**LAB 3:** Basic Dynamic Techniques

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 14/1/2023

**Purpose**

You will practice the techniques in chapter 3.

This project follows Lab 3-1 in the textbook. There are more detailed solutions in the back of the boo

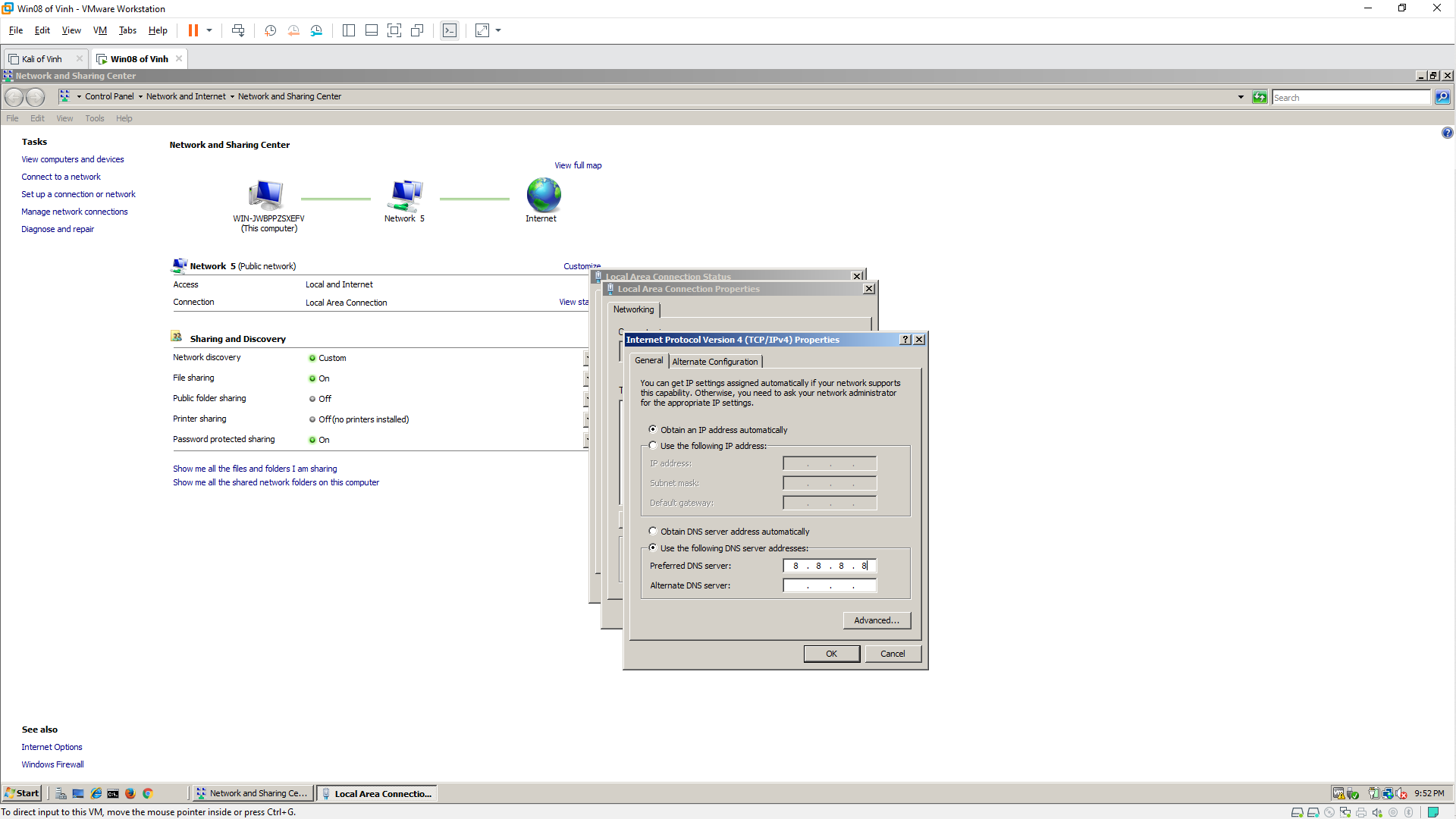
What you need:

* A Windows 2008 Server virtual machine with a Kali vitual machine running INetSim, which you prepred in the previous project.

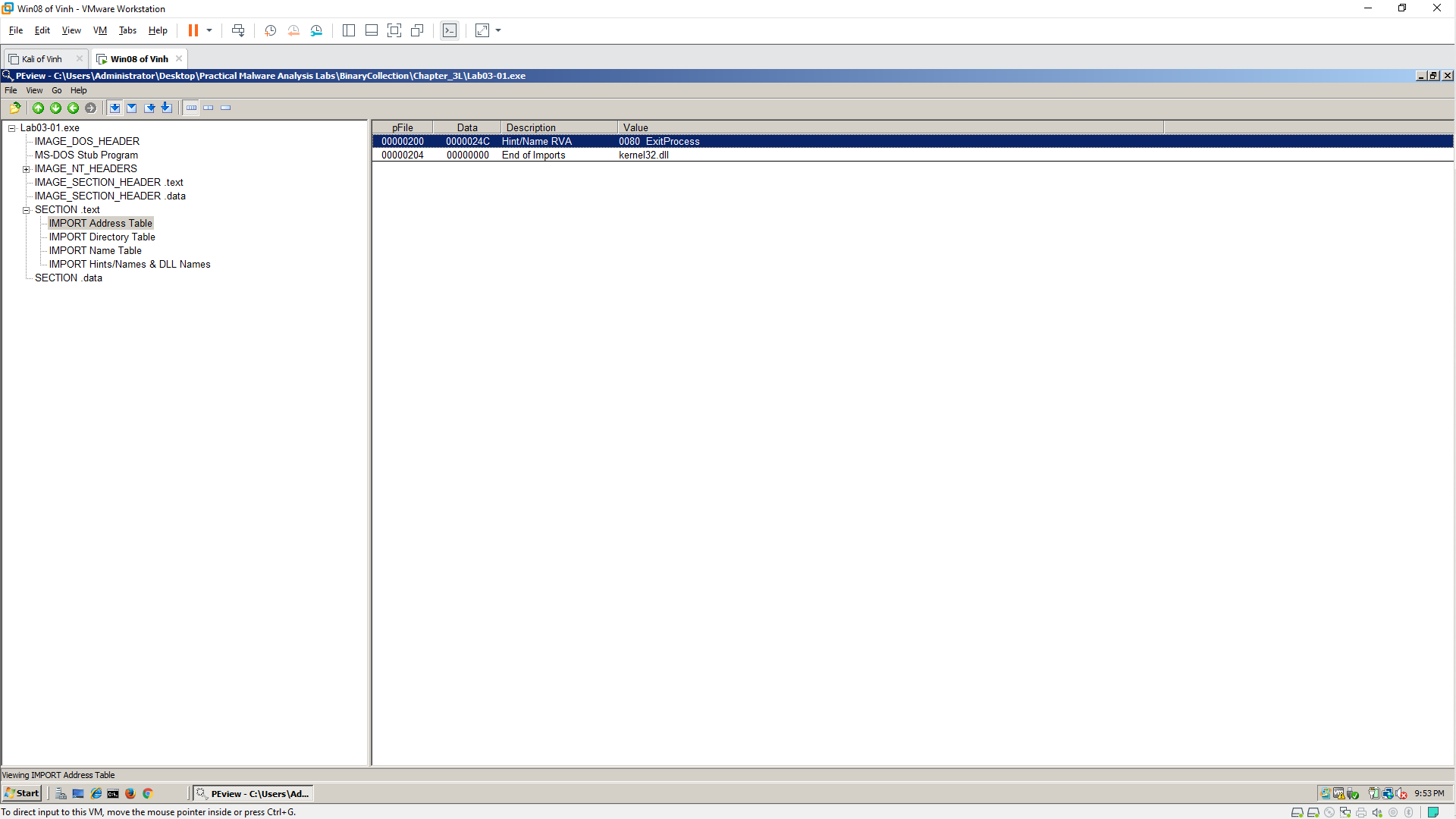
**NOTE: Windows 7 will not work for this project!**

* Recommended: the textbook: "Practical Malware Analysis"

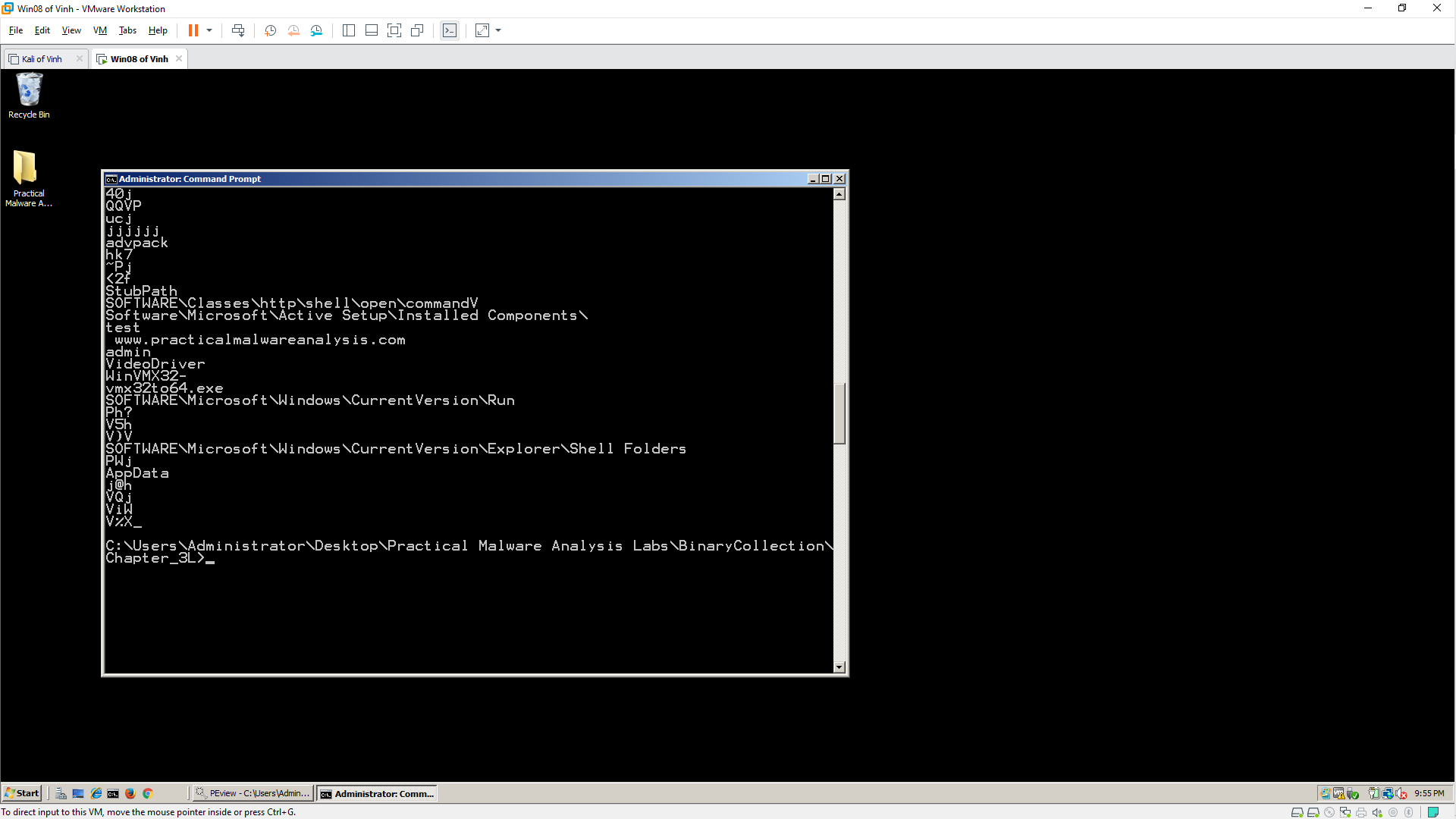
**Setting the DNS Server to 8.8.8.8**

****

**Using PEview**

****

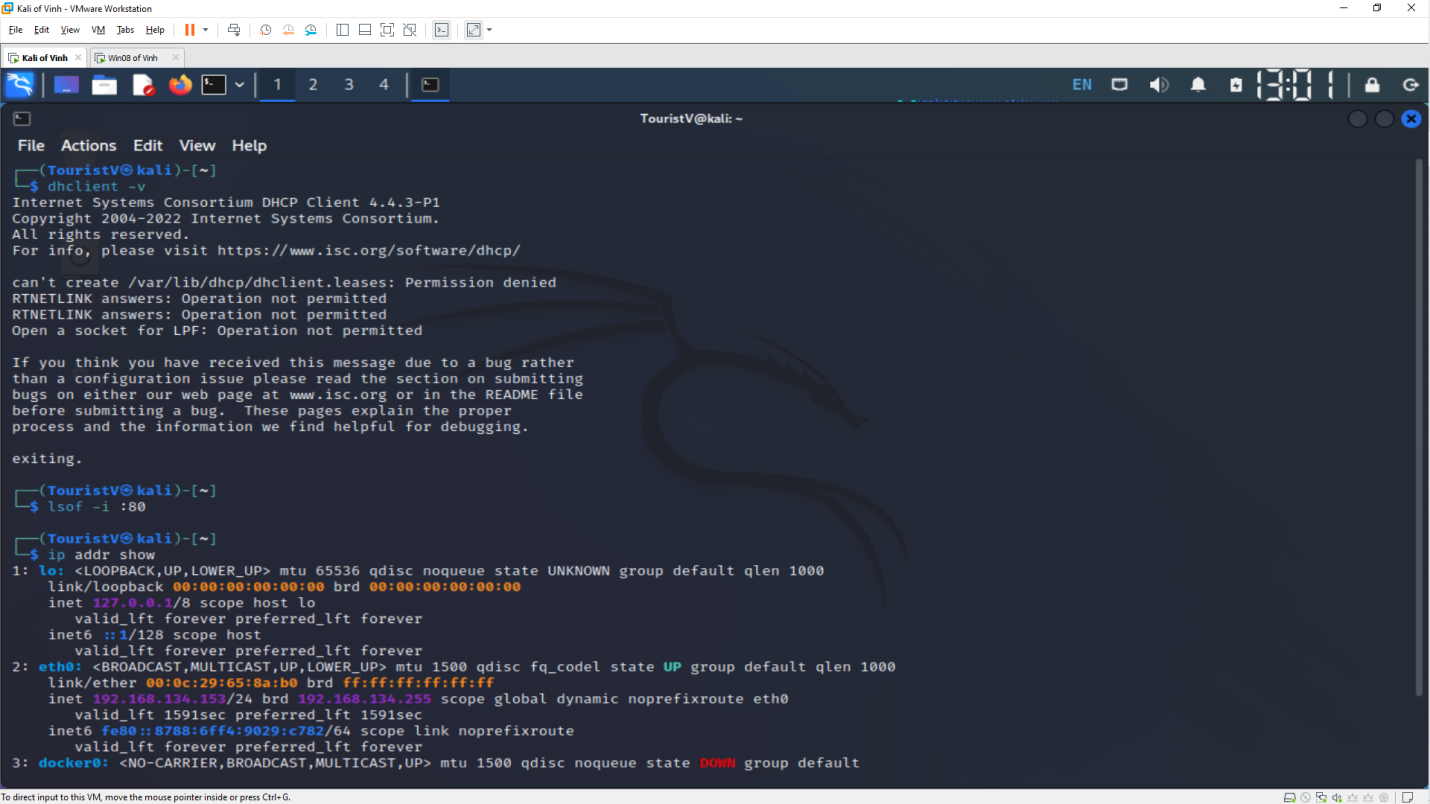
**Using Strings**

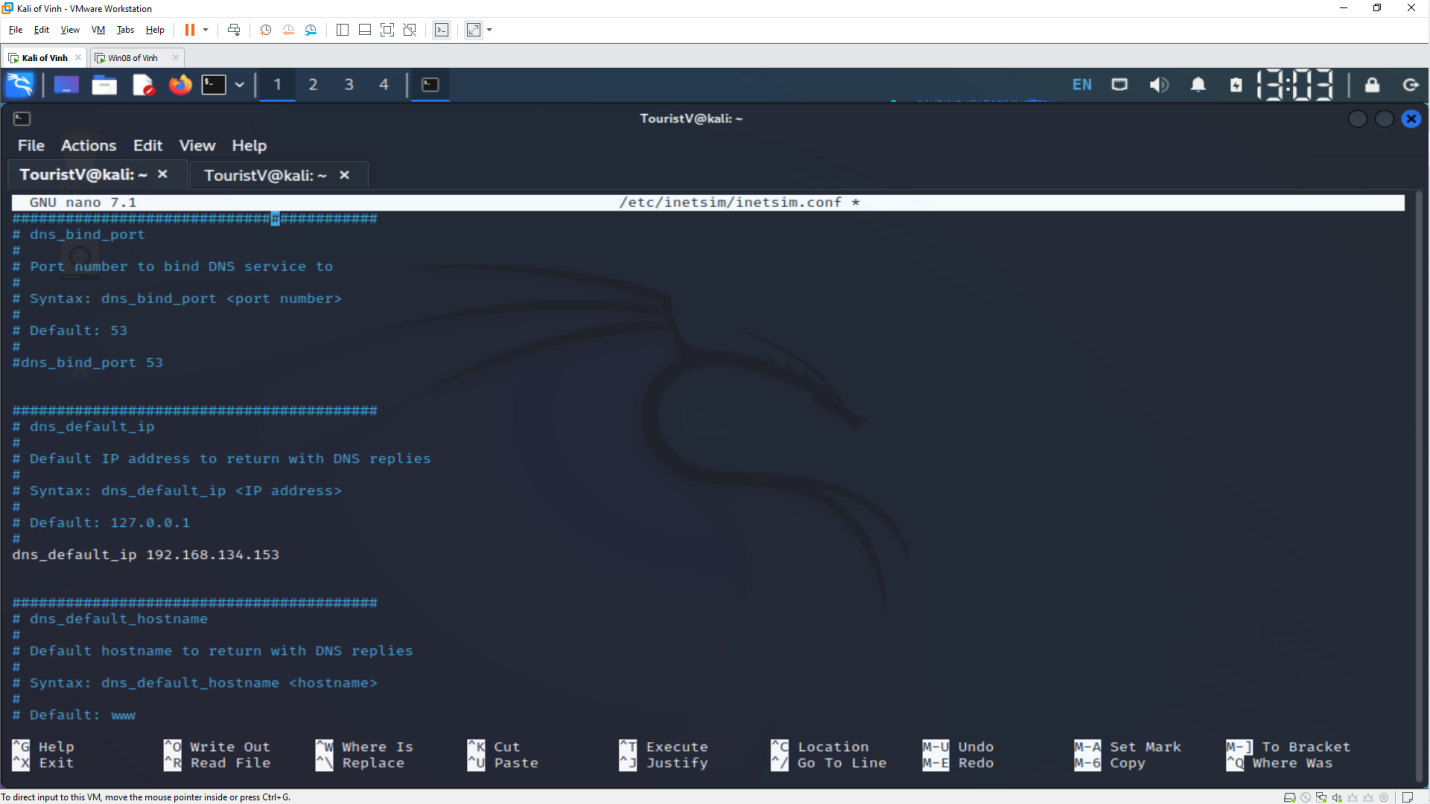
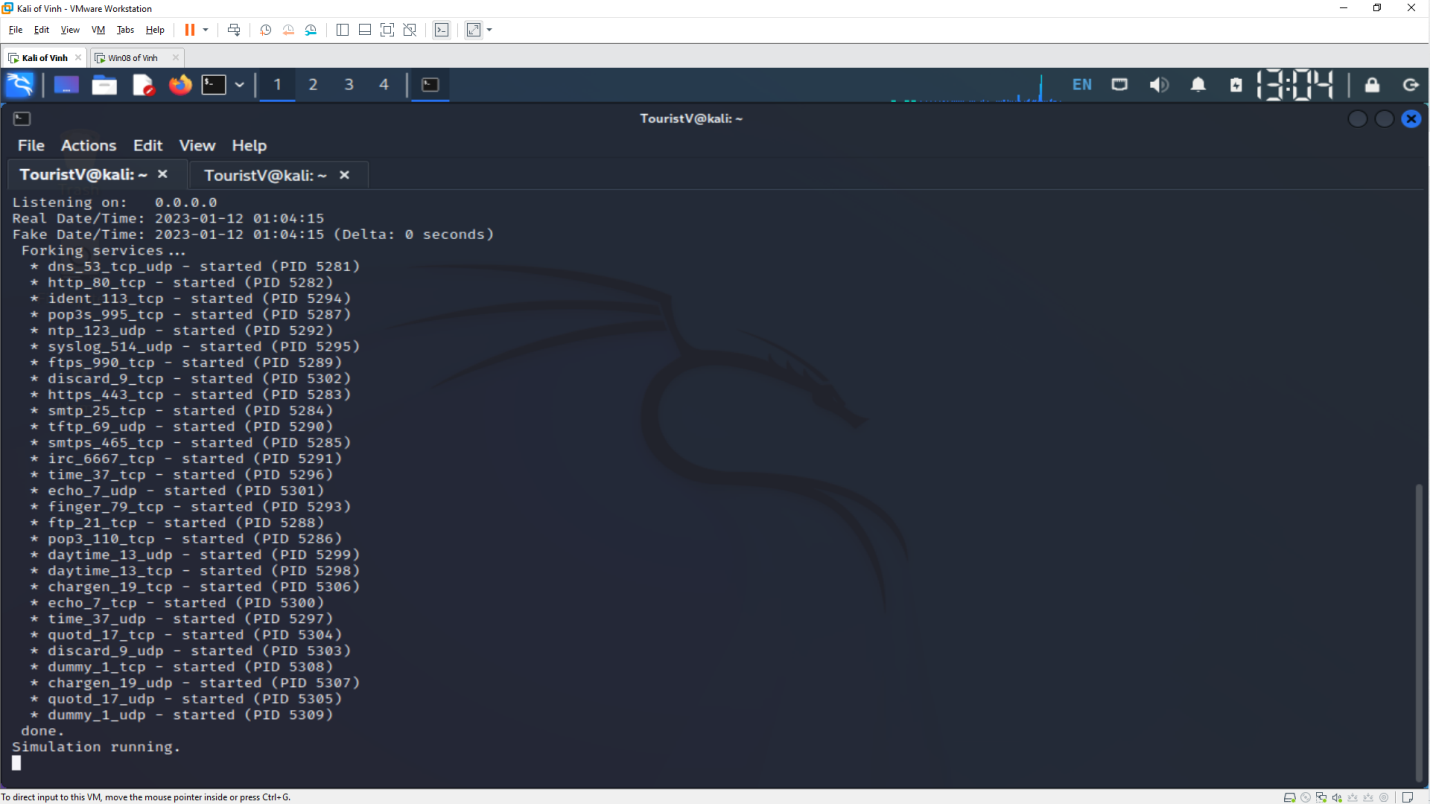
****

**Preparing for Dynamic Analysis**

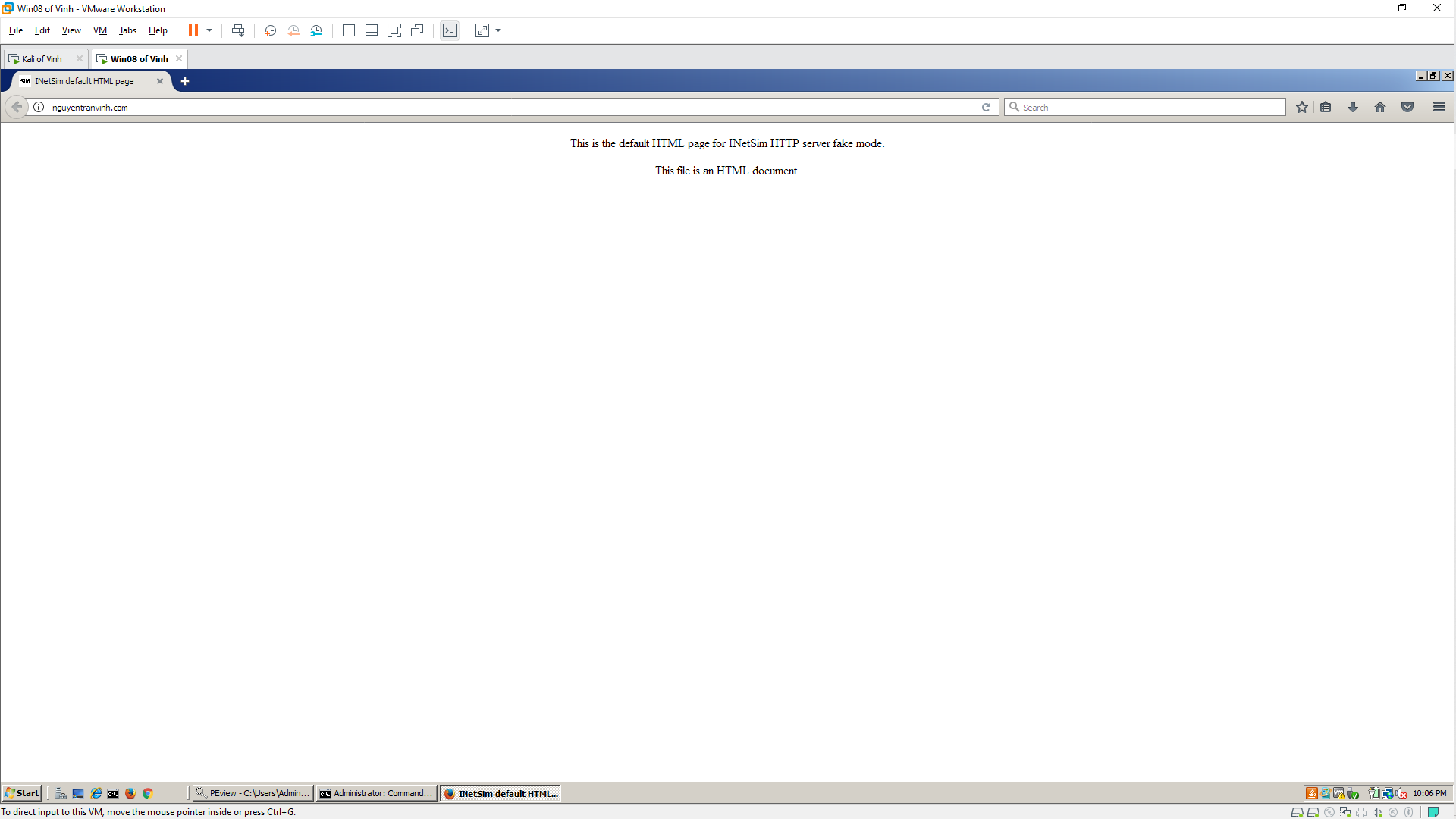
**1. Start INetSim**

- Kali Machine

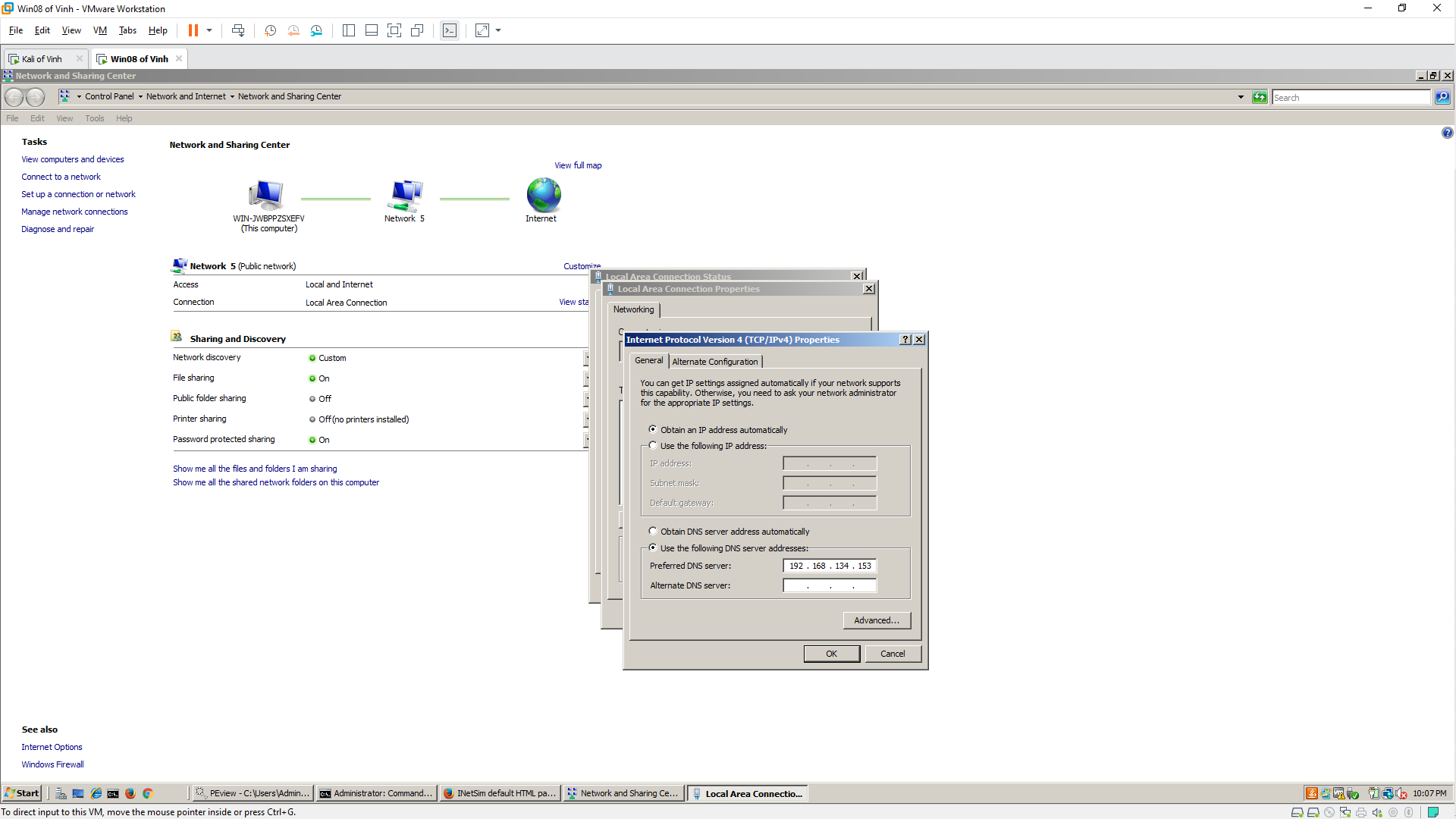
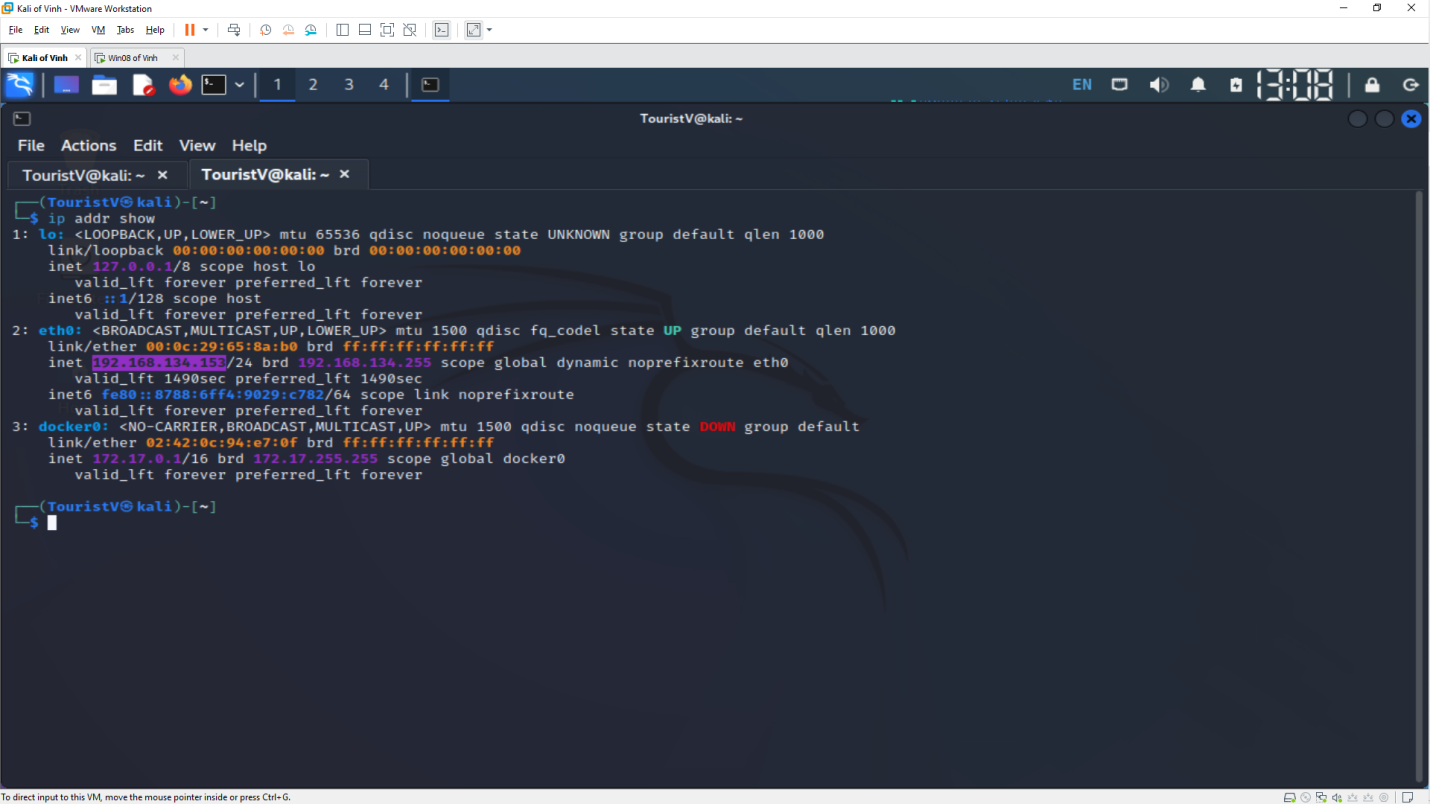
****

** **

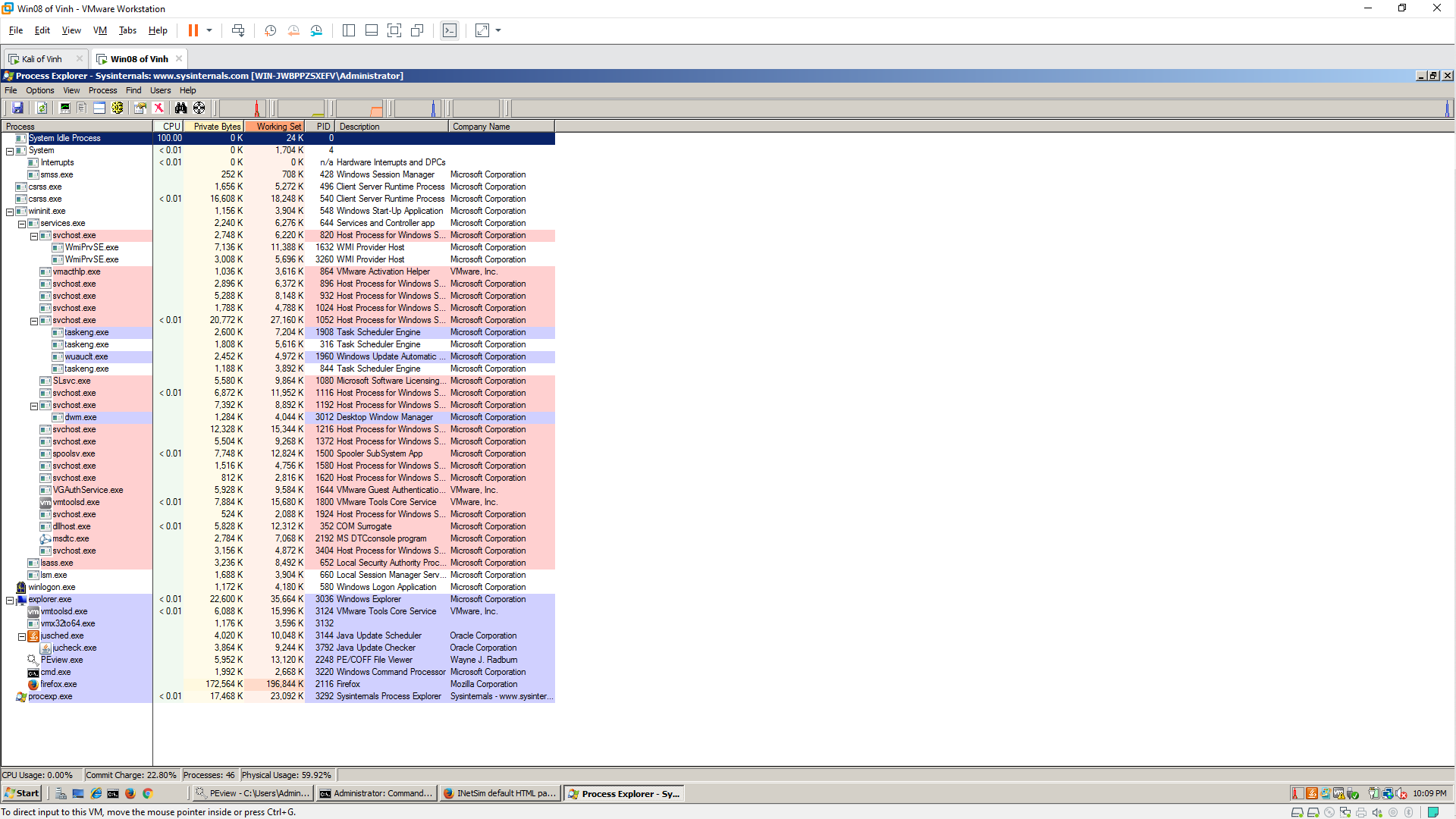
- Windows Machine



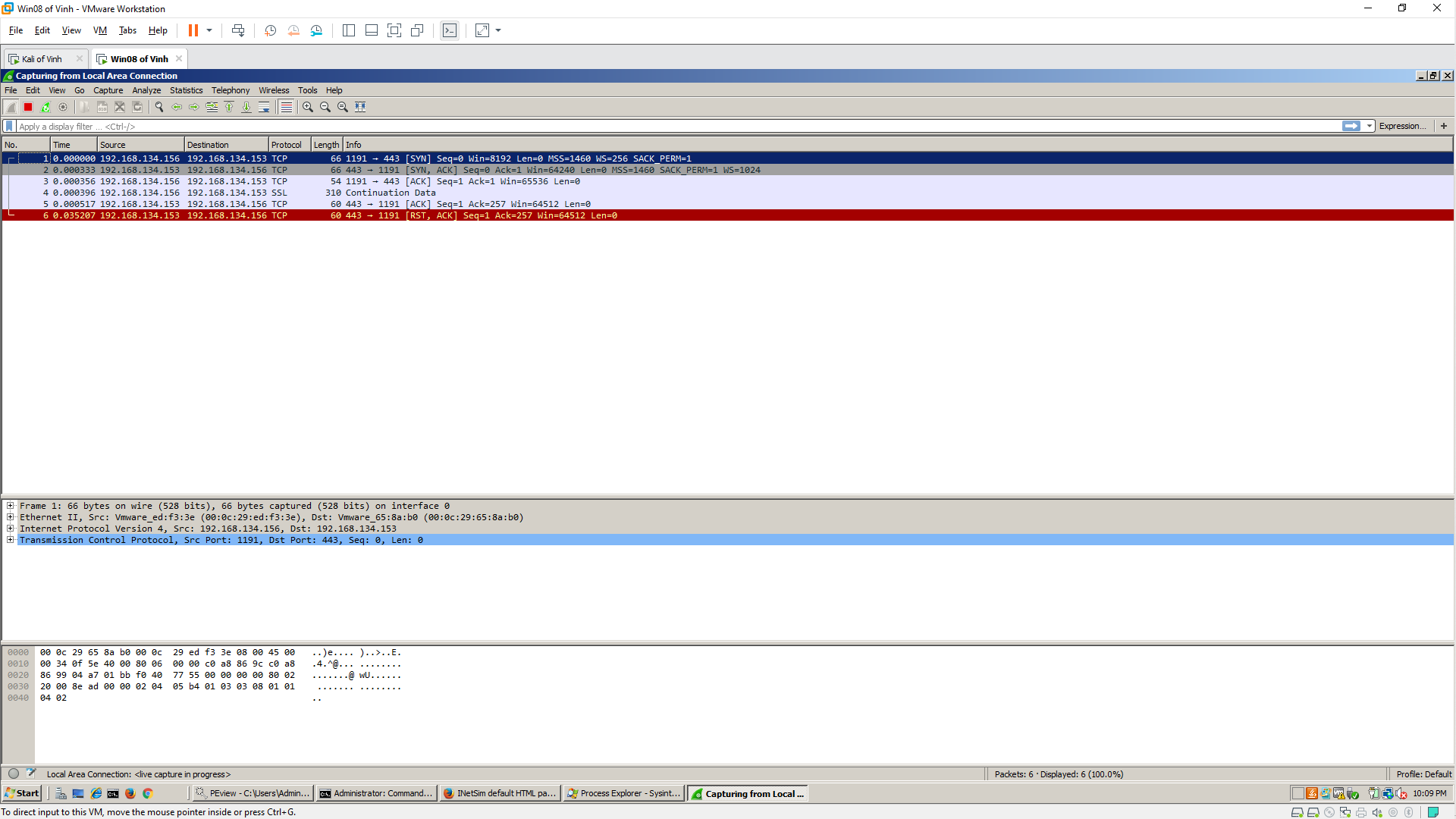
**2. Setting the DNS Server**

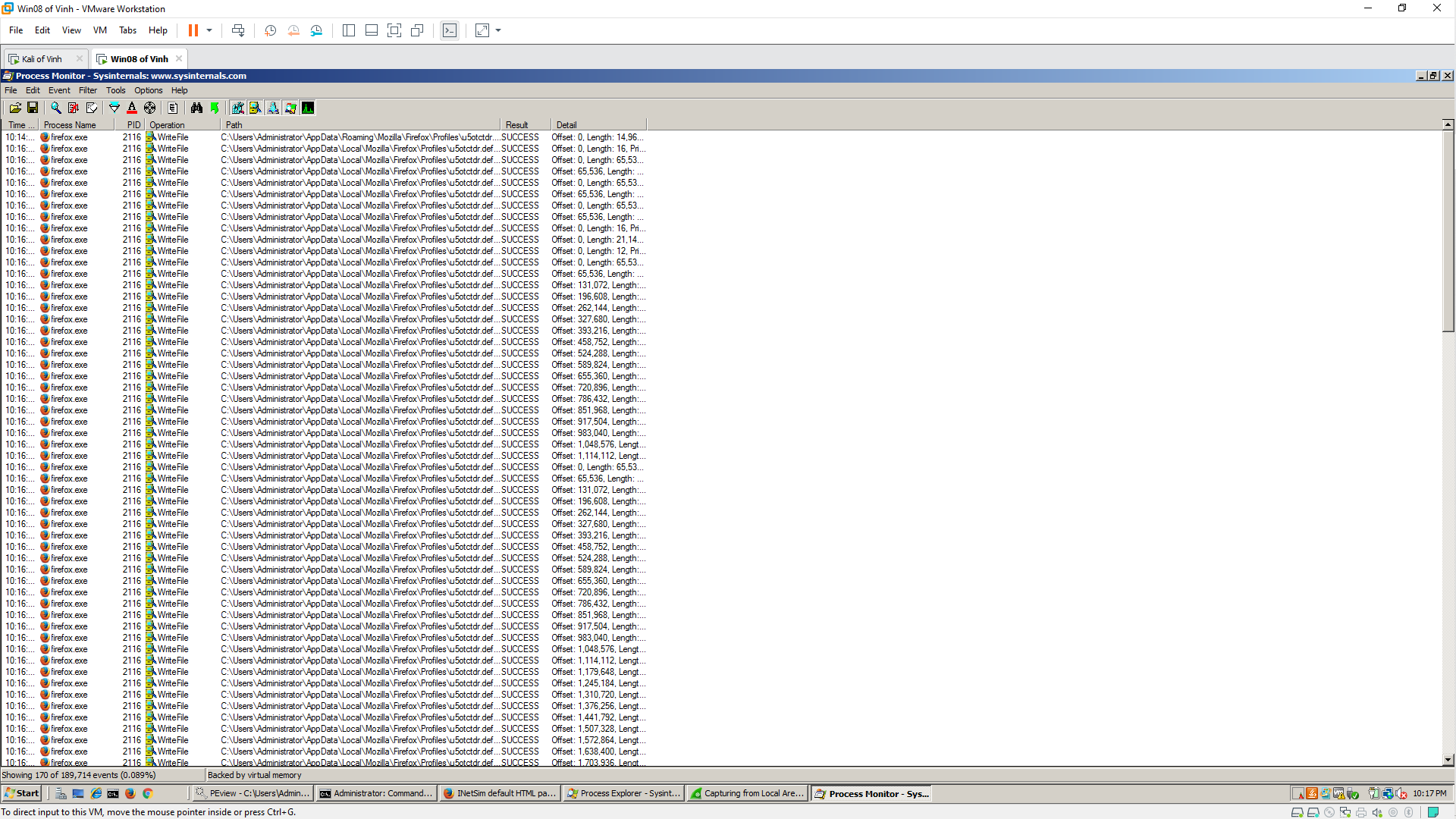
**3. Run Process Explorer**

****

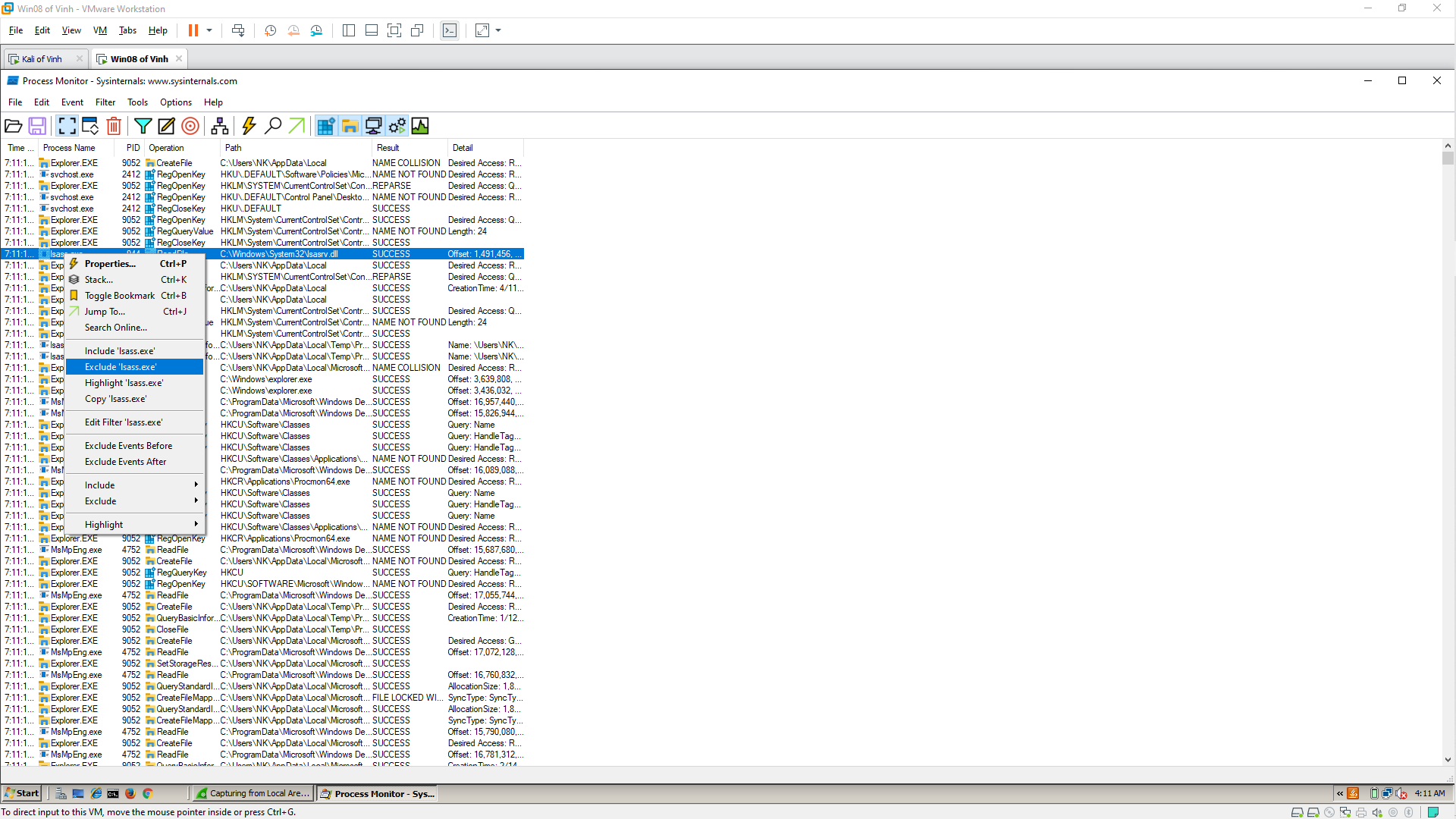
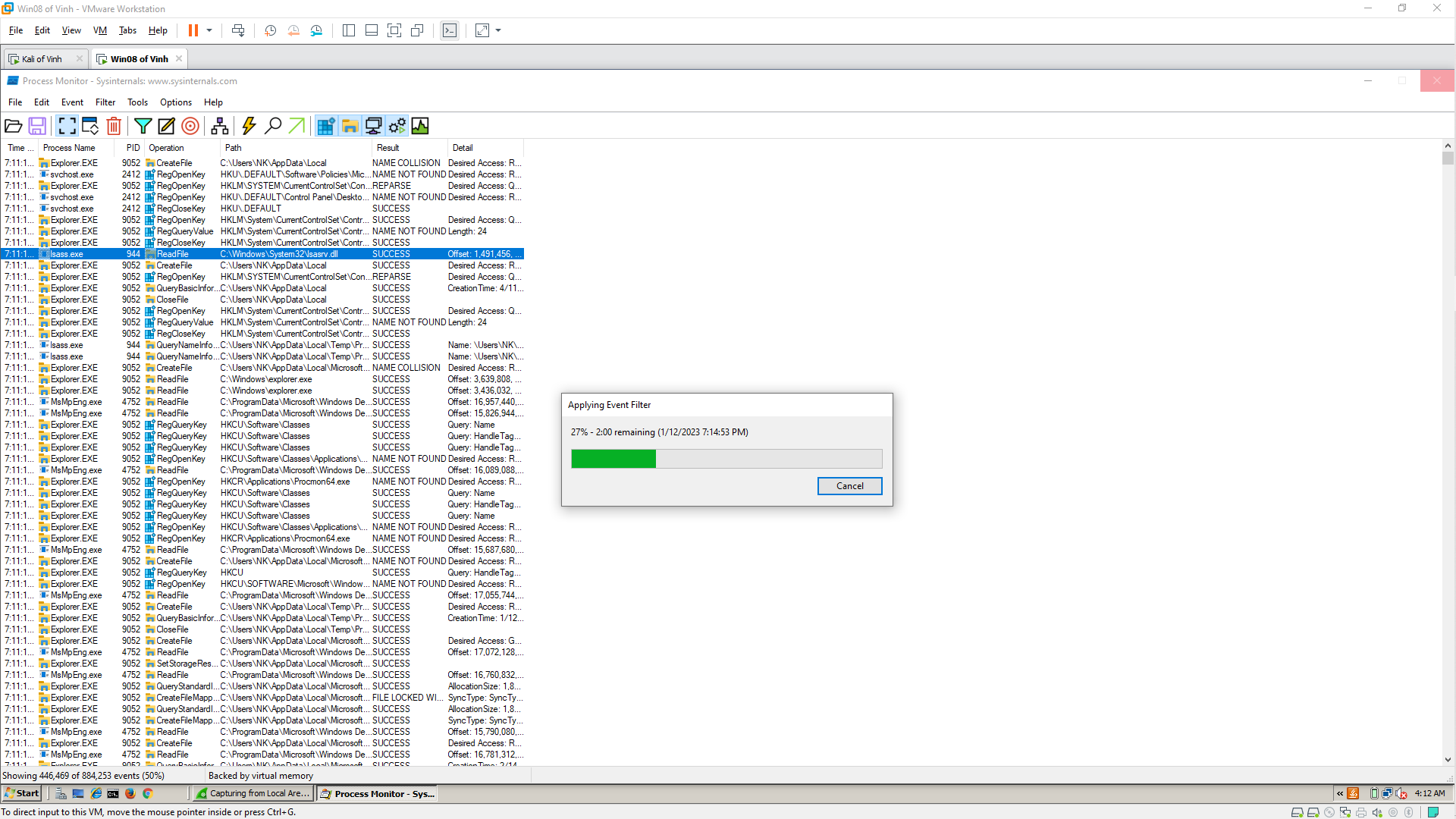
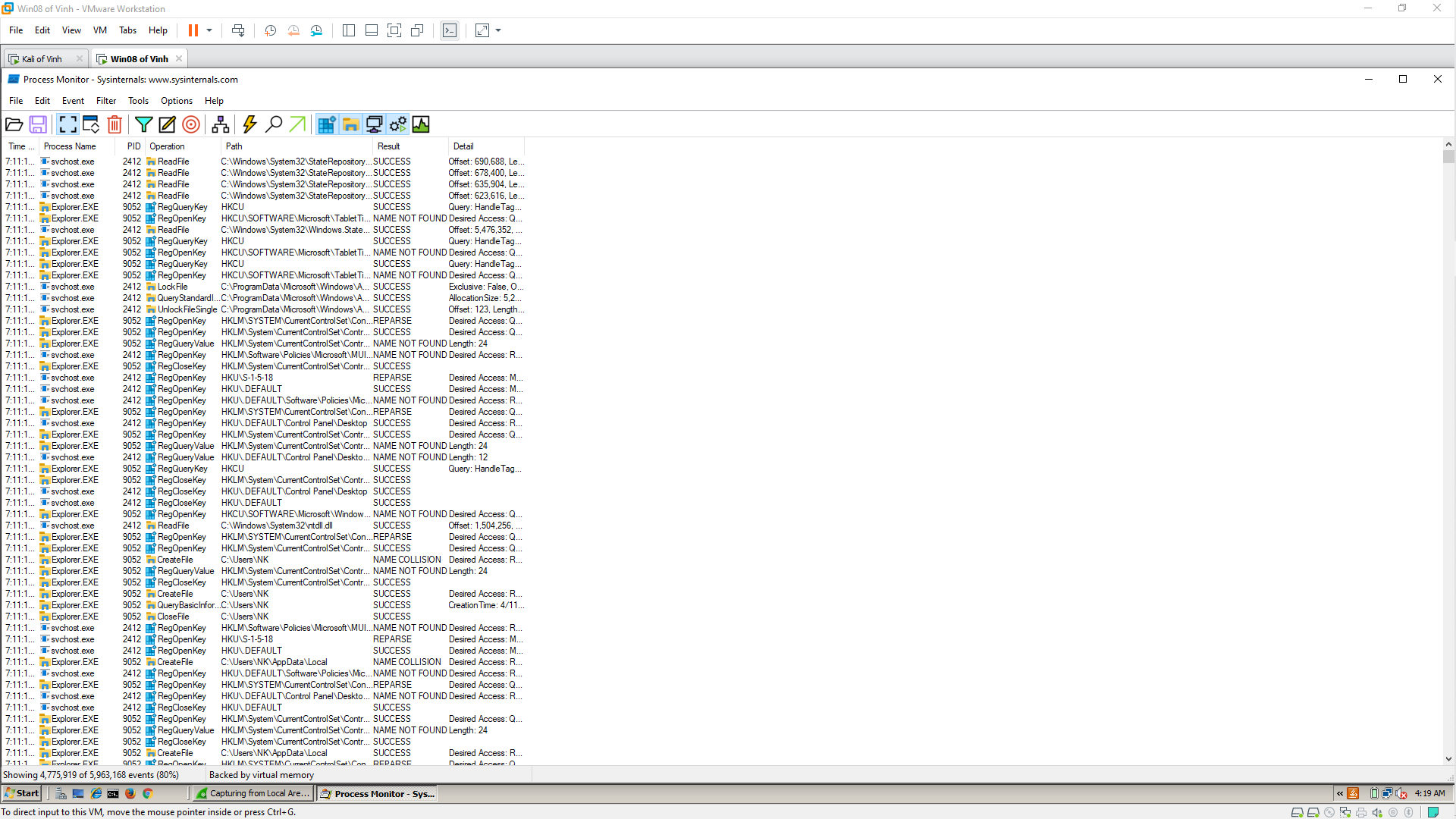
**4. Run Wireshark**

****

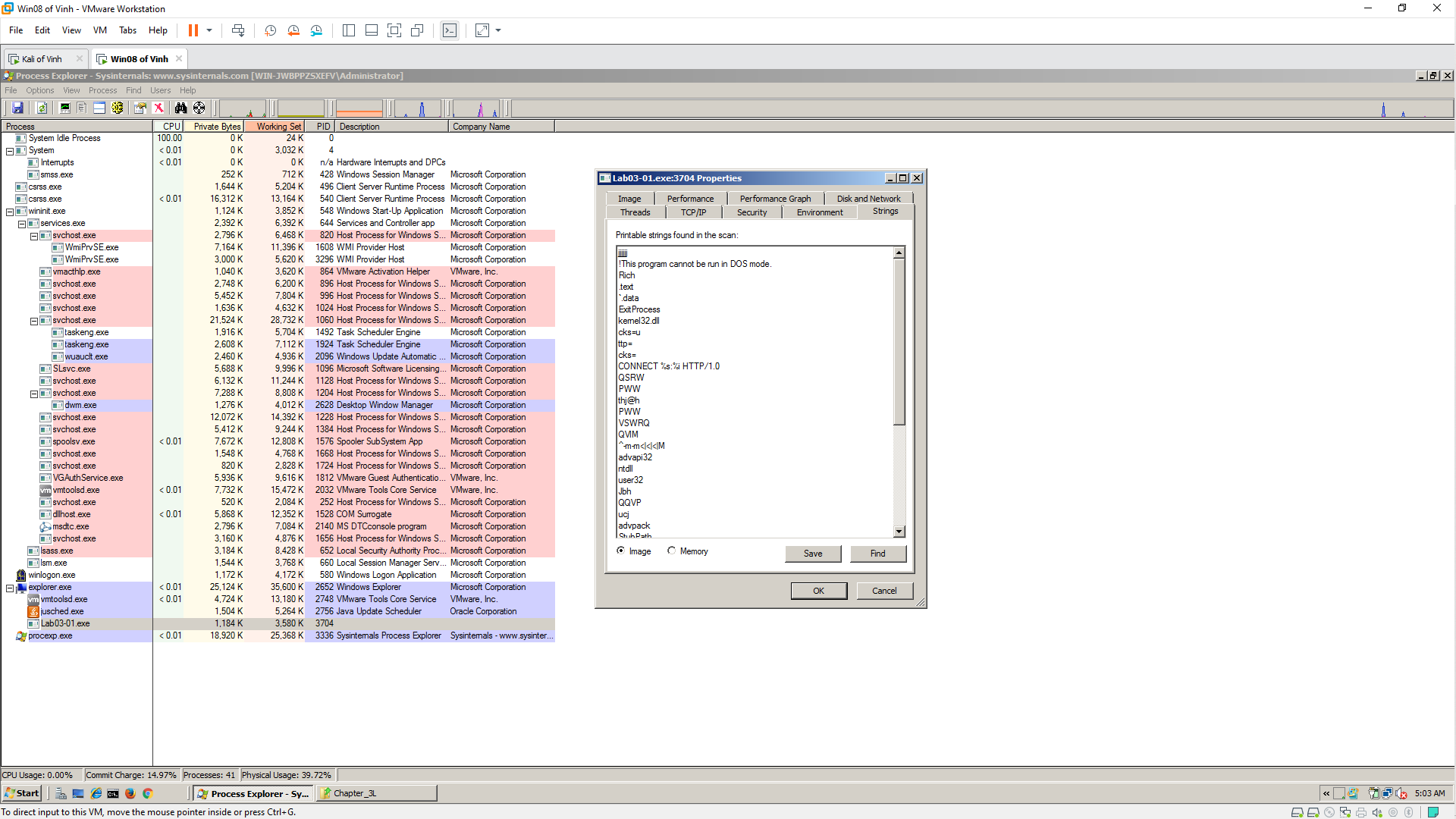
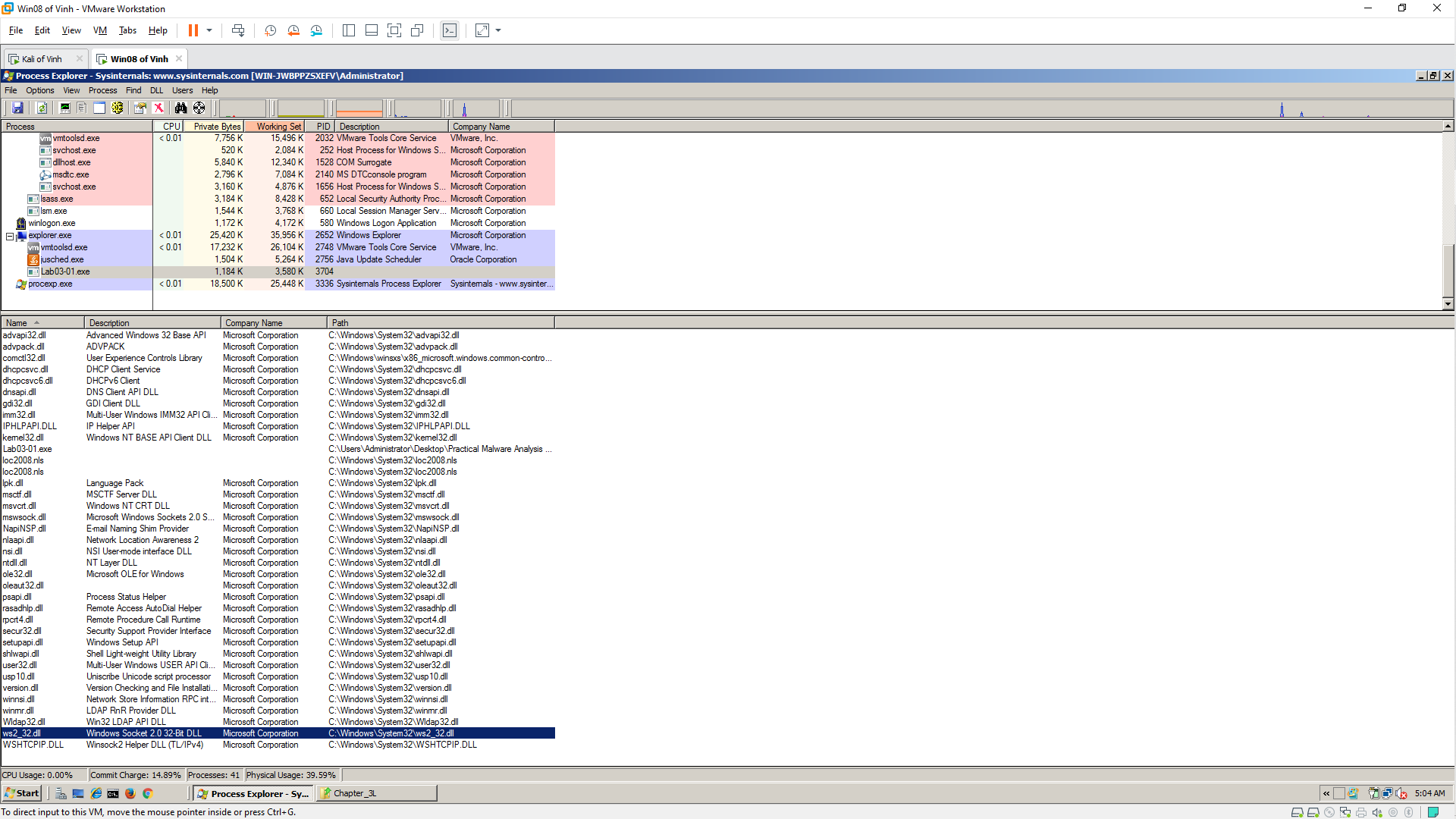
**5. Start Process Monitor**

****

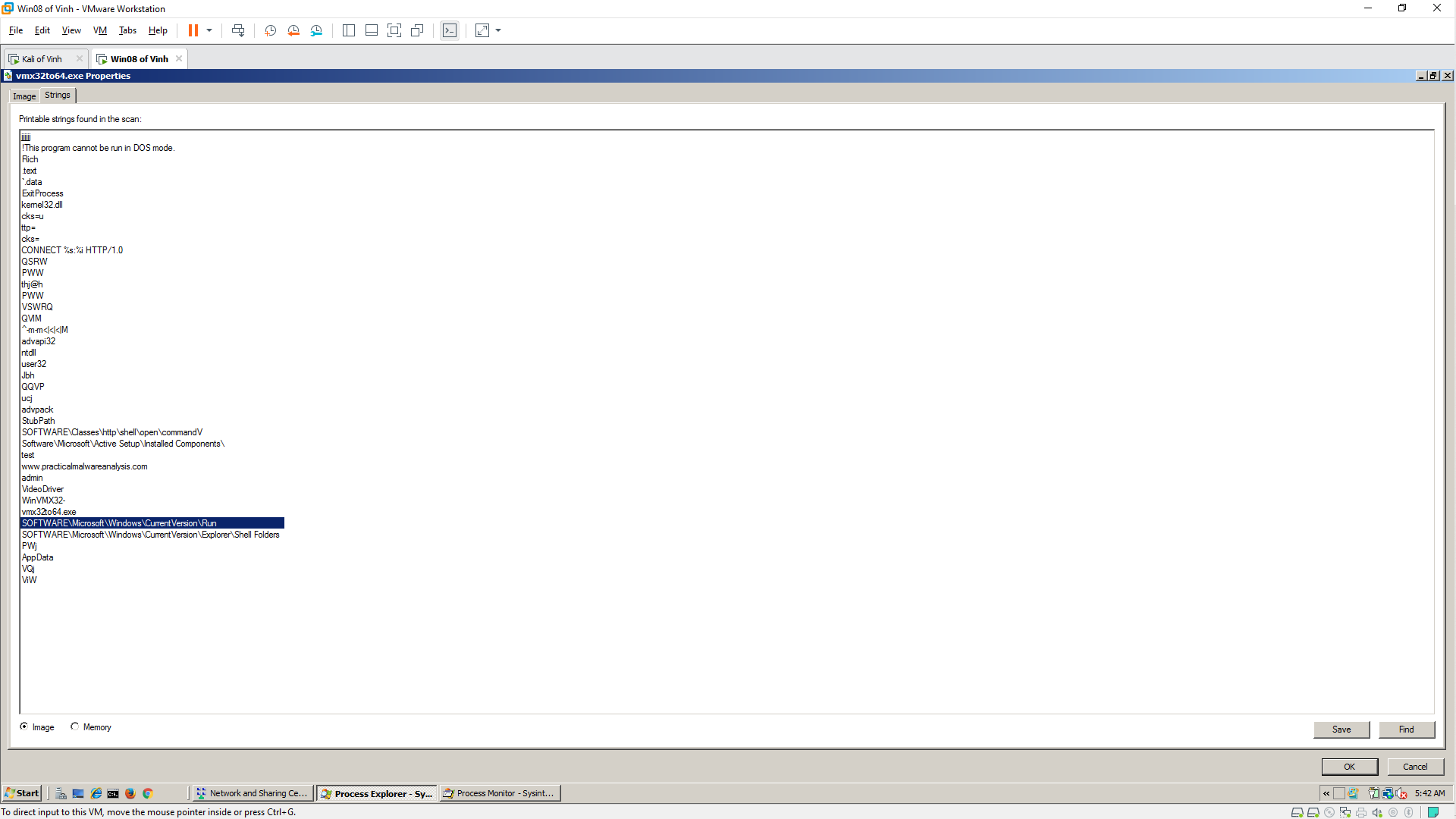
Excluding Harmless Processes

**  **

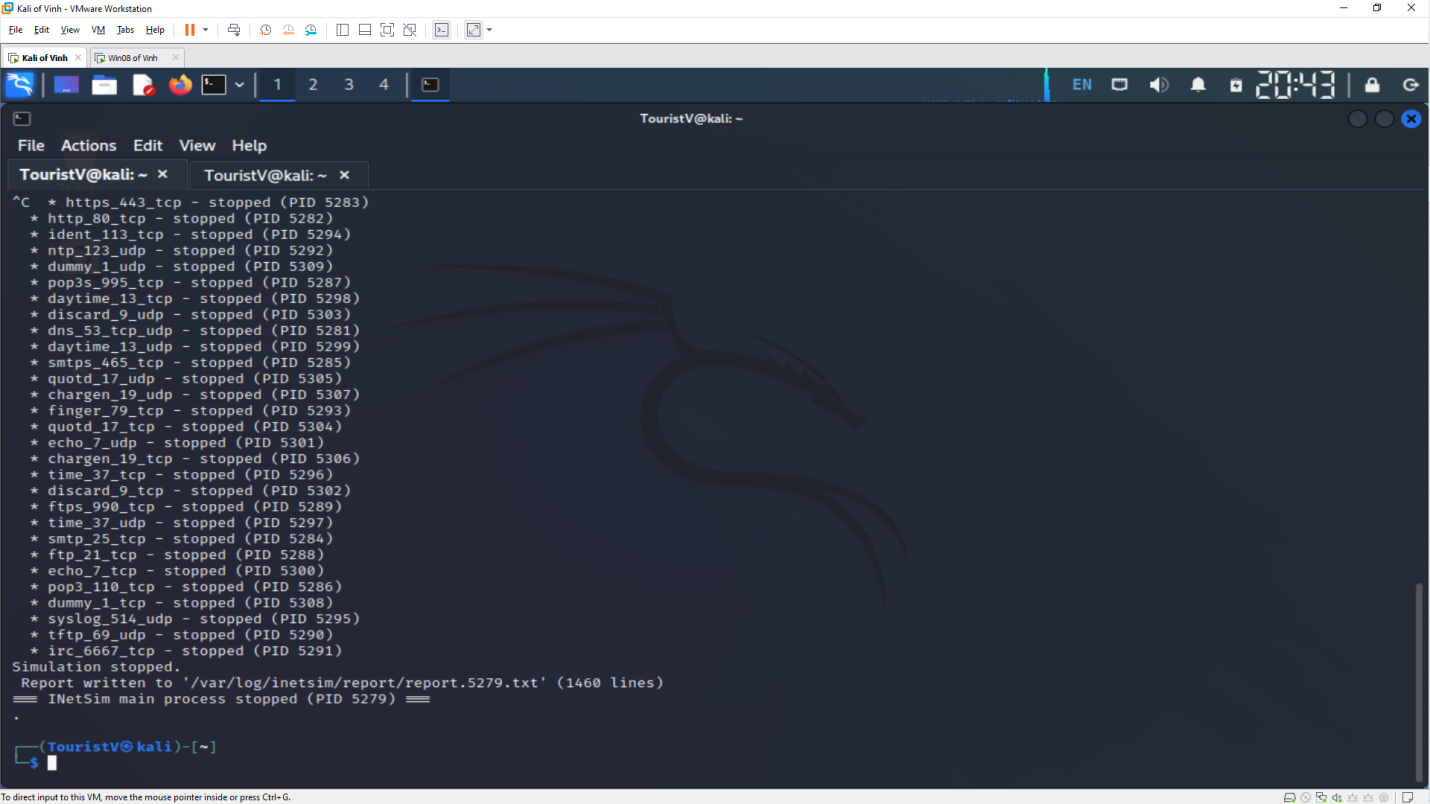
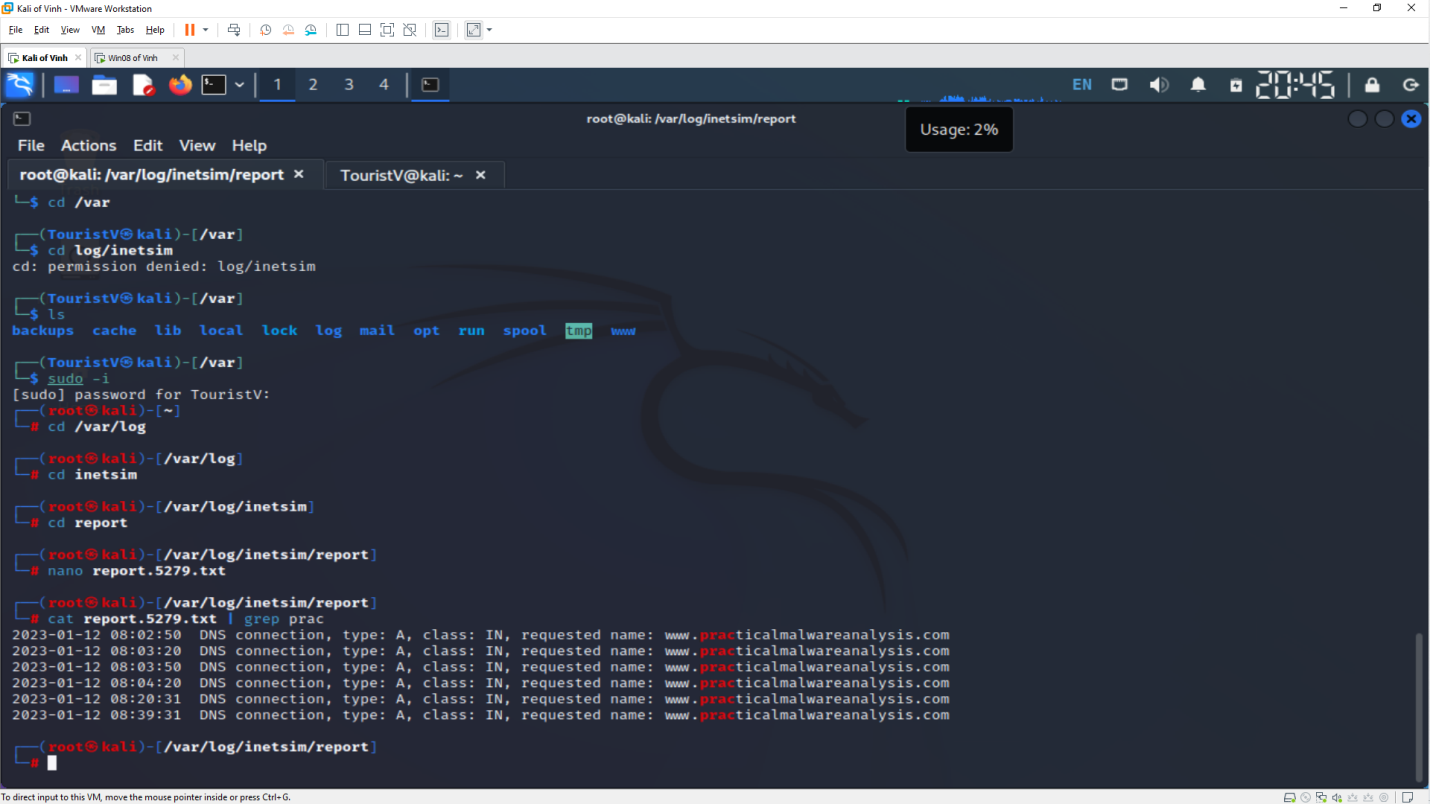
**Run the Lab03-01.exe File**

** **

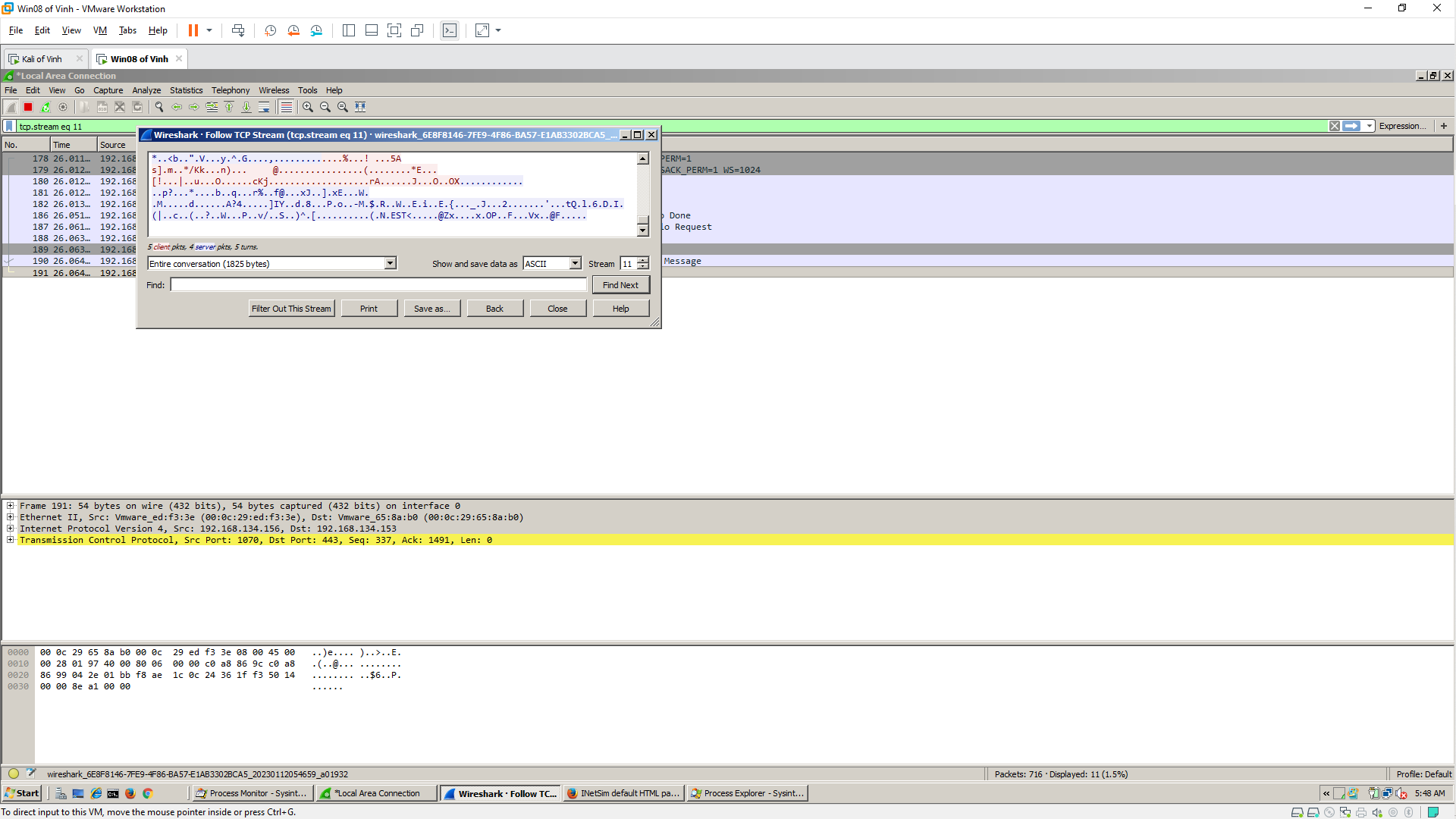
**Viewing the Malicious Process's Events in Process Monitor**

****

**Viewing INetSim Logs**

** **

**Viewing the Network Request in Wireshark**

****