**Lab 5: Keylogger**

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

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

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 8/2/2023

**Purpose**

You will practice the techniques in chapter 3.

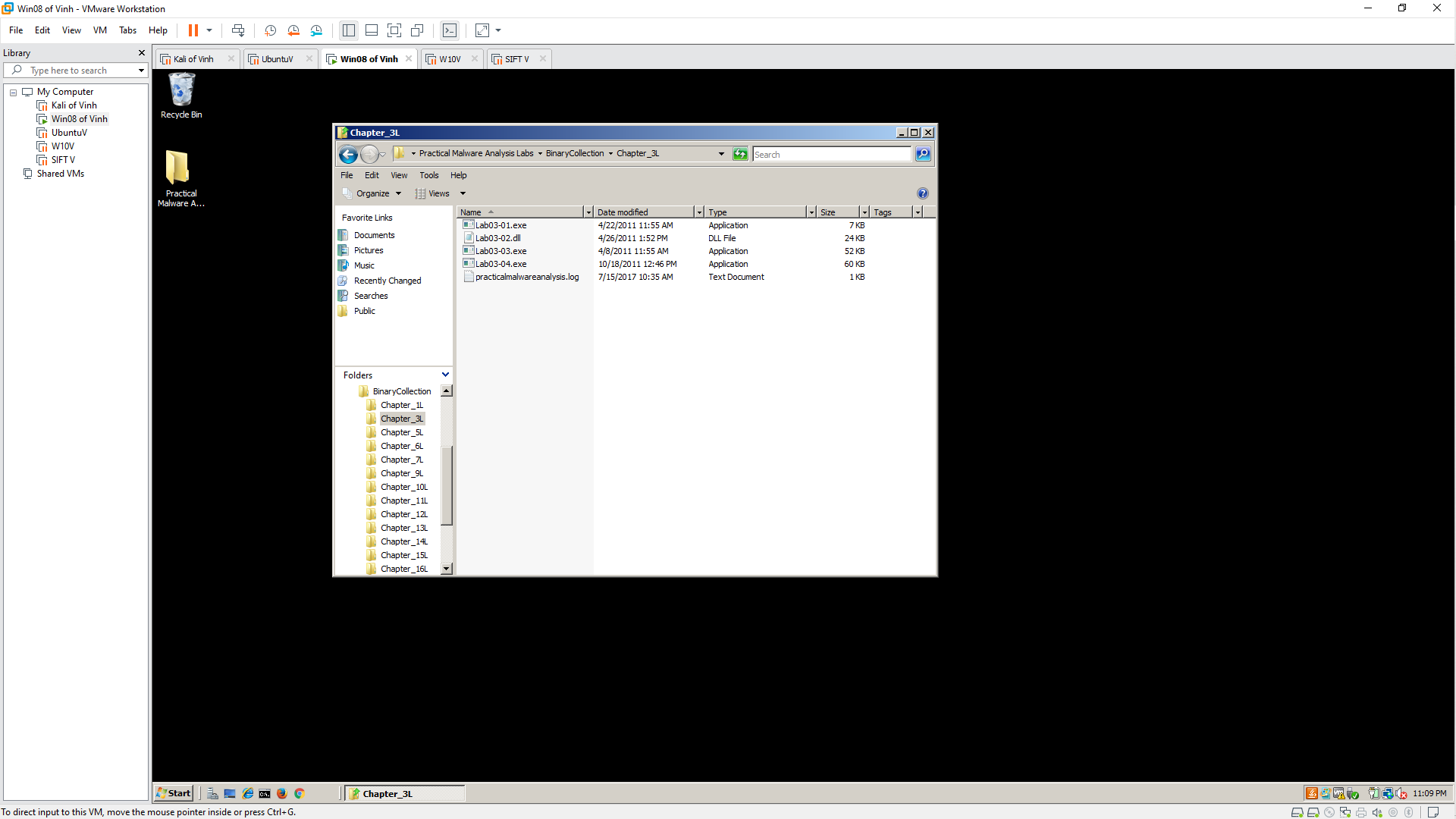
This project follows Lab 3-3 in the textbook.

**What you need:**

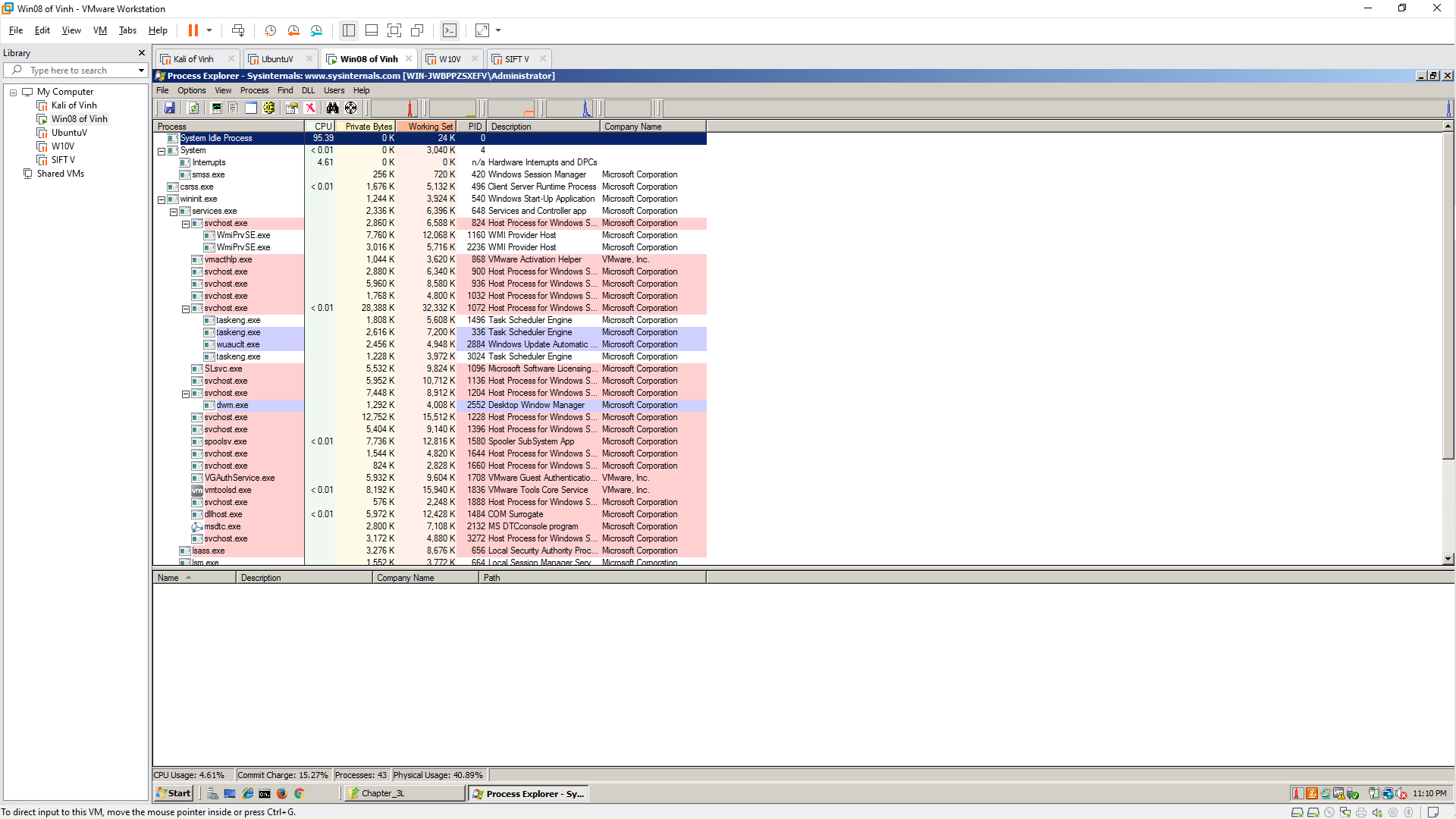
The Windows 2008 Server virtual machine we have been using

**Preparing Windows**

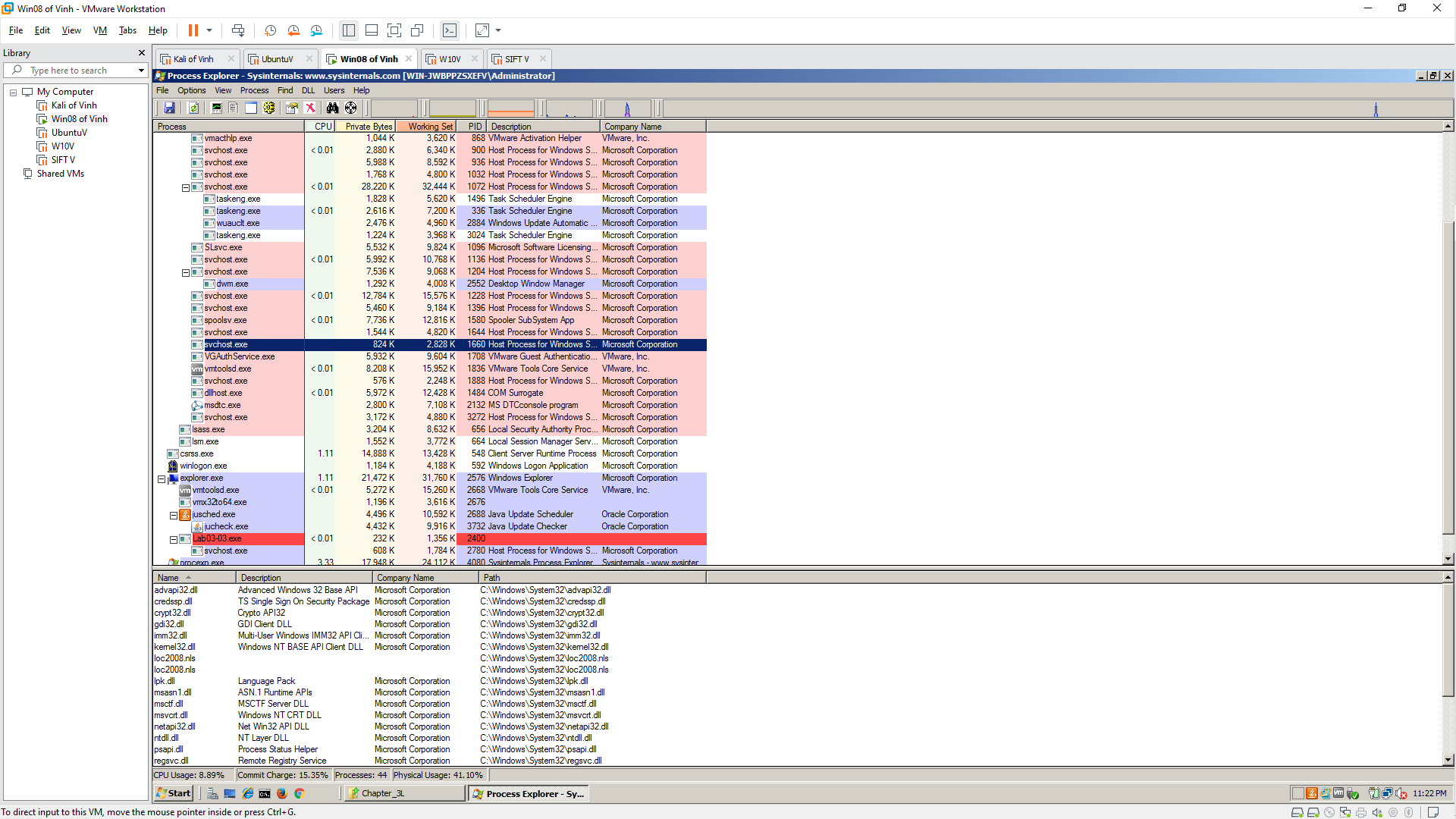
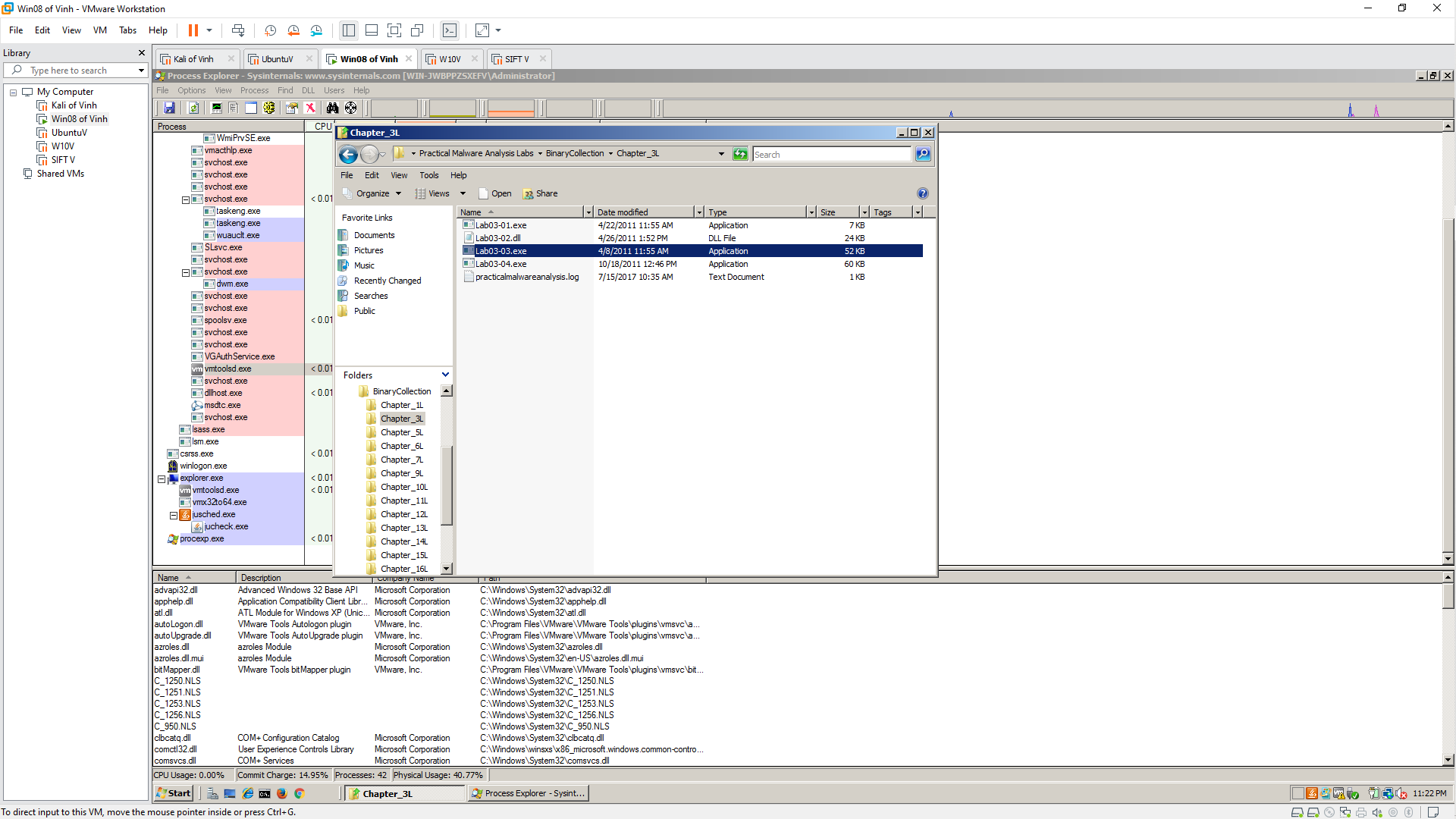
On your desktop, open the "Practical Malware Analysys Labs" folder. Open the "Binary Collection" and Chapter\_3L folders.

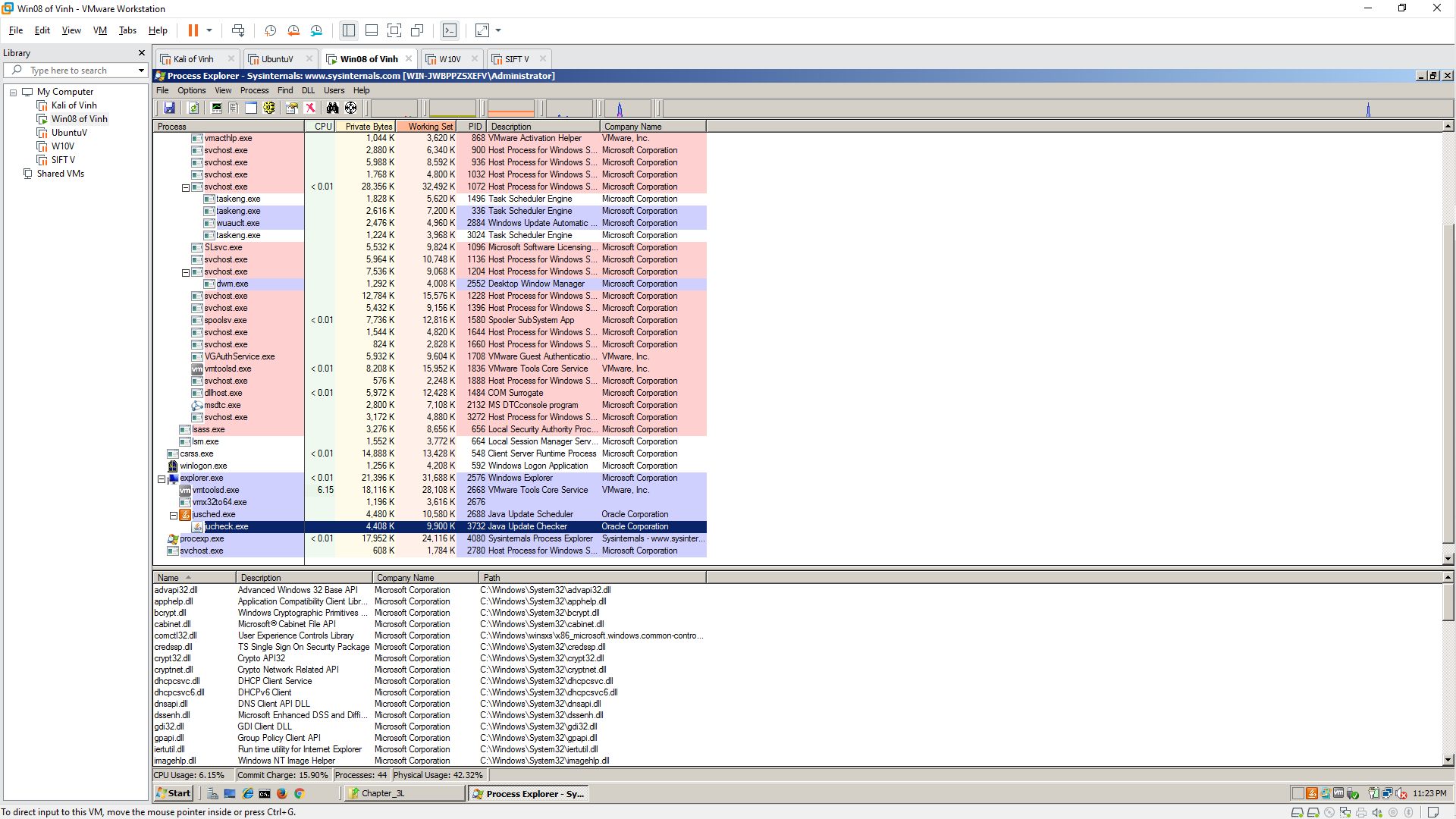
****

Open Process Explorer and move it so you can see it at the same time as the Explorer window. Scroll to the bottom to show explorer.exe (your desktop) and its children, which are processes launched by the currently logged-in user, as shown below.

****

**Launch the Malware**

****

After a second or two, the Lab03-03.exe process terminates, leaving the svchost.exe running as an orphan process, as shown below****

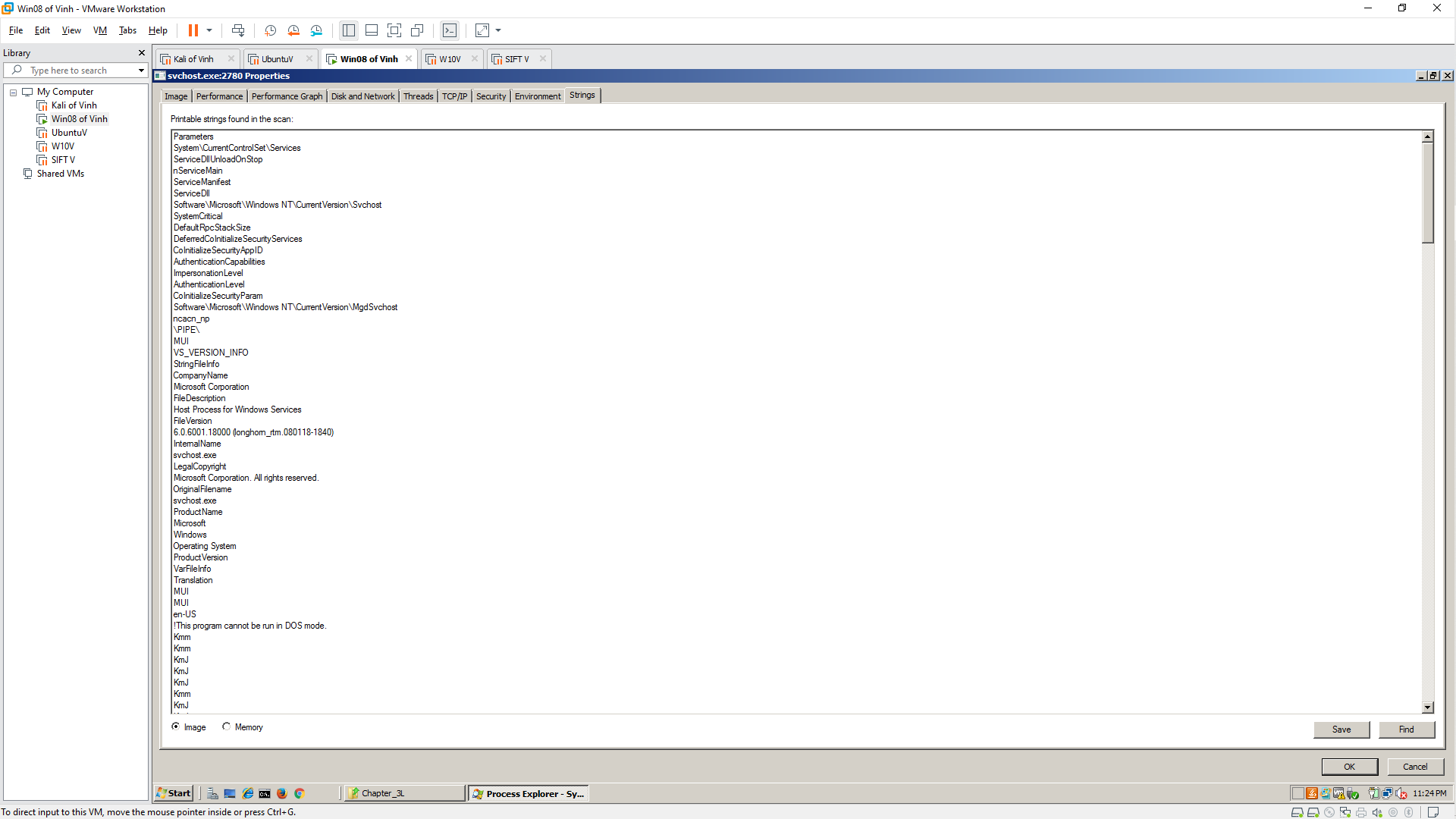
**Observing Process Replacement**

This svchost process is strange in another way: the code running in RAM does not match the code on the disk.

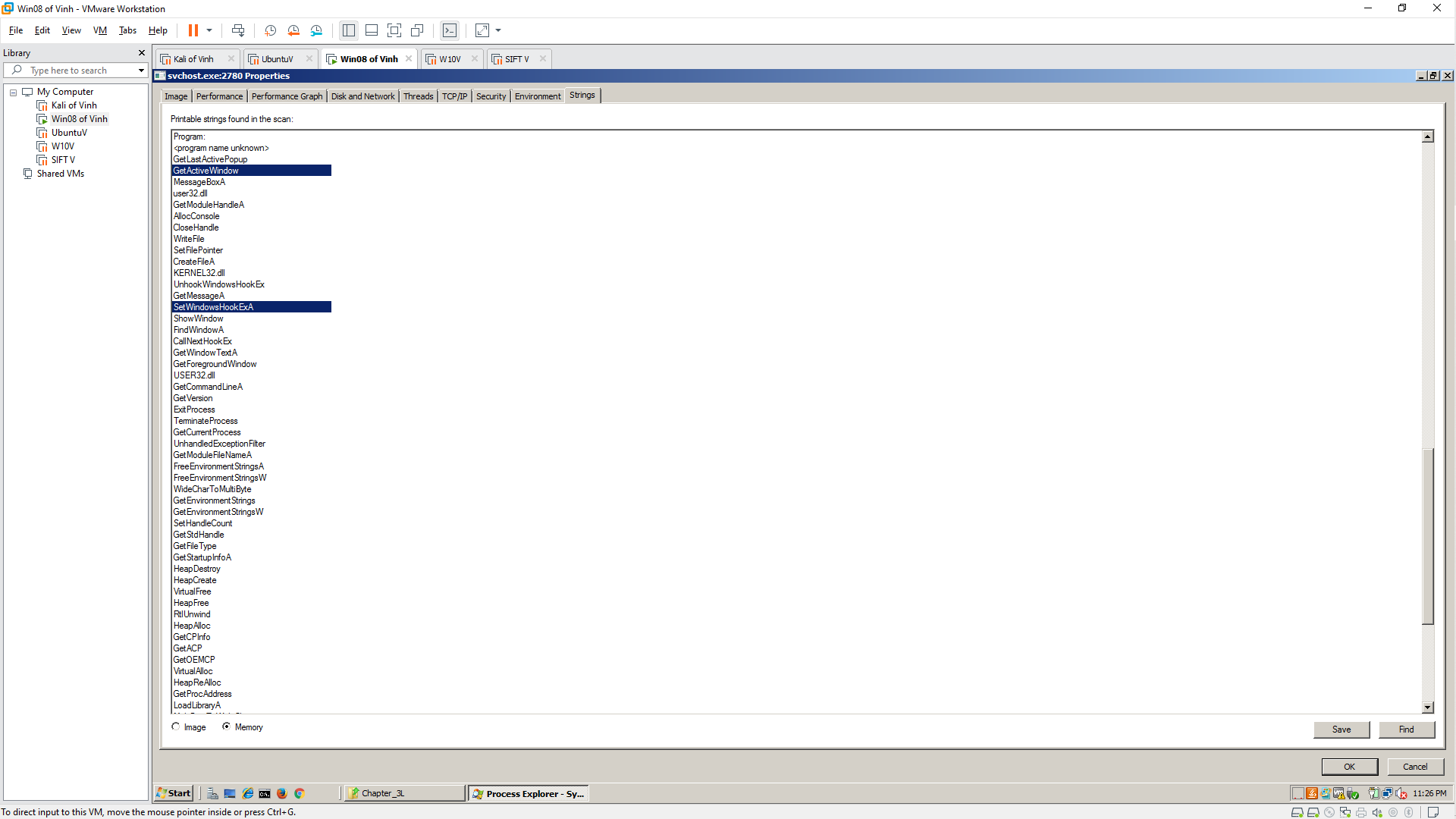
To see that, in Process Explorer, right-click svchost.exe and click Properties.

Click the Strings tab. At the bottom, make sure Image is selected, as shown below.

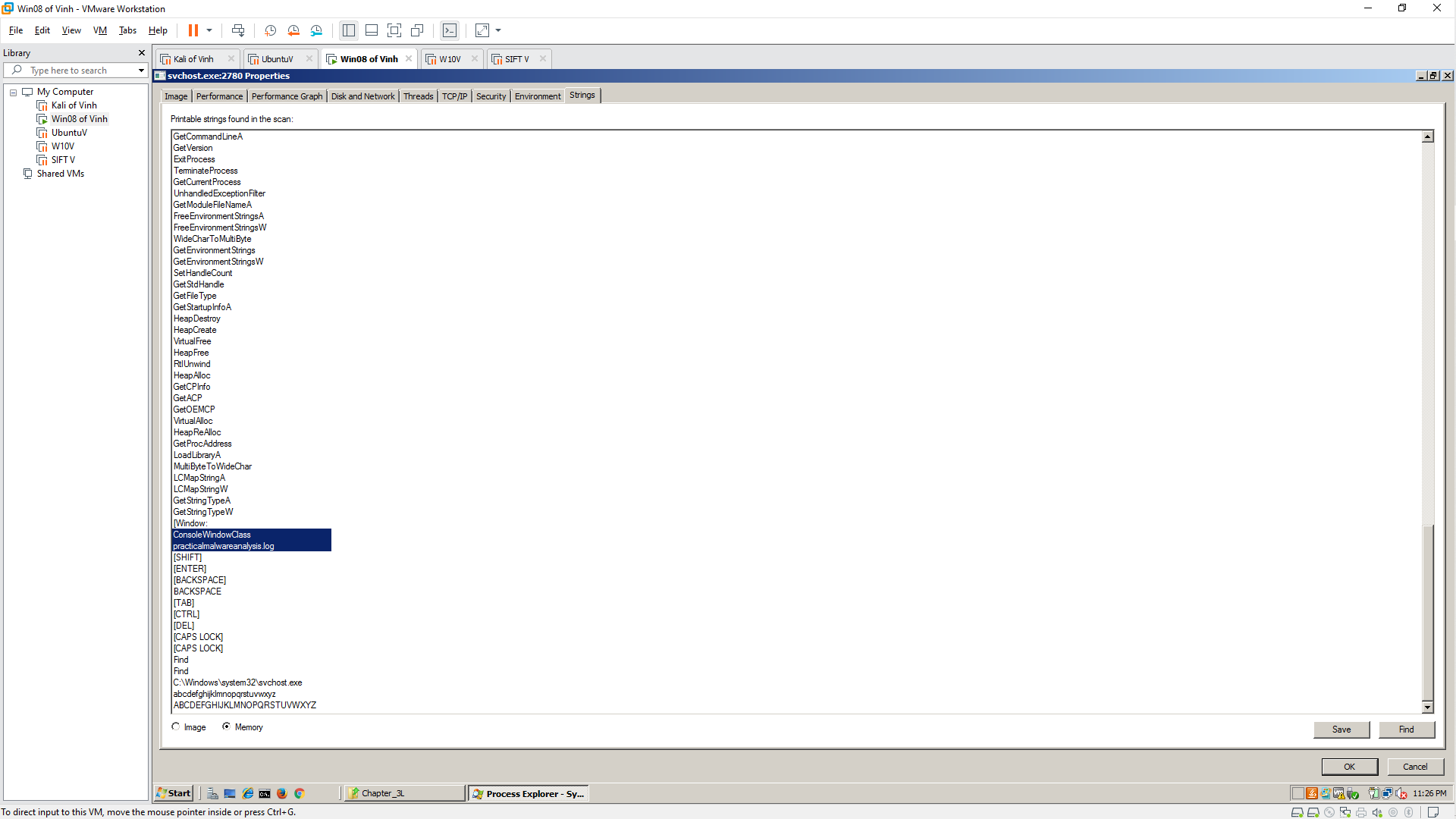
These are the strings on the disk, in the real svchost.exe file



At the bottom of the box, click the Memory button. Now the strings are completely different, and contain these suspicious items: GetActiveWindow and SetWindowsHookExA.

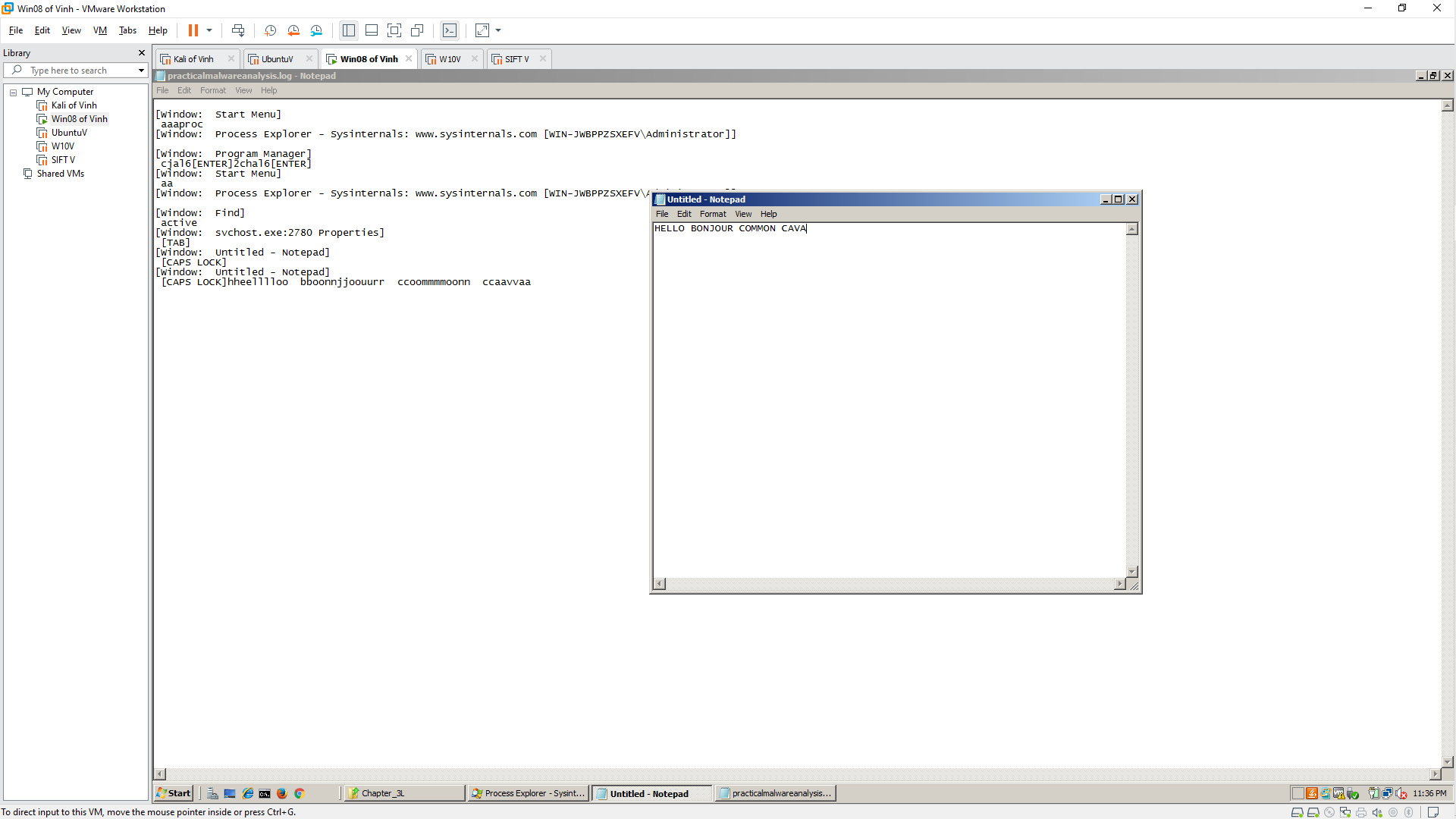
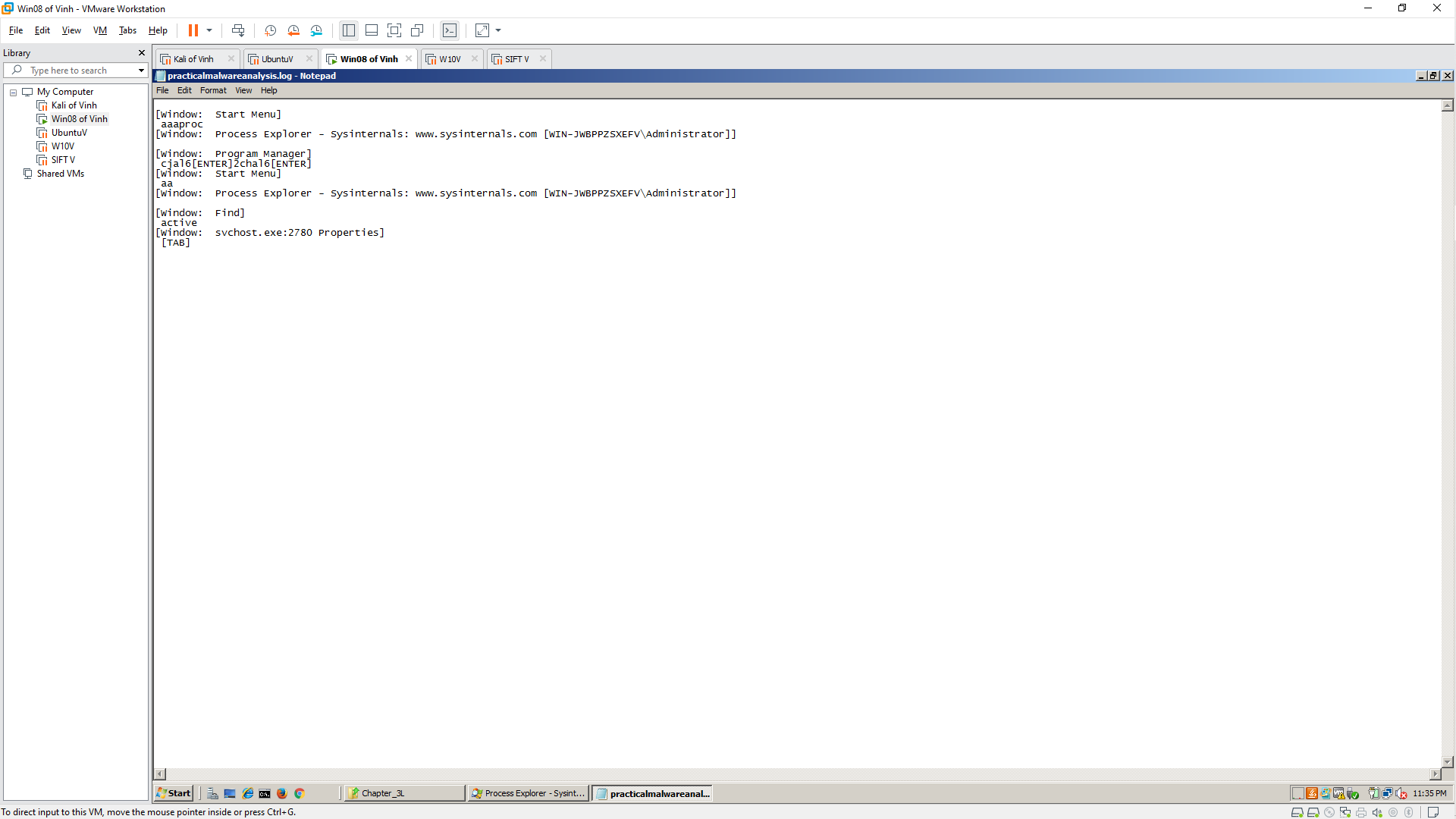


Scroll down and find the string practicalmalwareanalysis.log, as shown below. This may be the filename used to store the keypresses

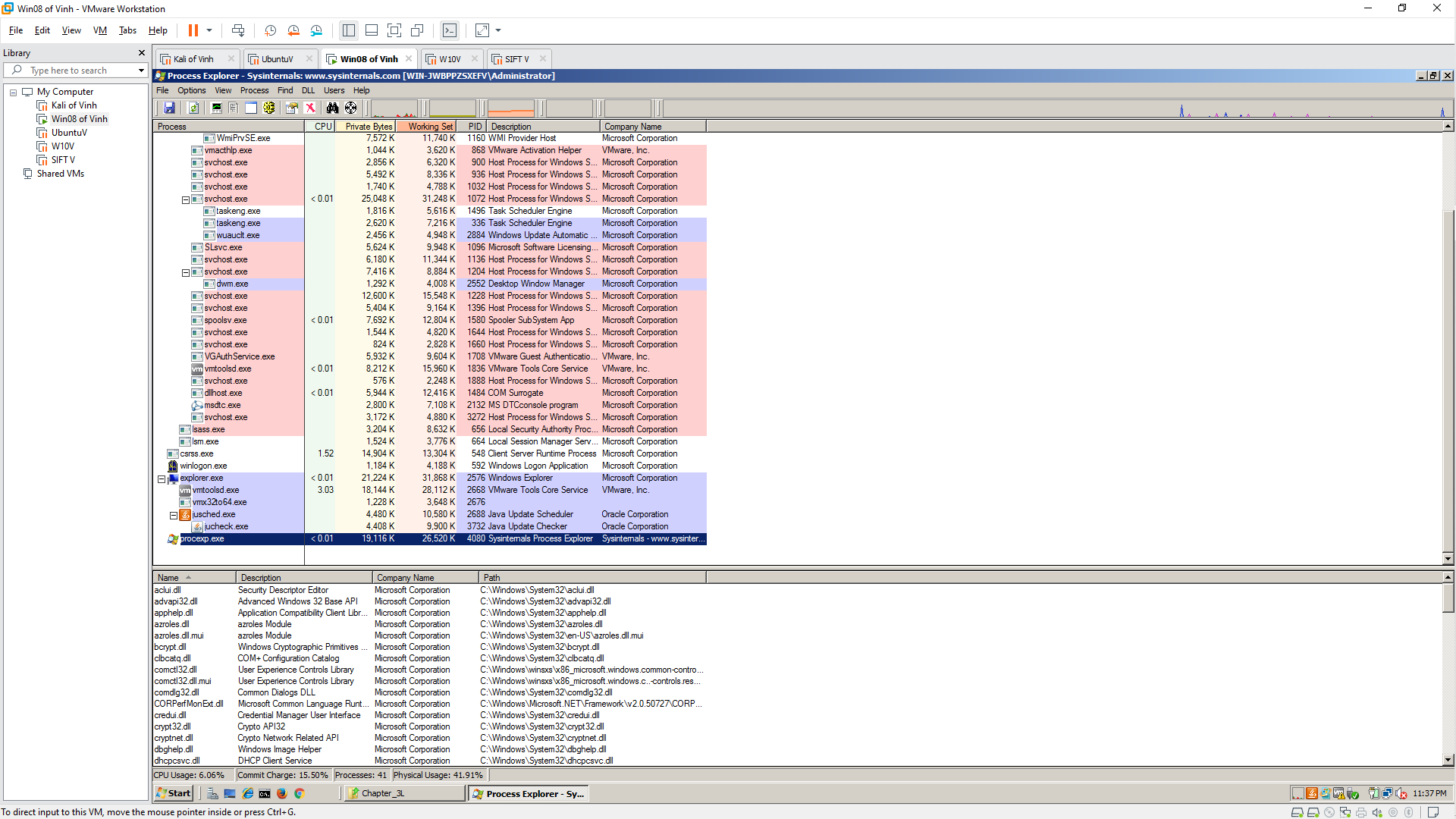
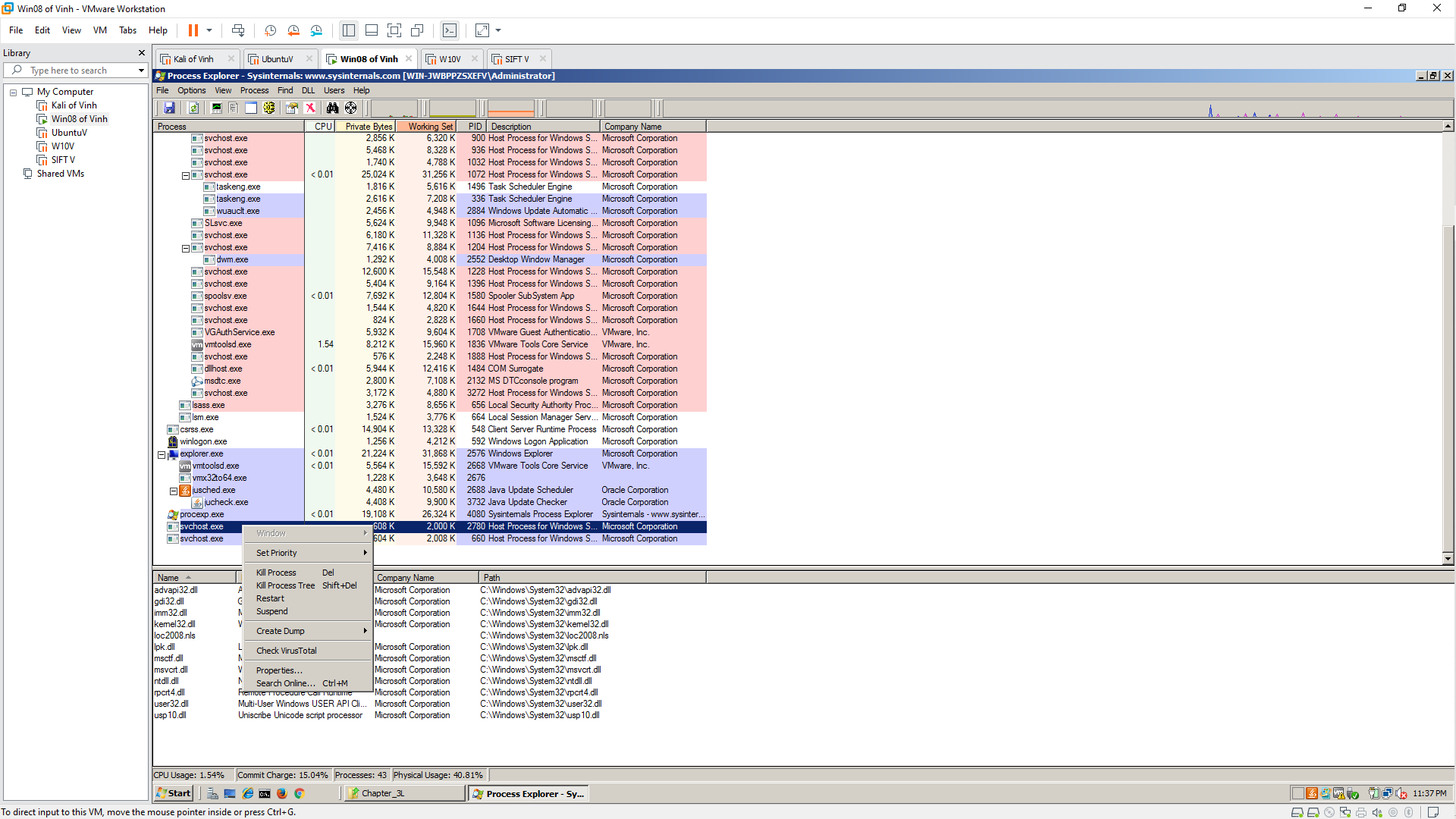


**5.1: Recording Your Success**

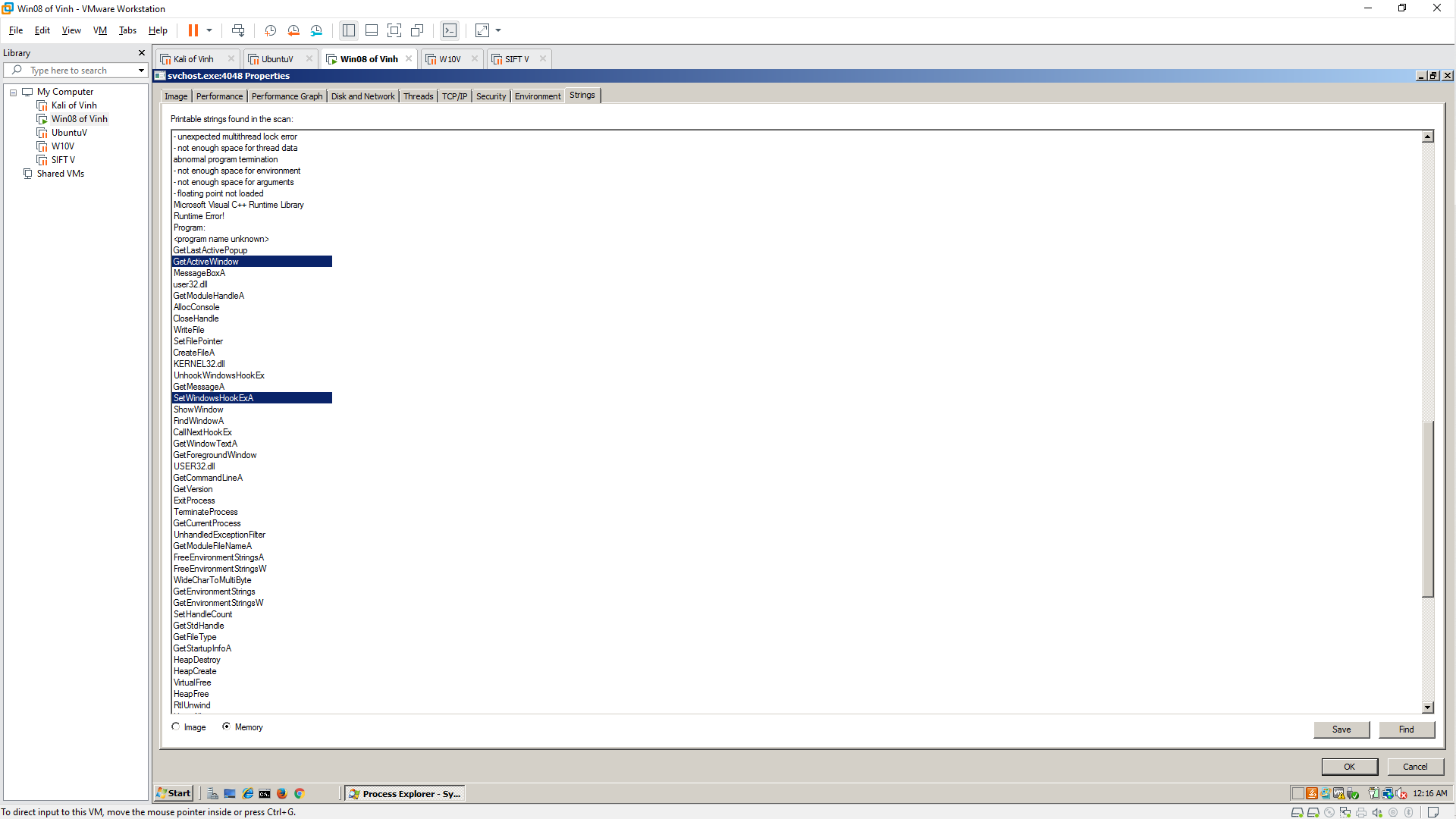
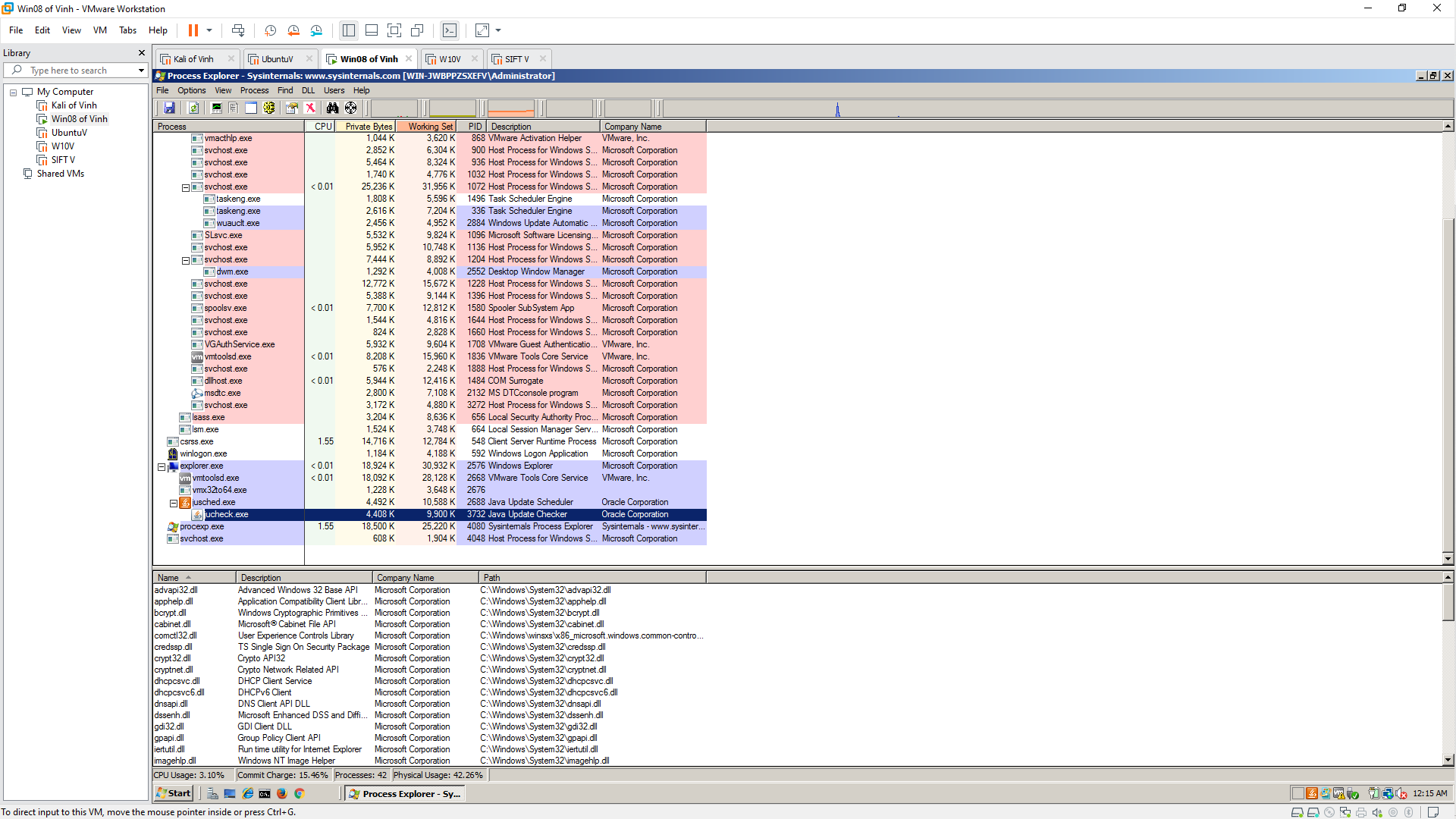
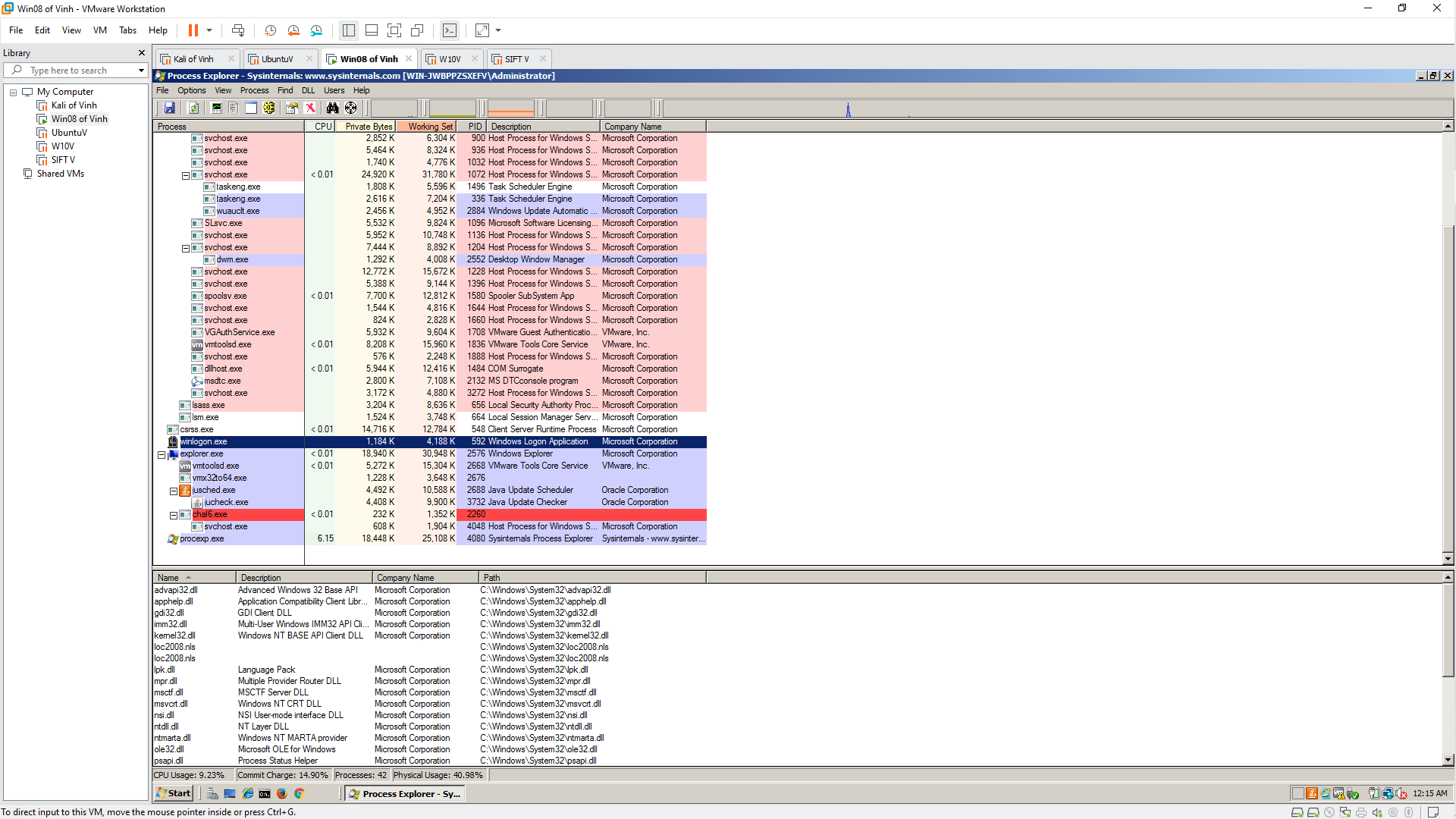
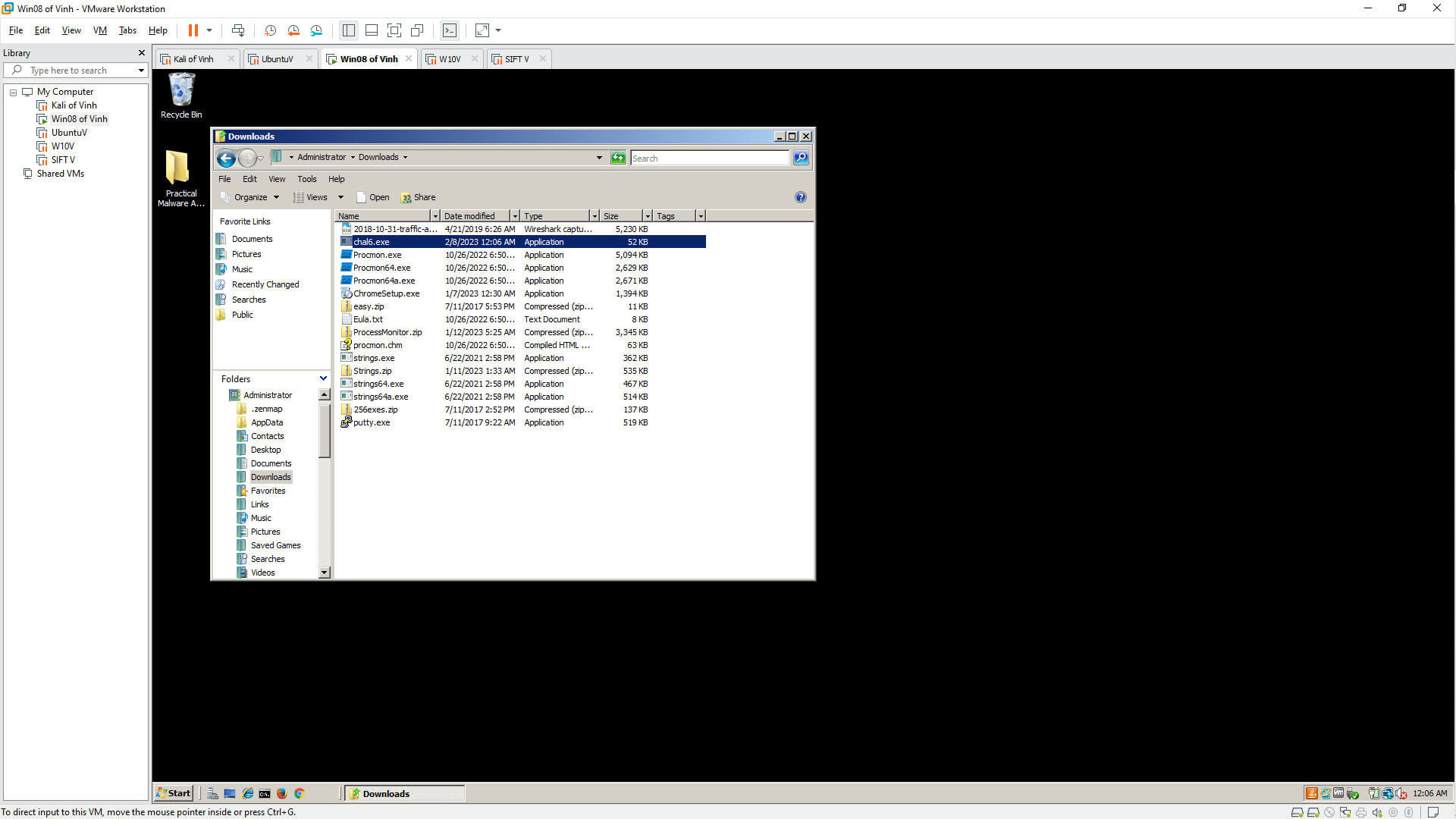
Testing the Keylogger

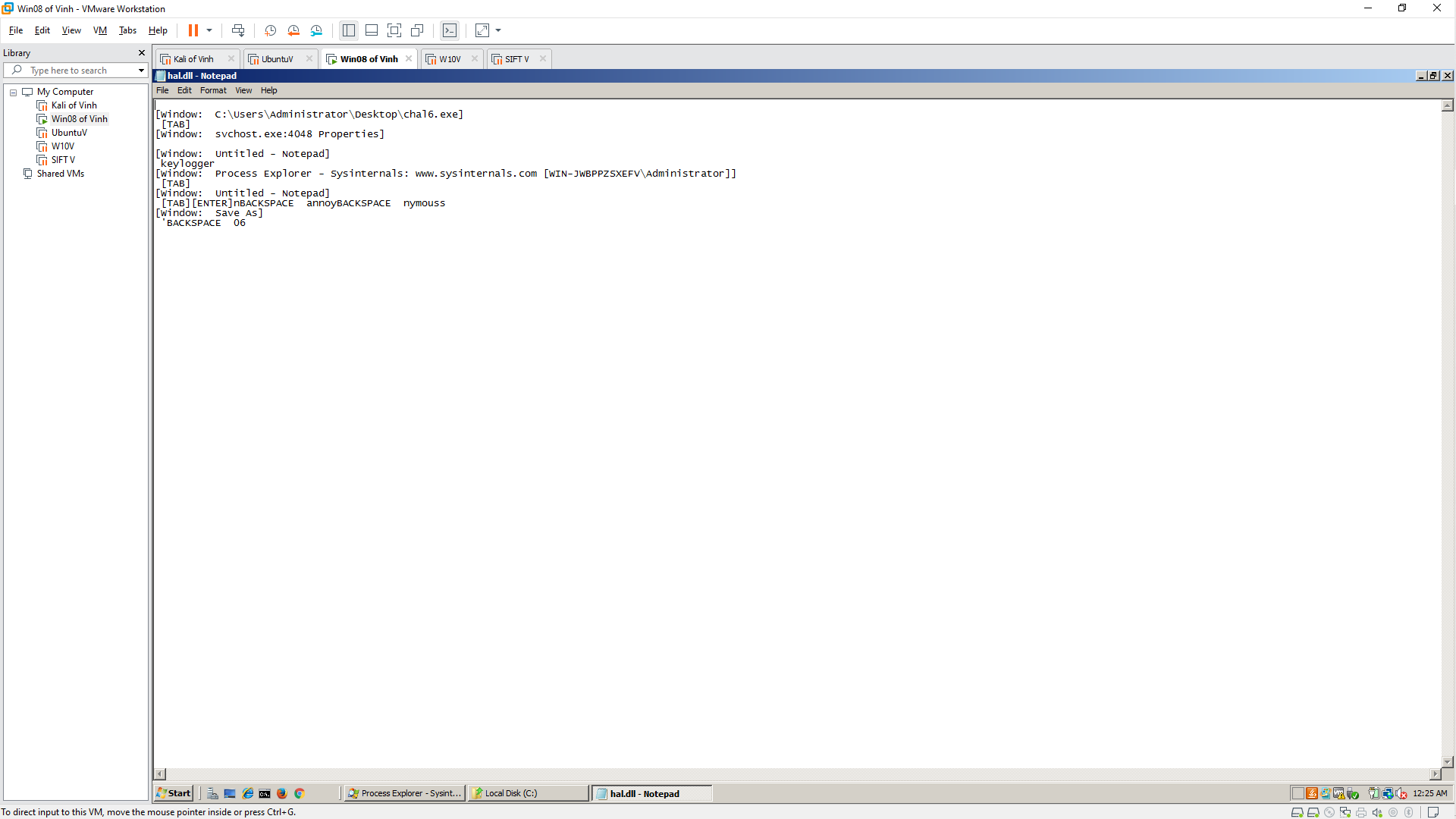
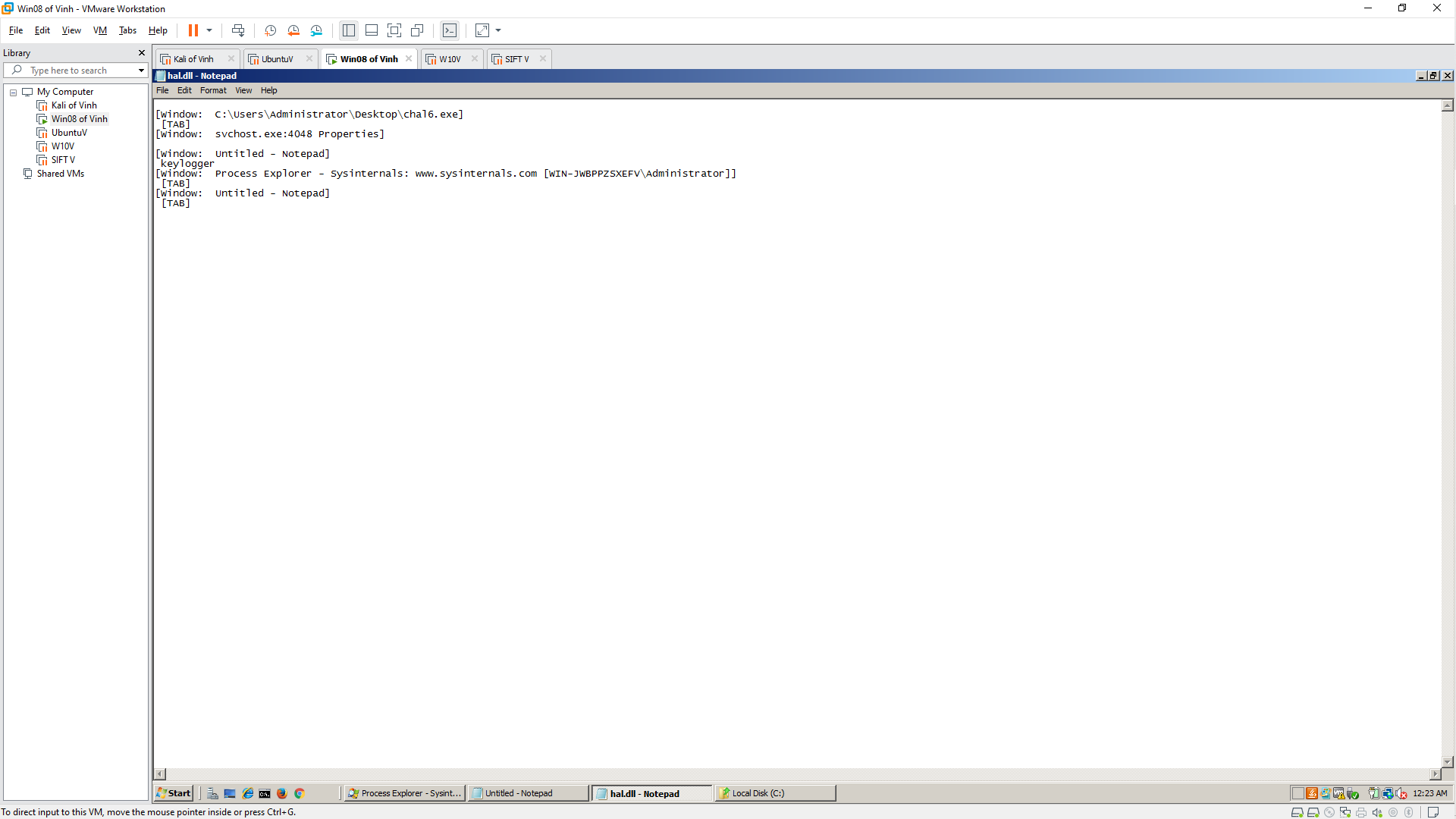
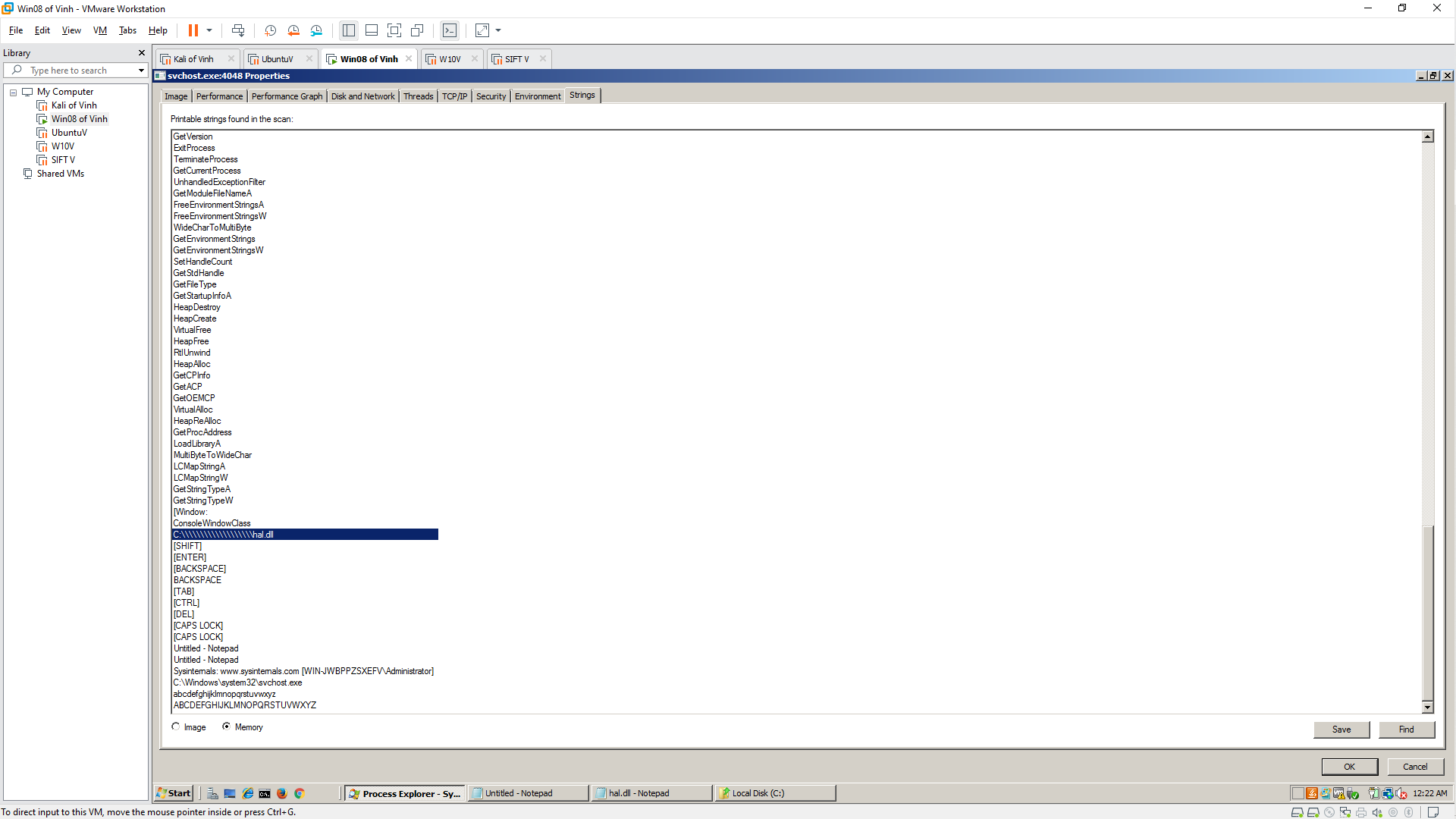
****

**Killing the Keylogger Process**

****

**Challenge 5.2: Find the Logfile**

In your Documents folder, find the file chal6.exe

****