

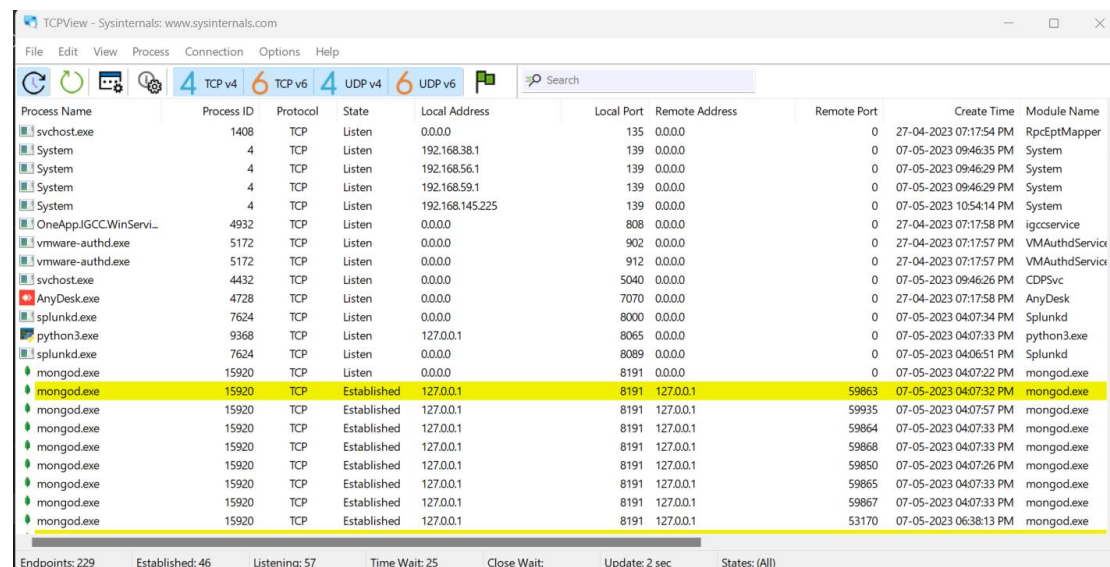
Class Activity - Identify Running Processes Objectives

In this lab, you will use TCP/UDP Endpoint Viewer, a tool in Sysinternals Suite, to identify any running processes on your computer.

Part 1: Download Windows Sysinternals Suite.

Part 2: Start TCP/UDP Endpoint Viewer.

Open Tcpview.exe. Accept the Process Explorer License Agreement when prompted. Click Yes to allow this app to make changes to your device



The screenshot shows the TCPView application window. The menu bar includes File, Edit, View, Process, Connection, Options, and Help. The toolbar has icons for refreshing, pausing, and filtering. The main table displays the following data:

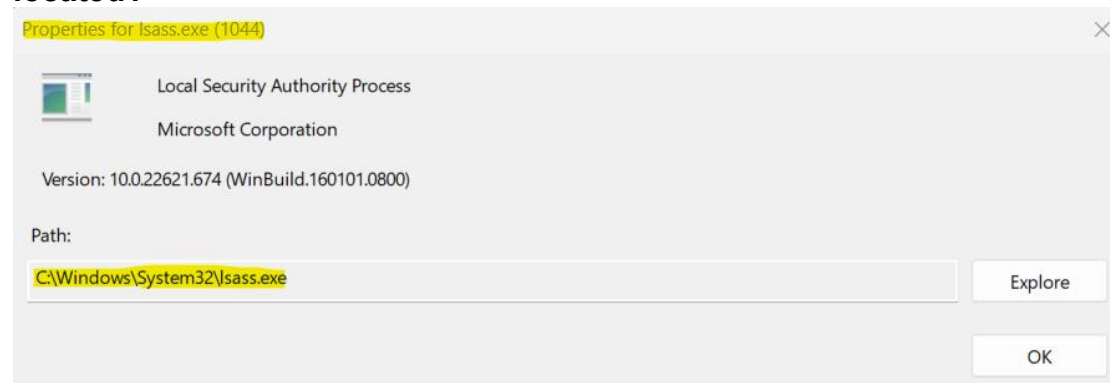
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1408	TCP	Listen	0.0.0.0	135	0.0.0.0	0	27-04-2023 07:17:54 PM	RpcEptMapper
System	4	TCP	Listen	192.168.38.1	139	0.0.0.0	0	07-05-2023 09:46:35 PM	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	07-05-2023 09:46:29 PM	System
System	4	TCP	Listen	192.168.59.1	139	0.0.0.0	0	07-05-2023 09:46:29 PM	System
System	4	TCP	Listen	192.168.145.225	139	0.0.0.0	0	07-05-2023 10:54:14 PM	System
OneApp.IGCC.WinServi...	4932	TCP	Listen	0.0.0.0	808	0.0.0.0	0	27-04-2023 07:17:58 PM	igccservice
vmware-authd.exe	5172	TCP	Listen	0.0.0.0	902	0.0.0.0	0	27-04-2023 07:17:57 PM	VMAuthService
vmware-authd.exe	5172	TCP	Listen	0.0.0.0	912	0.0.0.0	0	27-04-2023 07:17:57 PM	VMAuthService
svchost.exe	4432	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	07-05-2023 09:46:26 PM	CDPSvc
AnyDesk.exe	4728	TCP	Listen	0.0.0.0	7070	0.0.0.0	0	27-04-2023 07:17:58 PM	AnyDesk
splunkd.exe	7624	TCP	Listen	0.0.0.0	8000	0.0.0.0	0	07-05-2023 04:07:34 PM	Splunkd
python3.exe	9368	TCP	Listen	127.0.0.1	8065	0.0.0.0	0	07-05-2023 04:07:33 PM	python3.exe
splunkd.exe	7624	TCP	Listen	0.0.0.0	8089	0.0.0.0	0	07-05-2023 04:06:51 PM	Splunkd
mongod.exe	15920	TCP	Listen	0.0.0.0	8191	0.0.0.0	0	07-05-2023 04:07:22 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59863	07-05-2023 04:07:32 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59935	07-05-2023 04:07:57 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59864	07-05-2023 04:07:33 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59868	07-05-2023 04:07:33 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59850	07-05-2023 04:07:26 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59865	07-05-2023 04:07:33 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	59867	07-05-2023 04:07:33 PM	mongod.exe
mongod.exe	15920	TCP	Established	127.0.0.1	8191	127.0.0.1	53170	07-05-2023 06:38:13 PM	mongod.exe

At the bottom, summary statistics are shown: Endpoints: 229, Established: 46, Listening: 57, Time Wait: 25, Close Wait: , Update: 2 sec, States: (All).

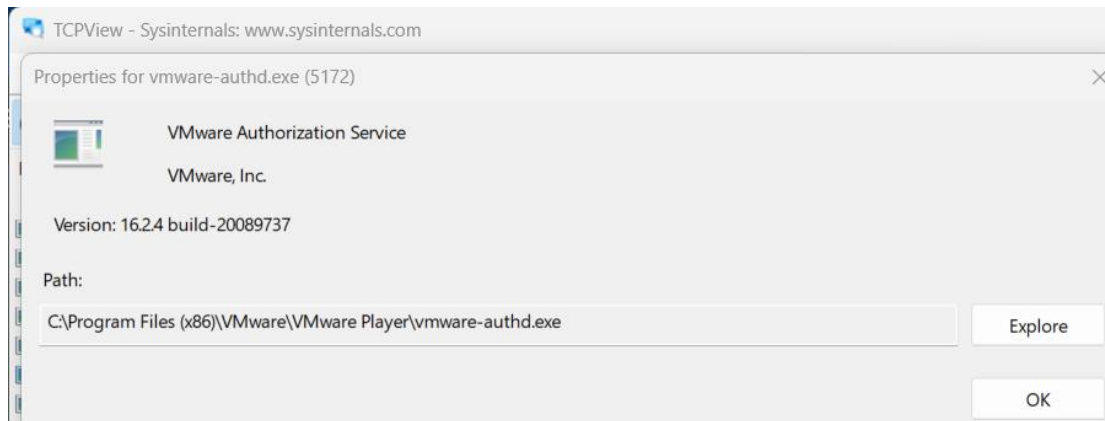
Part 3: Explore the running processes.

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

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



d. View the properties for the other running processes.













Part 4: Explore a user-started process.

a. Open a web browser.

What did you observe in the TCPView window?

Process	Local Address	Local Port	Remote Address	Remote Port	State	Time	Process
chrome.exe	27028	UDP	0.0.0.0	5353	*	07-05-2023 09:24:34 AM	chrome.exe
chrome.exe	27028	UDP	0.0.0.0	5353	*	07-05-2023 09:24:34 AM	chrome.exe
chrome.exe	27028	UDP	0.0.0.0	5353	*	07-05-2023 09:24:34 AM	chrome.exe
chrome.exe	1784	UDP	0.0.0.0	5353	*	07-05-2023 10:54:22 PM	chrome.exe
chrome.exe	1784	UDP	0.0.0.0	5353	*	07-05-2023 10:54:22 PM	chrome.exe
chrome.exe	1784	UDP	0.0.0.0	5353	*	07-05-2023 10:54:22 PM	chrome.exe
chrome.exe	27028	UDP	0.0.0.0	5353	*	07-05-2023 09:24:34 AM	chrome.exe
chrome.exe	1784	UDP	0.0.0.0	5353	*	07-05-2023 10:54:22 PM	chrome.exe

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

	chrome.exe	21212	TCPv6	Established	2409:40f4:100fc8f3:591c5...	49282	2404:6800:4007:81e:2003	443	07-05-2023 11:12:51 PM	chrome.exe
	chrome.exe	21212	UDPv6	:	:	58656	*		07-05-2023 11:13:16 PM	chrome.exe
	chrome.exe	21212	TCPv6	Close Wait	2409:40f4:100fc8f3:591c5...	49328	2600:140f:3f93:b33	443	07-05-2023 11:13:04 PM	chrome.exe
	chrome.exe	21212	TCPv6	Established	2409:40f4:100fc8f3:591c5...	49344	2600:9000:2242:a007:2bfb...	443	07-05-2023 11:13:11 PM	chrome.exe
	chrome.exe	21212	TCPv6	Established	2409:40f4:100fc8f3:591c5...	49315	2600:140f:3f97:1e6f	443	07-05-2023 11:13:00 PM	chrome.exe
	chrome.exe	21212	TCPv6	Established	2409:40f4:100fc8f3:591c5...	49314	2600:9000:2354:1e00:1d4...	443	07-05-2023 11:13:00 PM	chrome.exe
	chrome.exe	21212	TCPv6	Established	2409:40f4:100fc8f3:591c5...	49346	2600:140f:3ca9:11a6	443	07-05-2023 11:13:12 PM	chrome.exe
	chrome.exe	21212	UDPv6	:	:	62006	*		07-05-2023 11:12:52 PM	chrome.exe
	chrome.exe	21212	UDPv6	:	:	50718	*		07-05-2023 11:12:56 PM	chrome.exe
	chrome.exe	21212	UDPv6	:	:	59790	*		07-05-2023 11:12:55 PM	chrome.exe

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

Process	Local Address	Local Port	Remote Address	Remote Port	State	Time	Process
chrome.exe	16676	UDP	0.0.0.0	5353	*	07-05-2023 11:13:52 PM	chrome.exe
chrome.exe	16676	UDP	0.0.0.0	5353	*	07-05-2023 11:13:52 PM	chrome.exe
chrome.exe	16676	UDP	0.0.0.0	5353	*	07-05-2023 11:13:52 PM	chrome.exe
chrome.exe	16676	UDP	0.0.0.0	5353	*	07-05-2023 11:13:52 PM	chrome.exe