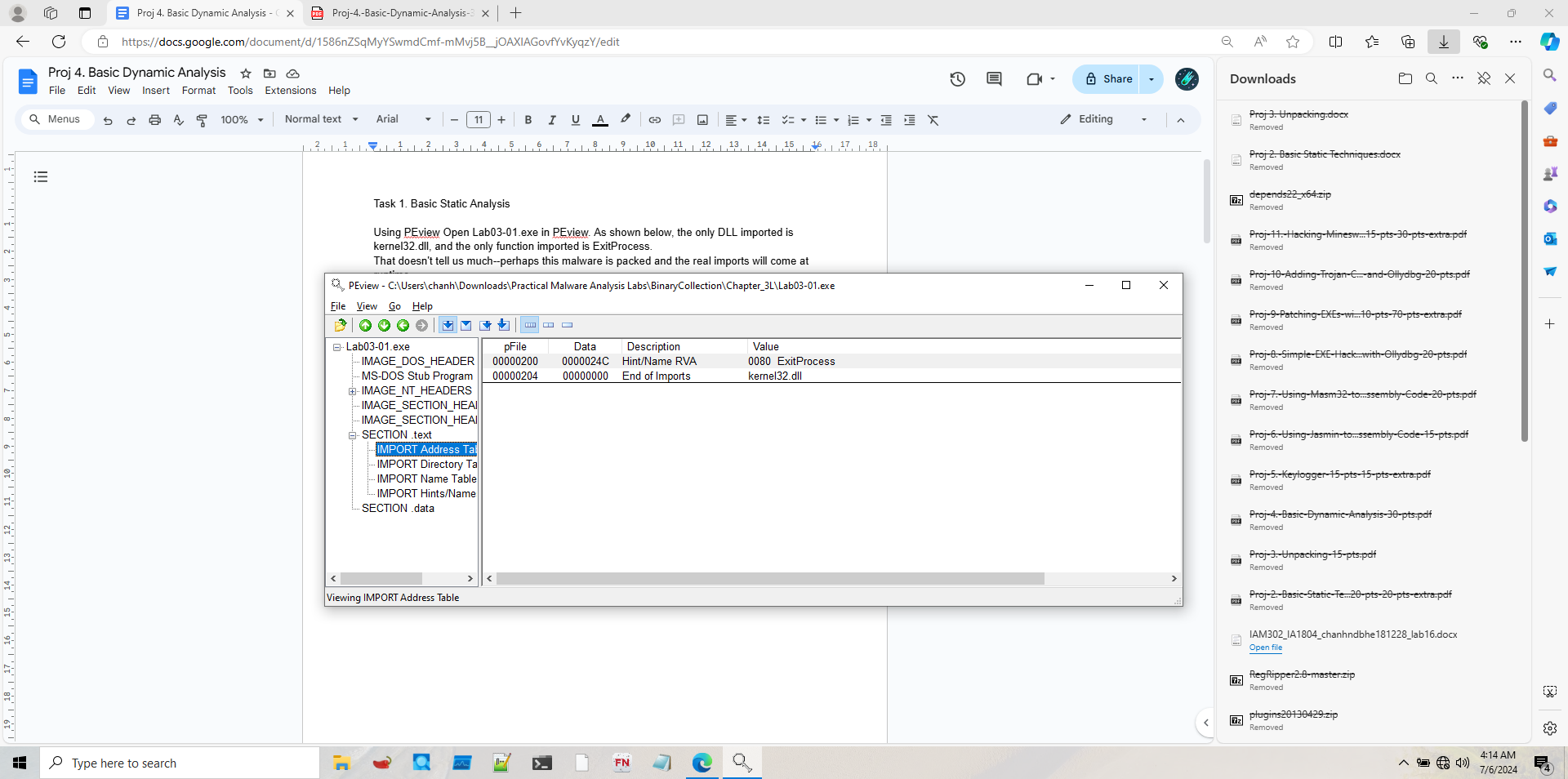
Task 1. Basic Static Analysis

Using PEview Open Lab03-01.exe in PEview. As shown below, the only DLL imported is kernel32.dll, and the only function imported is ExitProcess.

That doesn't tell us much--perhaps this malware is packed and the real imports will come at runtime

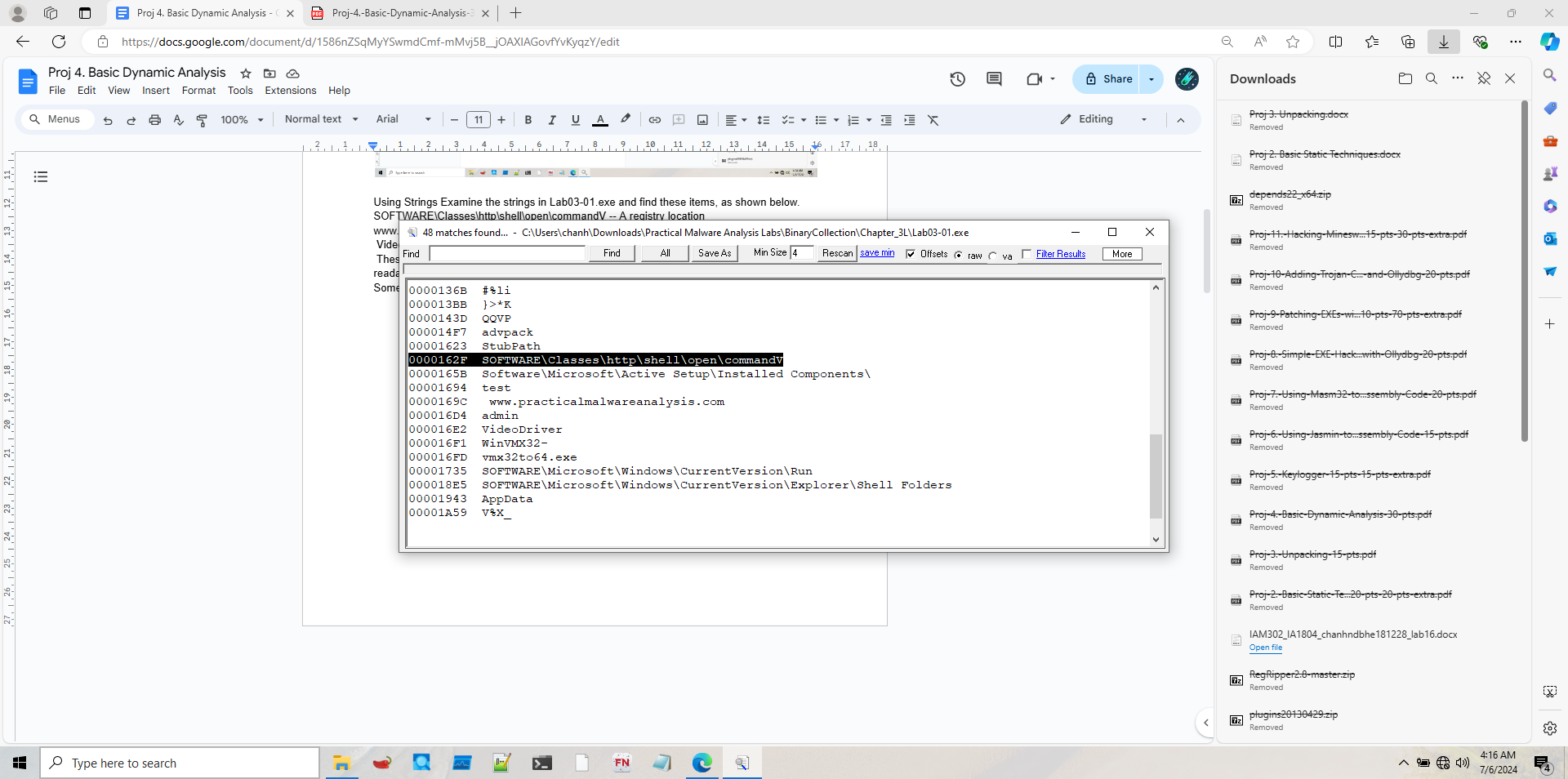


Using Strings Examine the strings in Lab03-01.exe and find these items, as shown below. SOFTWARE\Classes\http\shell\open\commandV -- A registry location www.practicalmalwareanalysis.com -- a URL

VideoDriver

These readable strings are surprising--if the malware were packed, the strings would not be readable.

Something strange is going on, and the easiest way to learn more is dynamic analysis



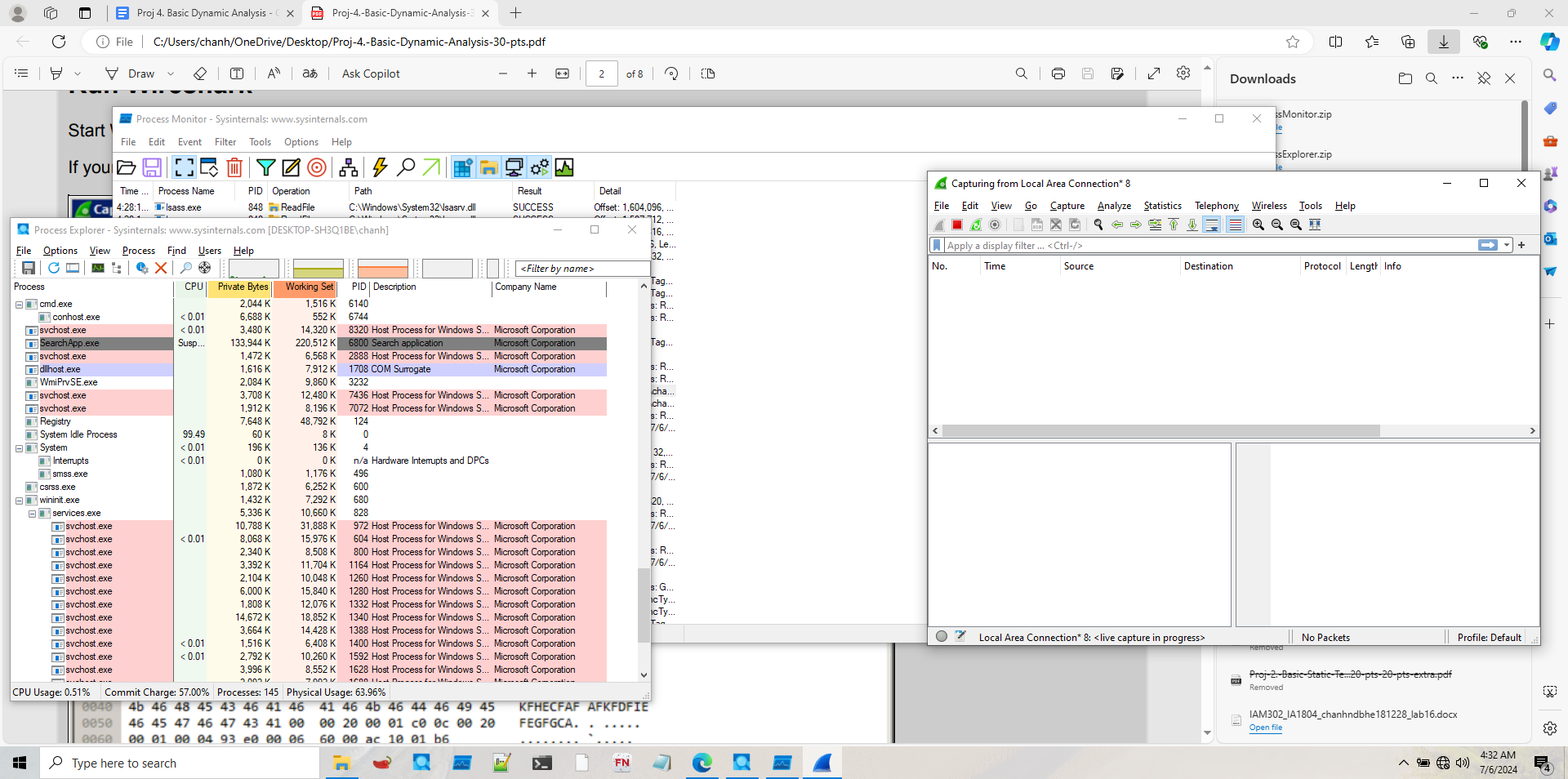
Task 2. Preparing for Dynamic Analysis

Dynamic analysis is simple: run monitoring tools, then run the malware, and let it have its way with our virtual machine. This is a sloppy technique, trusting a system that is being infected, but it usually works. We will use these three programs to see what the malware does:

1. Process Explorer

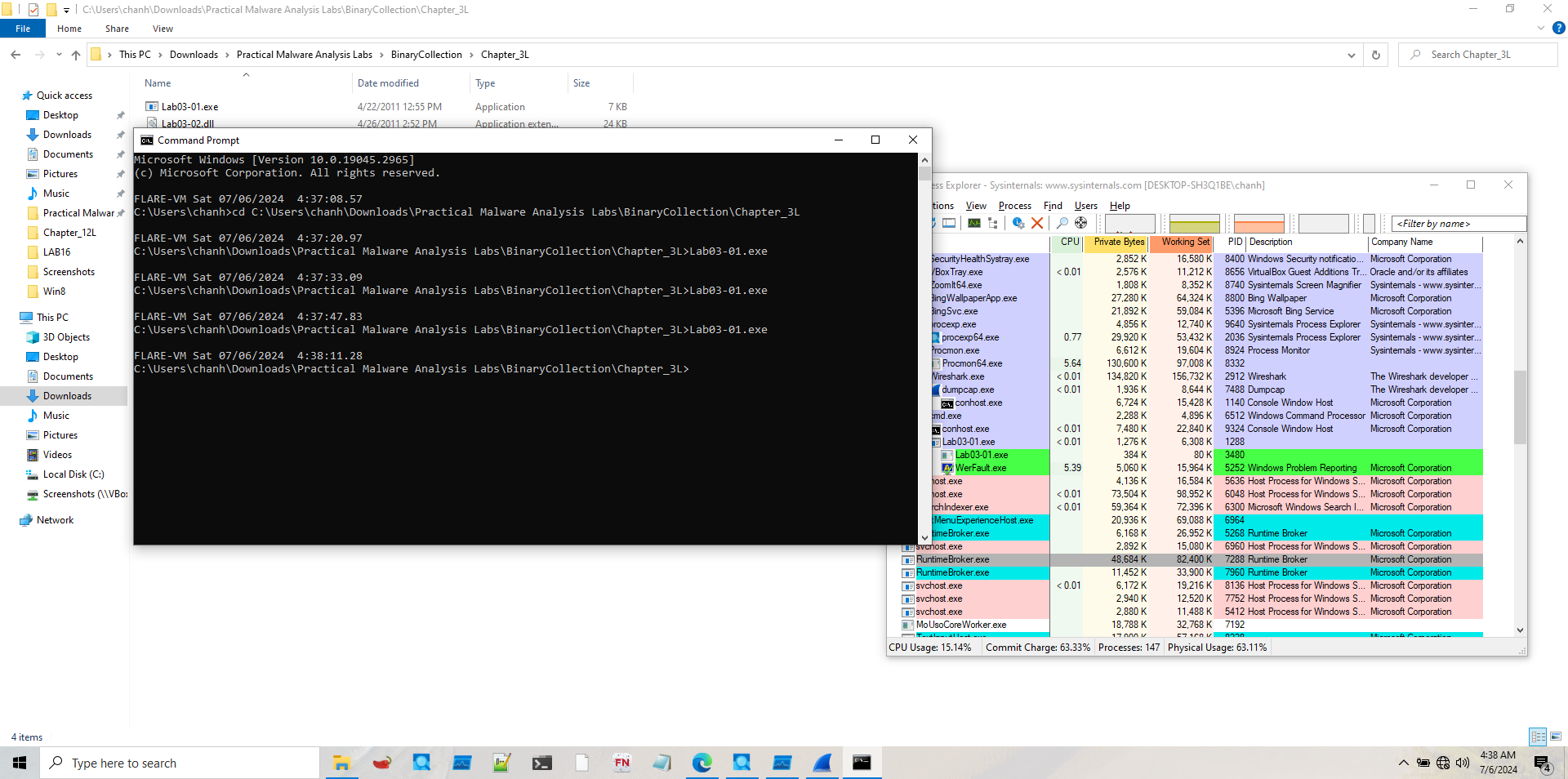
2. Wireshark

3. Process Monitor



Run the Lab03-01.exe File

Viewing the Running Malware in Process Explorer



Viewing the Malicious Process's Events in Process Monitor In Process Monitor, click the magnifying glass icon on the toolbar to stop capturing events. In Process Monitor, click Filter, Filter. Enter a Filter for "Process Name" is Lab03-01.exe, Include, as shown below. Click Add to add the filter

Add two more filters:

Operation of RegSetValue

Operation of WriteFile

Viewing Beacons in Wireshark In the Windows machine, in Wireshark, click Capture, Stop. At the top left of the Wireshark window, in the Filter bar, type a filter of frame contains malware Press Enter to see the filtered packets, as shown below

