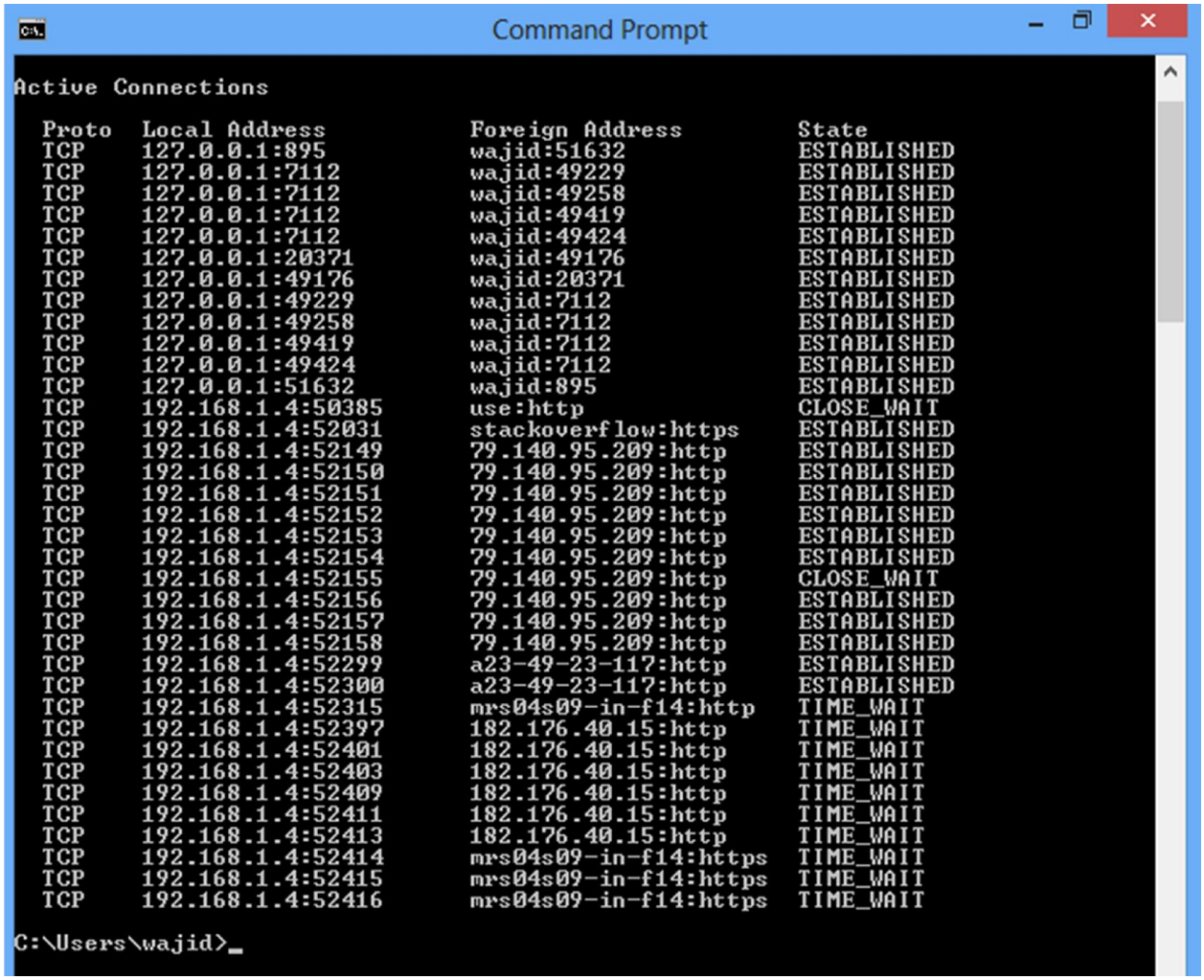
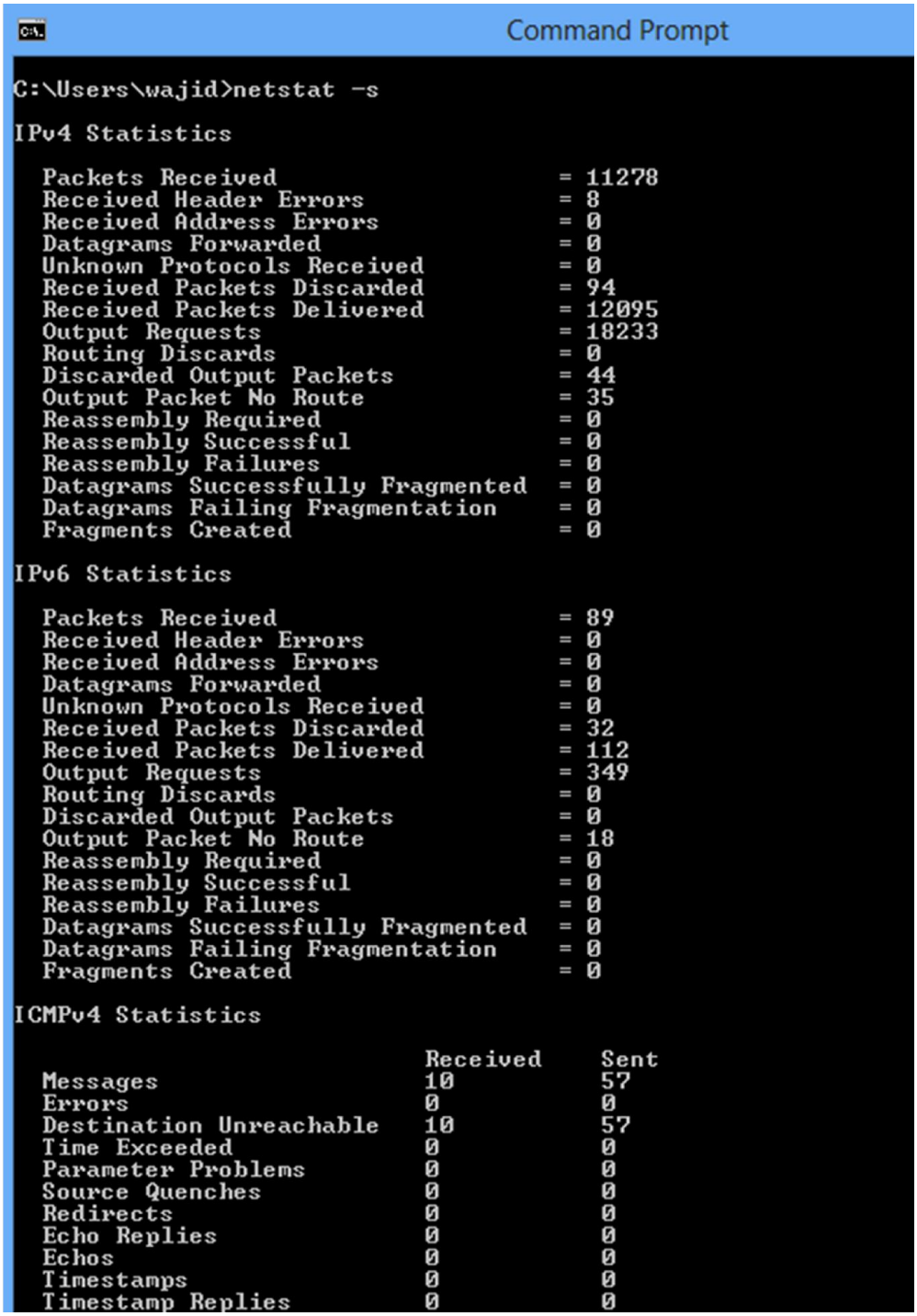
TCP connection

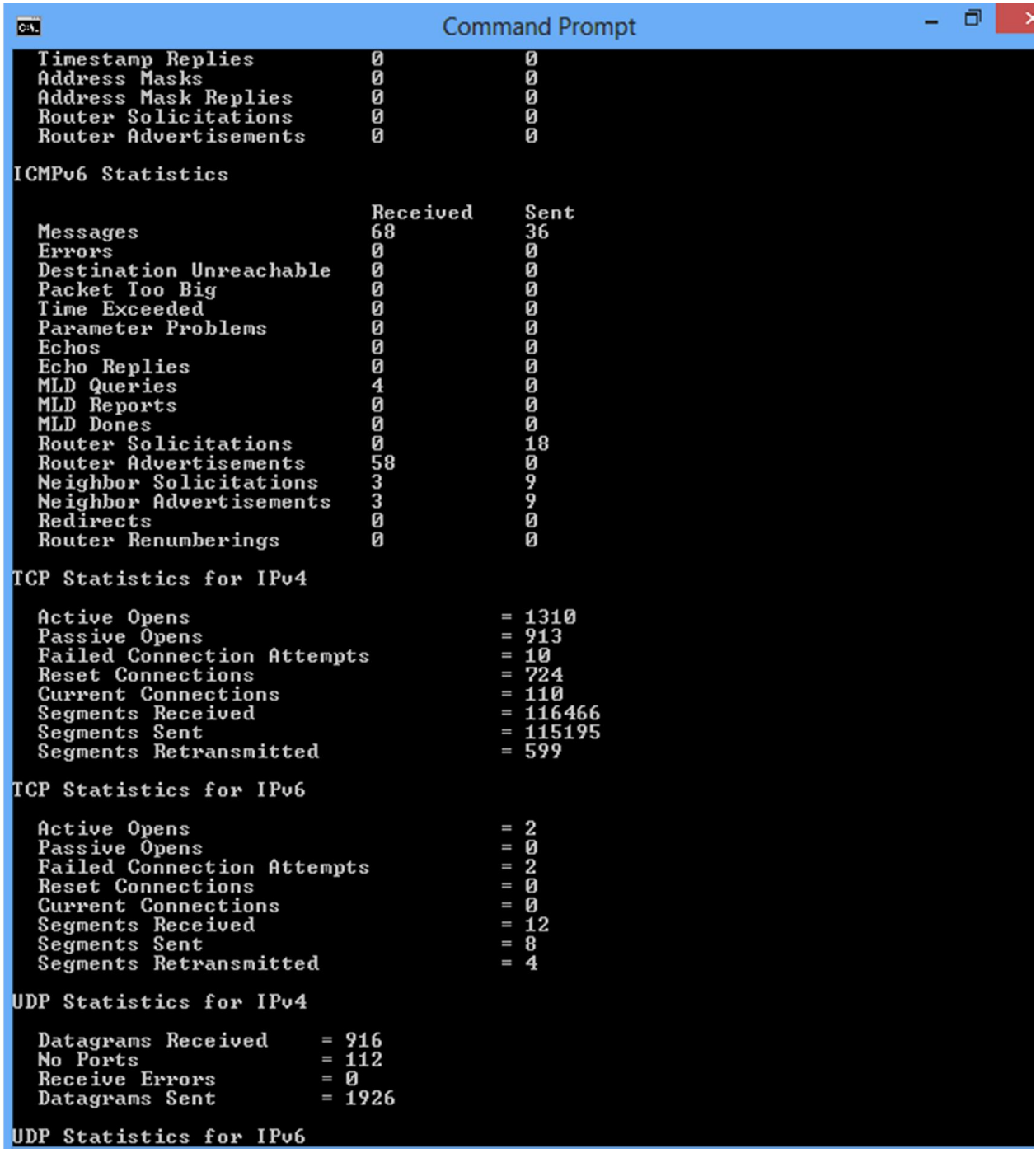
To See Active Network Connections (Windows)

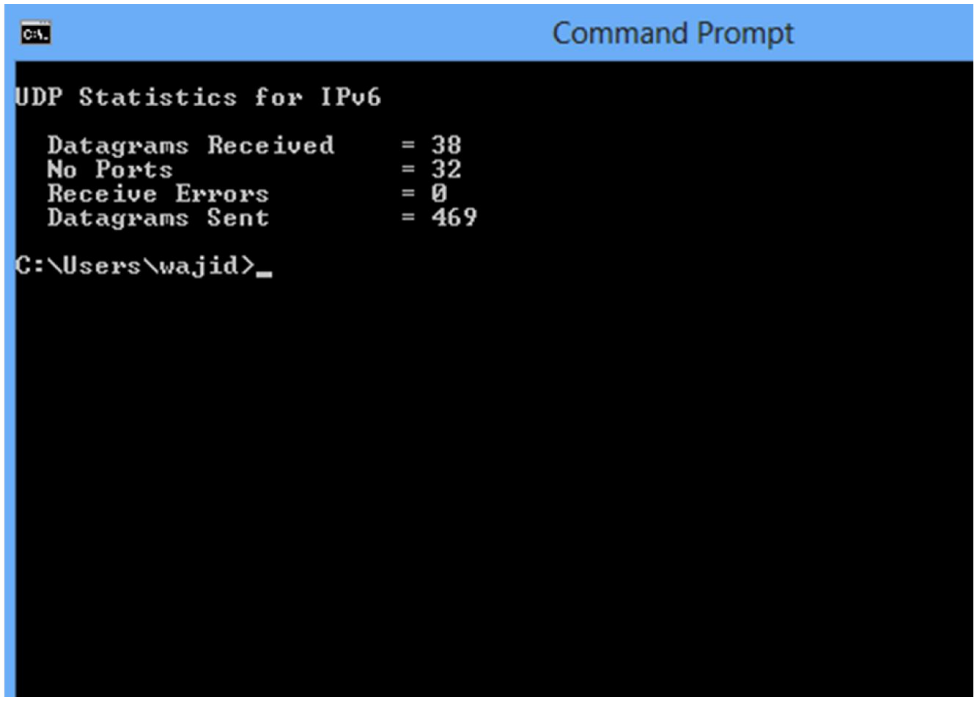
netstat: shows a list of your current TCP connections and ports, with the physical computer name listed for local addresses and the host name listed for remote addresses. It will also tell you the state of the port (waiting, established, etc...)



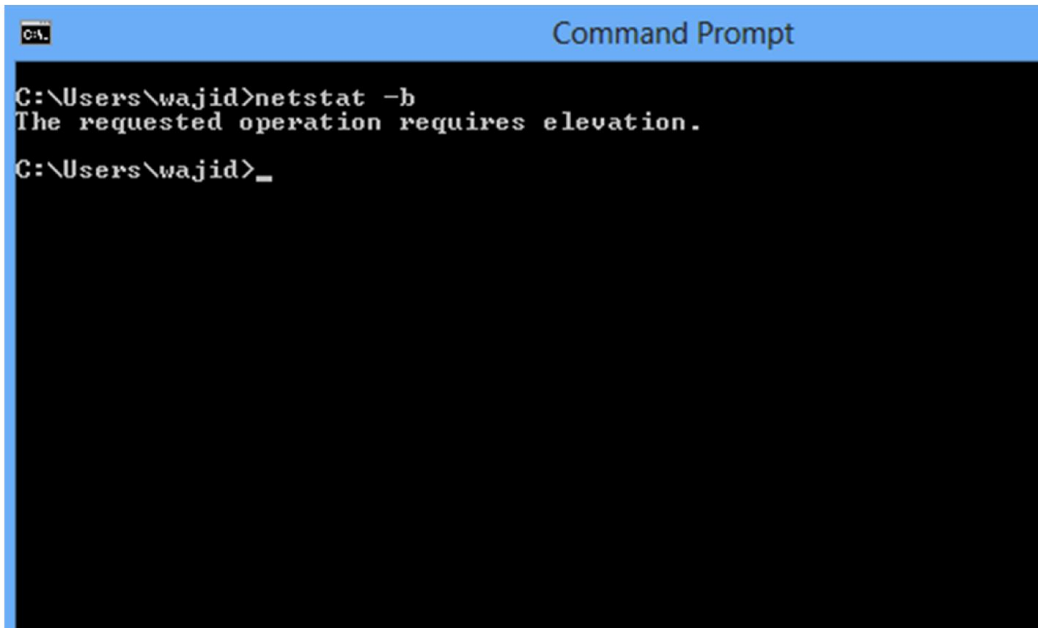
Netstat –s: Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols



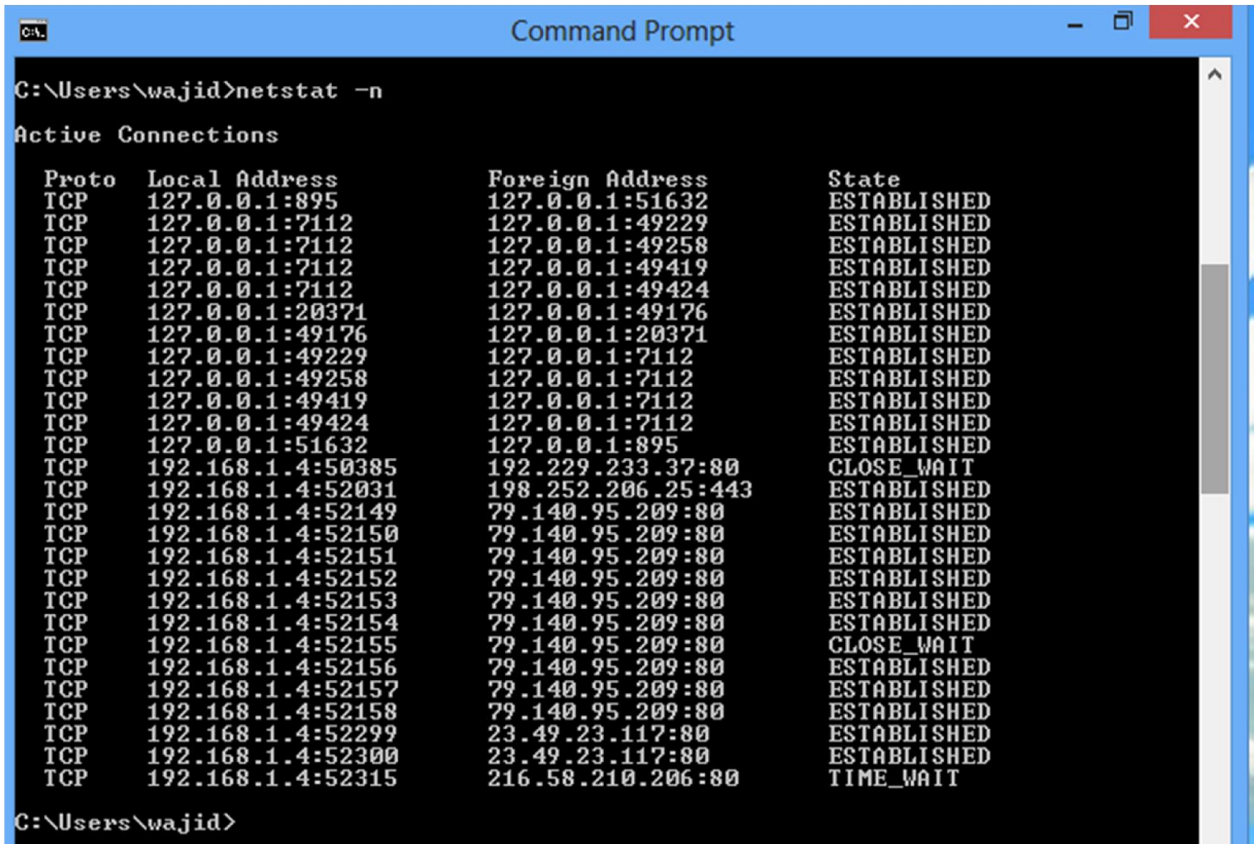

Command Prompt
Timestamp Replies 0 0
Address Masks 0 0
Address Mask Replies 0 0
Router Solicitations 0 0
Router Advertisements 0 0
ICMPv6 Statistics
Received Sent
Messages 68 36
Errors 0 0
Destination Unreachable 0 0
Packet Too Big 0 0
Time Exceeded 0 0
Parameter Problems 0 0
Echos 0 0
Echo Replies 0 0
MLD Queries 4 0
MLD Reports 0 0
MLD Dones 0 0
Router Solicitations 0 18
Router Advertisements 58 0
Neighbor Solicitations 3 9
Neighbor Advertisements 3 9
Redirects 0 0
Router Renumberings 0 0
TCP Statistics for IPv4
Active Opens = 1310
Passive Opens = 913
Failed Connection Attempts = 10
Reset Connections = 724
Current Connections = 110
Segments Received = 116466
Segments Sent = 115195
Segments Retransmitted = 599
TCP Statistics for IPv6
Active Opens = 2
Passive Opens = 0
Failed Connection Attempts = 2
Reset Connections = 0
Current Connections = 0
Segments Received = 12
Segments Sent = 8
Segments Retransmitted = 4
UDP Statistics for IPv4
Datagrams Received = 916
No Ports = 112
Receive Errors = 0
Datagrams Sent = 1926
UDP Statistics for IPv6



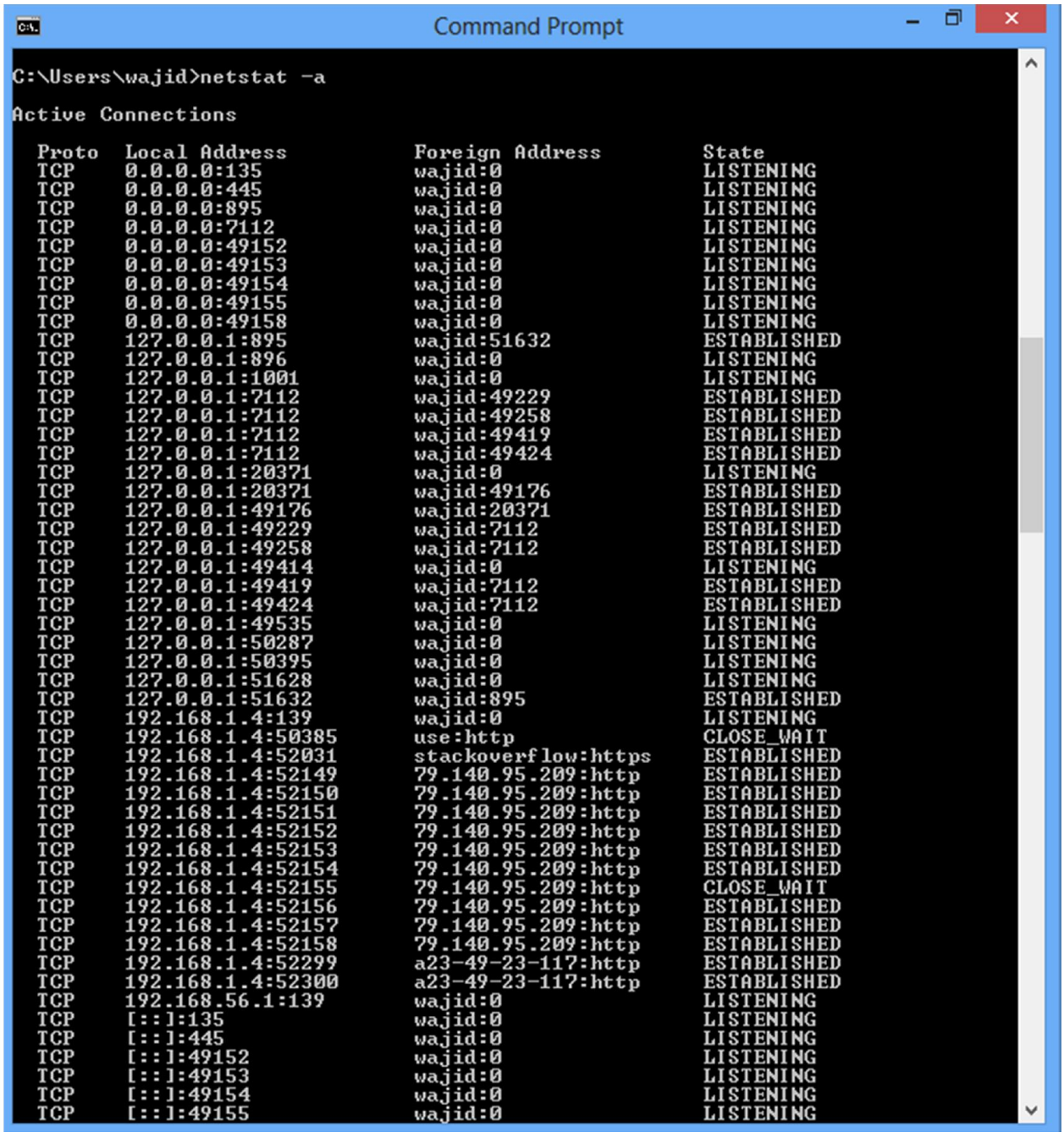
NETSTAT –b : Displays the executable involved in creating each connection or listening port. In some cases well-known executable host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.



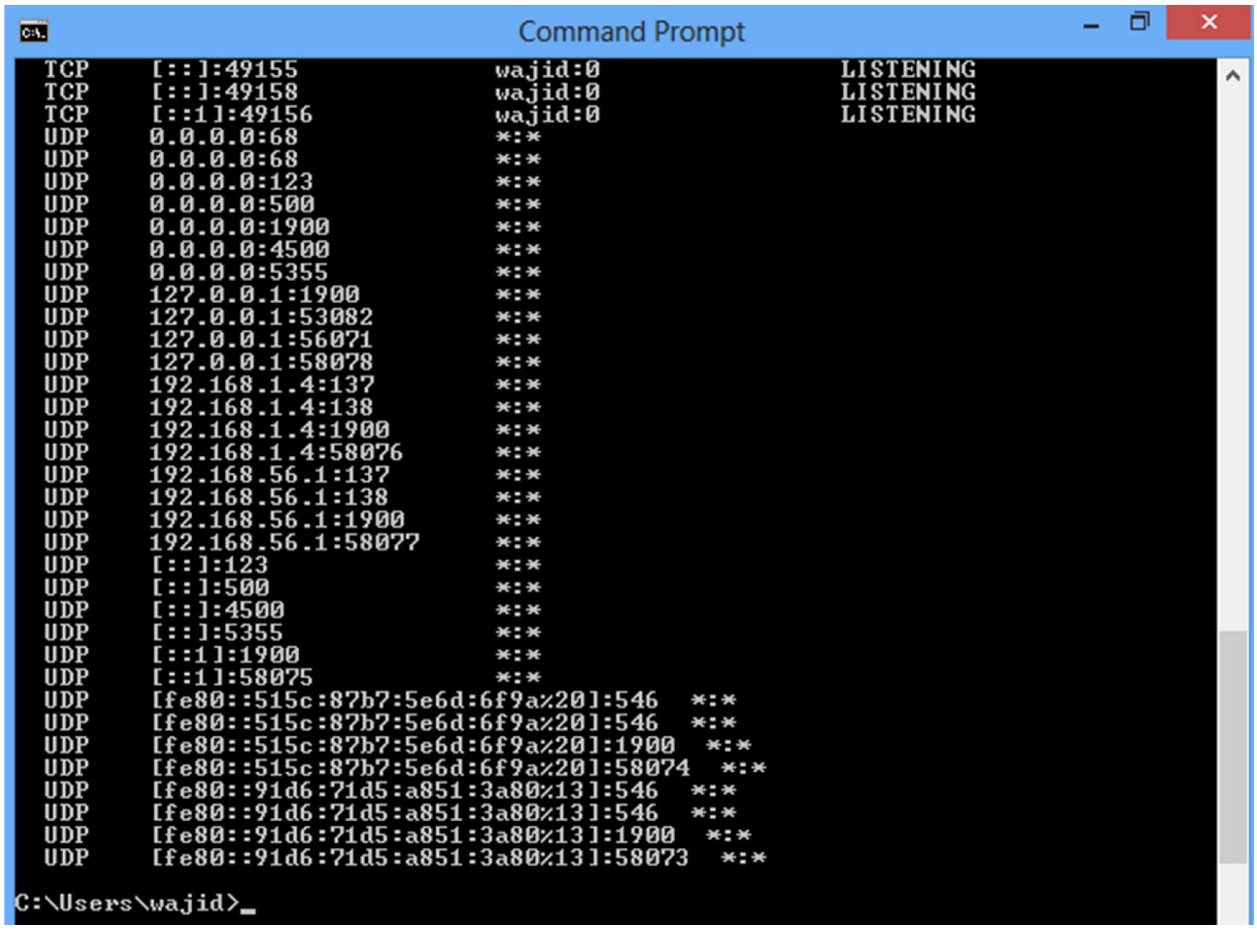
netstat –n: shows you the same list of TCP connections and ports, but with numerical, or ip addresses instead of the actual names of the computers or services.



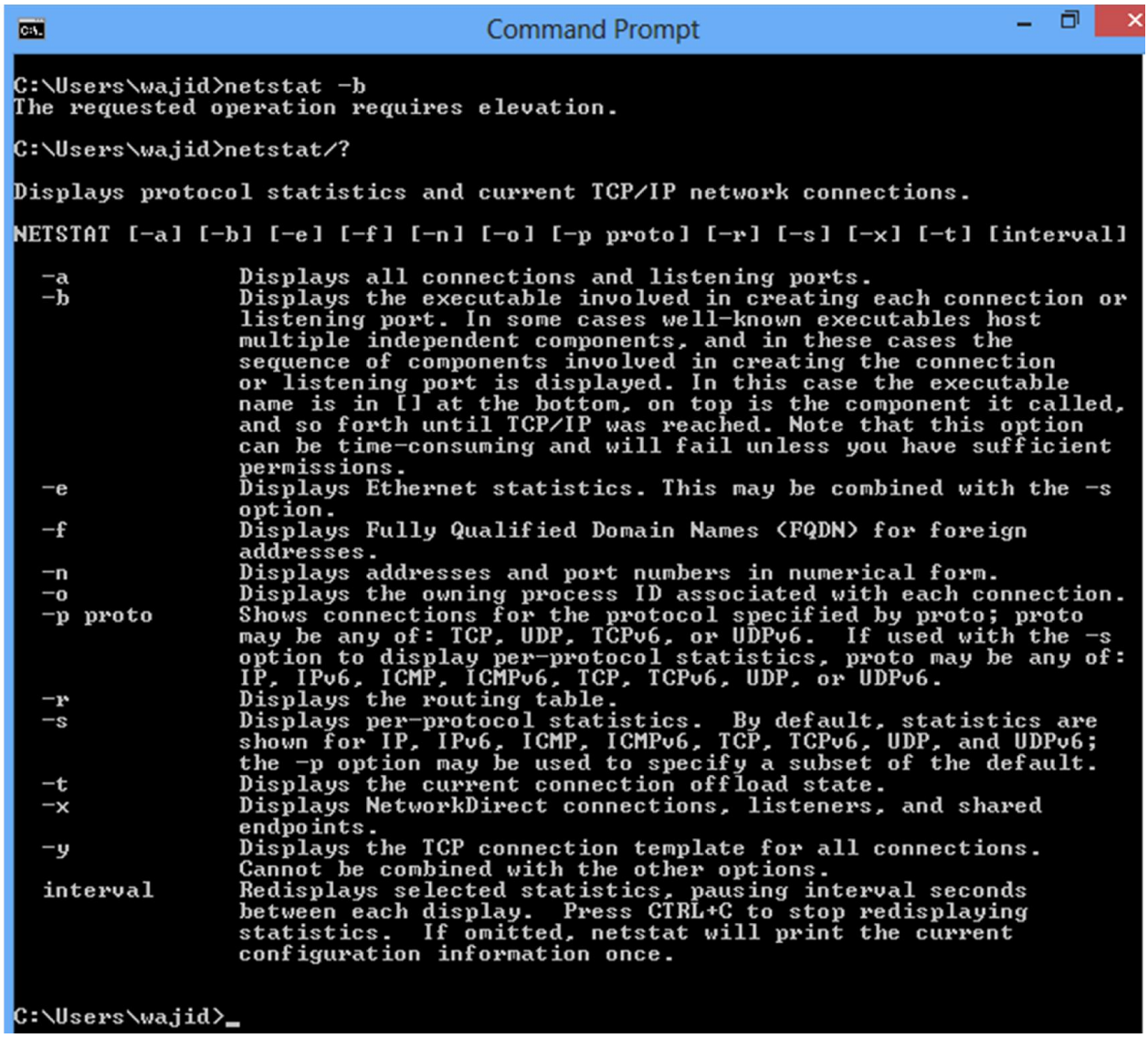
netstat -a : shows you a complete list of all connections on all protocols which are currently active on your machine. This list is not exhaustive, as it only shows the protocols that windows determine are relevant (typically TCP and UDP - ICMP and the like are not shown).



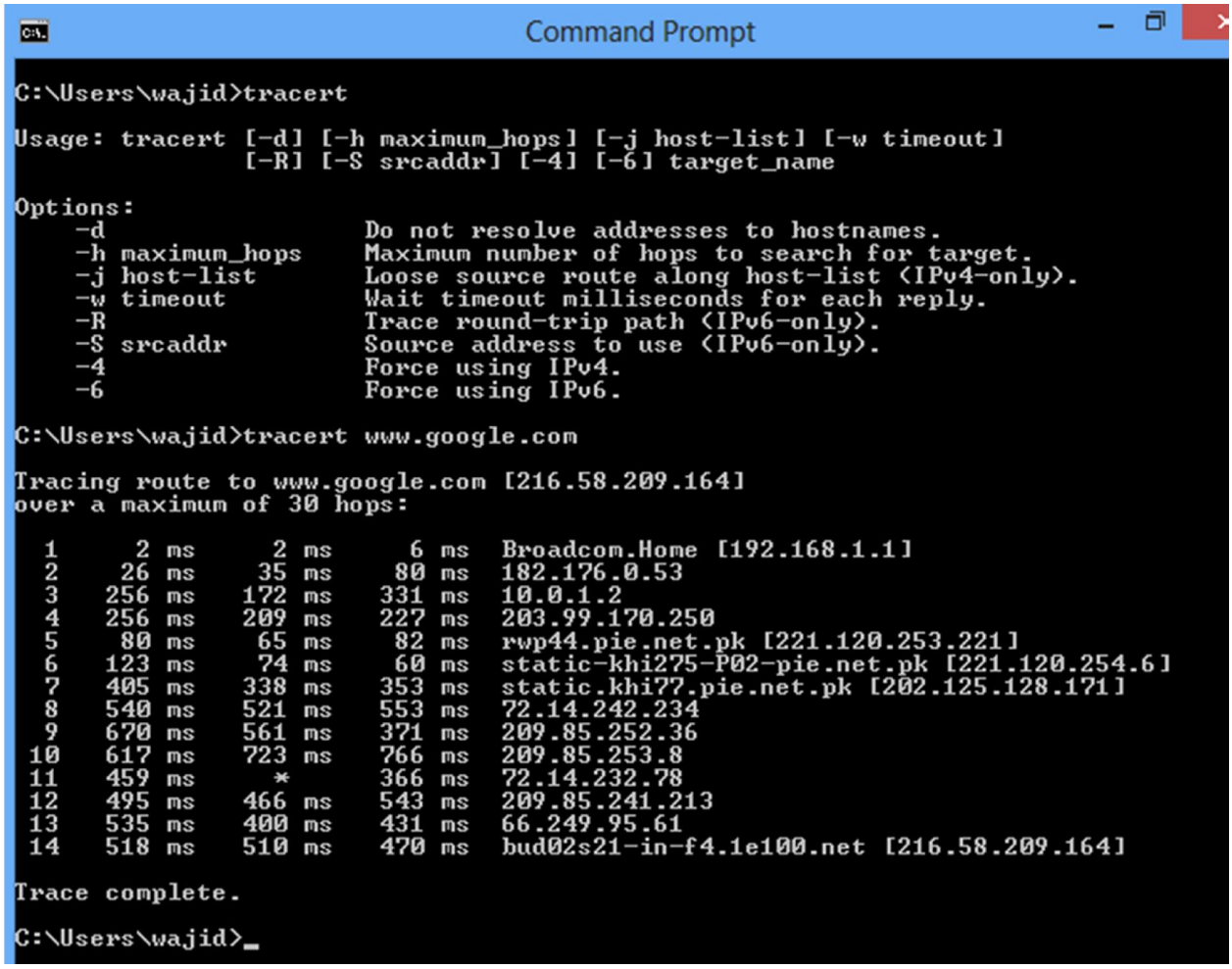
netstat -a


Command Prompt
TCP [::]:49155 wajid:0 LISTENING
TCP [::]:49158 wajid:0 LISTENING
TCP [::1]:49156 wajid:0 LISTENING
UDP 0.0.0.0:68 *:*
UDP 0.0.0.0:68 *:*
UDP 0.0.0.0:123 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1900 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5355 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:53082 *:*
UDP 127.0.0.1:56071 *:*
UDP 127.0.0.1:58078 *:*
UDP 192.168.1.4:137 *:*
UDP 192.168.1.4:138 *:*
UDP 192.168.1.4:1900 *:*
UDP 192.168.1.4:58076 *:*
UDP 192.168.56.1:137 *:*
UDP 192.168.56.1:138 *:*
UDP 192.168.56.1:1900 *:*
UDP 192.168.56.1:58077 *:*
UDP [::]:123 *:*
UDP [::]:500 *:*
UDP [::]:4500 *:*
UDP [::]:5355 *:*
UDP [::1]:1900 *:*
UDP [::1]:58075 *:*
UDP [fe80::515c:87b7:5e6d:6f9a%20]:546 *:*
UDP [fe80::515c:87b7:5e6d:6f9a%20]:546 *:*
UDP [fe80::515c:87b7:5e6d:6f9a%20]:1900 *:*
UDP [fe80::515c:87b7:5e6d:6f9a%20]:58074 *:*
UDP [fe80::91d6:71d5:a851:3a80%13]:546 *:*
UDP [fe80::91d6:71d5:a851:3a80%13]:546 *:*
UDP [fe80::91d6:71d5:a851:3a80%13]:1900 *:*
UDP [fe80::91d6:71d5:a851:3a80%13]:58073 *:*
C:\Users\wajid>

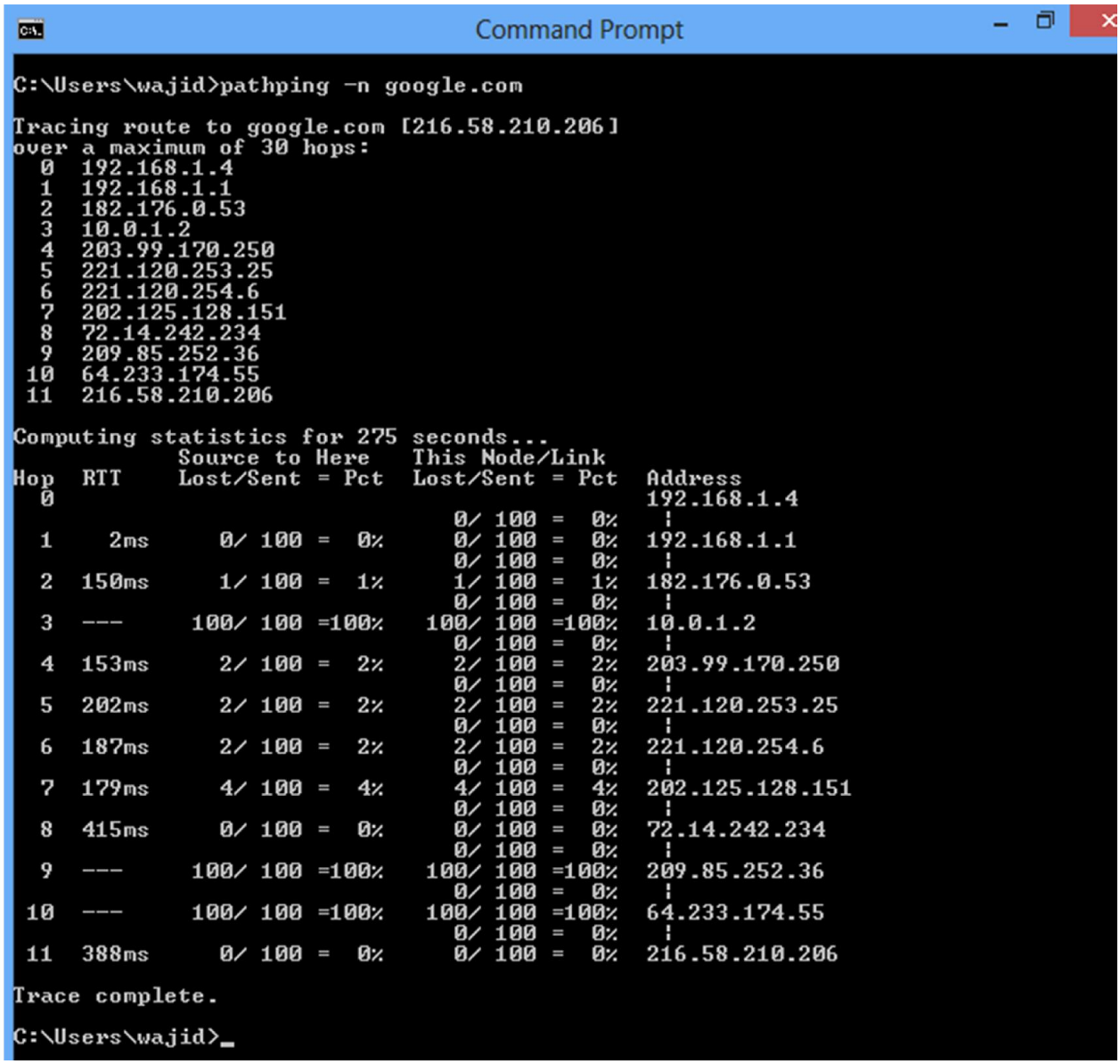
netstat /? : If you would like to see them all, type netstat /? for a complete listing and partial description (provided you have the background knowledge on what they imply).



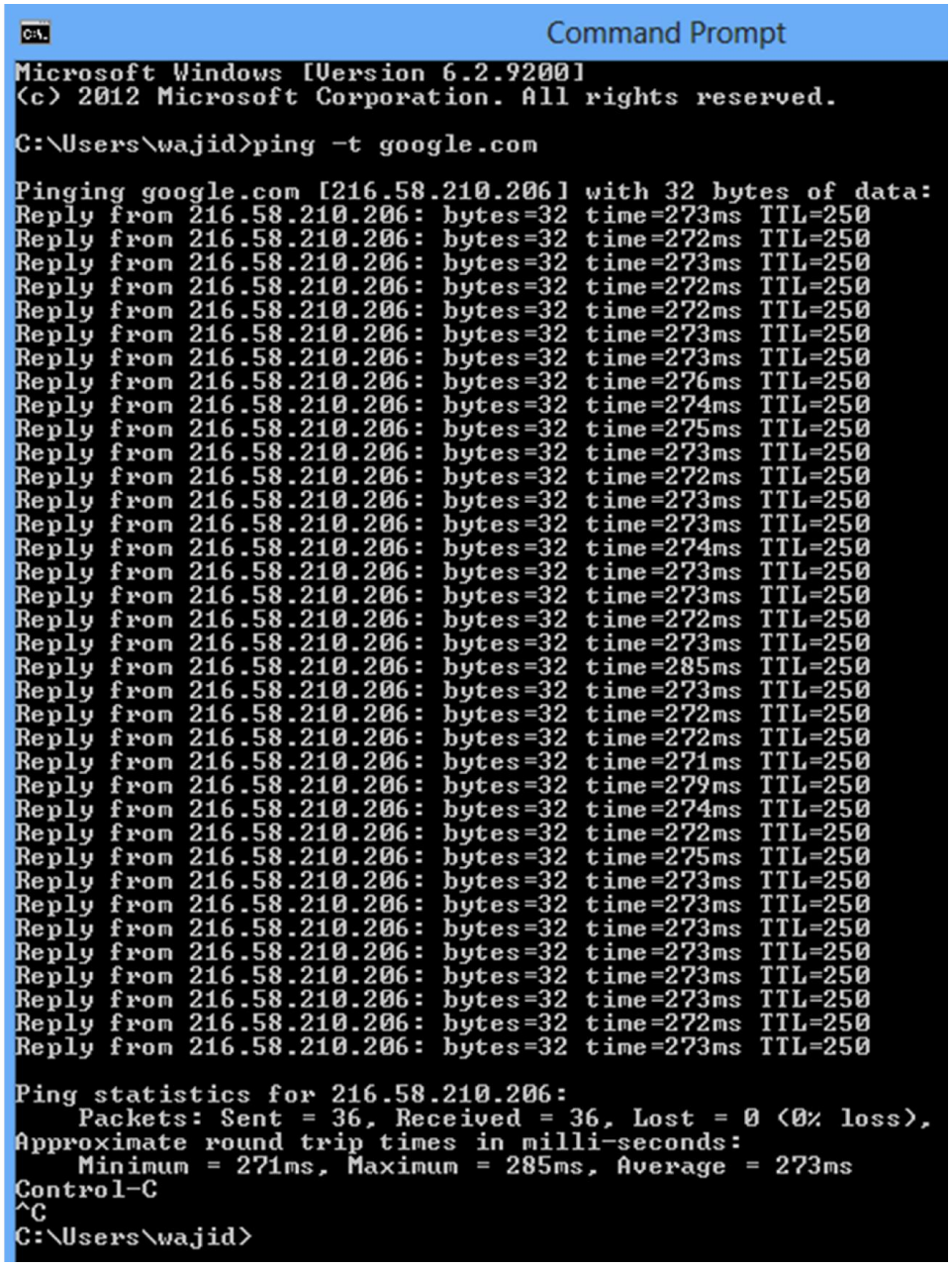
Tracert: trace a path



Pathping: for detail about packet forwarding and packet loss and each router and link in the path using pathping command.

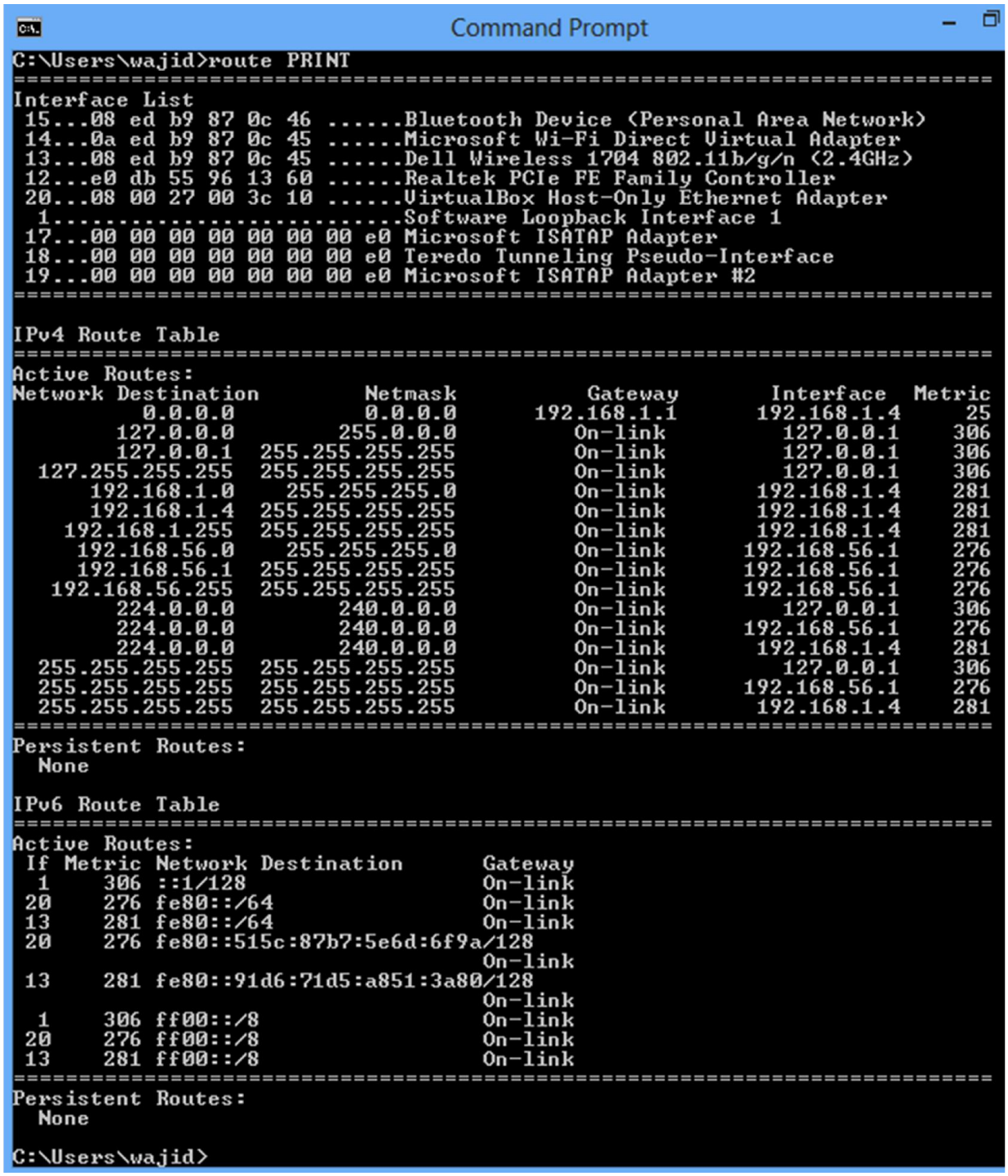


Ping: verifies and tests connectivity

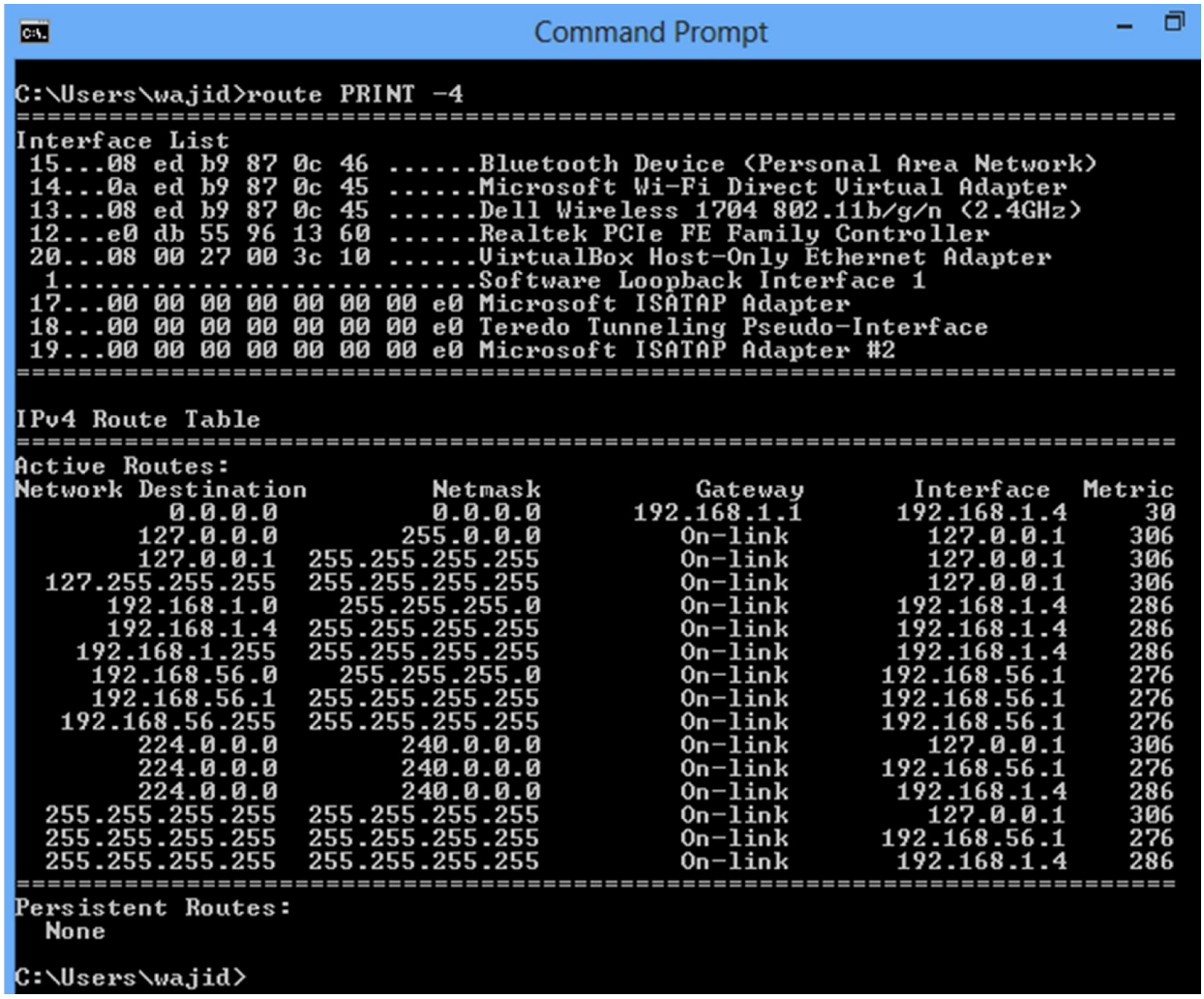


Ipconfig: Display the current tcp/ip configuration

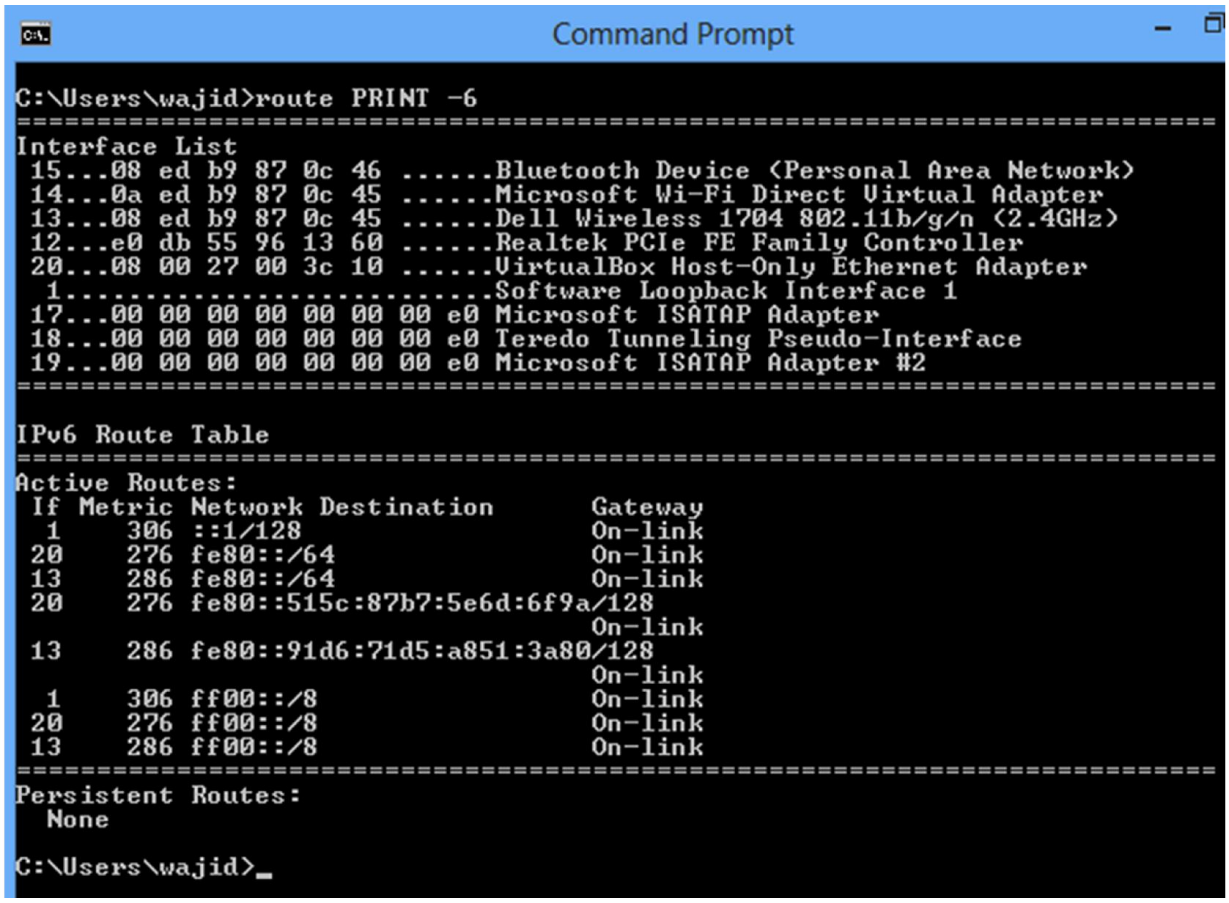
Route: Display or Modifies the local routing table


Command Prompt
C:\Users\wajid>route PRINT
Interface List
15...08 ed b9 87 0c 46 ......Bluetooth Device (Personal Area Network)
14...0a ed b9 87 0c 45 ......Microsoft Wi-Fi Direct Virtual Adapter
13...08 ed b9 87 0c 45 ......Dell Wireless 1704 802.11b/g/n (2.4GHz)
12...e0 db 55 96 13 60 ......Realtek PCIe FE Family Controller
20...08 00 27 00 3c 10 ......VirtualBox Host-Only Ethernet Adapter
1...........................Software Loopback Interface 1
17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
18...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
IPv4 Route Table
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.4 25
127.0.0.0 255.0.0.0 On-link 127.0.0.1 306
127.0.0.1 255.255.255.255 On-link 127.0.0.1 306
127.255.255.255 255.255.255.255 On-link 127.0.0.1 306
192.168.1.0 255.255.255.0 On-link 192.168.1.4 281
192.168.1.4 255.255.255.255 On-link 192.168.1.4 281
192.168.1.255 255.255.255.255 On-link 192.168.1.4 281
192.168.56.0 255.255.255.0 On-link 192.168.56.1 276
192.168.56.1 255.255.255.255 On-link 192.168.56.1 276
192.168.56.255 255.255.255.255 On-link 192.168.56.1 276
224.0.0.0 240.0.0.0 On-link 127.0.0.1 306
224.0.0.0 240.0.0.0 On-link 192.168.56.1 276
224.0.0.0 240.0.0.0 On-link 192.168.1.4 281
255.255.255.255 255.255.255.255 On-link 127.0.0.1 306
255.255.255.255 255.255.255.255 On-link 192.168.56.1 276
255.255.255.255 255.255.255.255 On-link 192.168.1.4 281
Persistent Routes:
None
IPv6 Route Table
Active Routes:
If Metric Network Destination Gateway
1 306 ::1/128 On-link
20 276 fe80::/64 On-link
13 281 fe80::/64 On-link
20 276 fe80::515c:87b7:5e6d:6f9a/128
On-link
13 281 fe80::91d6:71d5:a851:3a80/128
On-link
1 306 ff00::/8 On-link
20 276 ff00::/8 On-link
13 281 ff00::/8 On-link
Persistent Routes:
None
C:\Users\wajid>

Route -4 : only show the ipv4 table



Route -6 : only show the ipv6 routing table



Arp: Display the cache of locally IP address