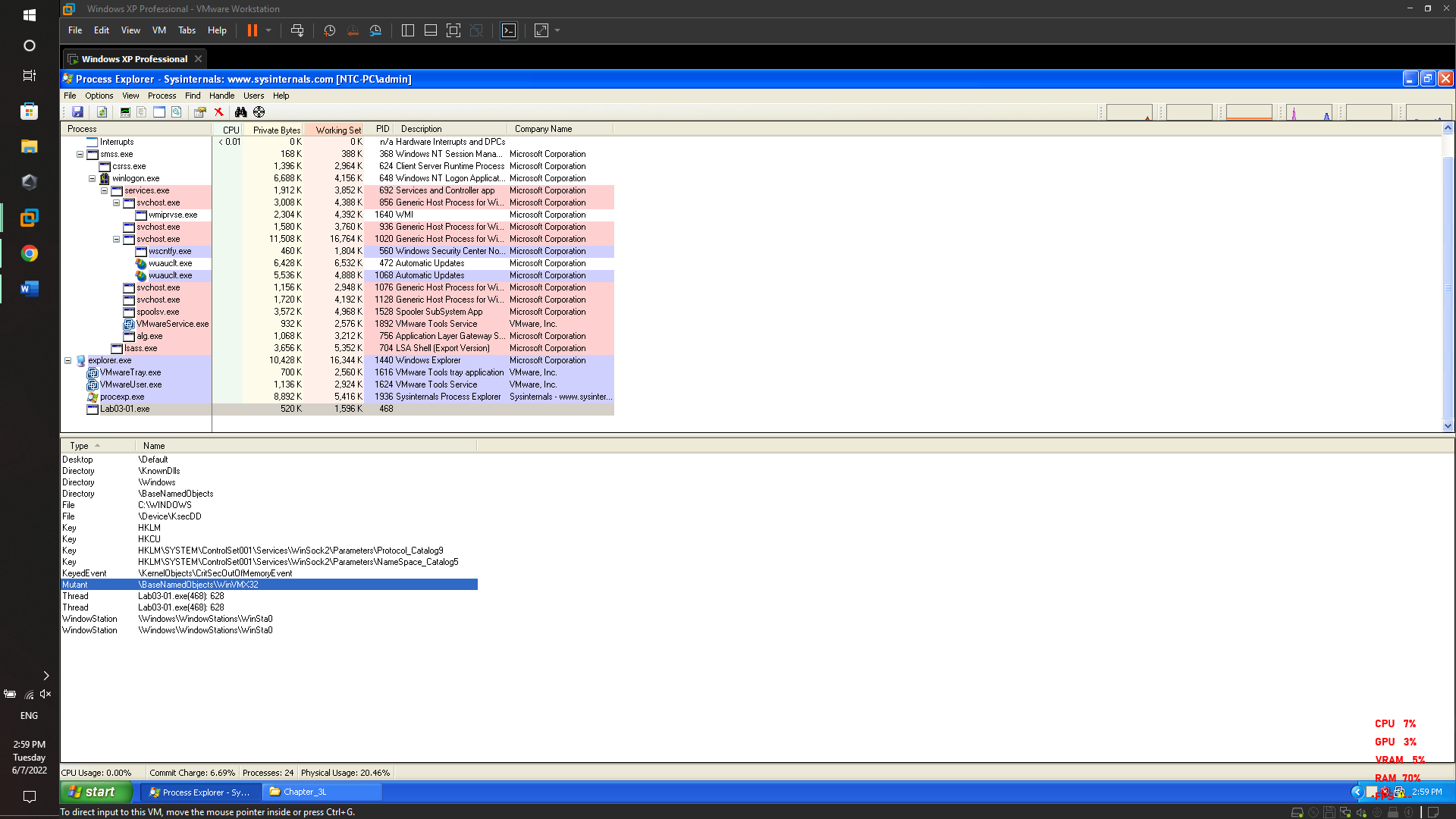
Lab 5

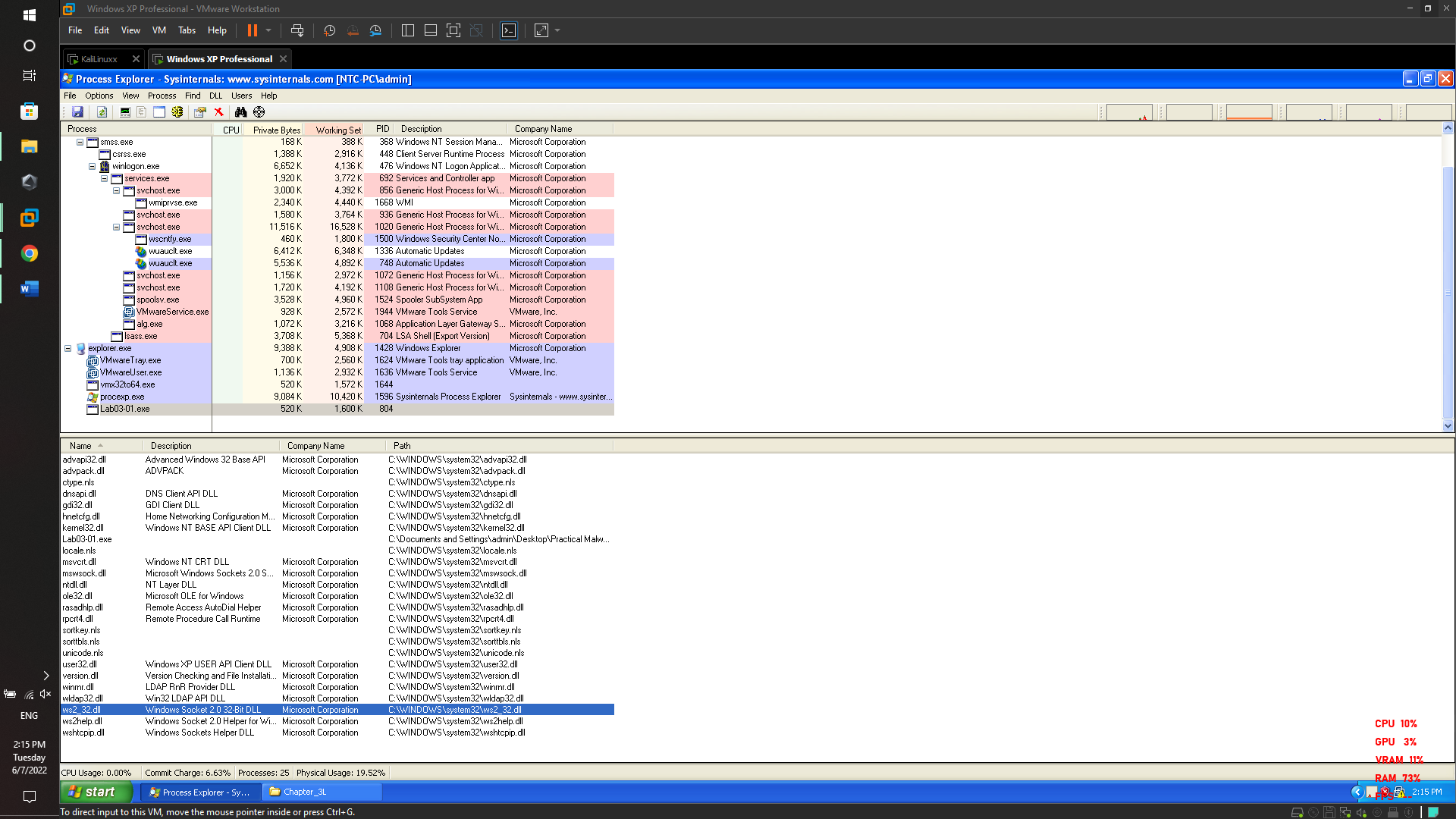
Nguyễn Thanh Hoài Lộc – SE151250

Viewing the Running Malware in Process Explorer

- You see the WinVMX32 mutant, as highlighted below. A mutant, also called a mutex, is used for interprocess connunication.

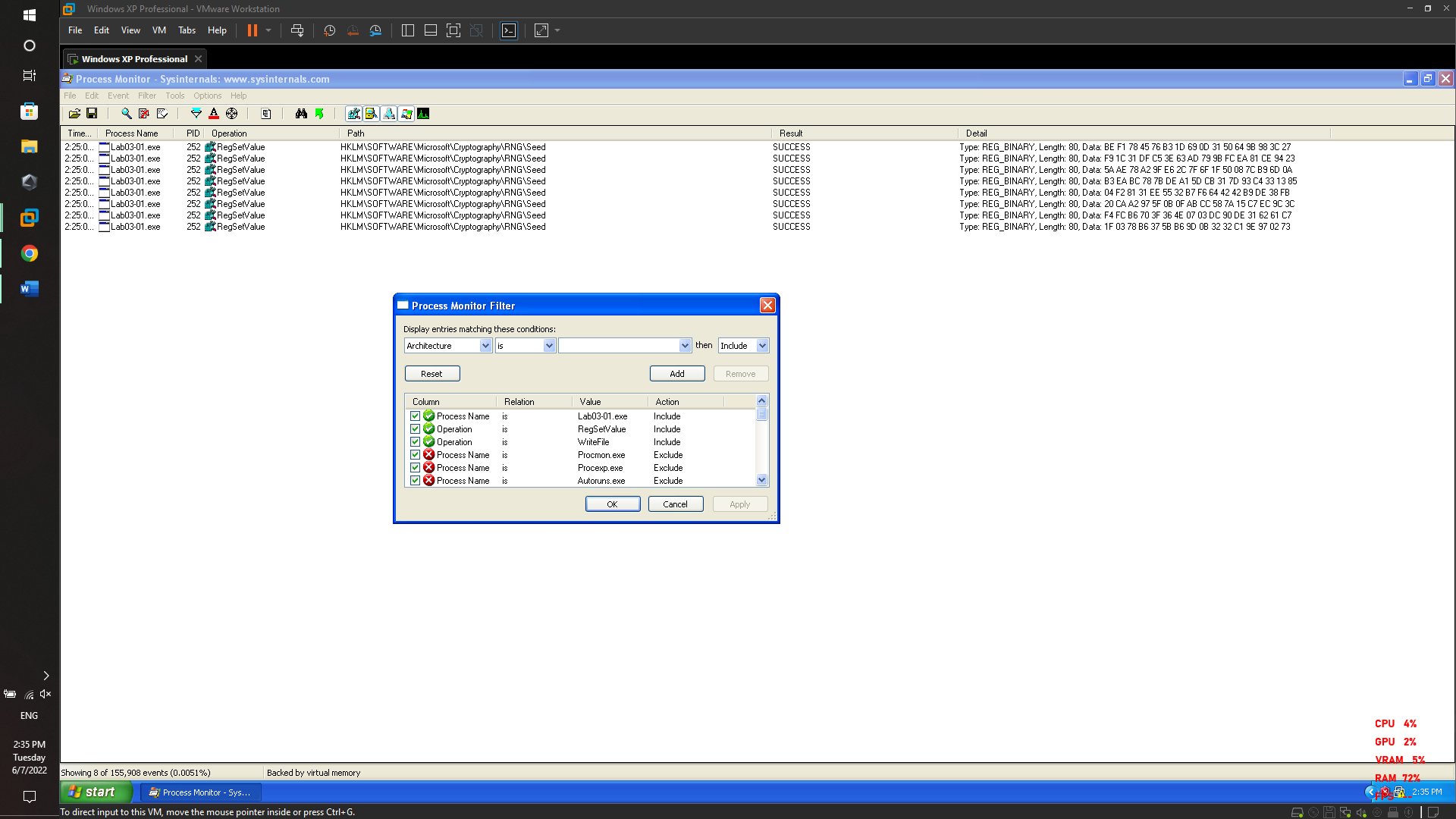
- In Process Explorer, click View, "Lower Pane View", DLLs. Scroll to the bottom to find ws2\_32.dll and wshtcpip.dll, as shown below. This shows that the malware has networking functionality.





Viewing the Malicious Process's Events in Process Monitor

* In Process Monitor, click Filter, Filter. Enter a Filter for "Process Name" is Lab03-01.exe



Regshot

Regshot before run brbbot.exe and after run brbbot.exe to compare it

