**Class Activity - Identify Running Processes**

Part 1: Download Windows Sysinternals Suite.

Part 2: Start TCP/UDP Endpoint Viewer.

Part 3: Explore the running processes.

a. TCPView lists the process that are currently on your Windows PC. At this time, only Windows processes are running.

b. Double-click lsass.exe. Question: What is lsass.exe? In what folder is it located?

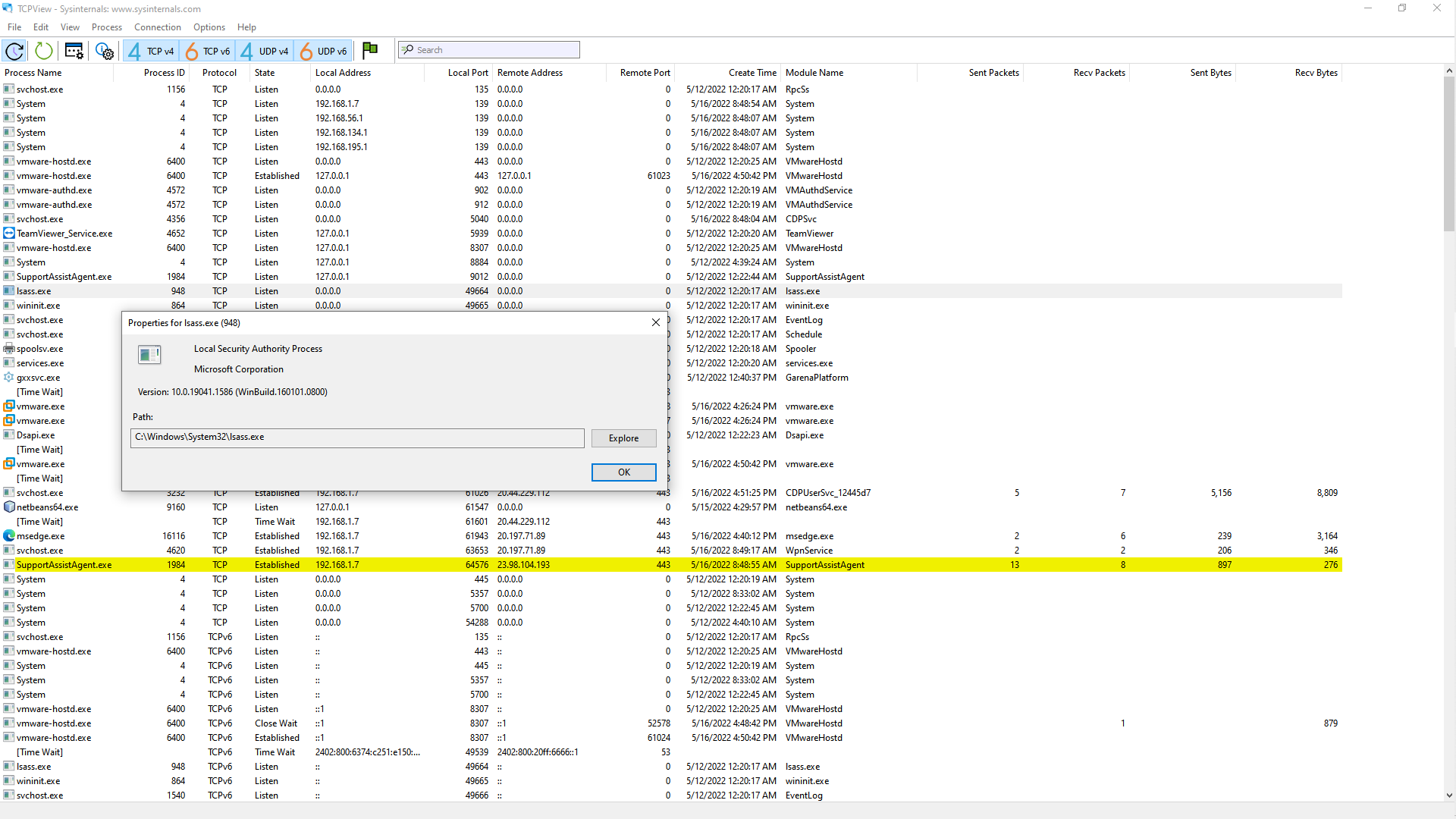
Answer:

- Local Security Authority Process is the name for lsass.exe.

- It is located in C:\Windows\System32\lsass.exe

c. Close the properties window for lsass.exe when done.

Answer:

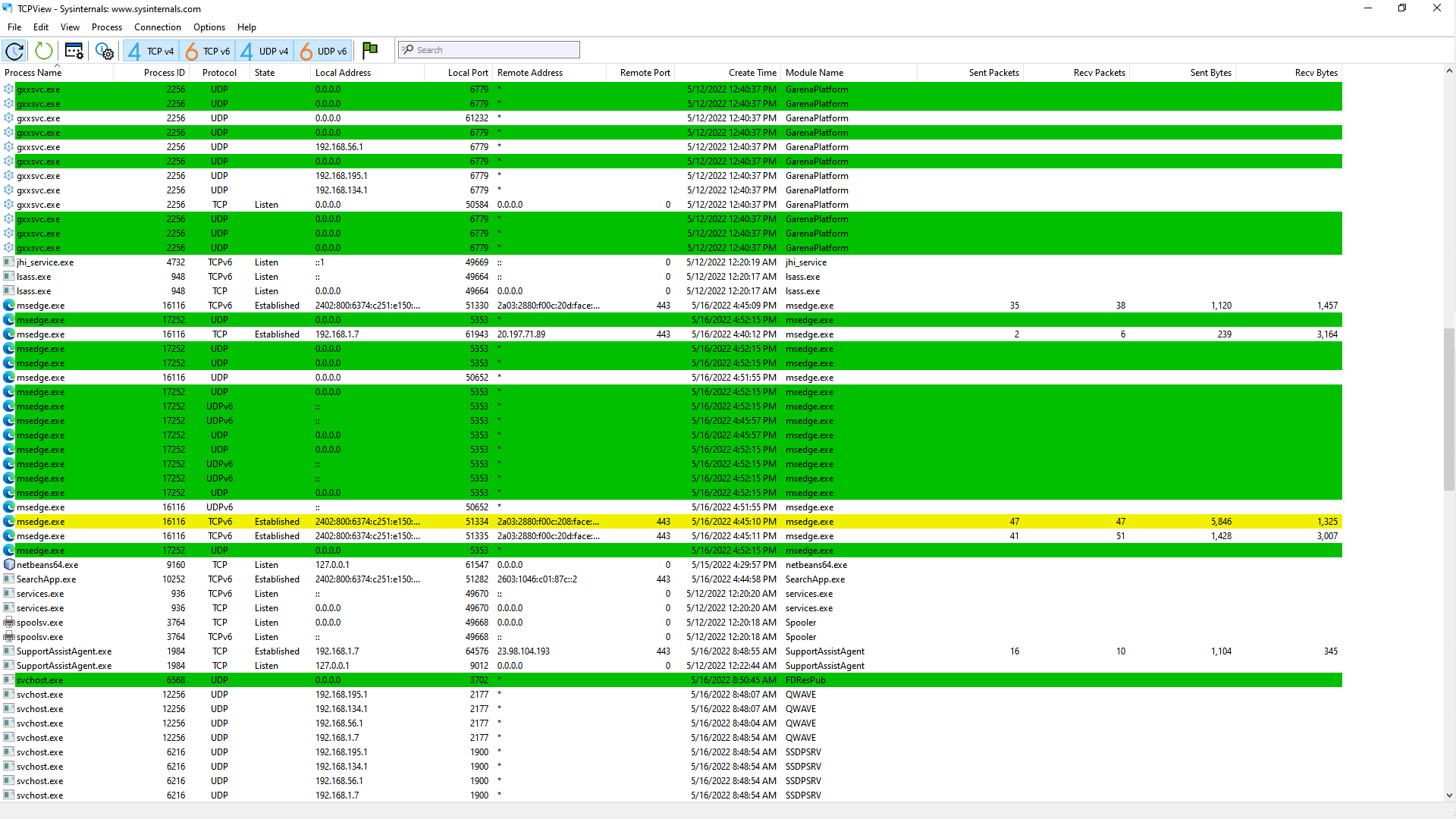


d. View the properties for the other running processes.

Part 4: Explore a user-started process.

a. Open a web browser, such as Microsoft Edge. What did you observe in the TCPView window?

Answer:

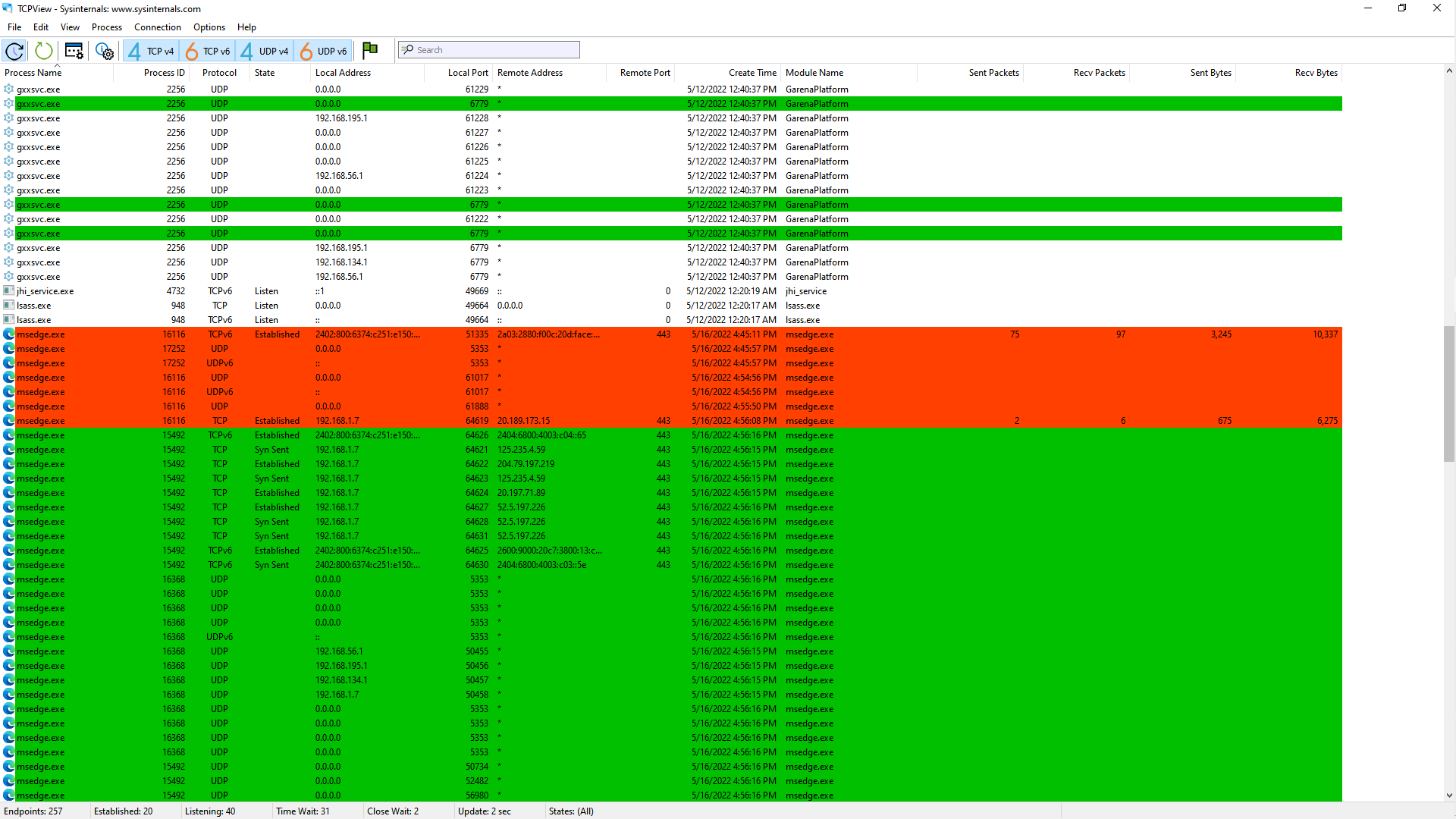


- The processes for the web browser are added to the TCPView window and they are painted green.

b. Close the web browser. Question: What did you observe in the TCPView window?

Answer:

- The processes for the web browser will be removed from the TCPView window and they are painted red.



c. Reopen the web browser. Research some of the processes listed in TCPView. Record your findings.

Answer:

https://drive.google.com/file/d/10Phz109qw2gAGUBDGQnAEASwn7XIEuB5/view?usp=sharing