Report for Lab2

By : Sneha Shukla

Task 1: To study the concept and purpose of network protocols.

Result: I have studied the concept and purpose of network protocols thoroughly and here's the summary of it .

What is Network Protocol?

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Similar to the way that speaking the same language simplifies communication between two people, network protocols make it possible for devices to interact with each other because of predetermined rules built into devices' software and hardware. Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols.

How do they work?

Network protocols take large-scale processes and break them down into small, specific tasks or functions. This occurs at every level of the network, and each function must cooperate at each level to complete the larger task at hand. The term protocol suite refers to a set of smaller network protocols working in conjunction with each other. Network protocols are typically created according to industry standard by various networking or information technology organizations.

Who uses the Network Protocol?

Network protocols aren't only relevant to certified network specialists or IT professionals. Billions of people use network protocols daily, whether they know it or not.

Every time you use the internet, you leverage network protocols. Though you may not know how network protocols work or how frequently you encounter them, they are necessary for using the internet or digital communications in any capacity.

Task 2: Become familiar with the OSI / ISO Interoperability Reference Model.

Result: I analysed the OSI Model several times and here's the short summary about the same.

The Open Systems Interconnection (OSI) reference model has served as the most basic elements of computer networking since the inception in 1984. The OSI Reference Model is based on a proposal developed by the International Standards Organization (ISO). The original objective of the OSI model was to provide a set of design standards for equipment manufacturers so they could communicate with each other. The OSI model defines a hierarchical architecture that logically partitions the functions required to support system-to-system communication.

The OSI model has seven layers, each of which has a different level of abstraction and performs a well-defined function. The principles that were applied to arrive at the seven layers are as follows:

- A layer should be created where a different level of abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

The layered approach offers several advantages. By separating networking functions into logical smaller pieces, network problems can more easily be solved through a divide-and-conquer methodology. OSI layers also allow extensibility. New protocols and other network services are generally easier to add to a layered architecture. The seven OSI layers are defined as follows:

7. Application: Provides different services to the application

6. Presentation: Converts the information

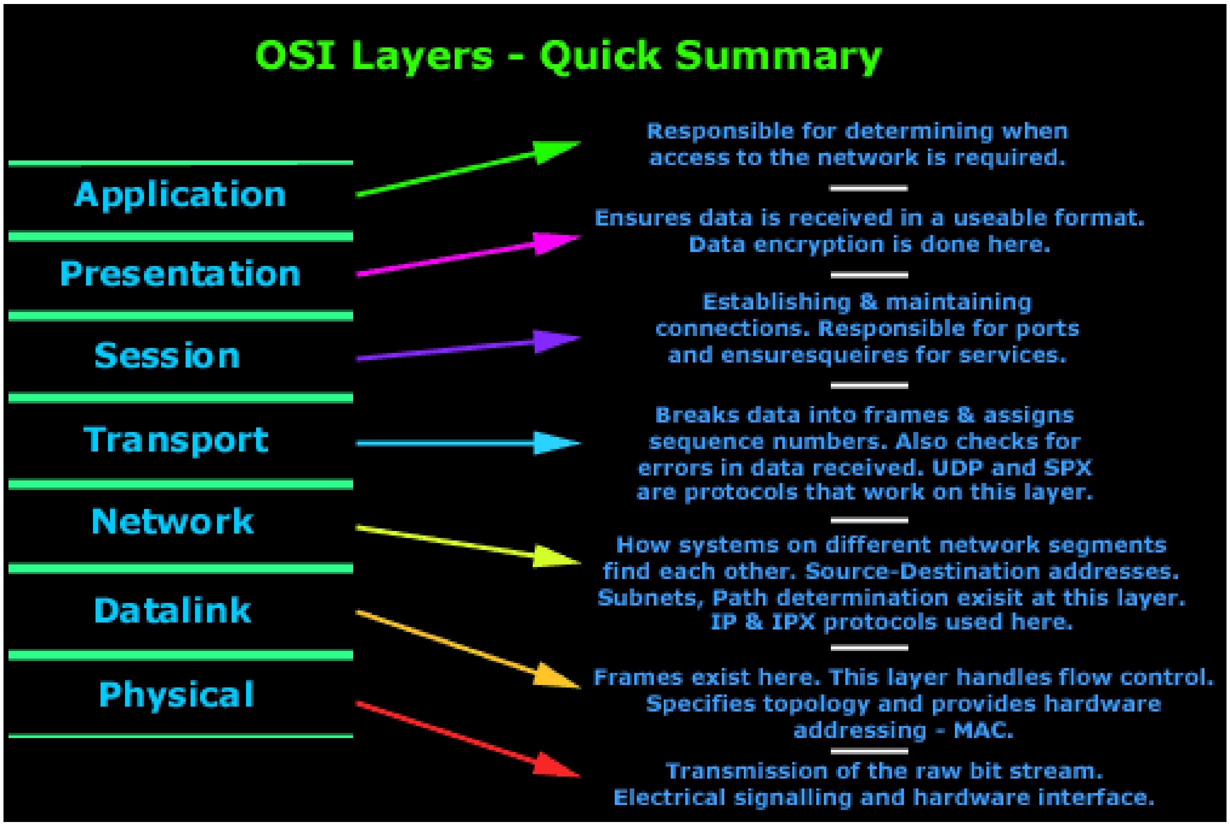
5. Session: Handles problems which are not communication issues

4. Transport: Provides end to end communication control

3. Network: Routes the information in the network

2. Data Link: Provides error control

1. Physical: Connects the entity to the transmission media



OSI Layers - Quick Summary

Application

Presentation

Session

Transport

Network

Datalink

Physical

Responsible for determining when access to the network is required.

Ensures data is received in a useable format. Data encryption is done here.

Establishing & maintaining connections. Responsible for ports and ensuresqueires for services.

Breaks data into frames & assigns sequence numbers. Also checks for errors in data received. UDP and SPX are protocols that work on this layer.

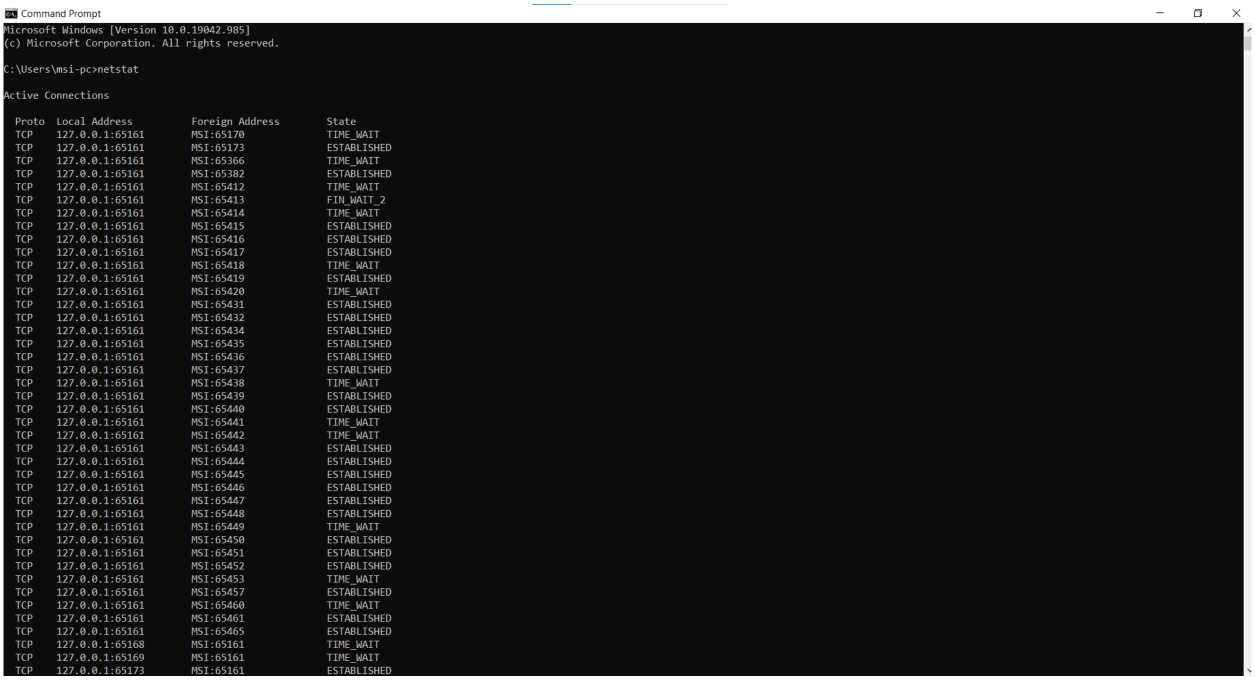
How systems on different network segments find each other. Source-Destination addresses. Subnets, Path determination exisit at this layer. IP & IPX protocols used here.

Frames exist here. This layer handles flow control. Specifies topology and provides hardware addressing - MAC.

Transmission of the raw bit stream. Electrical signalling and hardware interface.

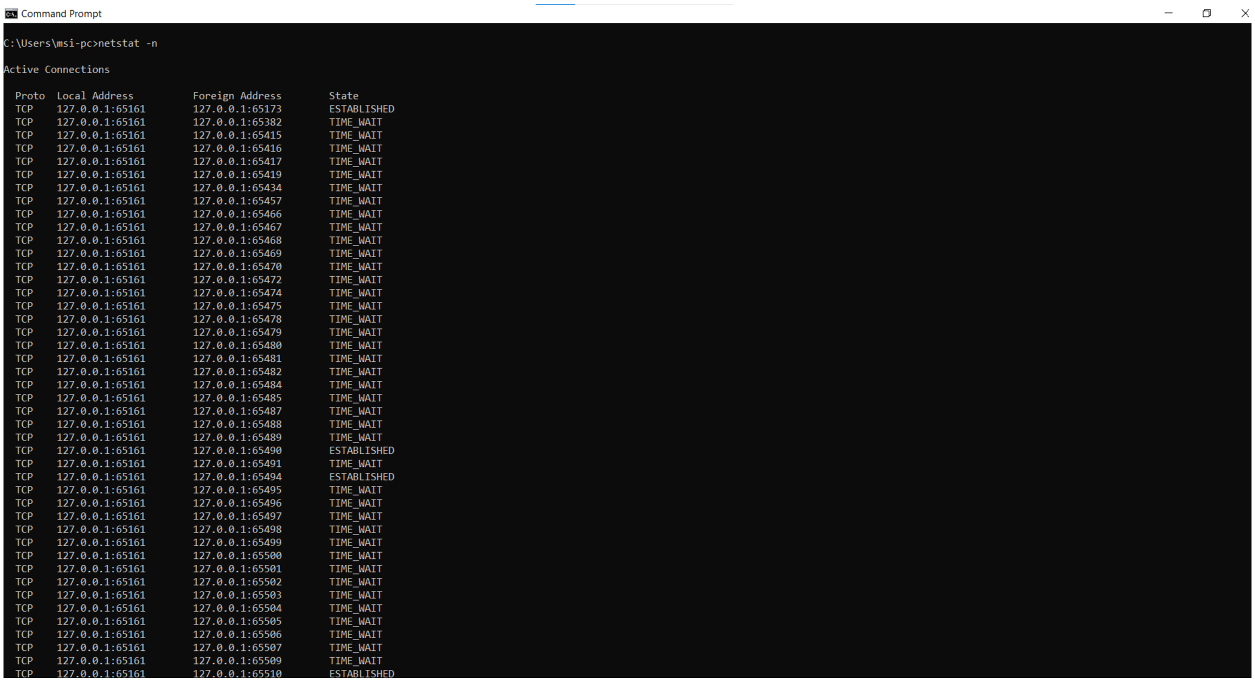
Task 3: Monitor network activity and analyze the operation of network applications using netstat and tcpview. Analyze current network connections on a network machine and get protocol statistics (netstat only).

Result: I analyzed the current network connections on a network machine and also got protocol statistics on netstat. The following figures below are evident to the work done for the given task.



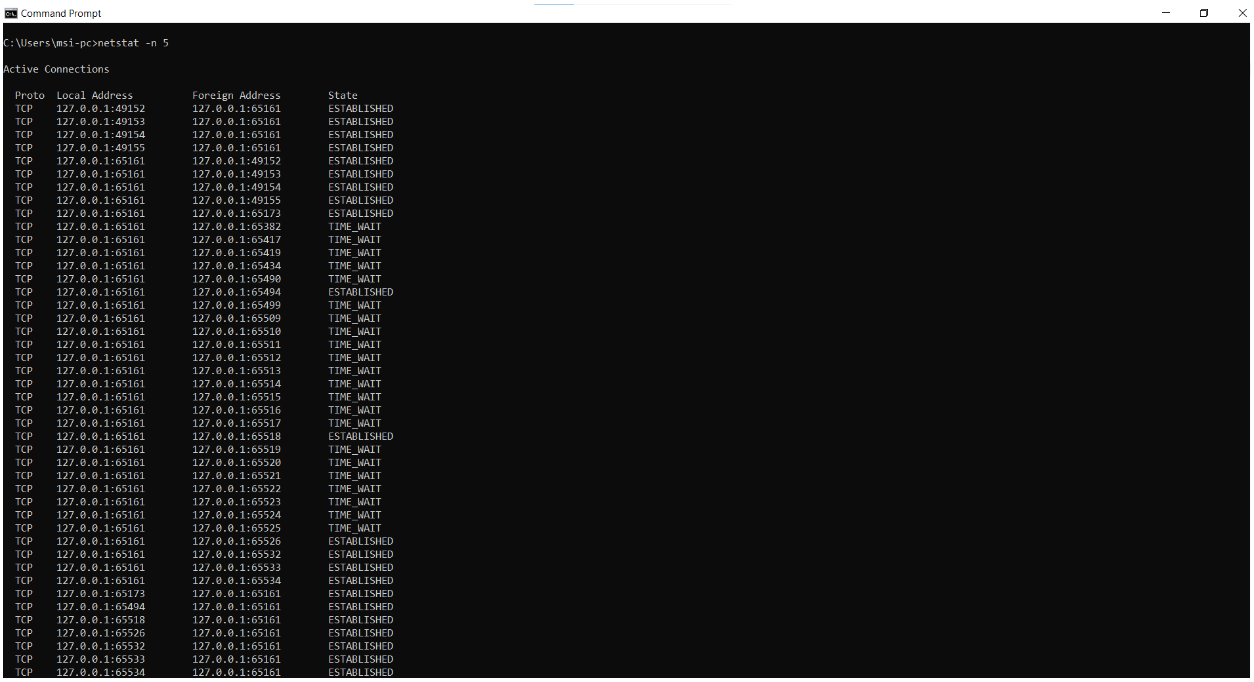
```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\msi-pc>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65161        MSI:65170              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65173              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65366              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65382              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65412              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65413              FIN_WAIT_2
  TCP    127.0.0.1:65161        MSI:65414              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65415              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65416              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65417              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65418              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65419              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65420              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65431              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65432              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65434              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65435              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65436              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65437              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65438              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65439              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65440              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65441              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65442              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65443              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65444              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65445              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65446              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65447              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65448              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65449              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65450              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65451              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65452              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65453              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65457              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65460              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65461              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65465              ESTABLISHED
  TCP    127.0.0.1:65168        MSI:65161              TIME_WAIT
  TCP    127.0.0.1:65169        MSI:65161              TIME_WAIT
  TCP    127.0.0.1:65173        MSI:65161              ESTABLISHED
```

Figure 1: Showing all active TCP connections



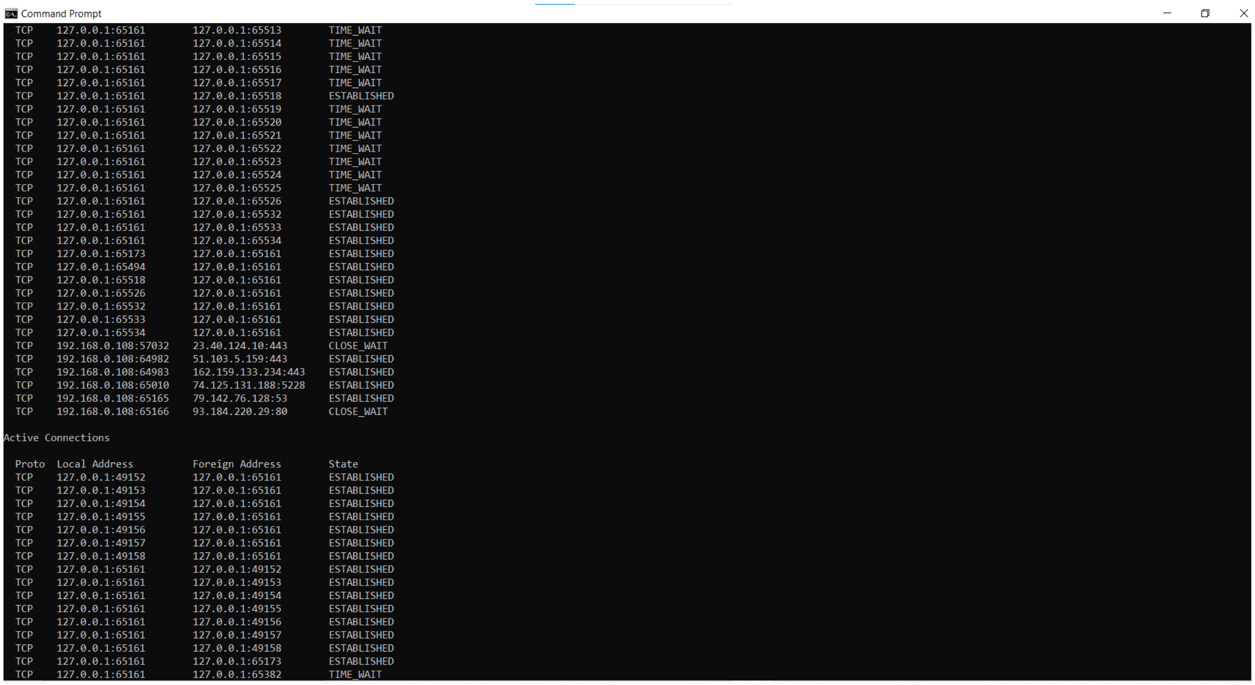
```
C:\Users\msi-pc>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65161        127.0.0.1:65173        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65382        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65415        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65416        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65417        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65419        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65434        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65457        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65466        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65467        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65468        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65469        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65470        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65472        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65474        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65475        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65478        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65479        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65480        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65481        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65482        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65484        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65485        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65487        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65488        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65489        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65490        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65491        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65494        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65495        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65496        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65497        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65498        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65499        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65500        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65501        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65502        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65503        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65504        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65505        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65506        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65507        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65509        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65510        ESTABLISHED
```

Figure 2: Displaying active connections showing numeric IP address and port number instead of trying to determine the names



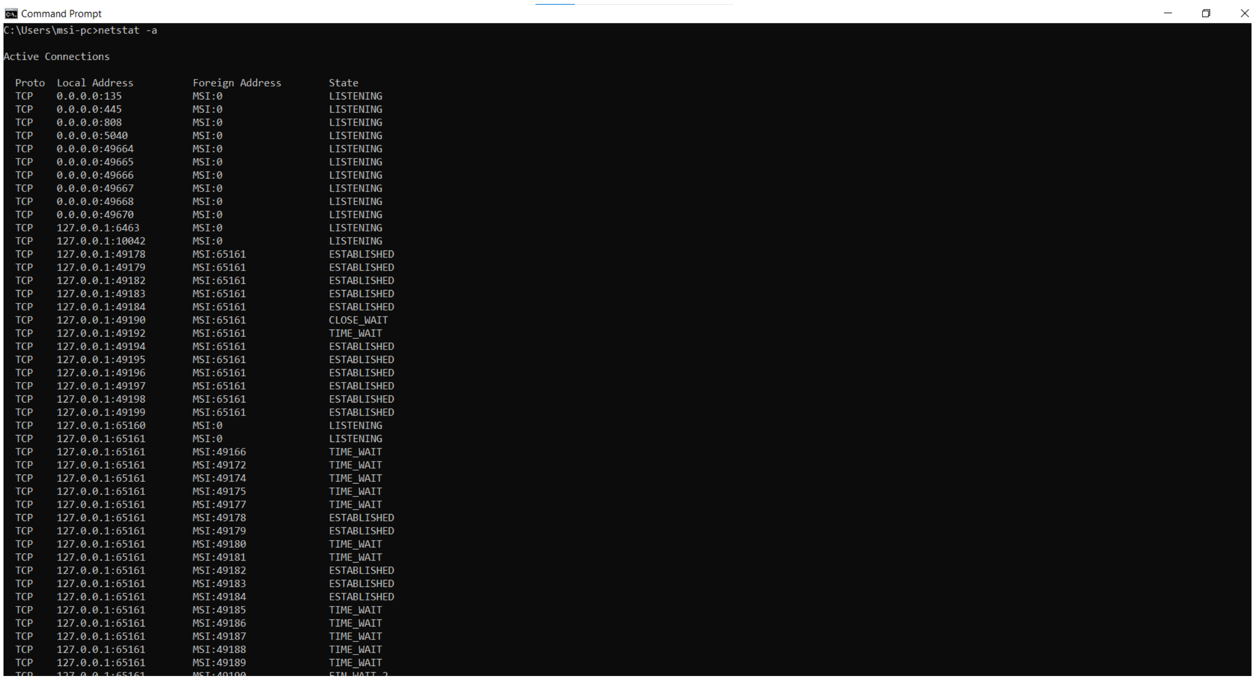
```
C:\Users\msi-pc>netstat -n 5

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49152        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49153        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49154        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49155        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49152        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49153        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49154        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49155        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65173        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65382        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65417        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65419        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65434        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65490        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65494        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65499        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65509        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65510        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65511        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65512        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65513        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65514        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65515        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65516        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65517        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65518        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65519        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65520        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65521        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65522        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65523        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65524        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65525        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65526        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65532        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65533        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65534        ESTABLISHED
  TCP    127.0.0.1:65173        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65494        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65518        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65526        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65532        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65533        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65534        127.0.0.1:65161        ESTABLISHED
```

Figure 3.1: Refresh the information at a specific interval. This example refreshes the command in question every five seconds



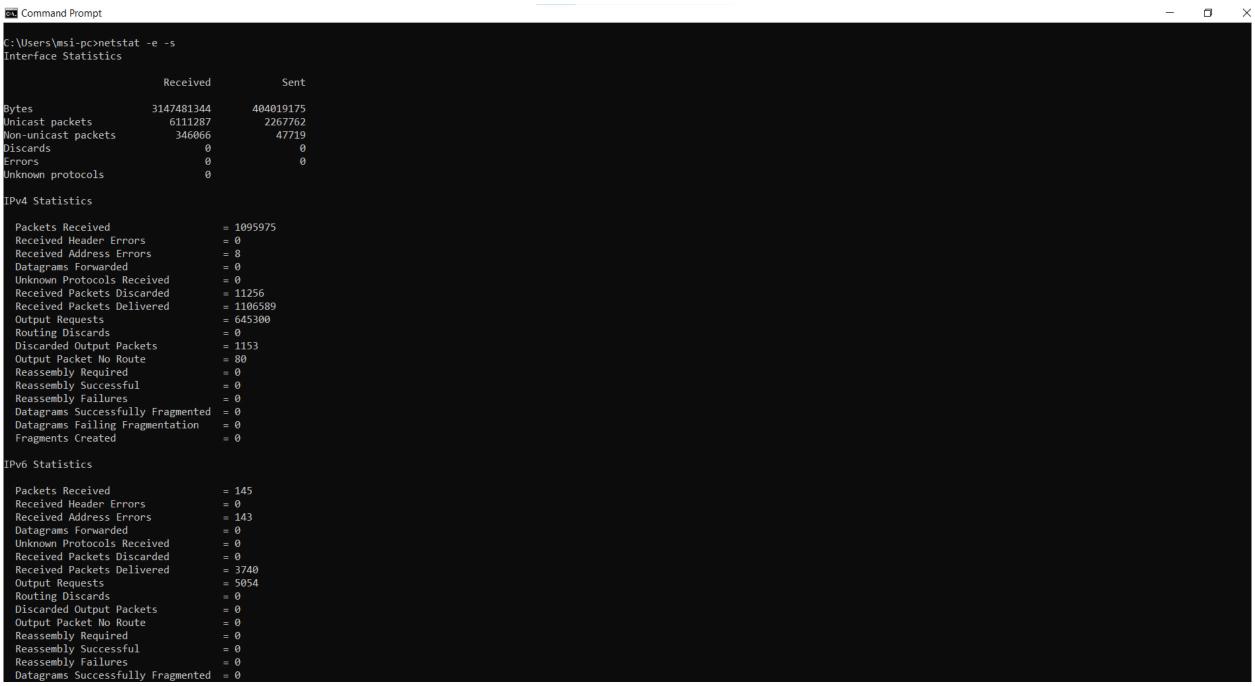
```
  TCP    127.0.0.1:65161        127.0.0.1:65513        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65514        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65515        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65516        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65517        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65518        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65519        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65520        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65521        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65522        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65523        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65524        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65525        TIME_WAIT
  TCP    127.0.0.1:65161        127.0.0.1:65526        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65532        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65533        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65534        ESTABLISHED
  TCP    127.0.0.1:65173        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65494        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65518        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65526        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65532        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65533        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65534        127.0.0.1:65161        ESTABLISHED
  TCP    192.168.0.108:57032    23.40.124.10:443       CLOSE_WAIT
  TCP    192.168.0.108:64982    51.103.5.159:443       ESTABLISHED
  TCP    192.168.0.108:64983    162.159.133.234:443    ESTABLISHED
  TCP    192.168.0.108:65010    74.125.131.188:5228    ESTABLISHED
  TCP    192.168.0.108:65165    79.142.76.128:53       ESTABLISHED
  TCP    192.168.0.108:65166    93.184.220.29:80       CLOSE_WAIT

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49152        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49153        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49154        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49155        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49156        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49157        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:49158        127.0.0.1:65161        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49152        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49153        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49154        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49155        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49156        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49157        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:49158        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65173        ESTABLISHED
  TCP    127.0.0.1:65161        127.0.0.1:65382        TIME_WAIT
```

Figure 3.2: Active connections in an interval of 5 seconds



```
C:\Users\msi-pc>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            MSI:0                  LISTENING
  TCP    0.0.0.0:445            MSI:0                  LISTENING
  TCP    0.0.0.0:808            MSI:0                  LISTENING
  TCP    0.0.0.0:5040           MSI:0                  LISTENING
  TCP    0.0.0.0:49664          MSI:0                  LISTENING
  TCP    0.0.0.0:49665          MSI:0                  LISTENING
  TCP    0.0.0.0:49666          MSI:0                  LISTENING
  TCP    0.0.0.0:49667          MSI:0                  LISTENING
  TCP    0.0.0.0:49668          MSI:0                  LISTENING
  TCP    0.0.0.0:49670          MSI:0                  LISTENING
  TCP    127.0.0.1:6463         MSI:0                  LISTENING
  TCP    127.0.0.1:10042        MSI:0                  LISTENING
  TCP    127.0.0.1:49178        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49179        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49182        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49183        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49184        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49190        MSI:65161              CLOSE_WAIT
  TCP    127.0.0.1:49192        MSI:65161              TIME_WAIT
  TCP    127.0.0.1:49194        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49195        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49196        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49197        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49198        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:49199        MSI:65161              ESTABLISHED
  TCP    127.0.0.1:65160        MSI:0                  LISTENING
  TCP    127.0.0.1:65161        MSI:0                  LISTENING
  TCP    127.0.0.1:65161        MSI:49166              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49172              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49174              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49175              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49177              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49178              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:49179              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:49180              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49181              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49182              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:49183              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:49184              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:49185              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49186              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49187              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49188              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49189              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:49190              FIN_WAIT_2
```

Figure 4: Displaying all active and inactive connections, and the TCP and UDP ports the device is currently listening.

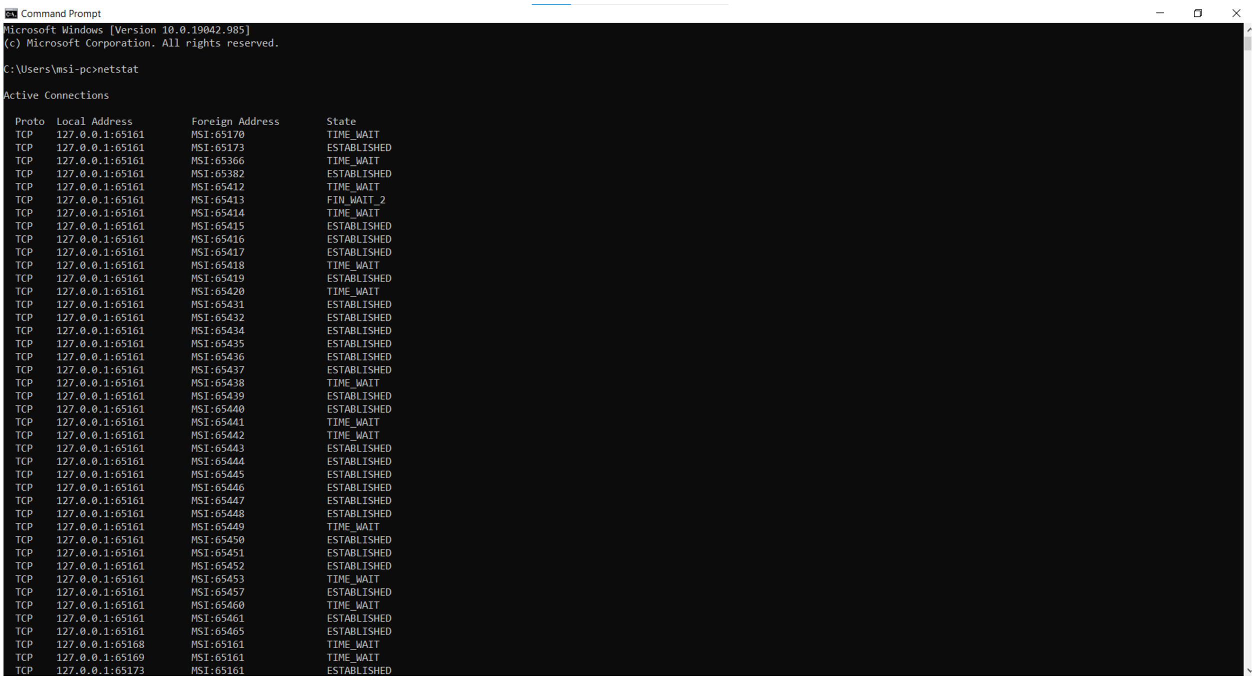


```
C:\Users\msi-pc>netstat -e -s
Interface Statistics

                           Received            Sent

Bytes                    3147481344       404019175
Unicast packets             6111287         2267762
Non-unicast packets          346066           47719
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                   = 1095975
  Received Header Errors             = 0
  Received Address Errors            = 8
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 11256
  Received Packets Delivered         = 1106589
  Output Requests                    = 645300
  Routing Discards                   = 0
  Discarded Output Packets           = 1153
  Output Packet No Route             = 80
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 145
  Received Header Errors             = 0
  Received Address Errors            = 143
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 3740
  Output Requests                    = 5054
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
```

Figure 5: Protocol Statistics

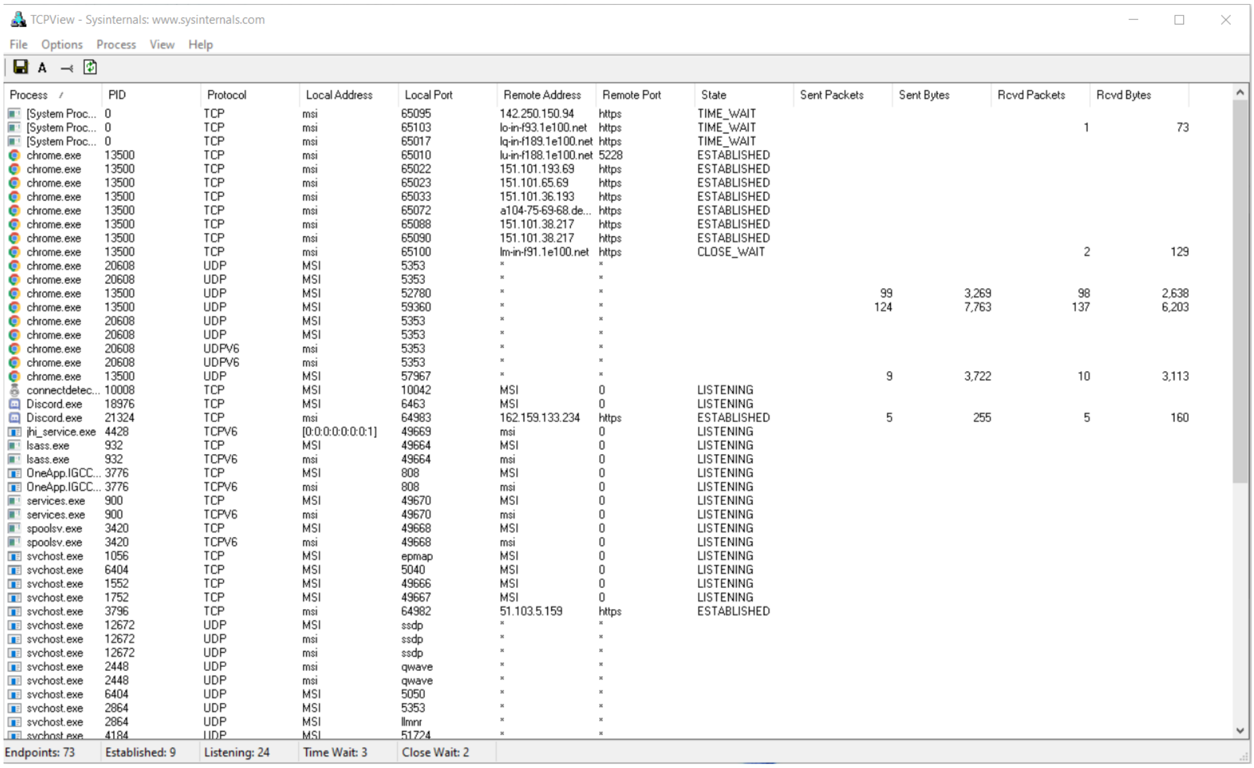
Task 4: Compare the results from netstat and tcpview. What applications or ports did you find suspicious and why?

Result:



```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\msi-pc>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65161        MSI:65170              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65173              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65366              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65382              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65412              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65413              FIN_WAIT_2
  TCP    127.0.0.1:65161        MSI:65414              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65415              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65416              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65417              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65418              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65419              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65420              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65431              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65432              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65434              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65435              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65436              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65437              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65438              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65439              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65440              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65441              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65442              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65443              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65444              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65445              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65446              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65447              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65448              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65449              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65450              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65451              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65452              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65453              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65457              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65460              TIME_WAIT
  TCP    127.0.0.1:65161        MSI:65461              ESTABLISHED
  TCP    127.0.0.1:65161        MSI:65465              ESTABLISHED
  TCP    127.0.0.1:65168        MSI:65161              TIME_WAIT
  TCP    127.0.0.1:65169        MSI:65161              TIME_WAIT
  TCP    127.0.0.1:65173        MSI:65161              ESTABLISHED
```

Figure 6: List of Active Connections displayed in netstat

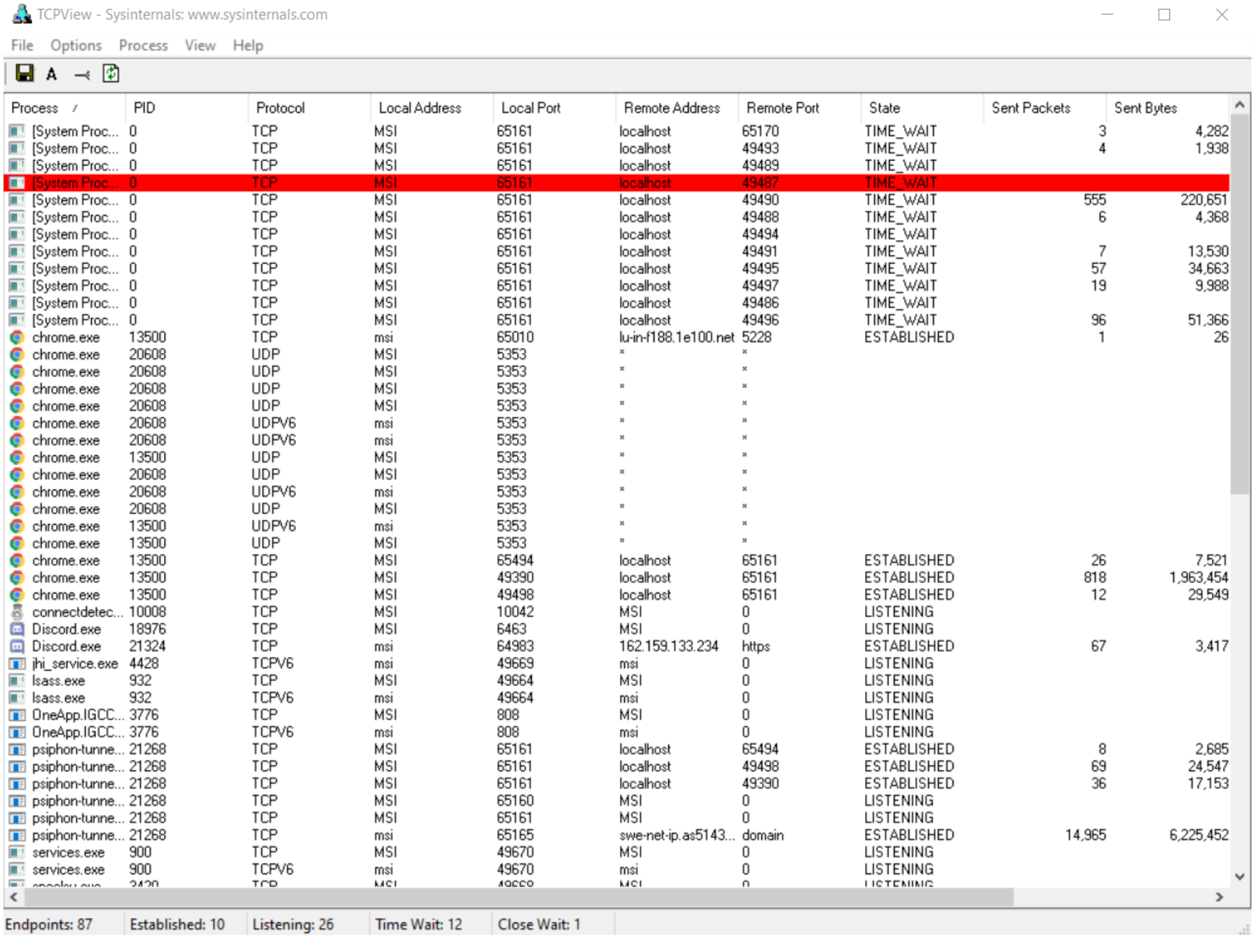


TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	msi	65095	142.250.150.94	https	TIME_WAIT				
[System Proc...	0	TCP	msi	65103	lo-in-f93.1e100.net	https	TIME_WAIT			1	73
[System Proc...	0	TCP	msi	65017	lq-in-f189.1e100.net	https	TIME_WAIT				
chrome.exe	13500	TCP	msi	65010	lu-in-f188.1e100.net	5228	ESTABLISHED				
chrome.exe	13500	TCP	msi	65022	151.101.193.69	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65023	151.101.65.69	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65033	151.101.36.193	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65072	a104-75-69-68.de...	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65088	151.101.38.217	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65090	151.101.38.217	https	ESTABLISHED				
chrome.exe	13500	TCP	msi	65100	lm-in-f91.1e100.net	https	CLOSE_WAIT			2	129
chrome.exe	20608	UDP	MSI	5353	*	*					
chrome.exe	20608	UDP	MSI	5353	*	*					
chrome.exe	13500	UDP	MSI	52780	*	*		99	3,269	98	2,638
chrome.exe	13500	UDP	MSI	59360	*	*		124	7,763	137	6,203
chrome.exe	20608	UDP	MSI	5353	*	*					
chrome.exe	20608	UDP	MSI	5353	*	*					
chrome.exe	20608	UDPV6	msi	5353	*	*					
chrome.exe	20608	UDPV6	msi	5353	*	*					
chrome.exe	13500	UDP	MSI	57967	*	*		9	3,722	10	3,113
connectdetec...	10008	TCP	MSI	10042	MSI	0	LISTENING				
Discord.exe	18976	TCP	MSI	6463	MSI	0	LISTENING				
Discord.exe	21324	TCP	msi	64983	162.159.133.234	https	ESTABLISHED	5	255	5	160
jhi_service.exe	4428	TCPV6	[0:0:0:0:0:0:0:1]	49669	msi	0	LISTENING				
lsass.exe	932	TCP	MSI	49664	MSI	0	LISTENING				
lsass.exe	932	TCPV6	msi	49664	msi	0	LISTENING				
OneApp.IGCC...	3776	TCP	MSI	808	MSI	0	LISTENING				
OneApp.IGCC...	3776	TCPV6	msi	808	msi	0	LISTENING				
services.exe	900	TCP	MSI	49670	MSI	0	LISTENING				
services.exe	900	TCPV6	msi	49670	msi	0	LISTENING				
spoolsv.exe	3420	TCP	MSI	49668	MSI	0	LISTENING				
spoolsv.exe	3420	TCPV6	msi	49668	msi	0	LISTENING				
svchost.exe	1056	TCP	MSI	epmap	MSI	0	LISTENING				
svchost.exe	6404	TCP	MSI	5040	MSI	0	LISTENING				
svchost.exe	1552	TCP	MSI	49666	MSI	0	LISTENING				
svchost.exe	1752	TCP	MSI	49667	MSI	0	LISTENING				
svchost.exe	3796	TCP	msi	64982	51.103.5.159	https	ESTABLISHED				
svchost.exe	12672	UDP	MSI	ssdp	*	*					
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	6404	UDP	MSI	5050	*	*					
svchost.exe	2864	UDP	MSI	5353	*	*					
svchost.exe	2864	UDP	MSI	llmnr	*	*					
svchost.exe	4184	UDP	MSI	51724	*	*					

Endpoints: 73 | Established: 9 | Listening: 24 | Time Wait: 3 | Close Wait: 2

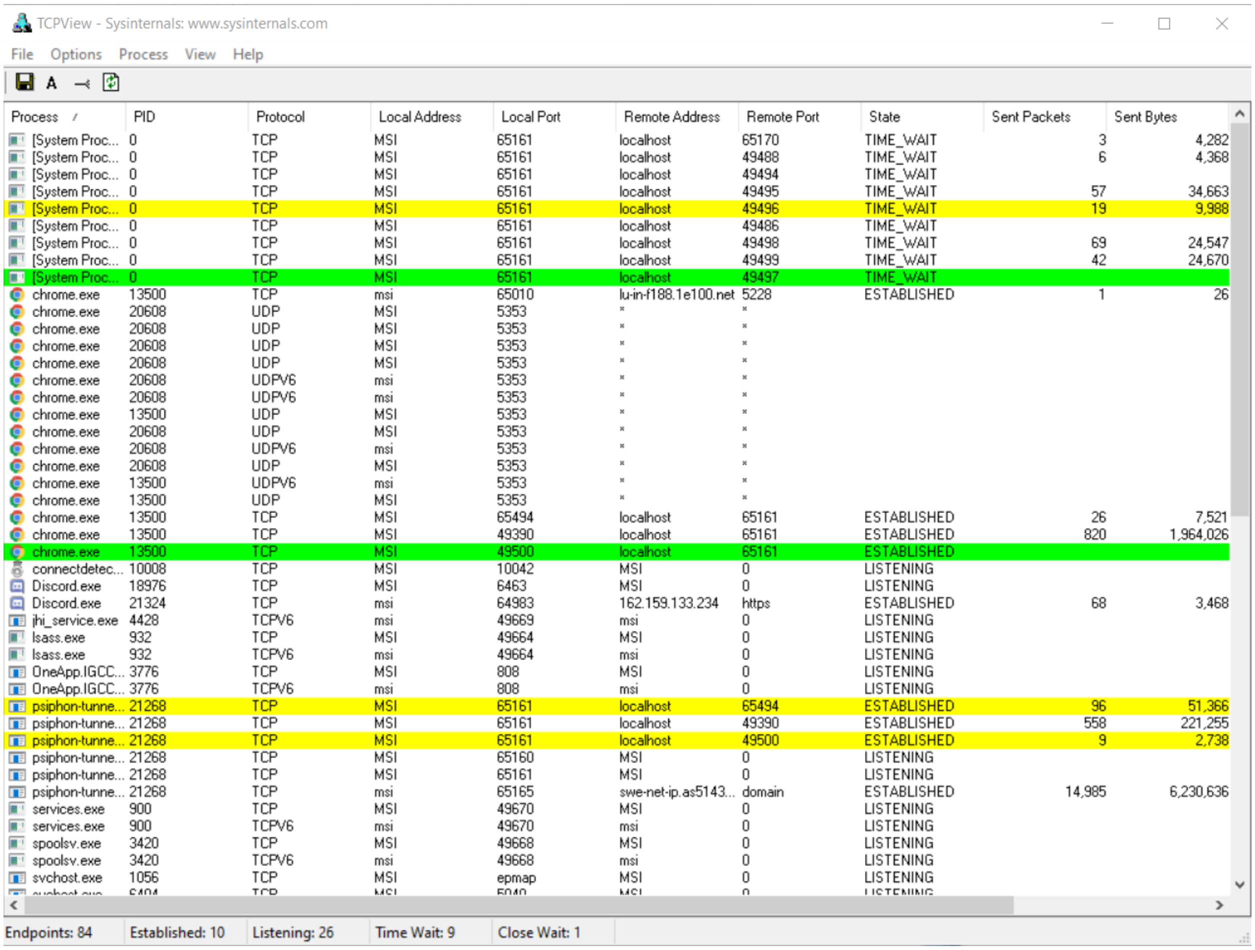
Figure 7: List of Active Connections displayed in tcpview



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
[System Proc...	0	TCP	MSI	65161	localhost	65170	TIME_WAIT	3	4,282
[System Proc...	0	TCP	MSI	65161	localhost	49493	TIME_WAIT	4	1,938
[System Proc...	0	TCP	MSI	65161	localhost	49489	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49487	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49490	TIME_WAIT	555	220,651
[System Proc...	0	TCP	MSI	65161	localhost	49488	TIME_WAIT	6	4,368
[System Proc...	0	TCP	MSI	65161	localhost	49494	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49491	TIME_WAIT	7	13,530
[System Proc...	0	TCP	MSI	65161	localhost	49495	TIME_WAIT	57	34,663
[System Proc...	0	TCP	MSI	65161	localhost	49497	TIME_WAIT	19	9,988
[System Proc...	0	TCP	MSI	65161	localhost	49486	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49496	TIME_WAIT	96	51,366
chrome.exe	13500	TCP	msi	65010	lu-in-f188.1e100.net	5228	ESTABLISHED	1	26
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	13500	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	13500	UDPV6	msi	5353	*	*			
chrome.exe	13500	UDP	MSI	5353	*	*			
chrome.exe	13500	TCP	MSI	65494	localhost	65161	ESTABLISHED	26	7,521
chrome.exe	13500	TCP	MSI	49390	localhost	65161	ESTABLISHED	818	1,963,454
chrome.exe	13500	TCP	MSI	49498	localhost	65161	ESTABLISHED	12	29,549
connectdetec...	10008	TCP	MSI	10042	MSI	0	LISTENING		
Discord.exe	18976	TCP	MSI	6463	MSI	0	LISTENING		
Discord.exe	21324	TCP	msi	64983	162.159.133.234	https	ESTABLISHED	67	3,417
jhi_service.exe	4428	TCPV6	msi	49669	msi	0	LISTENING		
lsass.exe	932	TCP	MSI	49664	MSI	0	LISTENING		
lsass.exe	932	TCPV6	msi	49664	msi	0	LISTENING		
OneApp.IGCC...	3776	TCP	MSI	808	MSI	0	LISTENING		
OneApp.IGCC...	3776	TCPV6	msi	808	msi	0	LISTENING		
psiphon-tunne...	21268	TCP	MSI	65161	localhost	65494	ESTABLISHED	8	2,685
psiphon-tunne...	21268	TCP	MSI	65161	localhost	49498	ESTABLISHED	69	24,547
psiphon-tunne...	21268	TCP	MSI	65161	localhost	49390	ESTABLISHED	36	17,153
psiphon-tunne...	21268	TCP	MSI	65160	MSI	0	LISTENING		
psiphon-tunne...	21268	TCP	MSI	65161	MSI	0	LISTENING		
psiphon-tunne...	21268	TCP	msi	65165	swe-net-ip.as5143...	domain	ESTABLISHED	14,965	6,225,452
services.exe	900	TCP	MSI	49670	MSI	0	LISTENING		
services.exe	900	TCPV6	msi	49670	msi	0	LISTENING		
spoolsv.exe	2420	TCP	MSI	49668	MSI	0	LISTENING		

Endpoints: 87 | Established: 10 | Listening: 26 | Time Wait: 12 | Close Wait: 1

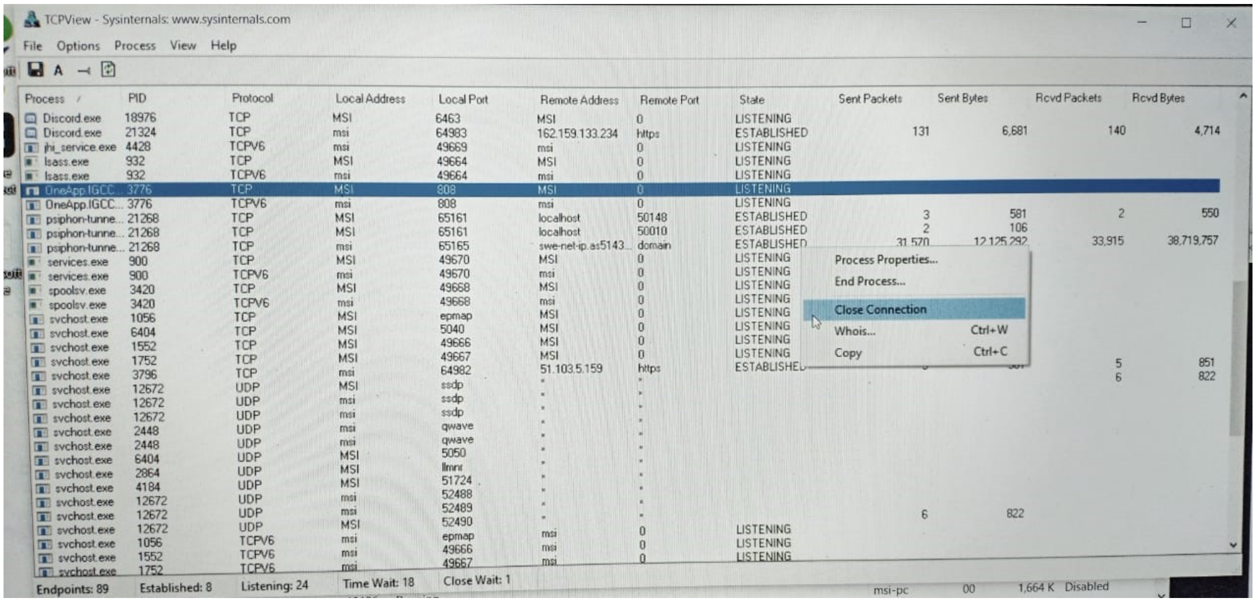
Figure 8: Deleted Connections are shown in red in tcpview



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
[System Proc...	0	TCP	MSI	65161	localhost	65170	TIME_WAIT	3	4,282
[System Proc...	0	TCP	MSI	65161	localhost	49488	TIME_WAIT	6	4,368
[System Proc...	0	TCP	MSI	65161	localhost	49494	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49495	TIME_WAIT	57	34,663
[System Proc...	0	TCP	MSI	65161	localhost	49496	TIME_WAIT	19	9,988
[System Proc...	0	TCP	MSI	65161	localhost	49486	TIME_WAIT		
[System Proc...	0	TCP	MSI	65161	localhost	49498	TIME_WAIT	69	24,547
[System Proc...	0	TCP	MSI	65161	localhost	49499	TIME_WAIT	42	24,670
[System Proc...	0	TCP	MSI	65161	localhost	49497	TIME_WAIT		
chrome.exe	13500	TCP	msi	65010	lu-in-f188.1e100.net	5228	ESTABLISHED	1	26
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	13500	UDP	MSI	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	20608	UDPV6	msi	5353	*	*			
chrome.exe	20608	UDP	MSI	5353	*	*			
chrome.exe	13500	UDPV6	msi	5353	*	*			
chrome.exe	13500	UDP	MSI	5353	*	*			
chrome.exe	13500	TCP	MSI	65494	localhost	65161	ESTABLISHED	26	7,521
chrome.exe	13500	TCP	MSI	49390	localhost	65161	ESTABLISHED	820	1,964,026
chrome.exe	13500	TCP	MSI	49500	localhost	65161	ESTABLISHED		
connectdetec...	10008	TCP	MSI	10042	MSI	0	LISTENING		
Discord.exe	18976	TCP	MSI	6463	MSI	0	LISTENING		
Discord.exe	21324	TCP	msi	64983	162.159.133.234	https	ESTABLISHED	68	3,468
jhi_service.exe	4428	TCPV6	msi	49669	msi	0	LISTENING		
lsass.exe	932	TCP	MSI	49664	MSI	0	LISTENING		
lsass.exe	932	TCPV6	msi	49664	msi	0	LISTENING		
OneApp.IGCC...	3776	TCP	MSI	808	MSI	0	LISTENING		
OneApp.IGCC...	3776	TCPV6	msi	808	msi	0	LISTENING		
psiphon-tunne...	21268	TCP	MSI	65161	localhost	65494	ESTABLISHED	96	51,366
psiphon-tunne...	21268	TCP	MSI	65161	localhost	49390	ESTABLISHED	558	221,255
psiphon-tunne...	21268	TCP	MSI	65161	localhost	49500	ESTABLISHED	9	2,738
psiphon-tunne...	21268	TCP	MSI	65160	MSI	0	LISTENING		
psiphon-tunne...	21268	TCP	MSI	65161	MSI	0	LISTENING		
psiphon-tunne...	21268	TCP	msi	65165	swe-net-ip.as5143...	domain	ESTABLISHED	14,985	6,230,636
services.exe	900	TCP	MSI	49670	MSI	0	LISTENING		
services.exe	900	TCPV6	msi	49670	msi	0	LISTENING		
spoolsv.exe	3420	TCP	MSI	49668	MSI	0	LISTENING		
spoolsv.exe	3420	TCPV6	msi	49668	msi	0	LISTENING		
svchost.exe	1056	TCP	MSI	epmap	MSI	0	LISTENING		
svchost.exe	6404	TCP	MSI	5040	MSI	0	LISTENING		

Endpoints: 84 | Established: 10 | Listening: 26 | Time Wait: 9 | Close Wait: 1

Figure 9: New Connections are shown in yellow in tcpview and connections that change state from one update to the next are highlighted in yellow



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
Discord.exe	18976	TCP	MSI	6463	MSI	0	LISTENING				
Discord.exe	21324	TCP	msi	64983	162.159.133.234	https	ESTABLISHED	131	6,681	140	4,714
jhi_service.exe	4428	TCPV6	msi	49669	msi	0	LISTENING				
lsass.exe	932	TCP	MSI	49664	MSI	0	LISTENING				
lsass.exe	932	TCPV6	msi	49664	msi	0	LISTENING				
OneApp.IGCC...	3776	TCP	MSI	808	MSI	0	LISTENING				
OneApp.IGCC...	3776	TCPV6	msi	808	msi	0	LISTENING				
psiphon-tunne...	21268	TCP	MSI	65161	localhost	50148	ESTABLISHED	3	581	2	550
psiphon-tunne...	21268	TCP	MSI	65161	localhost	50010	ESTABLISHED	2	106		
psiphon-tunne...	21268	TCP	msi	65165	swe-net-ip.as5143...	domain	ESTABLISHED	31,570	12,125,292	33,915	38,719,757
services.exe	900	TCP	MSI	49670	MSI	0	LISTENING				
services.exe	900	TCPV6	msi	49670	msi	0	LISTENING				
spoolsv.exe	3420	TCP	MSI	49668	MSI	0	LISTENING				
spoolsv.exe	3420	TCPV6	msi	49668	msi	0	LISTENING				
svchost.exe	1056	TCP	MSI	epmap	MSI	0	LISTENING				
svchost.exe	6404	TCP	MSI	5040	MSI	0	LISTENING				
svchost.exe	1552	TCP	MSI	49666	MSI	0	LISTENING				
svchost.exe	1752	TCP	MSI	49667	MSI	0	LISTENING				
svchost.exe	3796	TCP	msi	64982	51.103.5.159	https	ESTABLISHED	[illegible]	[illegible]	5	851
svchost.exe	12672	UDP	MSI	ssdp	*	*				6	822
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	6404	UDP	MSI	5050	*	*					
svchost.exe	2864	UDP	MSI	llmnr	*	*					
svchost.exe	4184	UDP	MSI	51724	*	*					
svchost.exe	12672	UDP	msi	52488	*	*					
svchost.exe	12672	UDP	msi	52489	*	*		6	822		
svchost.exe	12672	UDP	MSI	52490	*	*					
svchost.exe	1056	TCPV6	msi	epmap	msi	0	LISTENING				
svchost.exe	1552	TCPV6	msi	49666	msi	0	LISTENING				
svchost.exe	1752	TCPV6	msi	49667	msi	0	LISTENING				

Endpoints: 89 Established: 8 Listening: 24 Time Wait: 18 Close Wait: 1

msi-pc 00 1,664 K Disabled

Figure 10: Closing a connection on tcpview

Comparison of results from netstat and tcpview:

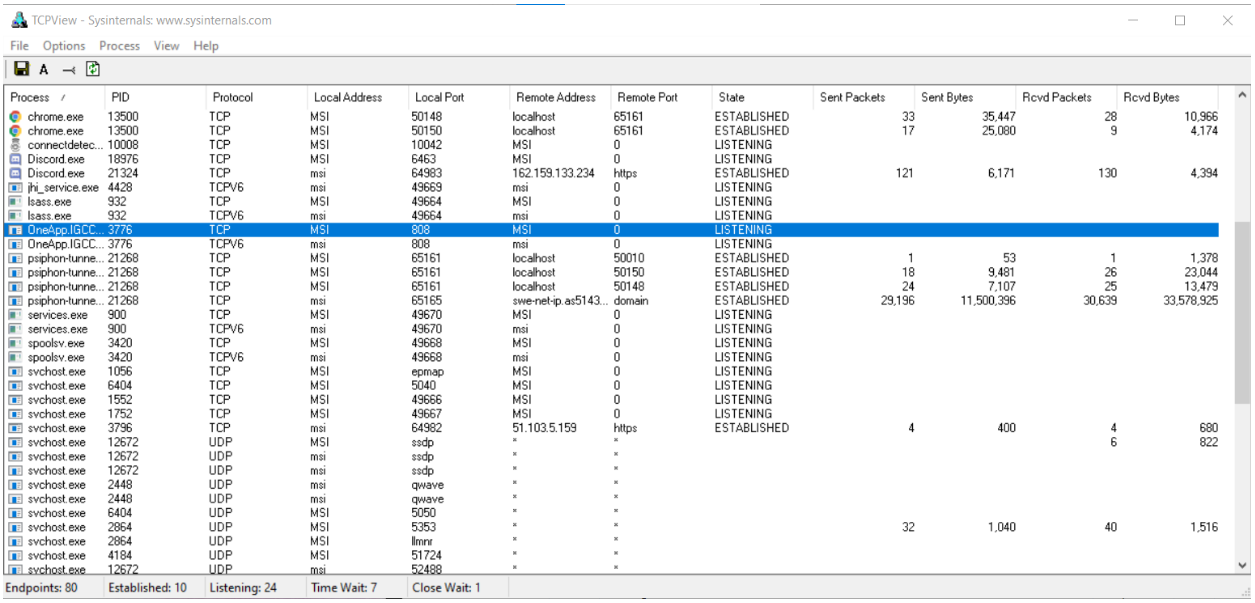
- The netstat command is a fine tool, but it is command line driven as opposed to having a standard graphical user interface (GUI). It also just runs once unless the command is issued repeatedly. Therefore, it can't show changes in connections as they occur. The upside is that it comes installed on Windows 2000 and above though, so it's pretty much guaranteed to be there. (Although the -o option is only available in Windows XP and above.)

- TCPView displays a list of the current TCP and UDP connections established with the computer upon which it is run. It's very much the same information that netstat had, but in a nicer viewing format. Additionally, TCPView can be set to recheck the connections at 1, 2 or 5 second intervals and display the differences from the previous check. Connections that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new connections are shown in green. (TCPView calls the connections to other IPs, "endpoints.") The owning processes name and PID are also shown, which saves looking them up via other means.

- Using TCPView, you can look for unexpected connections as before. However, with TCPView, you can immediately see what processes those connections are from/to. Additionally, if any of those connections look questionable, you can close them by right clicking on the connection and choosing "Close Connection" from the popup menu.

Suspicious port or application:

I found the “OneApp.IGCC.winservice.exe” in Figure 11 process to be suspicious because I have never heard of such a process or file . So I was curious about it and therefore I searched about it on the internet and got the following information.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
chrome.exe	13500	TCP	MSI	50148	localhost	65161	ESTABLISHED	33	35,447	28	10,966
chrome.exe	13500	TCP	MSI	50150	localhost	65161	ESTABLISHED	17	25,080	9	4,174
connectdetec...	10008	TCP	MSI	10042	MSI	0	LISTENING				
Discord.exe	18976	TCP	MSI	6463	MSI	0	LISTENING				
Discord.exe	21324	TCP	msi	64983	162.159.133.234	https	ESTABLISHED	121	6,171	130	4,394
jhi_service.exe	4428	TCPV6	msi	49669	msi	0	LISTENING				
lsass.exe	932	TCP	MSI	49664	MSI	0	LISTENING				
lsass.exe	932	TCPV6	msi	49664	msi	0	LISTENING				
OneApp.IGCC...	3776	TCP	MSI	808	MSI	0	LISTENING				
OneApp.IGCC...	3776	TCPV6	msi	808	msi	0	LISTENING				
psiphon-tunne...	21268	TCP	MSI	65161	localhost	50010	ESTABLISHED	1	53	1	1,378
psiphon-tunne...	21268	TCP	MSI	65161	localhost	50150	ESTABLISHED	18	9,481	26	23,044
psiphon-tunne...	21268	TCP	MSI	65161	localhost	50148	ESTABLISHED	24	7,107	25	13,479
psiphon-tunne...	21268	TCP	msi	65165	swe-net-ip.as5143...	domain	ESTABLISHED	29,196	11,500,396	30,639	33,578,925
services.exe	900	TCP	MSI	49670	MSI	0	LISTENING				
services.exe	900	TCPV6	msi	49670	msi	0	LISTENING				
spoolsv.exe	3420	TCP	MSI	49668	MSI	0	LISTENING				
spoolsv.exe	3420	TCPV6	msi	49668	msi	0	LISTENING				
svchost.exe	1056	TCP	MSI	epmap	MSI	0	LISTENING				
svchost.exe	6404	TCP	MSI	5040	MSI	0	LISTENING				
svchost.exe	1552	TCP	MSI	49666	MSI	0	LISTENING				
svchost.exe	1752	TCP	MSI	49667	MSI	0	LISTENING				
svchost.exe	3796	TCP	msi	64982	51.103.5.159	https	ESTABLISHED	4	400	4	680
svchost.exe	12672	UDP	MSI	ssdp	*	*				6	822
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	12672	UDP	msi	ssdp	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	2448	UDP	msi	qwave	*	*					
svchost.exe	6404	UDP	MSI	5050	*	*					
svchost.exe	2864	UDP	MSI	5353	*	*		32	1,040	40	1,516
svchost.exe	2864	UDP	MSI	llmnr	*	*					
svchost.exe	4184	UDP	MSI	51724	*	*					
svchost.exe	12672	UDP	msi	52488	*	*					

Endpoints: 80 Established: 10 Listening: 24 Time Wait: 7 Close Wait: 1

Figure 11: OneApp.IGCC.winservice.exe process I found to be “suspicious”

Information about OneApp.IGCC.winservice.exe process:

> The process known as OneApp.IGCC.WinService belongs to software OneApp.IGCC.WinService by Intel® pGFX (version 2020).
>
> **Description:** OneApp.IGCC.WinService.exe is not essential for the Windows OS and causes relatively few problems. OneApp.IGCC.WinService.exe is located in a subfolder of C:\Windows\System32—generally *C:\Windows\System32\DriverStore\FileRepository\igcc_dch.inf_amd64_12bdb8127c4c0458\* or *C:\Windows\System32\DriverStore\FileRepository\igcc_dch.inf_amd64_577475639d32bfed\*. Known file sizes on Windows 10/8/7/XP are 27,608 bytes (18% of all occurrences), 31,584 bytes and 9 more variants.
>
> The OneApp.IGCC.WinService.exe file is a trustworthy file from Microsoft. The file is digitally signed. The file is not a Windows system file. The process uses ports to connect to or from a LAN or the Internet. The program is not visible. OneApp.IGCC.WinService.exe appears to be a compressed file. Therefore the technical security rating is *5% dangerous*
>
> Important: Some malware camouflages itself as OneApp.IGCC.WinService.exe, particularly when located in the C:\Windows or C:\Windows\System32 folder. Therefore, you should check the OneApp.IGCC.WinService.exe process on your PC to see if it is a threat. We recommend **Security Task Manager** for verifying your computer's security.

On the basis of the information provided above, I considered killing the OneApp.IGCC.winservice.exe process.

Task 5: Answer questions:
a. What is the fundamental difference between the TCP and UDP protocols?
b. What is a socket?
c. Why was the network ports mechanism introduced?
d. Is there a difference in the protocols implemented, for example, for Windows and Linux?

Ans a) Fundamental difference between the TCP and UDP protocols is that TCP is a connection-oriented protocol whereas the UDP is connectionless protocol.

Also there are more key differences between the TCP and UDP protocols. They are as follows:

TCP	UDP
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	Header size is 8 bytes.
TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.
TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism which is used for checksums.

Ans b) Socket: Any 2 network processes can identify each other using 3 components: ip-address, protocol (TCP / UDP), port. These components are often referred to as sockets. Sockets are the name of a software interface for providing information exchange between processes. Those for network application processes, communication is carried out via sockets.

Ans c) First it was important for me to understand what actually the Network Port is.

A network port is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication. A port number is a 16-bit unsigned integer that ranges from 0 to 65535.

The most common reason for introducing the network ports is for remote access.

Let’s try to understand it in this way:

Imagine that you have two cameras on your network, connecting through the same router (your router has a single external IP address which is accessible from the Internet) and you want to be able to connect remotely to both your cameras which are both on port 80. You decide that you want to access your cameras from the Internet and so set up port forwarding. However, you can’t forward a single port onto more than one local IP address at the same time. As such you can’t access both cameras simultaneously when they’re both using port 80.

The solution is to use two separate ports. In the case above you could use port 8000 for the HTTP port on one camera and 8001 for the other. To access your cameras from the Internet you would then type http://IPADDRESS:8000 and http://IPADDRESS:8001 where the IP address is the external IP address of the router. You must make sure to type in the http before the address. Your browser will know that any information on port 80 is to be displayed as a web page but because you are using a different port number the information could be just about anything. Adding the http:// tells the browser that the information received should be displayed on the screen.

Ans d) Yes, there are many different implementations with slightly different (but still compliant) behavior in corner cases, although it could be argued that many have their roots in the implementation of TCP/IP in UNIX 4.2 BSD (1983).Small differences in implementations makes TCP/IP stack fingerprinting possible, for example. And also using an implementation that is specifically designed for one operating system for another implementation is not easy and requires many changes as there are different requirements for different operating systems. Therefore, there is a difference in implementations of protocols of different operating systems.