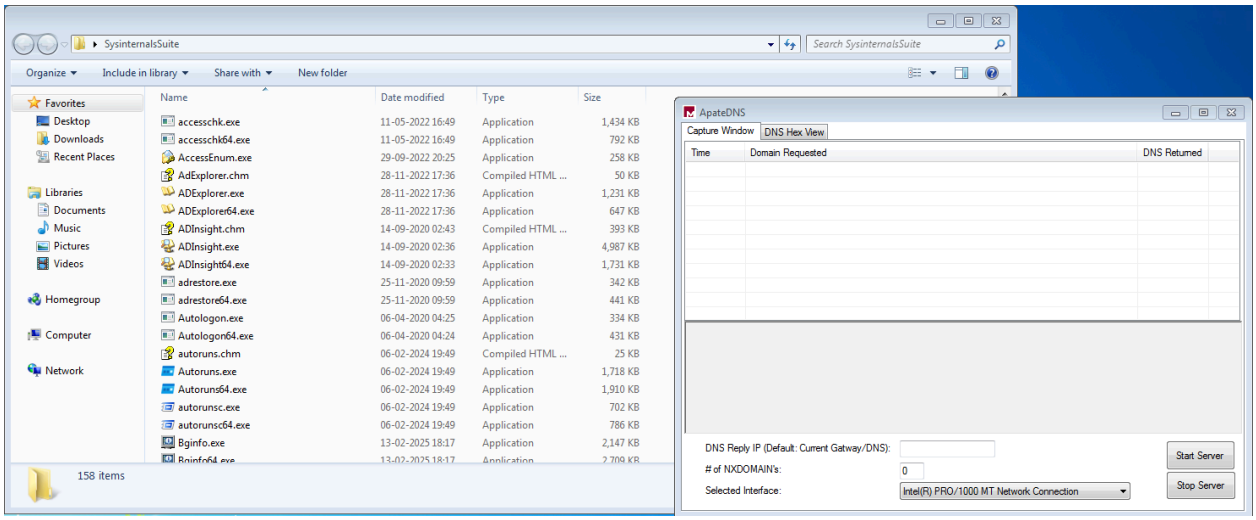


4.Install minimum requirements for normal operations in both the VMs. (i.e.browser, office, pdf reader, etc.)

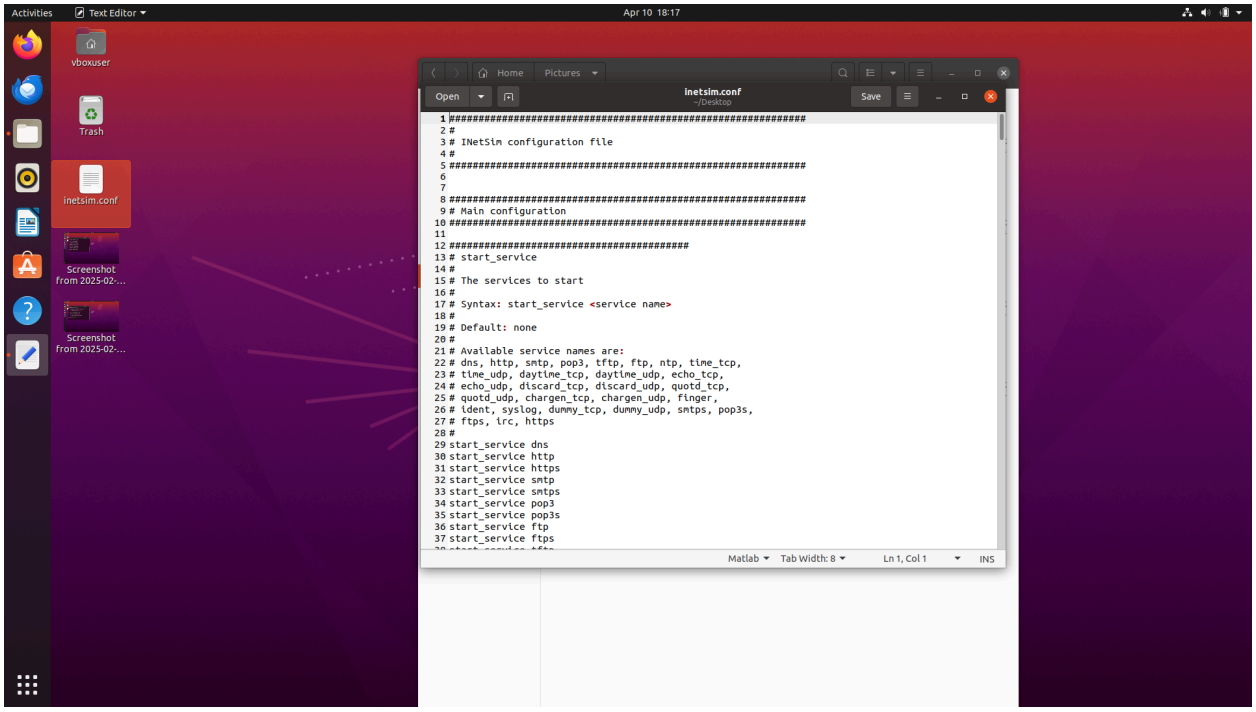




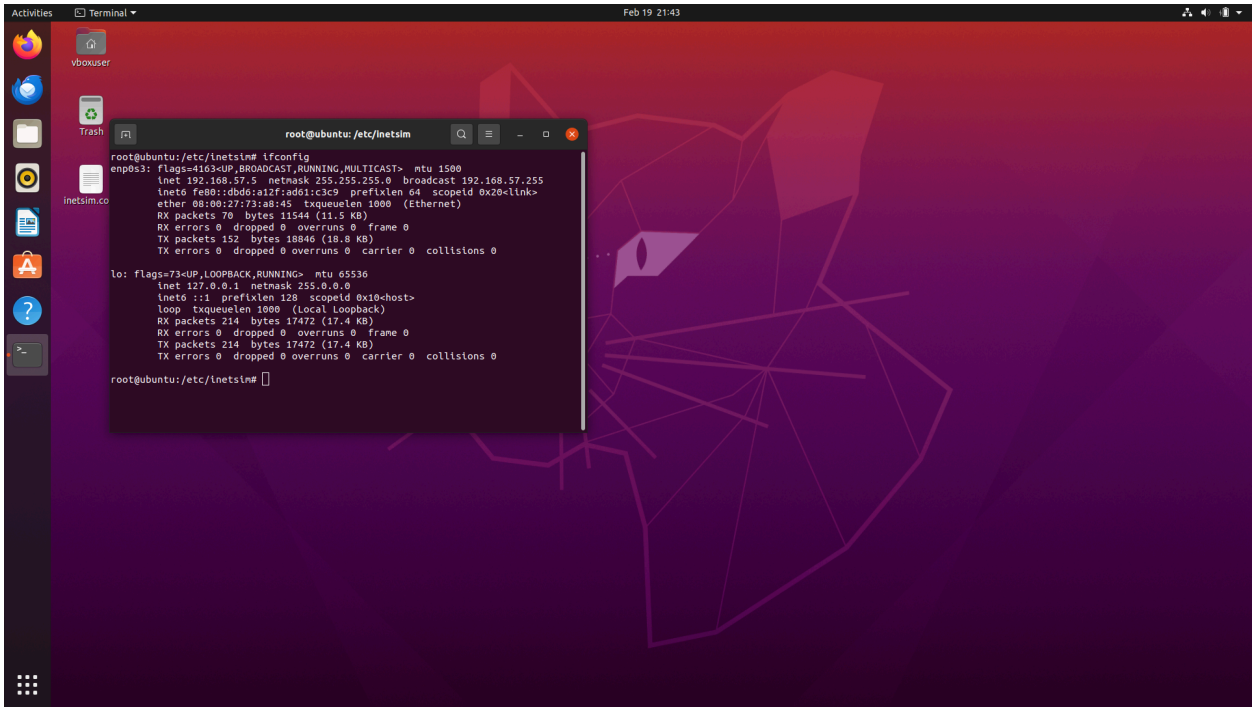
5. Install sysinternals and Apate DNS in windows VM



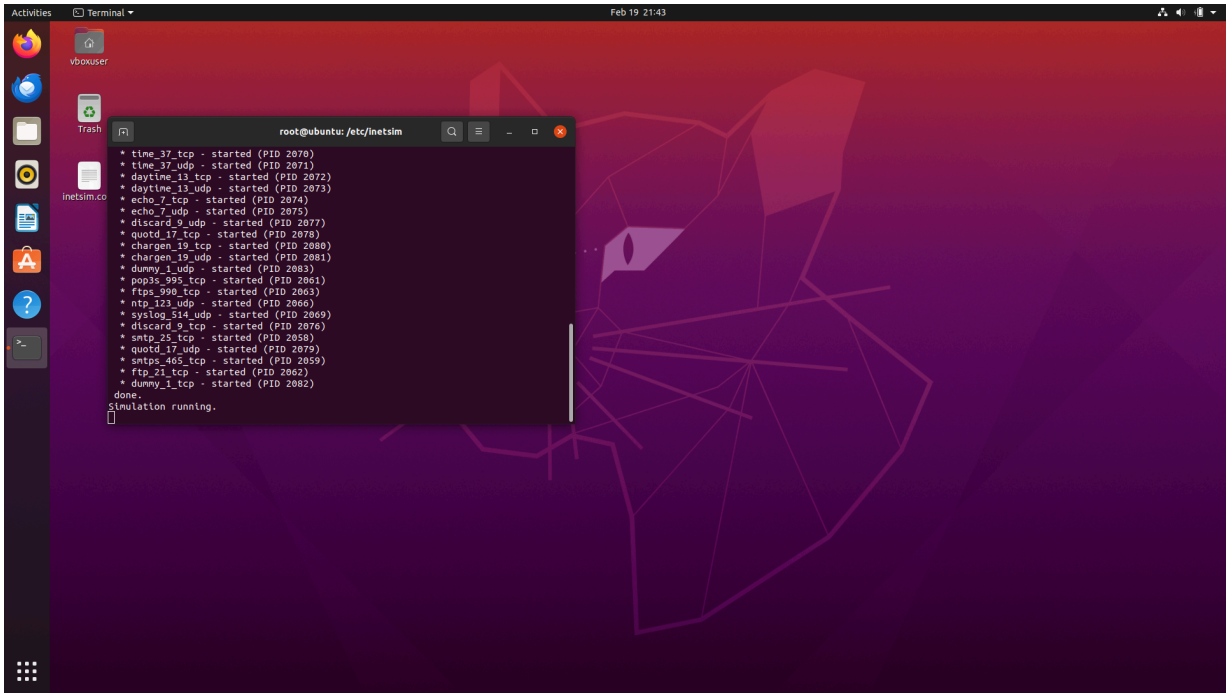
6. Install and configure inetsim in Linux



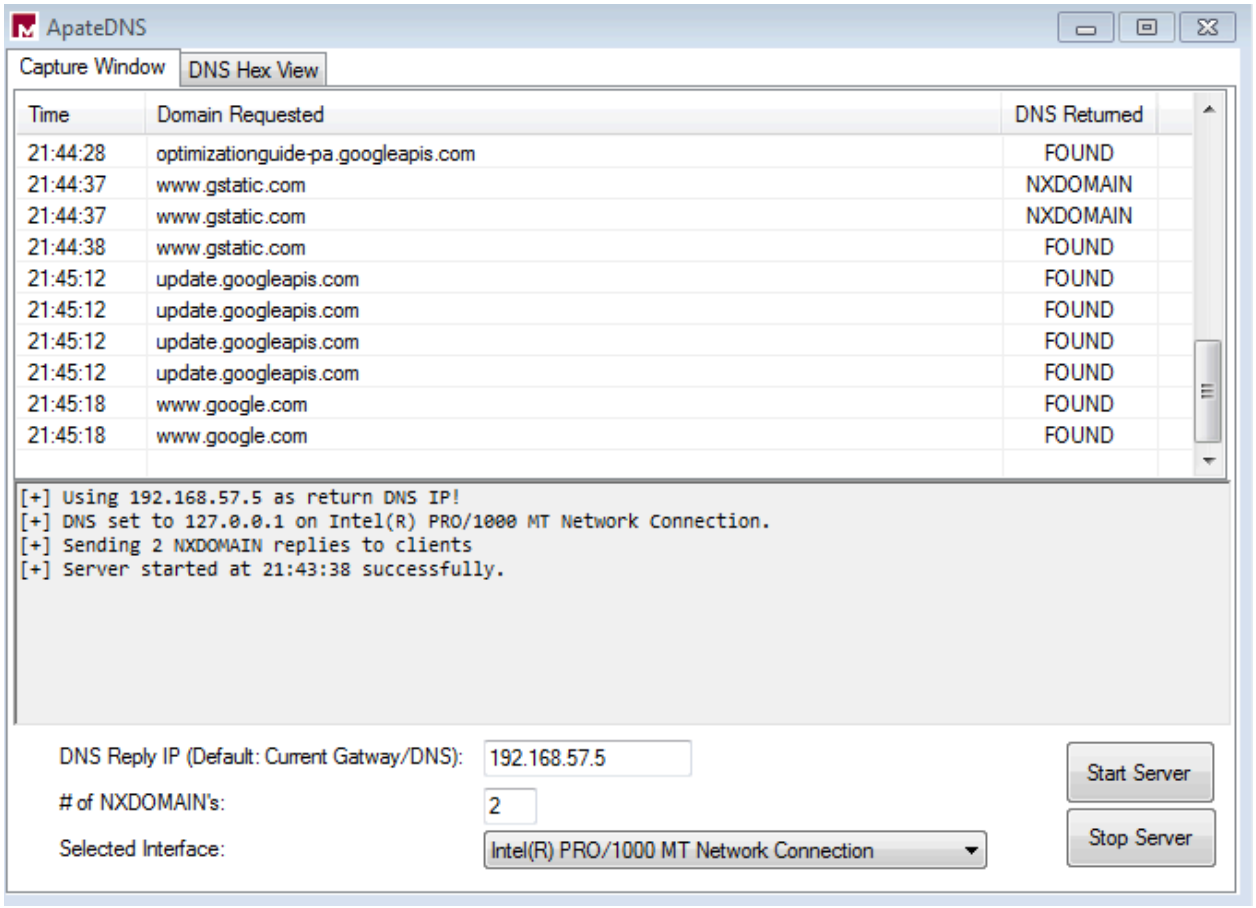
7. Simulate the fake internet in windows as mentioned in the chapter-03 of the Practical Malware Analysis Book.



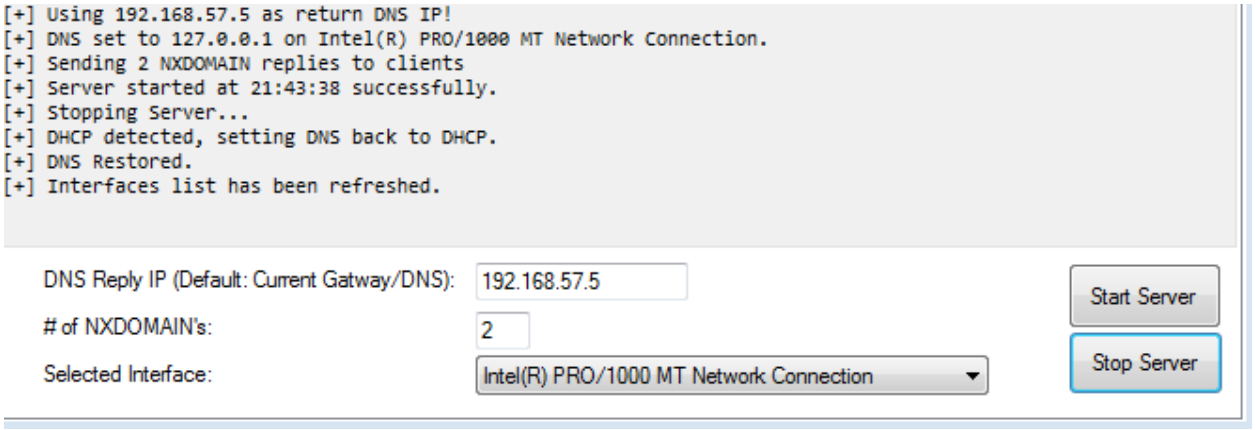
Configuring inetsim using IP Address of Linux VM

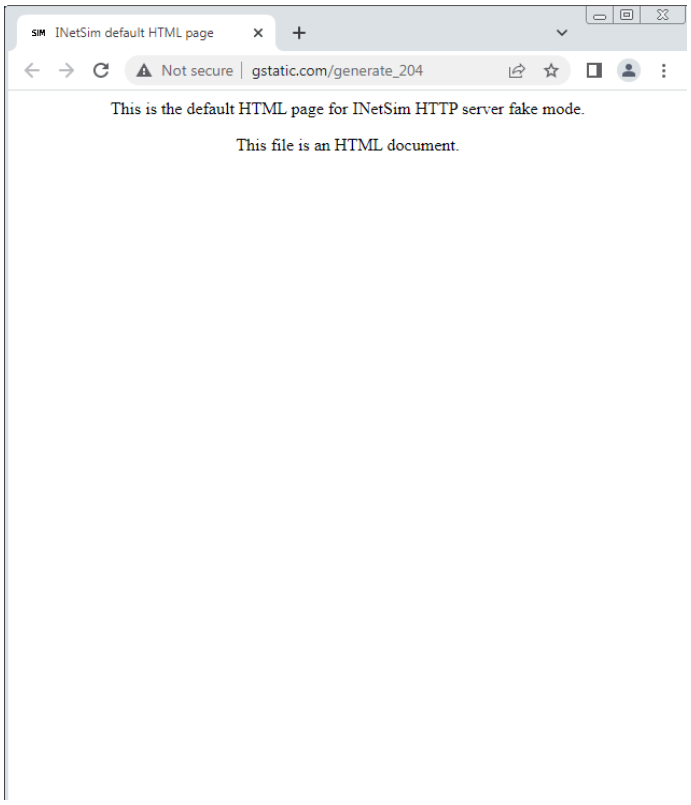


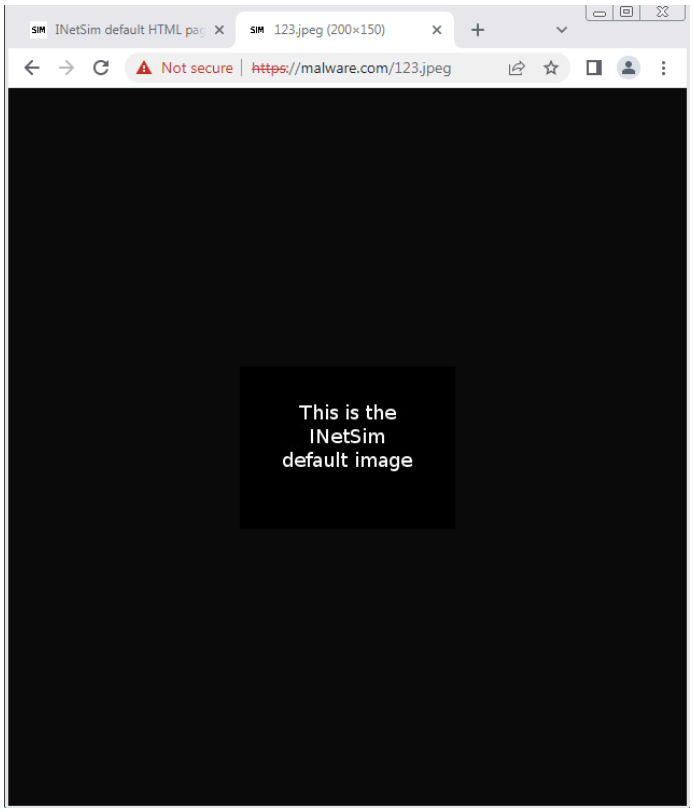
Running the Inetsim simulation



Starting the server at ApateDNS.





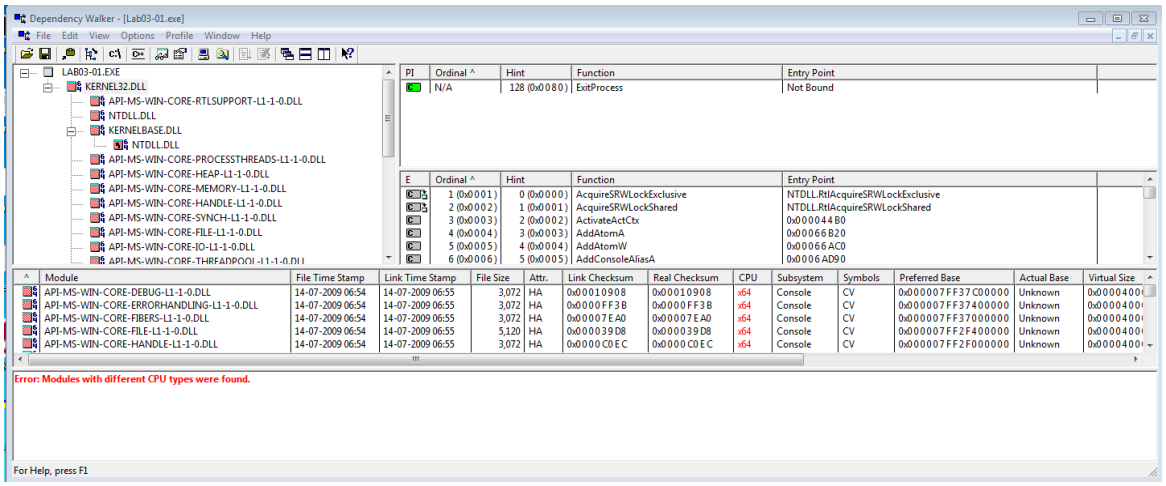


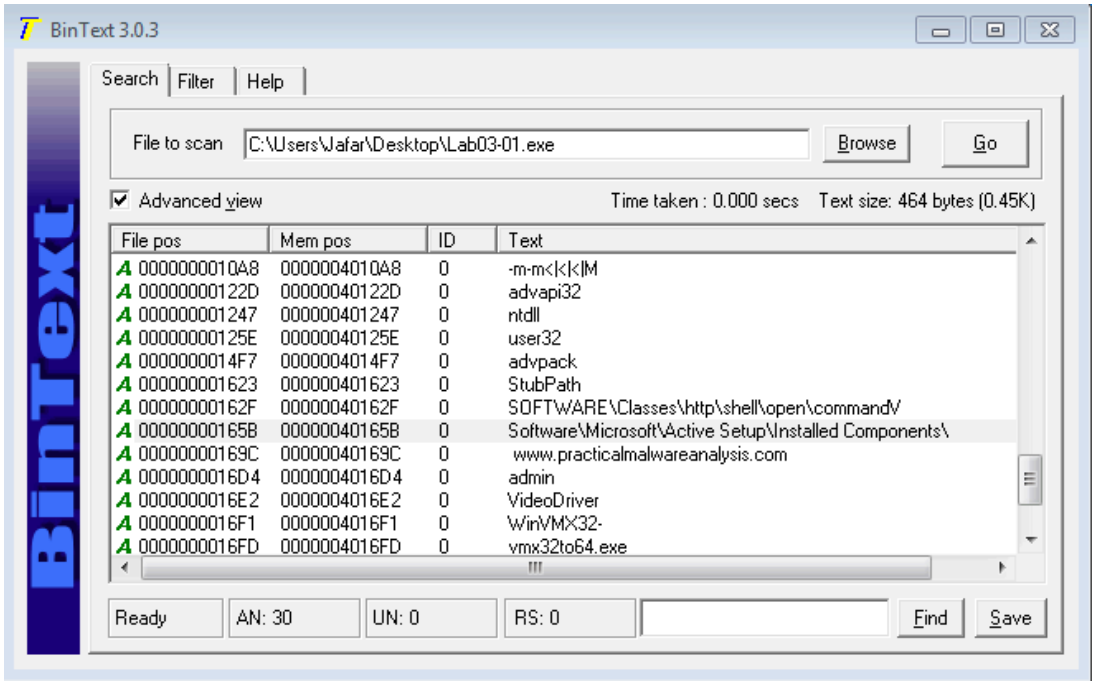
Successfully configured Inetsim

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.

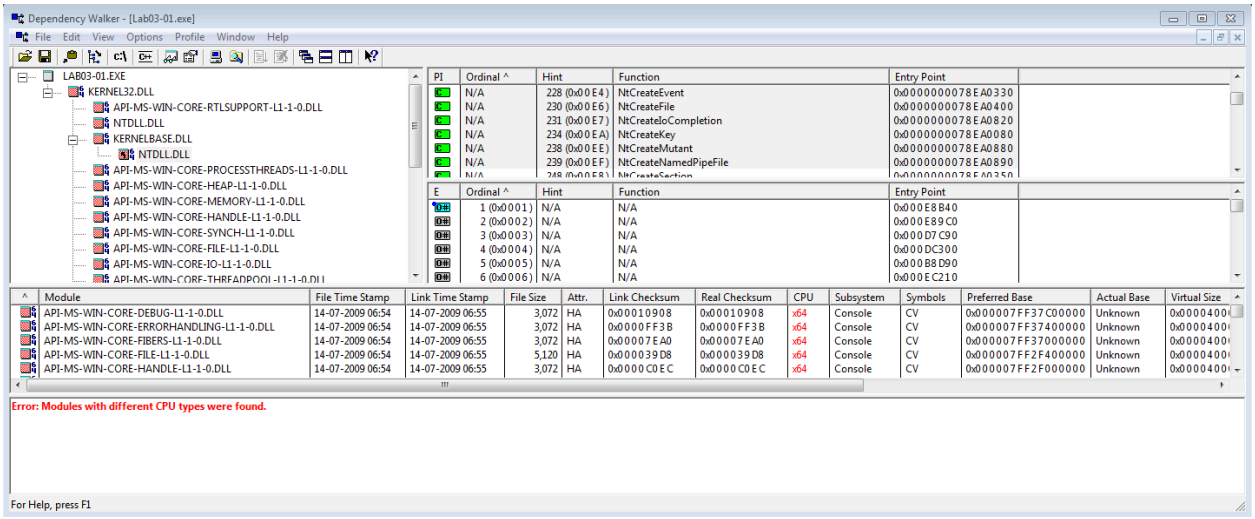
3-1
Analyze the malware found in the file Lab03-01.exe using basic dynamic analy-
sis tools.

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

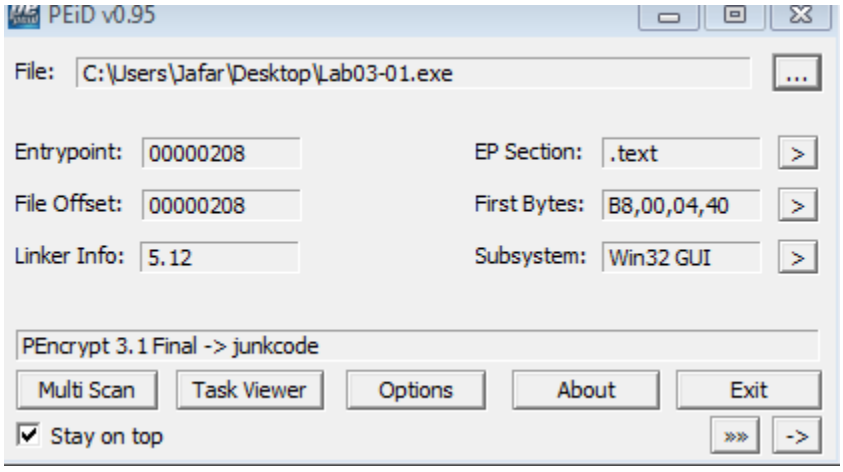




2.What are the malware's host-based indicators?

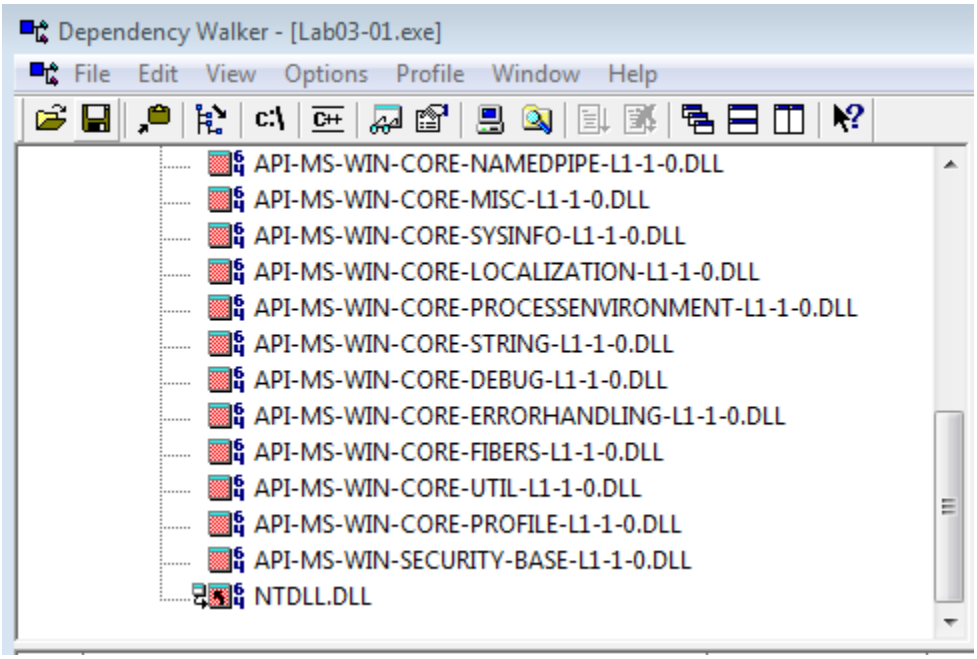


The NTdll.dll imports functions related to creating and modifying files, events and keys.



The file has also been packed using the PEncrypt packer

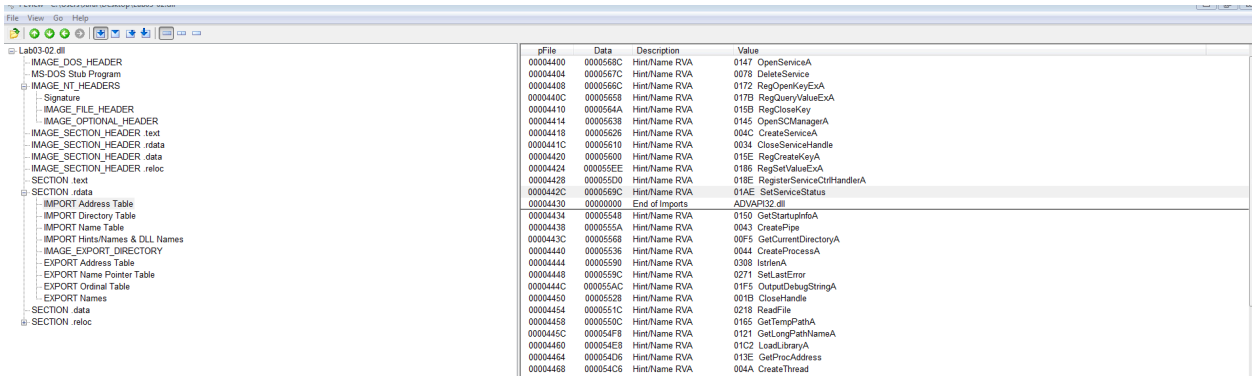
3.Are there any useful network-based signatures for this malware? If so, what are they?



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

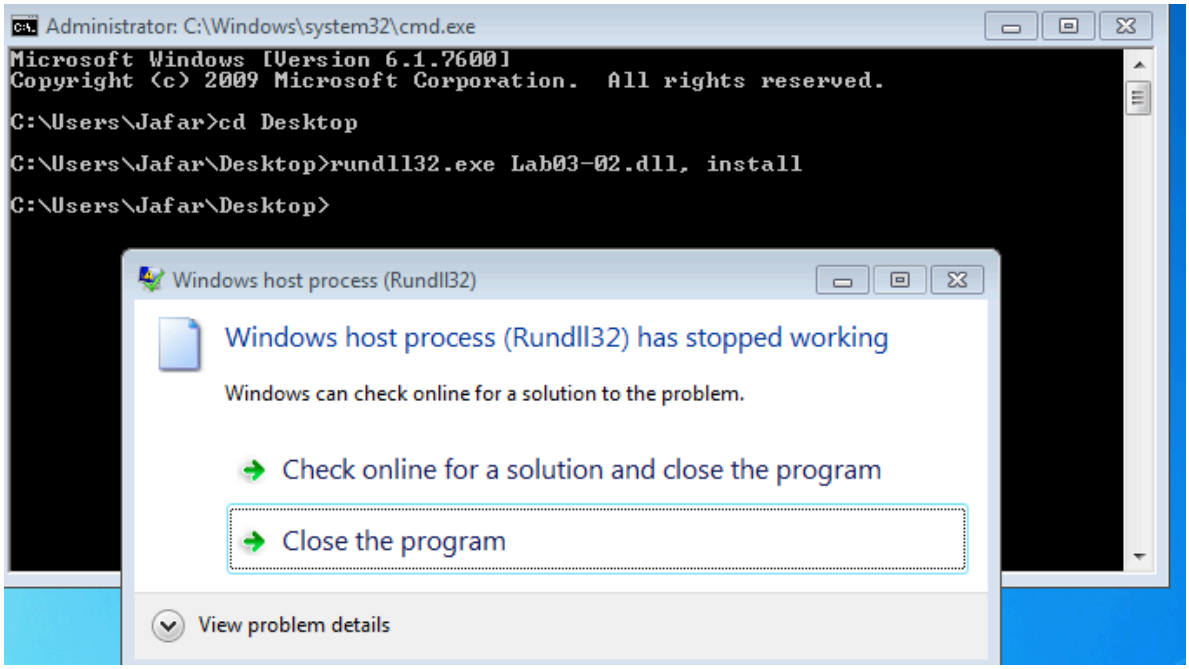
3-2
Analyze the malware found in the file Lab03-02.dll using basic dynamic analy-
sis tools.

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



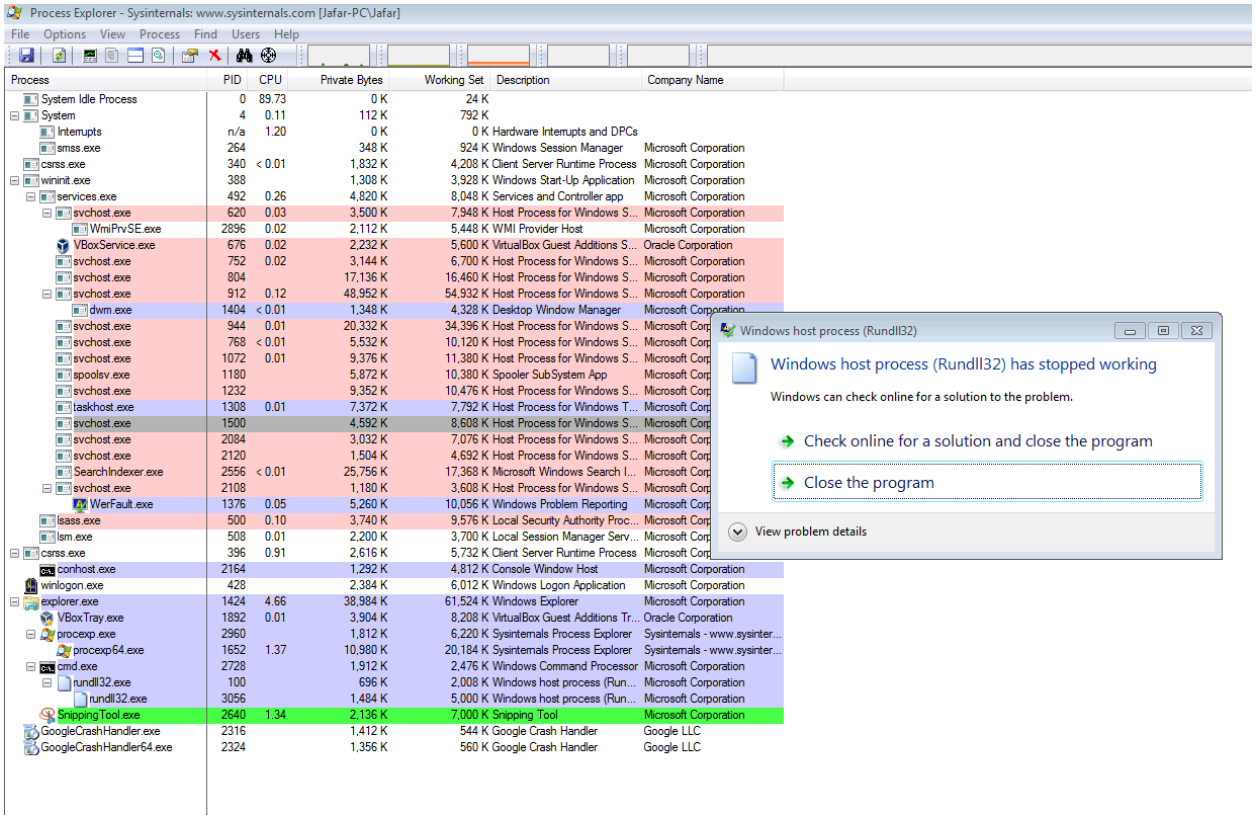
The malware runs as a service and thus installs itself.

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?

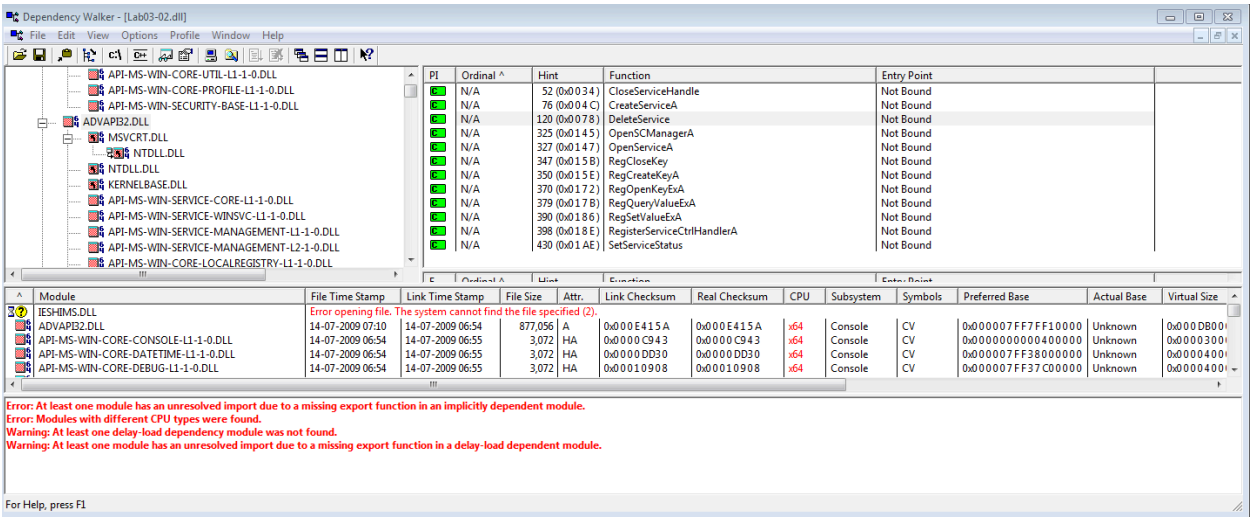


The system crashes on running the respective dll.

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

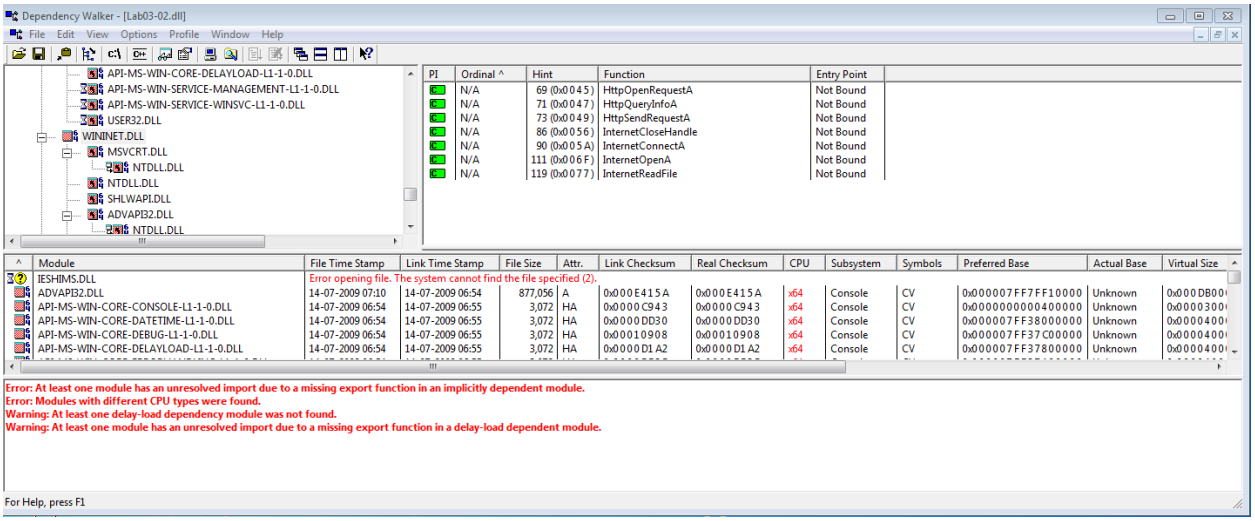
Because there's likely to be multiple svchost processes, we can filter by the Process ID to glean information only on the svchost process responsible for running this malware.

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



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?

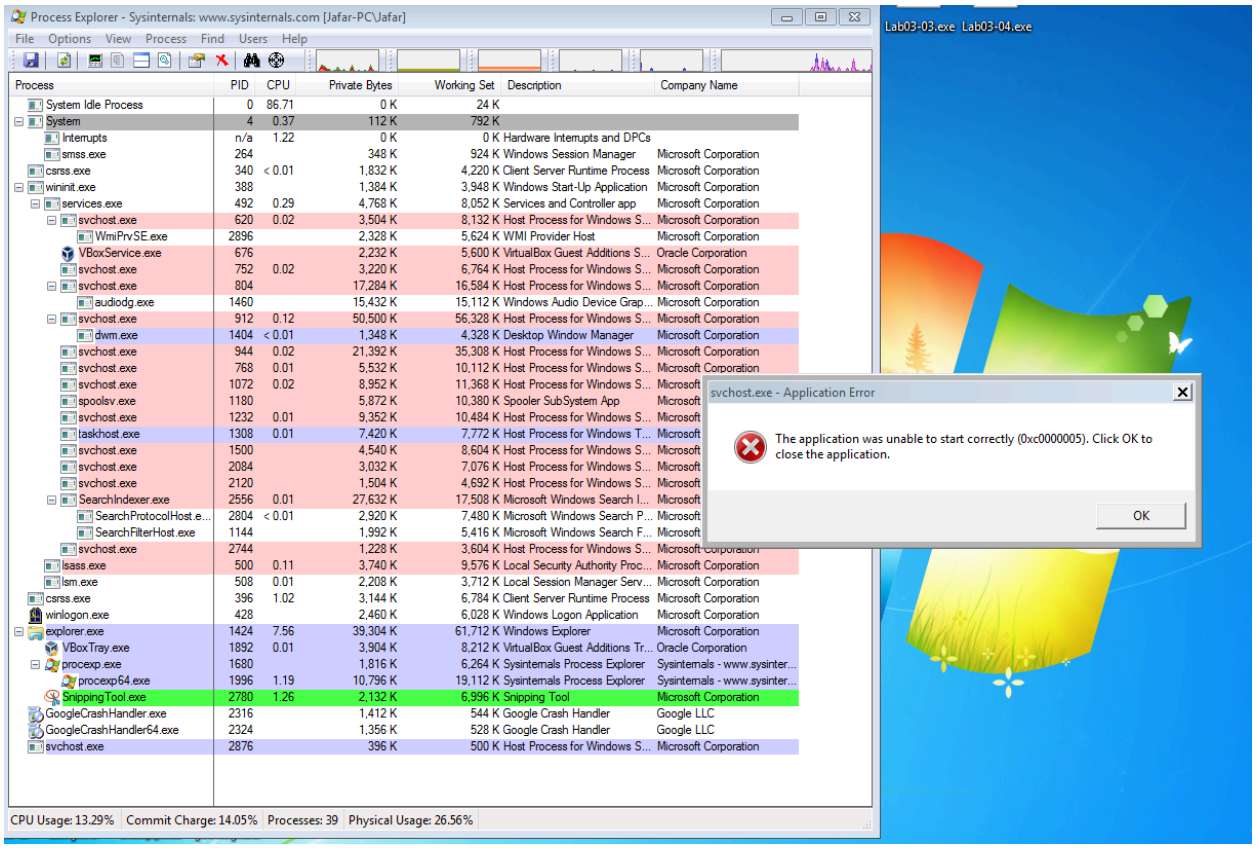


The file shows the presence of network based dlls as well as network based functions as network based indicators.

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?

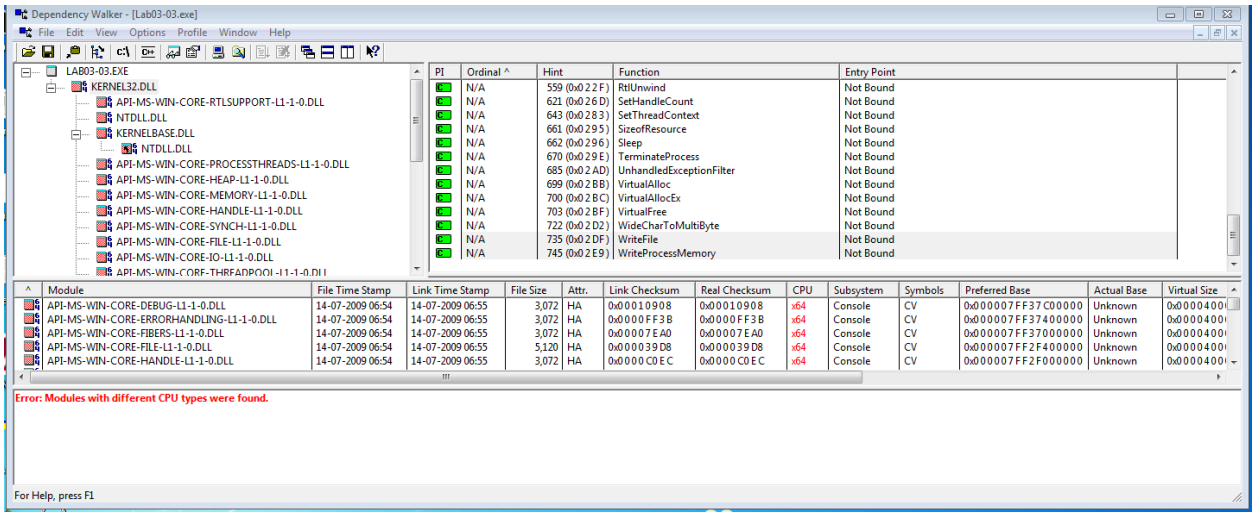


The executable crashes while running even with admin privileges

2.Can you identify any live memory modifications?

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

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



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

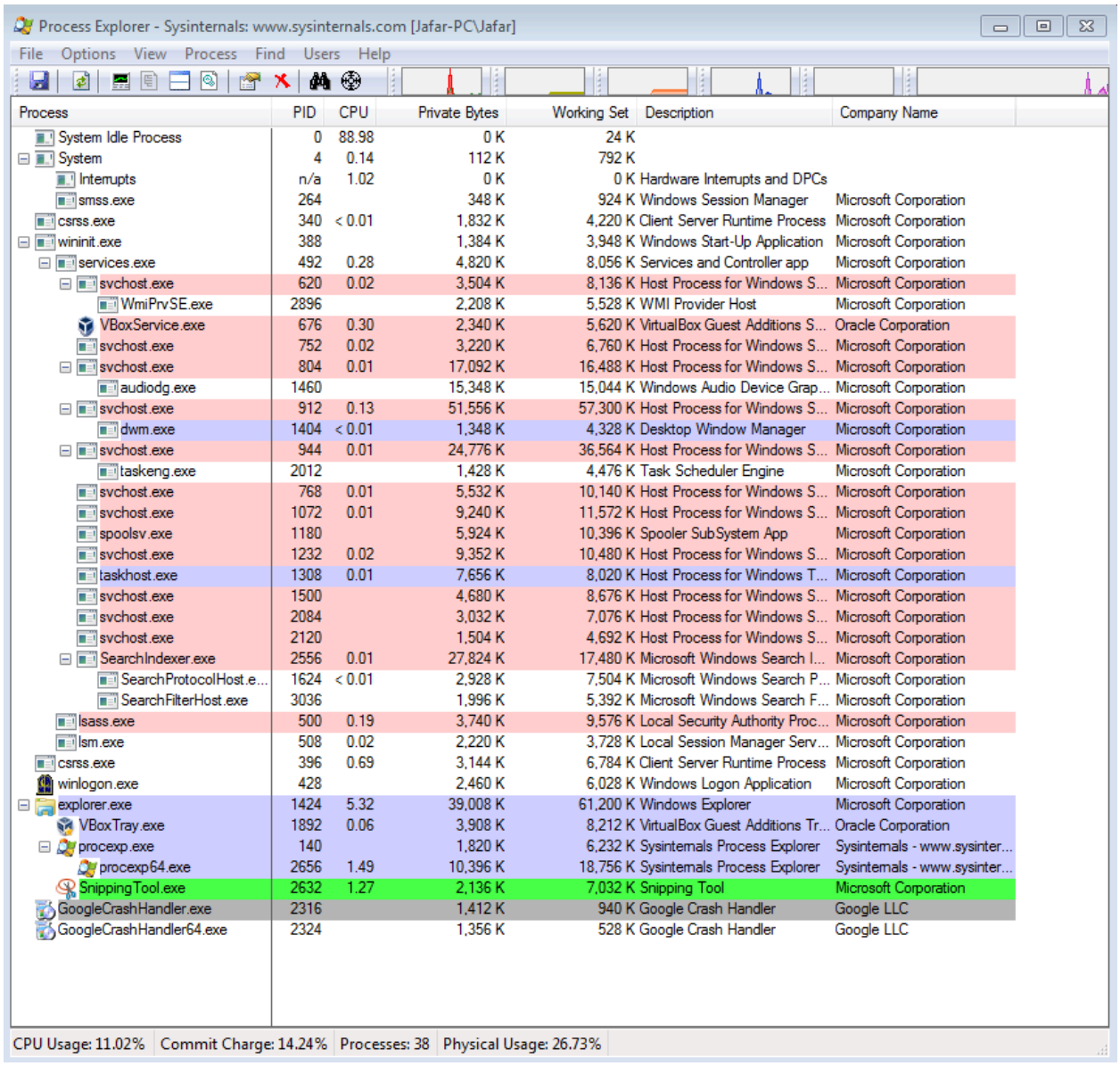
4.What is the purpose of this program?

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?



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.