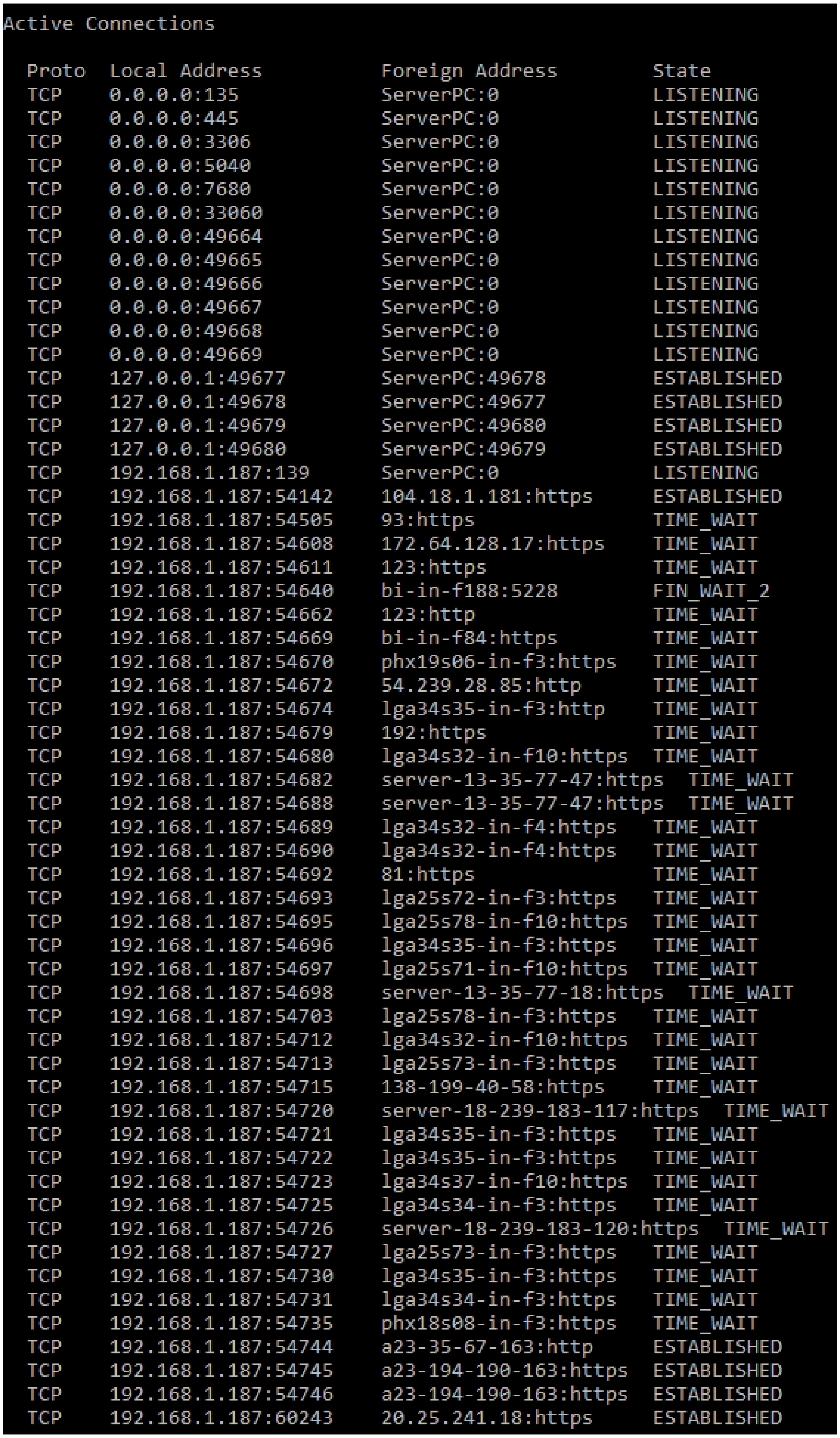
Lab 6 Step 6 Using netstat and ShieldsUp

Joshua Richardson

Step 1: netstat -a

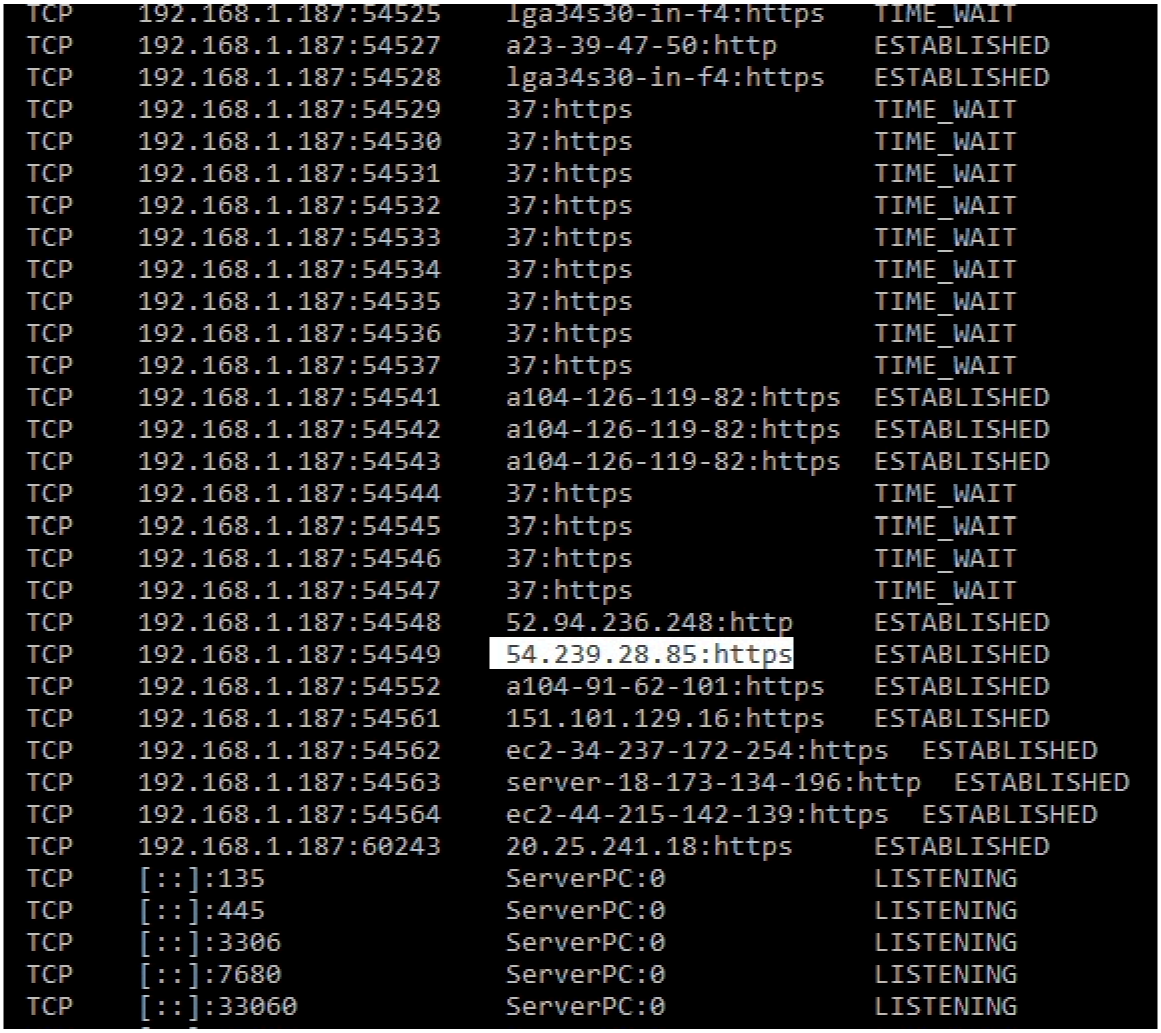
Running netstat -a returns a list of all TCP and UDP connections.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            ServerPC:0             LISTENING
  TCP    0.0.0.0:445            ServerPC:0             LISTENING
  TCP    0.0.0.0:3306           ServerPC:0             LISTENING
  TCP    0.0.0.0:5040           ServerPC:0             LISTENING
  TCP    0.0.0.0:7680           ServerPC:0             LISTENING
  TCP    0.0.0.0:33060          ServerPC:0             LISTENING
  TCP    0.0.0.0:49664          ServerPC:0             LISTENING
  TCP    0.0.0.0:49665          ServerPC:0             LISTENING
  TCP    0.0.0.0:49666          ServerPC:0             LISTENING
  TCP    0.0.0.0:49667          ServerPC:0             LISTENING
  TCP    0.0.0.0:49668          ServerPC:0             LISTENING
  TCP    0.0.0.0:49669          ServerPC:0             LISTENING
  TCP    127.0.0.1:49677        ServerPC:49678         ESTABLISHED
  TCP    127.0.0.1:49678        ServerPC:49677         ESTABLISHED
  TCP    127.0.0.1:49679        ServerPC:49680         ESTABLISHED
  TCP    127.0.0.1:49680        ServerPC:49679         ESTABLISHED
  TCP    192.168.1.187:139      ServerPC:0             LISTENING
  TCP    192.168.1.187:54142    104.18.1.181:https     ESTABLISHED
  TCP    192.168.1.187:54505    93:https               TIME_WAIT
  TCP    192.168.1.187:54608    172.64.128.17:https    TIME_WAIT
  TCP    192.168.1.187:54611    123:https              TIME_WAIT
  TCP    192.168.1.187:54640    bi-in-f188:5228        FIN_WAIT_2
  TCP    192.168.1.187:54662    123:http               TIME_WAIT
  TCP    192.168.1.187:54669    bi-in-f84:https        TIME_WAIT
  TCP    192.168.1.187:54670    phx19s06-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54672    54.239.28.85:http      TIME_WAIT
  TCP    192.168.1.187:54674    lga34s35-in-f3:http    TIME_WAIT
  TCP    192.168.1.187:54679    192:https              TIME_WAIT
  TCP    192.168.1.187:54680    lga34s32-in-f10:https  TIME_WAIT
  TCP    192.168.1.187:54682    server-13-35-77-47:https  TIME_WAIT
  TCP    192.168.1.187:54688    server-13-35-77-47:https  TIME_WAIT
  TCP    192.168.1.187:54689    lga34s32-in-f4:https   TIME_WAIT
  TCP    192.168.1.187:54690    lga34s32-in-f4:https   TIME_WAIT
  TCP    192.168.1.187:54692    81:https               TIME_WAIT
  TCP    192.168.1.187:54693    lga25s72-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54695    lga25s78-in-f10:https  TIME_WAIT
  TCP    192.168.1.187:54696    lga34s35-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54697    lga25s71-in-f10:https  TIME_WAIT
  TCP    192.168.1.187:54698    server-13-35-77-18:https  TIME_WAIT
  TCP    192.168.1.187:54703    lga25s78-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54712    lga34s32-in-f10:https  TIME_WAIT
  TCP    192.168.1.187:54713    lga25s73-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54715    138-199-40-58:https    TIME_WAIT
  TCP    192.168.1.187:54720    server-18-239-183-117:https  TIME_WAIT
  TCP    192.168.1.187:54721    lga34s35-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54722    lga34s35-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54723    lga34s37-in-f10:https  TIME_WAIT
  TCP    192.168.1.187:54725    lga34s34-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54726    server-18-239-183-120:https  TIME_WAIT
  TCP    192.168.1.187:54727    lga25s73-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54730    lga34s35-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54731    lga34s34-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54735    phx18s08-in-f3:https   TIME_WAIT
  TCP    192.168.1.187:54744    a23-35-67-163:http     ESTABLISHED
  TCP    192.168.1.187:54745    a23-194-190-163:https  ESTABLISHED
  TCP    192.168.1.187:54746    a23-194-190-163:https  ESTABLISHED
  TCP    192.168.1.187:60243    20.25.241.18:https     ESTABLISHED
```

Opening Firefox and going to Amazon and running the command again returns a connection to amazon, which is highlighted.

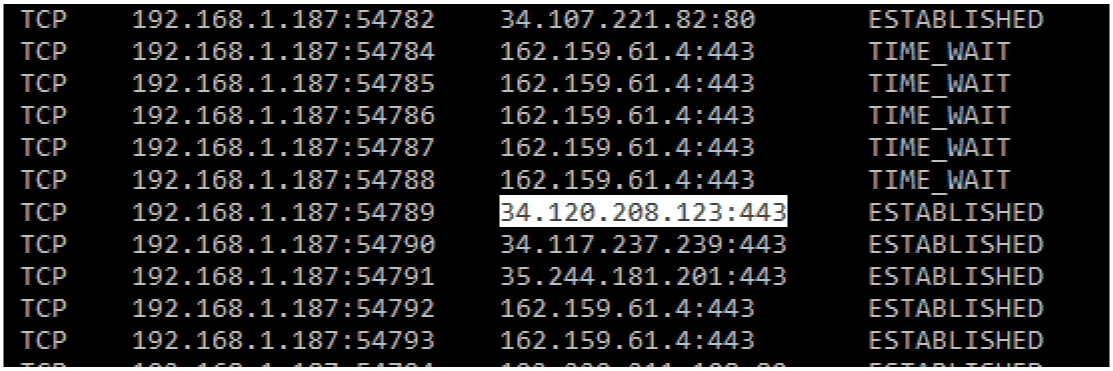


```
  TCP    192.168.1.187:54525    lga34s30-in-f4:https   TIME_WAIT
  TCP    192.168.1.187:54527    a23-39-47-50:http      ESTABLISHED
  TCP    192.168.1.187:54528    lga34s30-in-f4:https   ESTABLISHED
  TCP    192.168.1.187:54529    37:https               TIME_WAIT
  TCP    192.168.1.187:54530    37:https               TIME_WAIT
  TCP    192.168.1.187:54531    37:https               TIME_WAIT
  TCP    192.168.1.187:54532    37:https               TIME_WAIT
  TCP    192.168.1.187:54533    37:https               TIME_WAIT
  TCP    192.168.1.187:54534    37:https               TIME_WAIT
  TCP    192.168.1.187:54535    37:https               TIME_WAIT
  TCP    192.168.1.187:54536    37:https               TIME_WAIT
  TCP    192.168.1.187:54537    37:https               TIME_WAIT
  TCP    192.168.1.187:54541    a104-126-119-82:https  ESTABLISHED
  TCP    192.168.1.187:54542    a104-126-119-82:https  ESTABLISHED
  TCP    192.168.1.187:54543    a104-126-119-82:https  ESTABLISHED
  TCP    192.168.1.187:54544    37:https               TIME_WAIT
  TCP    192.168.1.187:54545    37:https               TIME_WAIT
  TCP    192.168.1.187:54546    37:https               TIME_WAIT
  TCP    192.168.1.187:54547    37:https               TIME_WAIT
  TCP    192.168.1.187:54548    52.94.236.248:http     ESTABLISHED
  TCP    192.168.1.187:54549    54.239.28.85:https     ESTABLISHED
  TCP    192.168.1.187:54552    a104-91-62-101:https   ESTABLISHED
  TCP    192.168.1.187:54561    151.101.129.16:https   ESTABLISHED
  TCP    192.168.1.187:54562    ec2-34-237-172-254:https  ESTABLISHED
  TCP    192.168.1.187:54563    server-18-173-134-196:http  ESTABLISHED
  TCP    192.168.1.187:54564    ec2-44-215-142-139:https  ESTABLISHED
  TCP    192.168.1.187:60243    20.25.241.18:https     ESTABLISHED
  TCP    [::]:135               ServerPC:0             LISTENING
  TCP    [::]:445               ServerPC:0             LISTENING
  TCP    [::]:3306              ServerPC:0             LISTENING
  TCP    [::]:7680              ServerPC:0             LISTENING
  TCP    [::]:33060             ServerPC:0             LISTENING
```

		Comments
Protocol	TCP	Protocol used
Local Address	192.168.1.187	Client’s local address
Local Port	54549	Port used by the client locally
Foreign Address	54.239.28.85	Remote IP address
Remote Port	443	Remote port
Remote Application	HTTPS	HTTPS server
Status	Established	The connection is running

Step 2: netstat -na

Running netstat -na returns a list of all the networks, but using IP addresses instead of names.



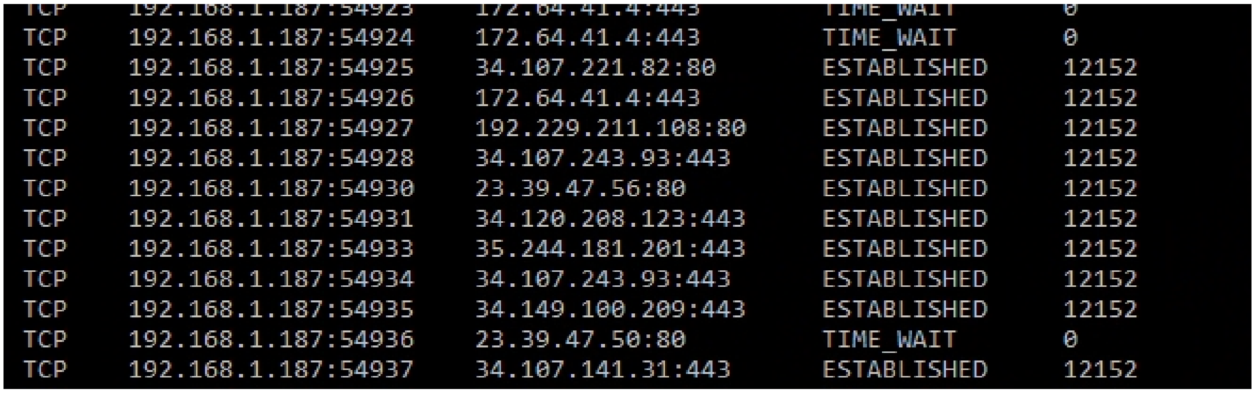
```
TCP    192.168.1.187:54782    34.107.221.82:80       ESTABLISHED
TCP    192.168.1.187:54784    162.159.61.4:443       TIME_WAIT
TCP    192.168.1.187:54785    162.159.61.4:443       TIME_WAIT
TCP    192.168.1.187:54786    162.159.61.4:443       TIME_WAIT
TCP    192.168.1.187:54787    162.159.61.4:443       TIME_WAIT
TCP    192.168.1.187:54788    162.159.61.4:443       TIME_WAIT
TCP    192.168.1.187:54789    34.120.208.123:443     ESTABLISHED
TCP    192.168.1.187:54790    34.117.237.239:443     ESTABLISHED
TCP    192.168.1.187:54791    35.244.181.201:443     ESTABLISHED
TCP    192.168.1.187:54792    162.159.61.4:443       ESTABLISHED
TCP    192.168.1.187:54793    162.159.61.4:443       ESTABLISHED
```

		Comments
Protocol	TCP	Protocol used
Local Address	192.168.1.187	Client's local address
Local Port	54789	Port used by the client locally
Foreign Address	34.120.208.123	Remote IP address
Remote Port	443	Remote port
Remote Application	HTTPS	HTTPS server
Status	Established	The connection is running

This appears to be from Google, as looking it up returns information about it being used for googleusercontent. The foreign address shown when running netstat -a is "192:https"

Step 3: netstat -ano

Running netstat -ano returns the same thing as netstat -an, but it includes the PID column, which displays the process id of the application using it.



```
TCP    192.168.1.187:54923    172.64.41.4:443        TIME_WAIT       0
TCP    192.168.1.187:54924    172.64.41.4:443        TIME_WAIT       0
TCP    192.168.1.187:54925    34.107.221.82:80       ESTABLISHED     12152
TCP    192.168.1.187:54926    172.64.41.4:443        ESTABLISHED     12152
TCP    192.168.1.187:54927    192.229.211.108:80     ESTABLISHED     12152
TCP    192.168.1.187:54928    34.107.243.93:443      ESTABLISHED     12152
TCP    192.168.1.187:54930    23.39.47.56:80         ESTABLISHED     12152
TCP    192.168.1.187:54931    34.120.208.123:443     ESTABLISHED     12152
TCP    192.168.1.187:54933    35.244.181.201:443     ESTABLISHED     12152
TCP    192.168.1.187:54934    34.107.243.93:443      ESTABLISHED     12152
TCP    192.168.1.187:54935    34.149.100.209:443     ESTABLISHED     12152
TCP    192.168.1.187:54936    23.39.47.50:80         TIME_WAIT       0
TCP    192.168.1.187:54937    34.107.141.31:443      ESTABLISHED     12152
```

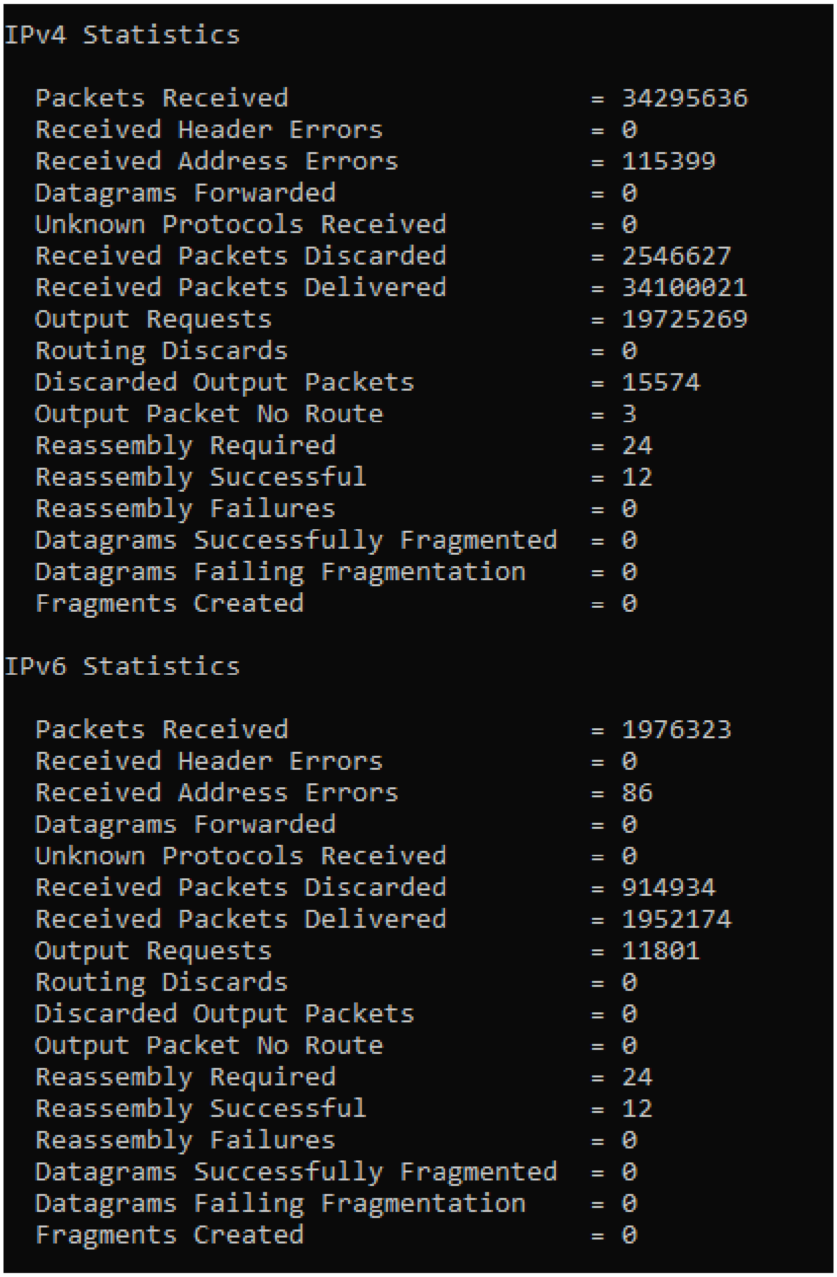
12152 is one of the PIDs for Firefox, obviously Firefox uses many PIDs as there are 10 of them listed on Task Manager.

Step 4: Remote Connections

I used my computer that I use to host game servers for this lab. I was remotely connected to it from school, so there are some connections used for that. My mom works from home and she does a lot of networking for her job (programming wireless security cameras), so I'm sure there are many connections that are involved there.

Step 5: netstat -e

This prints the network statistics for the computer.



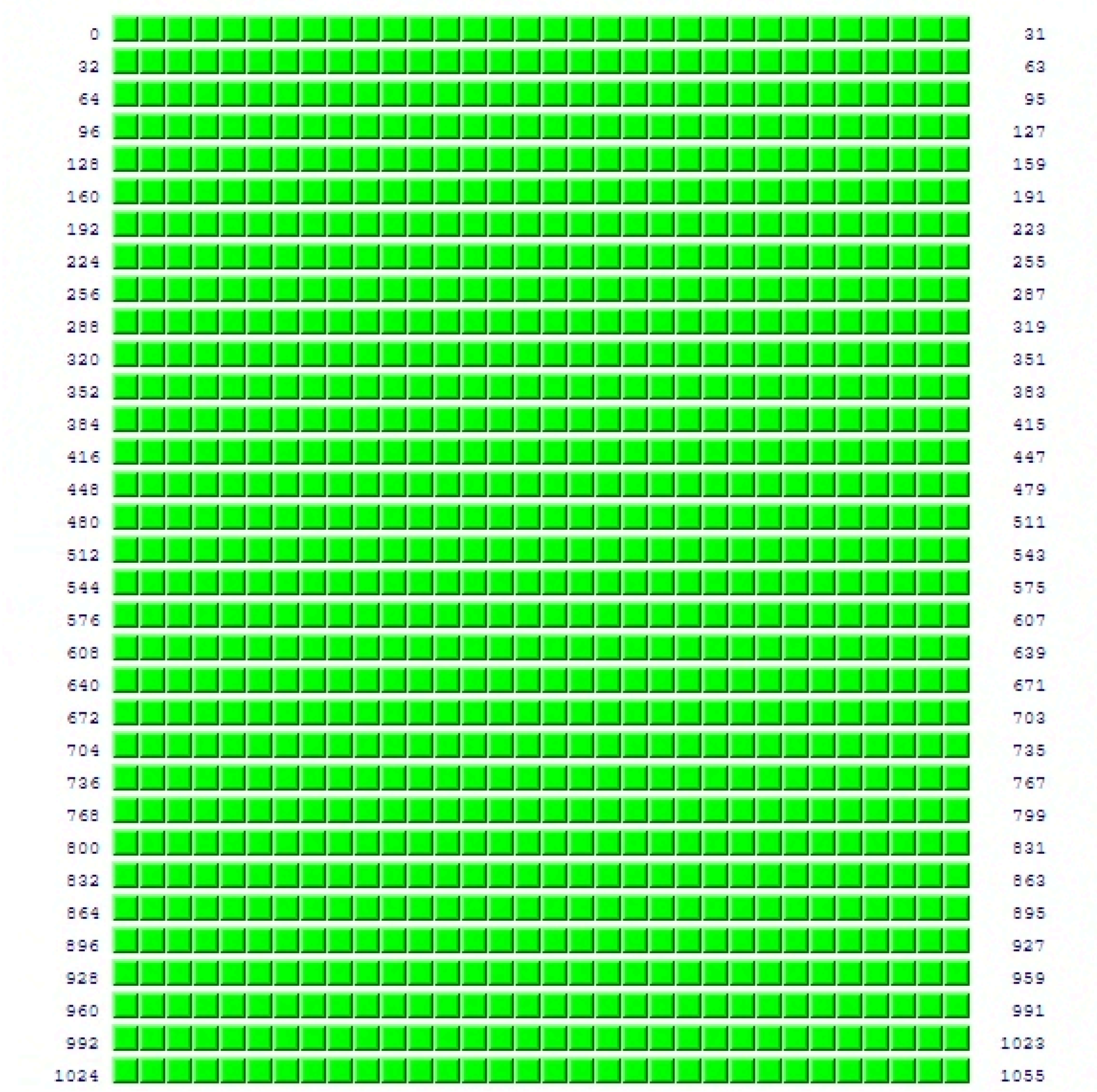
```
IPv4 Statistics

  Packets Received                   = 34295636
  Received Header Errors             = 0
  Received Address Errors            = 115399
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 2546627
  Received Packets Delivered         = 34100021
  Output Requests                    = 19725269
  Routing Discards                   = 0
  Discarded Output Packets           = 15574
  Output Packet No Route             = 3
  Reassembly Required                = 24
  Reassembly Successful              = 12
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 1976323
  Received Header Errors             = 0
  Received Address Errors            = 86
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 914934
  Received Packets Delivered         = 1952174
  Output Requests                    = 11801
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 24
  Reassembly Successful              = 12
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

Step 6: ShieldsUP



```
   0 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩   31
  32 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩   63
  64 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩   95
  96 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  127
 128 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  159
 160 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  191
 192 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  223
 224 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  255
 256 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  287
 288 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  319
 320 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  351
 352 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  383
 384 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  415
 416 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  447
 448 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  479
 480 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  511
 512 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  543
 544 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  575
 576 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  607
 608 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  639
 640 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  671
 672 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  703
 704 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  735
 736 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  767
 768 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  799
 800 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  831
 832 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  863
 864 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  895
 896 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  927
 928 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  959
 960 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩  991
 992 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩 1023
1024 🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩 1055
```

All of the scanned ports are all green. I know for a fact that I have the ports 27015, 25565, and 7777 open, but those weren’t scanned, as those are used for servers I host.