Proj 5. Keylogger (15 pts + 15 pts extra)

What you need:

- The Windows 2008 Server virtual machine we have been using

Purpose

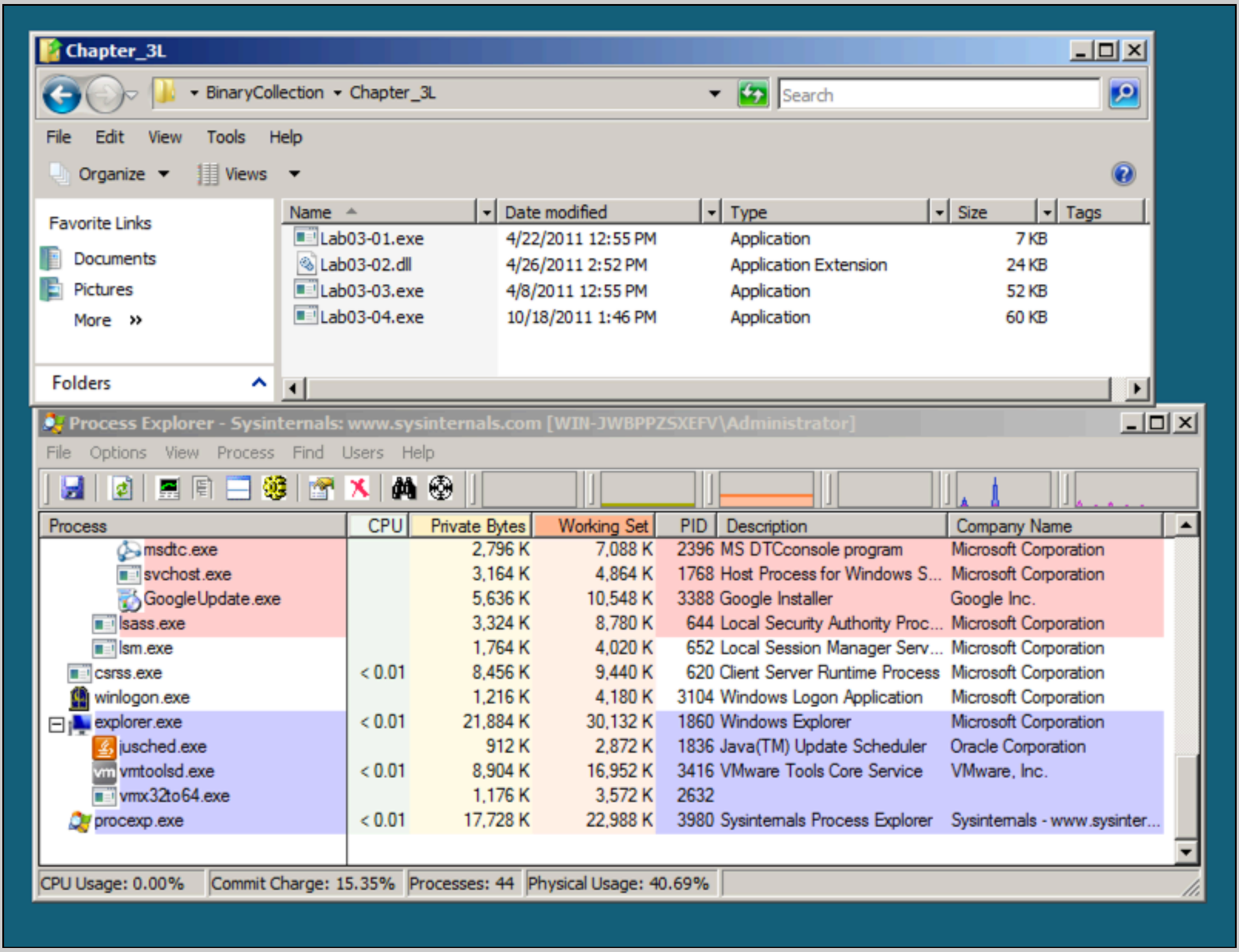
You will practice the techniques in chapter 3.

This project follows **Lab 3-3** in the textbook.

Preparing Windows

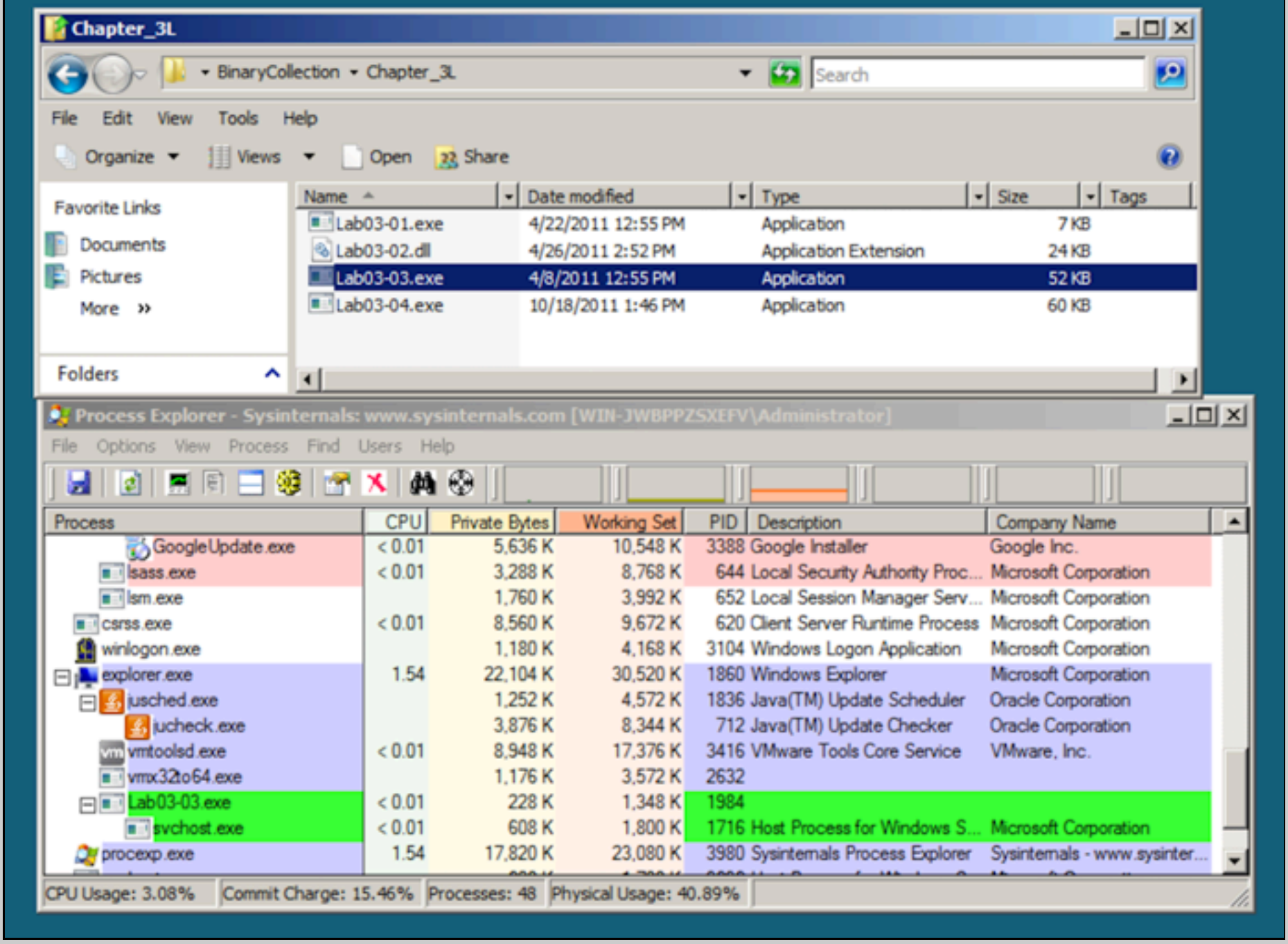
On your desktop, open the "**Practical Malware Analysys Labs**" folder. Open the "**Binary Collection**" and **Chapter_3L** folders.

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.



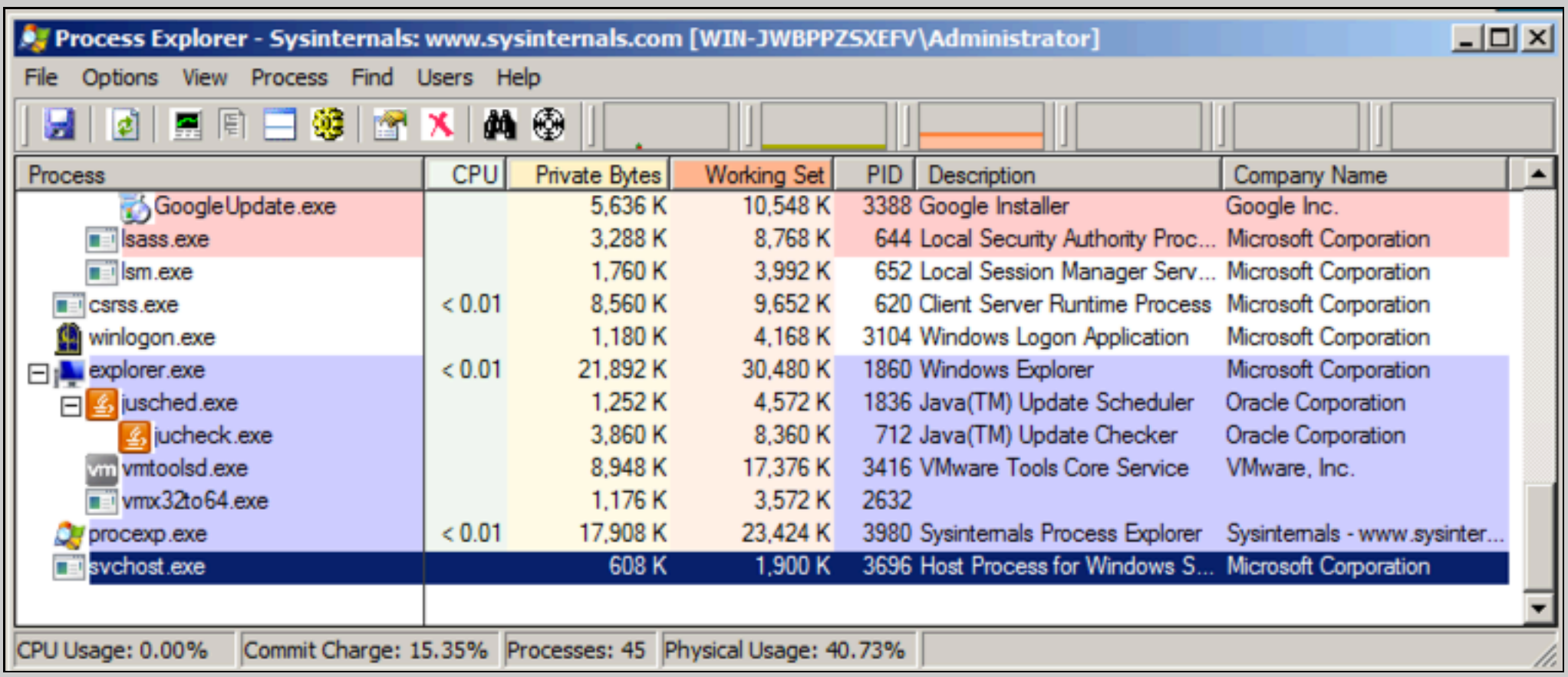
Launch the Malware

Double-click **Lab03-03.exe** and watch what happens in Process Explorer. First two new processes appear, shown in green below: **Lab03-03.exe** and **svchost.exe**.



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

This is highly unusual and suspicious behavior.



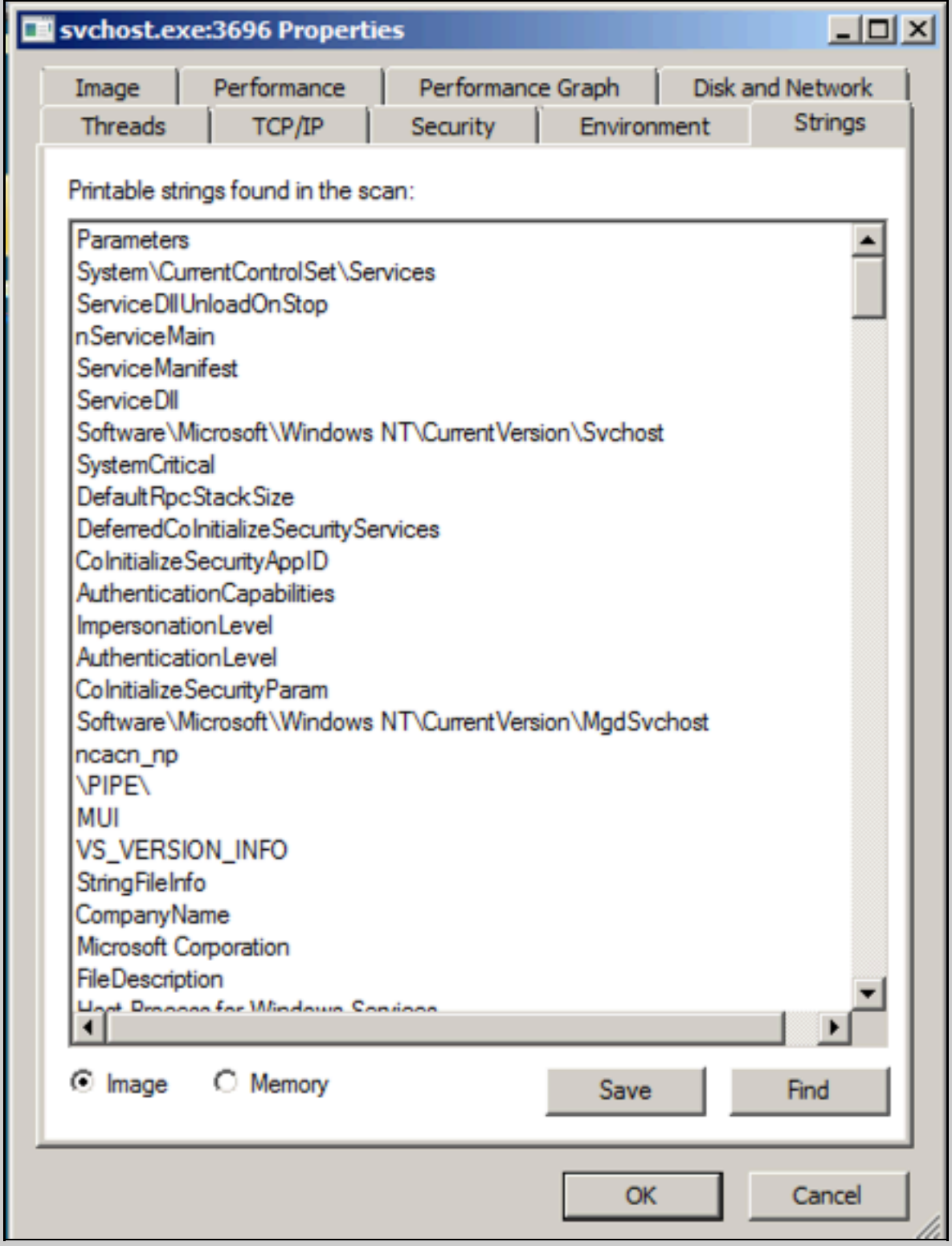
Observing Process Replacement

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**.

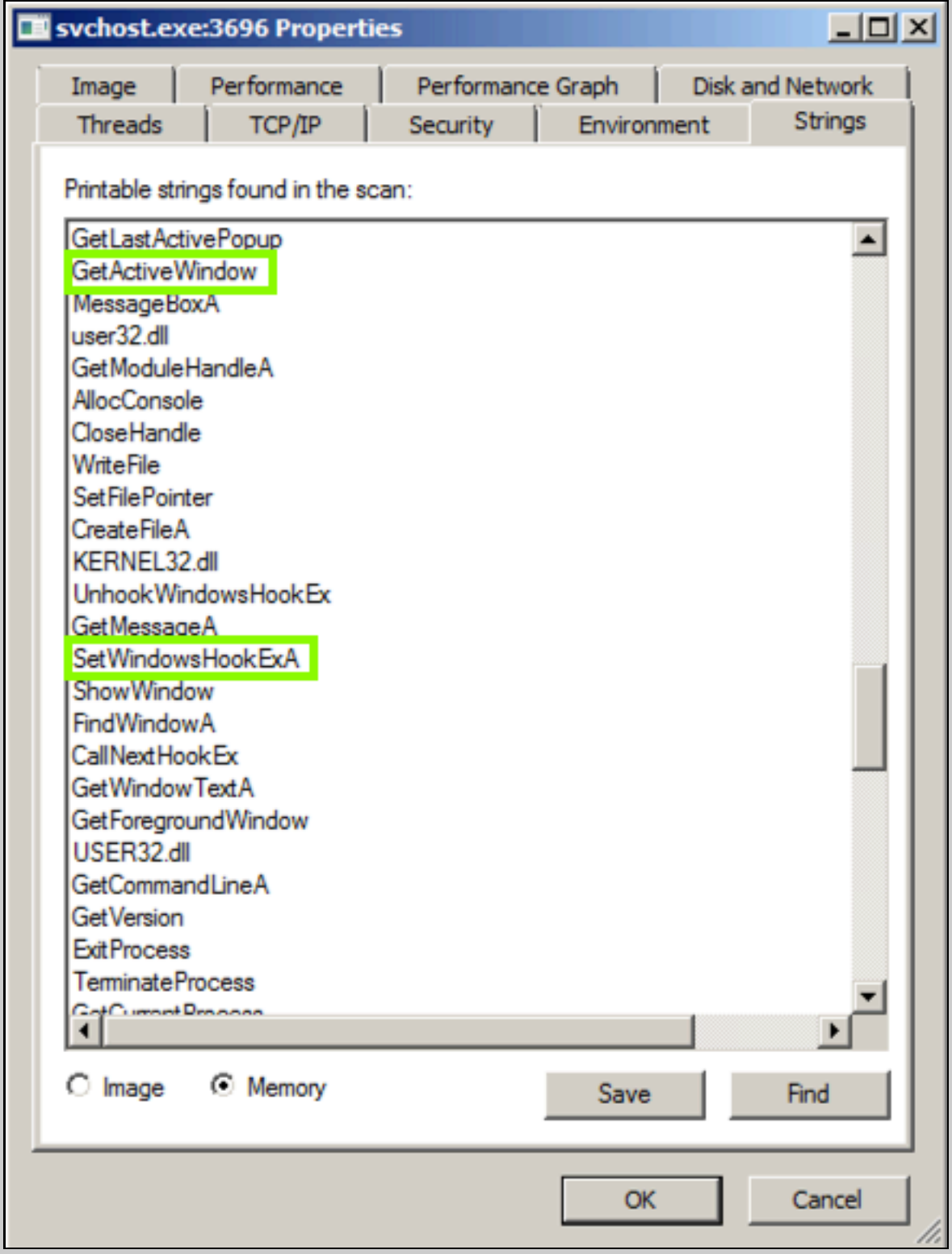
Click the **Strings** tab. At the bottom, make sure **Image** is selected, as shown below.

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

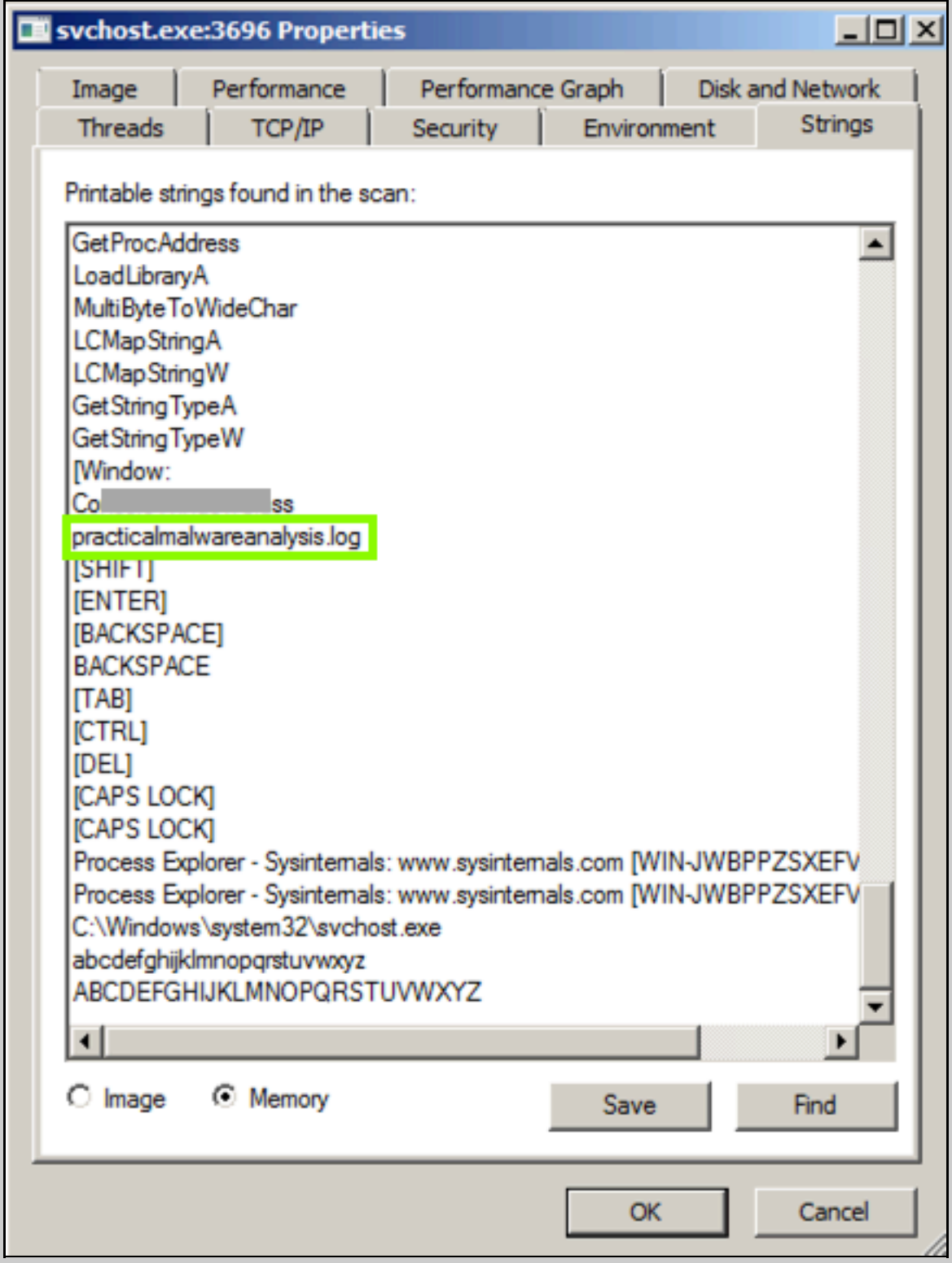


At the bottom of the box, click the **Memory** button. Now the strings are completely different, and contain these suspicious items: **GetActiveWindow** and **SetWindowsHookExA**.

Those functions can be used by a keylogger, to hook the keypresses and run added code to record them.



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



Just above "practicalmalwareanalysis.log" there is another string, beginning with "Co", partially covered by a gray box in the image above.

Enter that string into the form below.

5.1: Recording Your Success (15 pts.)

Use the form below to record your score in Canvas.

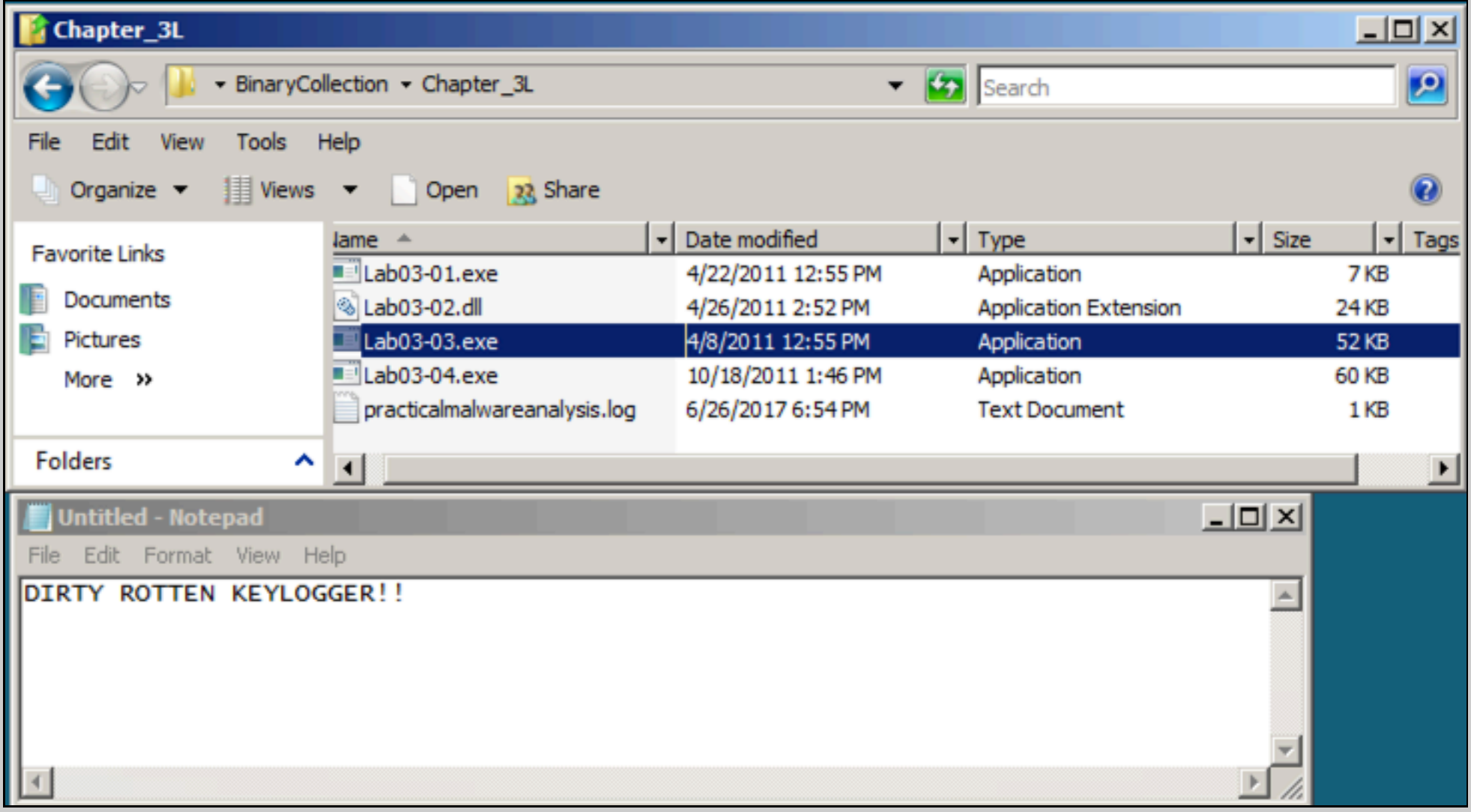
Name or Email:

String:

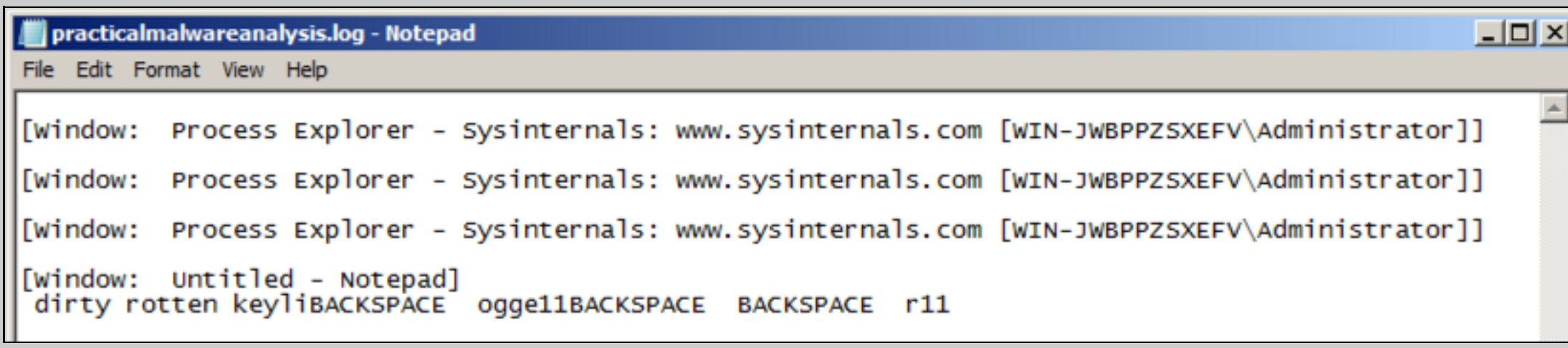
SUBMIT

Testing the Keylogger

Open Notepad and type in some text. A file appears in the Chapter_3L folder named **practicalmalwareanalysis.log**, as shown below.

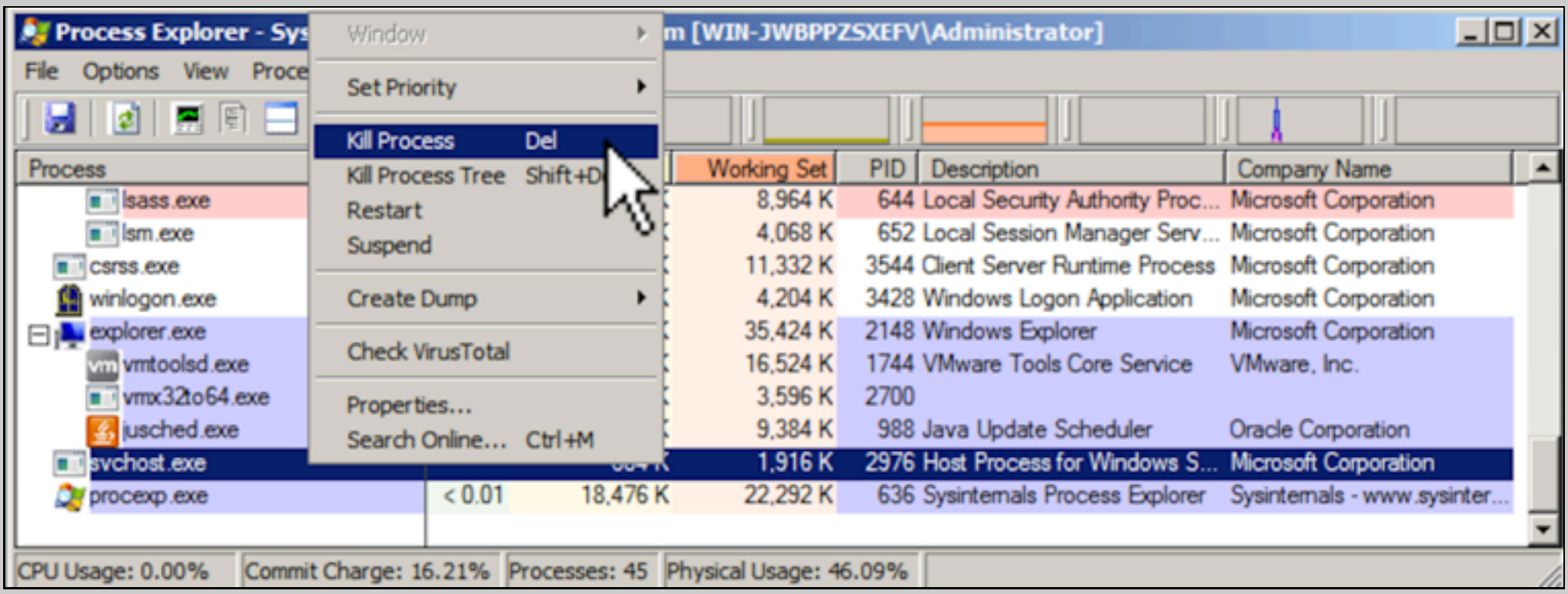


Double-click the **practicalmalwareanalysis.log** file. The stolen keystrokes appear, as shown below.



Killing the Keylogger Process

In Process Explorer, below "explorer.exe", find the **svchost.exe** process. Right-click it, as shown below, and click "**Kill Process**".



Challenge 5.2: Find the Logfile (15 pts extra)

In your Documents folder, find the file **chal6.exe**

If you aren't using the VM your instructor provided, download the file here.

This file is a keylogger. Find the file containing the captured keystrokes.

5.2: Recording Your Success (15 pts extra)

Use the form below to record your score in Canvas.

Posted 8-28-18