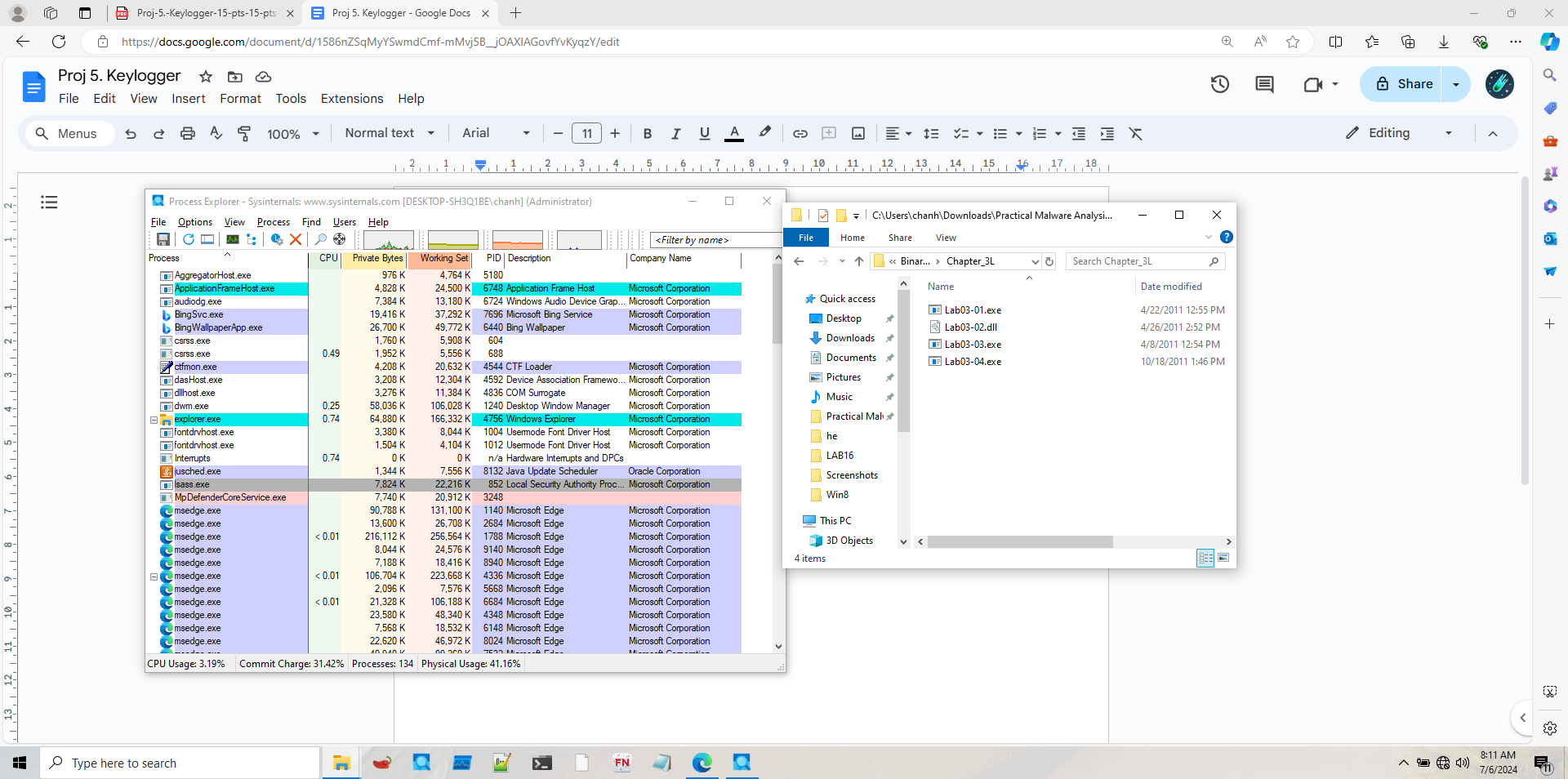
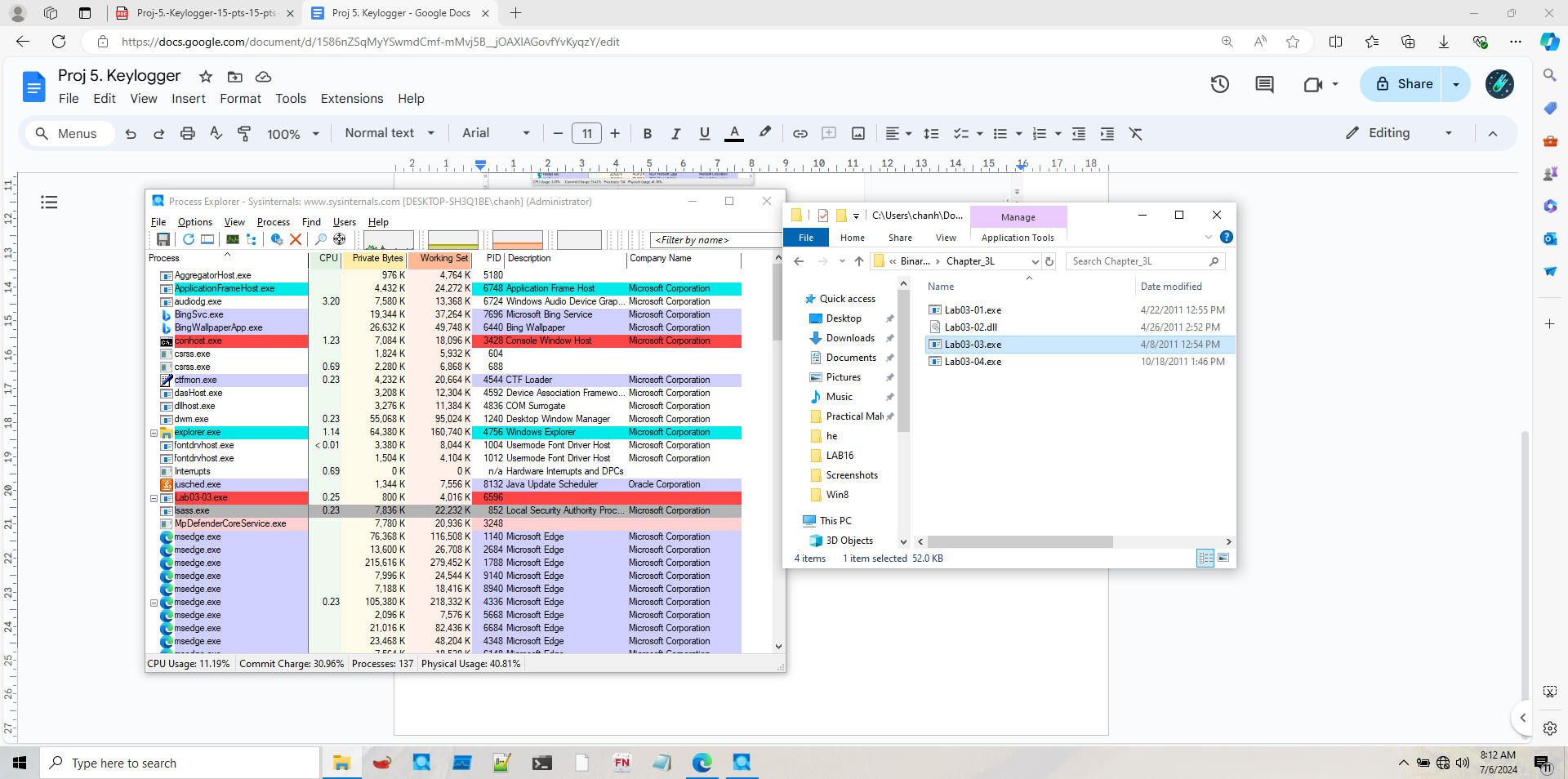
Preparing Windows On your desktop, open the "Practical Malware Analysys Labs" folder.

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

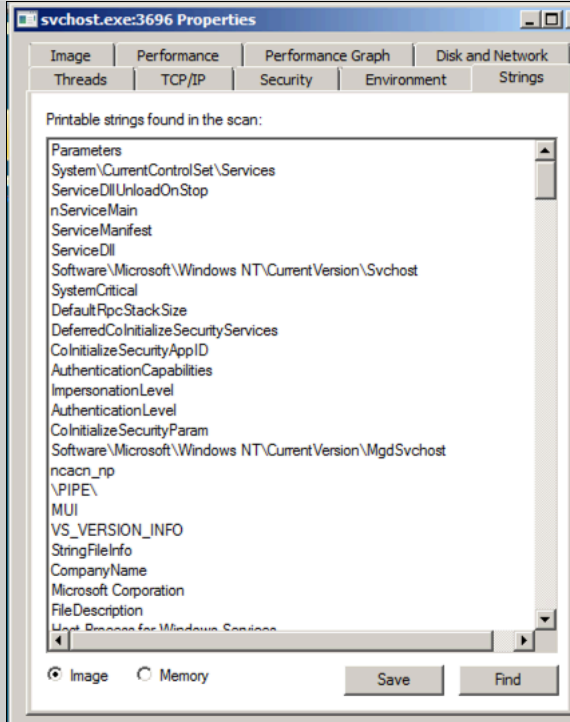


Launch the Malware Double-click Lab03-03.exe and watch what happens in Process Explorer. First two new processes appear, shown in green below: Lab03-03.exe and svchost.exe.

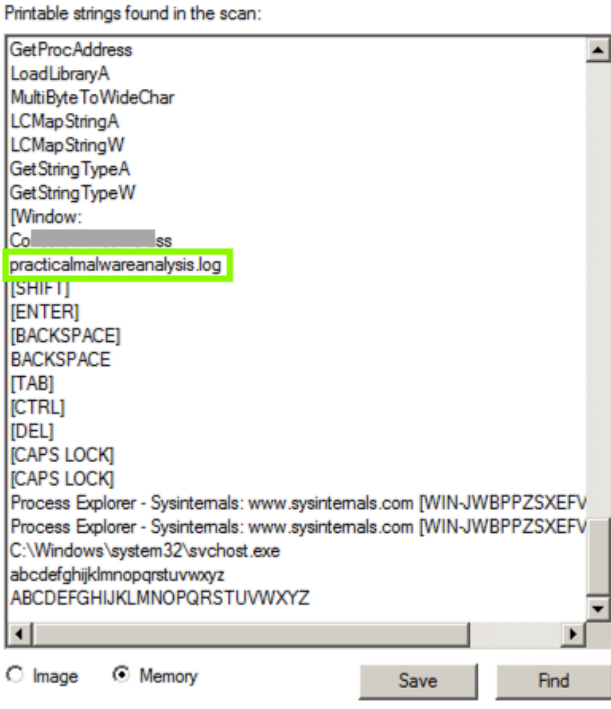


After a second or two, the Lab03-03.exe process terminates, leaving the svchost.exe running as an orphan process, as shown below. This is highly unusual and suspicious behavior

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



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

