



UNITECH
TIC-HAÏTI-BRH

Gestion de Risques Informatiques

Austin Waffo Kouhoué

Marie France Logea DORCIN
logeadorcinmf@gmail.com

Nestat est un outil puissant pour surveiller les connexions réseau, les ports ouverts et les statistiques réseaux

netstat help

```
Command Prompt
C:\Users\DELL>netstat help

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables 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.
-c          Displays a list of processes sorted by the number of TCP or UDP
           ports currently consumed.
-d          Displays DSCP value associated with each connection.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-i          Displays the time spent by a TCP connection in its current state.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
```

1. Lister toutes les connexions réseau actives

```
Command Prompt  Windows PowerShell
C:\Users\DELL>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              Mayoooh509:0           LISTENING
TCP   0.0.0.0:445              Mayoooh509:0           LISTENING
TCP   0.0.0.0:5040             Mayoooh509:0           LISTENING
TCP   0.0.0.0:7070             Mayoooh509:0           LISTENING
TCP   0.0.0.0:49664            Mayoooh509:0           LISTENING
TCP   0.0.0.0:49665            Mayoooh509:0           LISTENING
TCP   0.0.0.0:49666            Mayoooh509:0           LISTENING
TCP   0.0.0.0:49667            Mayoooh509:0           LISTENING
TCP   0.0.0.0:49668            Mayoooh509:0           LISTENING
TCP   0.0.0.0:49671            Mayoooh509:0           LISTENING
TCP   127.0.0.1:60223          Mayoooh509:0           LISTENING
TCP   192.168.1.188:139        Mayoooh509:0           LISTENING
TCP   192.168.1.188:60083      relay-718abfda:https   ESTABLISHED
TCP   192.168.1.188:60180      20.116.248.103:https   ESTABLISHED
TCP   192.168.1.188:60183      172.172.255.218:https  ESTABLISHED
TCP   192.168.1.188:60194      vz-in-f188:5228        ESTABLISHED
TCP   192.168.1.188:60201      4.172.11.173:https     ESTABLISHED
TCP   192.168.1.188:60210      149.154.175.51:https   ESTABLISHED
TCP   192.168.1.188:60601      a23-204-77-189:https   CLOSE_WAIT
TCP   192.168.1.188:60834      20.169.174.231:https   ESTABLISHED
TCP   192.168.1.188:60986      172.64.155.209:https   ESTABLISHED
TCP   192.168.1.188:60987      104.18.32.47:https     ESTABLISHED
TCP   192.168.1.188:60992      a23-50-112-5:https     ESTABLISHED
TCP   192.168.1.188:60993      a23-50-112-9:https     ESTABLISHED
```

2. Identifier les connexions établies

```
C:\Users\DELL>netstat -a | findstr ESTABLISHED
TCP   192.168.1.188:60083      relay-718abfda:https   ESTABLISHED
TCP   192.168.1.188:60180      20.116.248.103:https   ESTABLISHED
TCP   192.168.1.188:60183      172.172.255.218:https  ESTABLISHED
TCP   192.168.1.188:60201      4.172.11.173:https     ESTABLISHED
TCP   192.168.1.188:60210      149.154.175.51:https   ESTABLISHED
TCP   192.168.1.188:61015      20.169.174.231:https   ESTABLISHED
TCP   192.168.1.188:61016      ua-in-f188:5228        ESTABLISHED
TCP   192.168.1.188:61019      52.96.189.18:https     ESTABLISHED
TCP   192.168.1.188:61052      172.64.155.209:https   ESTABLISHED
TCP   192.168.1.188:61053      104.18.32.47:https     ESTABLISHED
```

3. Identifier les ports en écoute

```
C:\Users\DELL>netstat -a | findstr LISTENING
TCP    0.0.0.0:135           Mayoooh509:0      LISTENING
TCP    0.0.0.0:445           Mayoooh509:0      LISTENING
TCP    0.0.0.0:5040          Mayoooh509:0      LISTENING
TCP    0.0.0.0:7070          Mayoooh509:0      LISTENING
TCP    0.0.0.0:7680          Mayoooh509:0      LISTENING
TCP    0.0.0.0:49664         Mayoooh509:0      LISTENING
TCP    0.0.0.0:49665         Mayoooh509:0      LISTENING
TCP    0.0.0.0:49666         Mayoooh509:0      LISTENING
TCP    0.0.0.0:49667         Mayoooh509:0      LISTENING
TCP    0.0.0.0:49668         Mayoooh509:0      LISTENING
TCP    0.0.0.0:49671         Mayoooh509:0      LISTENING
TCP    127.0.0.1:60223       Mayoooh509:0      LISTENING
TCP    192.168.1.188:139     Mayoooh509:0      LISTENING
```

4. Afficher les connexions avec les noms des processus

```
Administrator: Command Prompt

C:\Windows\System32>netstat -b -o

Active Connections

  Proto Local Address          Foreign Address         State       PID
  TCP    192.168.1.188:60601     a23-204-77-189:https    CLOSE_WAIT 13128
[backgroundTaskHost.exe]
  TCP    192.168.1.188:61015     20.169.174.231:https    ESTABLISHED 15452
[msedge.exe]
  TCP    192.168.1.188:61016     ua-in-f188:5228        ESTABLISHED 8984
[chrome.exe]
  TCP    192.168.1.188:61095     149.154.175.51:https    ESTABLISHED 6800
[Telegram.exe]
  TCP    192.168.1.188:61099     4.172.11.173:https      ESTABLISHED 4432
[ms-teams.exe]
  TCP    192.168.1.188:61101     172.64.155.209:https    ESTABLISHED 8984
[chrome.exe]
  TCP    192.168.1.188:61109     20.116.248.103:https    ESTABLISHED 16400
[msedgewebview2.exe]
  TCP    192.168.1.188:61110     relay-53f849aa:https    ESTABLISHED 4200
[AnyDesk.exe]
  TCP    192.168.1.188:61112     172.64.155.209:https    ESTABLISHED 8984
[chrome.exe]
  TCP    192.168.1.188:61119     172.172.255.218:https    ESTABLISHED 4780
WpnService
[svchost.exe]
  TCP    192.168.1.188:61129     52.96.189.18:https      TIME_WAIT   0
  TCP    192.168.1.188:61132     mia07s54-in-f3:https    TIME_WAIT   0
  TCP    192.168.1.188:61133     a23-50-112-5:https      ESTABLISHED 9620
```

5. Afficher les statistiques réseaux

```
C:\Users\DELL>netstat -e
Interface Statistics

  Received Sent
  Bytes 567893392 171987168
  Unicast packets 652808 374288
  Non-unicast packets 90232 12728
  Discards 0 0
  Errors 0 0
  Unknown protocols 0
```


6 Afficher la table de routage

Voir les routes utilisées par mon PC pour communiquer avec d’autres réseaux.

```
Command Prompt
Windows PowerShell

C:\Users\DELL>netstat -r

=====
Interface List
=====
15...6c 2b 59 6e 12 7e .....Realtek PCIe GbE Family Controller
6...0a 00 27 00 00 06 .....VirtualBox Host-Only Ethernet Adapter
11...                .....Microsoft Wi-Fi Direct Virtual Adapter
8..                  .....Microsoft Wi-Fi Direct Virtual Adapter #2
17..                 .....Intel(R) Wireless-AC 9560
19.....              .....Bluetooth Device (Personal Area Network)
1.....              .....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                  0.0.0.0          192.168.1.1      192.168.1.188     50
127.0.0.0                255.0.0.0         On-link          127.0.0.1         331
127.0.0.1                255.255.255.255   On-link          127.0.0.1         331
127.255.255.255          255.255.255.255   On-link          127.0.0.1         331
192.168.1.0              255.255.255.0     On-link          192.168.1.188     306
192.168.1.188            255.255.255.255   On-link          192.168.1.188     306
192.168.1.255            255.255.255.255   On-link          192.168.1.188     306
192.168.56.0              255.255.255.0     On-link          192.168.56.1      281
192.168.56.1            255.255.255.255   On-link          192.168.56.1      281
192.168.56.255           255.255.255.255   On-link          192.168.56.1      281
224.0.0.0                240.0.0.0         On-link          127.0.0.1         331
224.0.0.0                240.0.0.0         On-link          192.168.56.1      281
224.0.0.0                240.0.0.0         On-link          192.168.1.188     306
255.255.255.255          255.255.255.255   On-link          127.0.0.1         331
255.255.255.255          255.255.255.255   On-link          192.168.56.1      281
255.255.255.255          255.255.255.255   On-link          192.168.1.188     306
```

```
IPv6 Route Table
=====
Active Routes:
If Metric Network Destination Gateway
-----
1 331 ::1/128 On-link
6 281 fe80::/64 On-link
17 306 fe80::/64 On-link
17 306 fe80::2fd3:37d0:e206:32e4/128 On-link
6 281 fe80::d309:9dda:7327:52d0/128 On-link
1 331 ff00::/8 On-link
6 281 ff00::/8 On-link
17 306 ff00::/8 On-link

Persistent Routes:
None
```

7 Actualiser l’affichage en temps réel

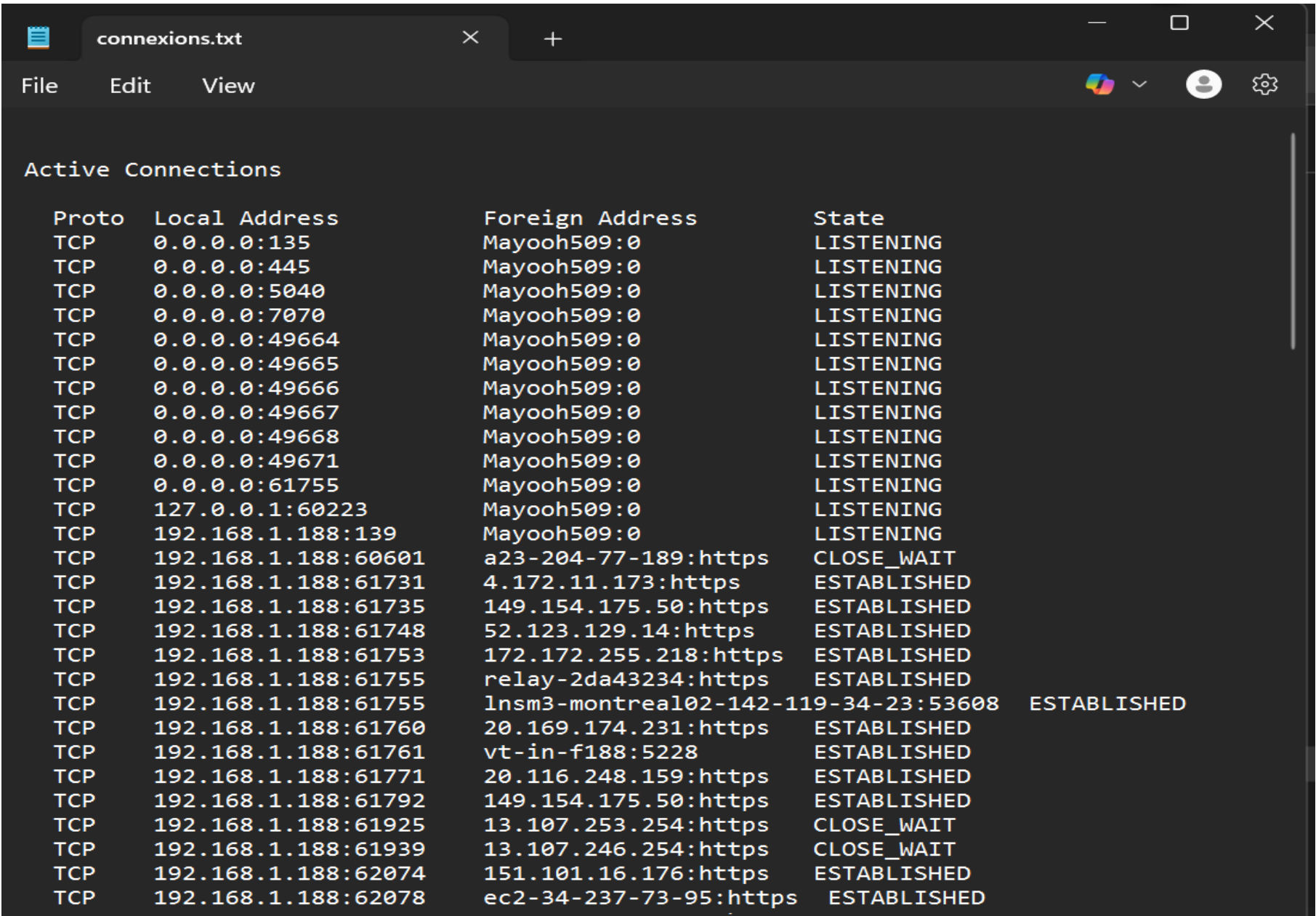
```
Command Prompt
Windows PowerShell

C:\Users\DELL>netstat -a 5

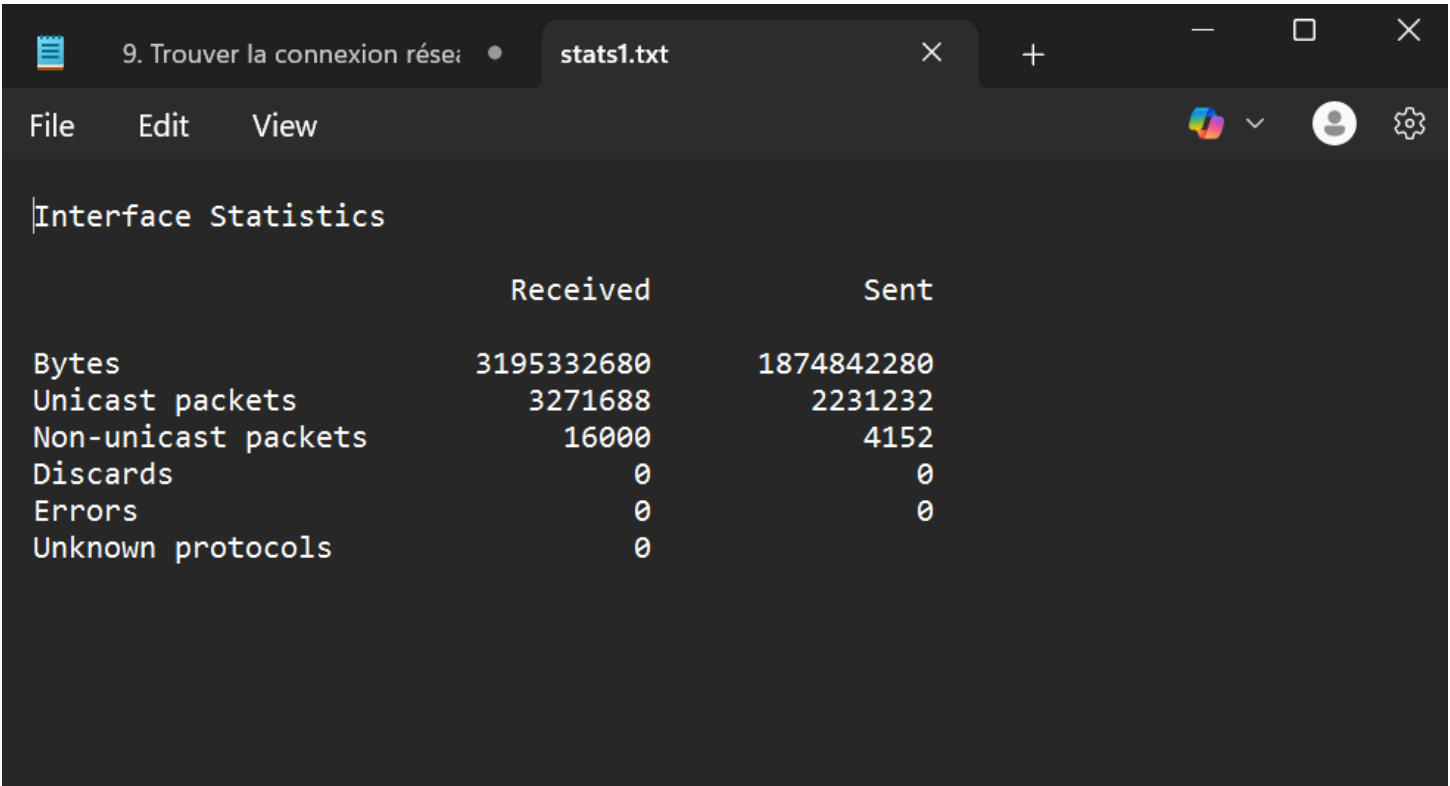
Active Connections

Proto Local Address          Foreign Address         State
----
TCP 0.0.0.0:135             Mayoooh509:0           LISTENING
TCP 0.0.0.0:445             Mayoooh509:0           LISTENING
TCP 0.0.0.0:5040            Mayoooh509:0           LISTENING
TCP 0.0.0.0:7070            Mayoooh509:0           LISTENING
TCP 0.0.0.0:7680            Mayoooh509:0           LISTENING
TCP 0.0.0.0:49664           Mayoooh509:0           LISTENING
TCP 0.0.0.0:49665           Mayoooh509:0           LISTENING
TCP 0.0.0.0:49666           Mayoooh509:0           LISTENING
TCP 0.0.0.0:49667           Mayoooh509:0           LISTENING
TCP 0.0.0.0:49668           Mayoooh509:0           LISTENING
TCP 0.0.0.0:49671           Mayoooh509:0           LISTENING
TCP 127.0.0.1:60223         Mayoooh509:0           LISTENING
TCP 192.168.1.188:139        Mayoooh509:0           LISTENING
TCP 192.168.1.188:60601     a23-204-77-189:https   CLOSE_WAIT
TCP 192.168.1.188:61015     20.169.174.231:https   ESTABLISHED
TCP 192.168.1.188:61016     ua-in-f188:5228        ESTABLISHED
TCP 192.168.1.188:61095     149.154.175.51:https   ESTABLISHED
TCP 192.168.1.188:61099     4.172.11.173:https     ESTABLISHED
TCP 192.168.1.188:61109     20.116.248.103:https   ESTABLISHED
TCP 192.168.1.188:61110     relay-53f849aa:https   ESTABLISHED
TCP 192.168.1.188:61119     172.172.255.218:https  ESTABLISHED
TCP 192.168.1.188:61133     a23-50-112-5:https     CLOSE_WAIT
TCP 192.168.1.188:61141     13.107.246.40:https    CLOSE_WAIT
TCP 192.168.1.188:61240     20.189.173.25:https    TIME_WAIT
TCP 192.168.1.188:61244     104.18.32.47:https     ESTABLISHED
```

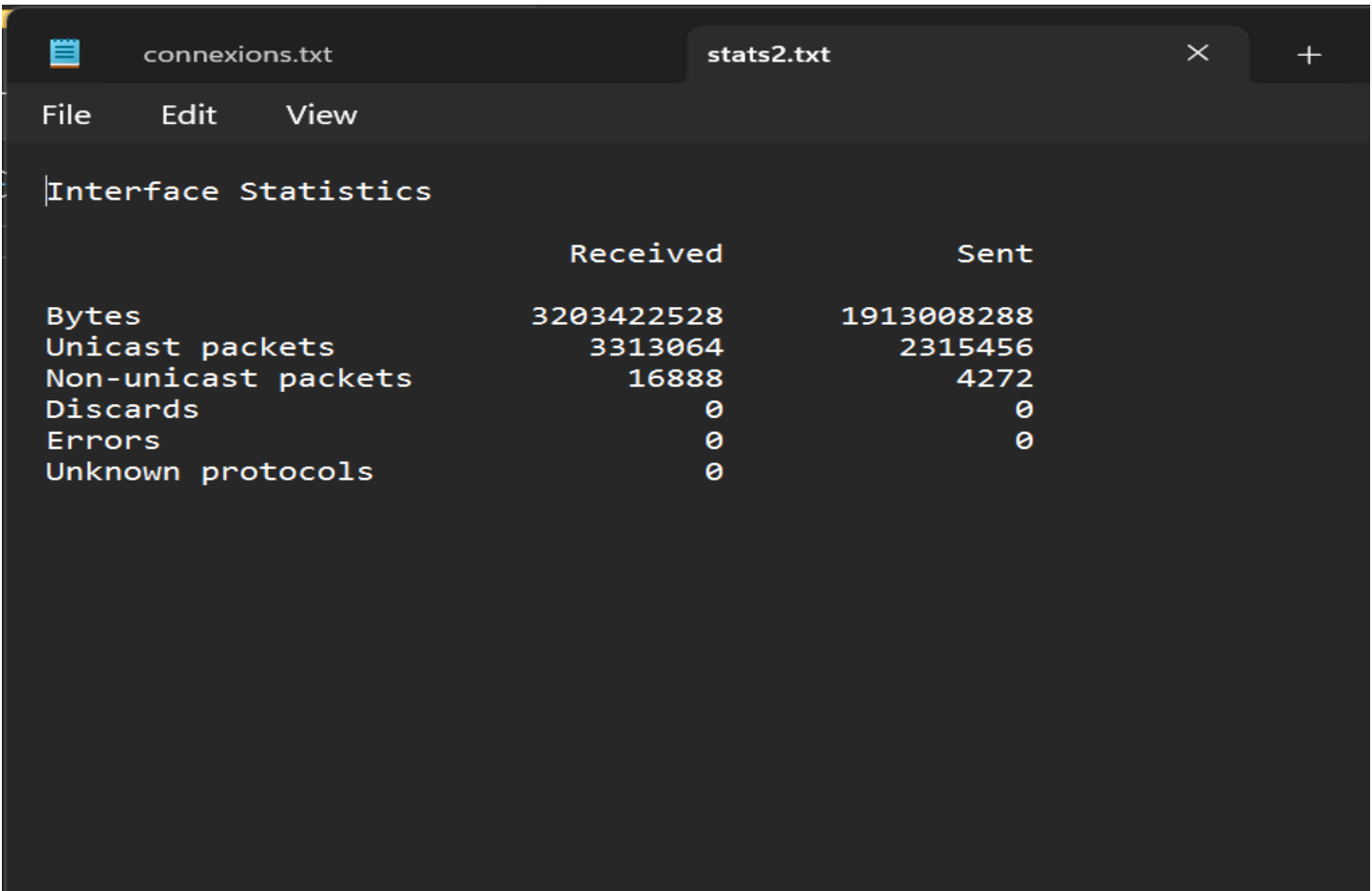
8. Lister les connexions réseau et exporter les résultats
netstat -a > connexions.txt



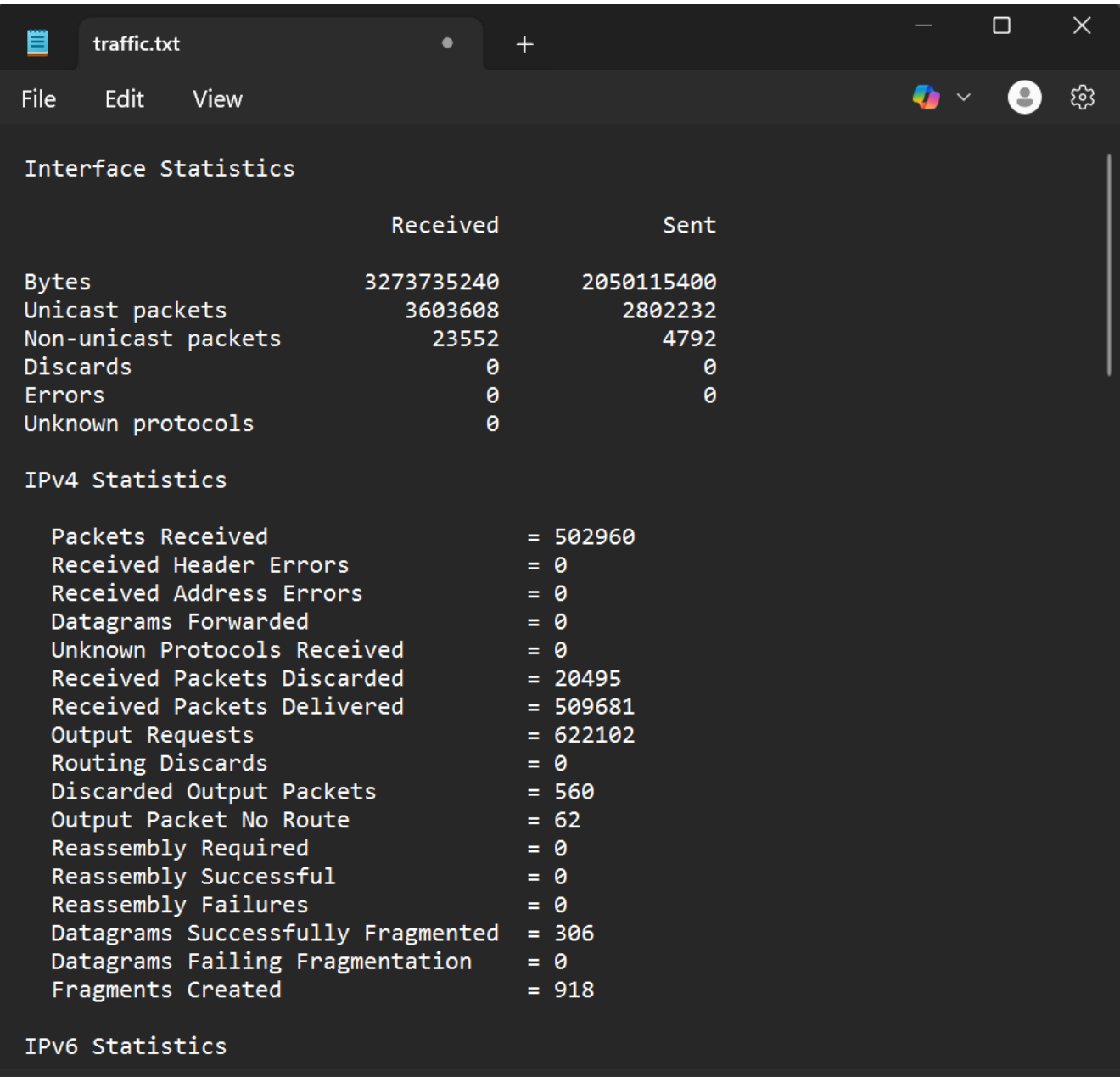
9. Trouver la connexion réseau la plus active
a) netstat -e > stats1.txt



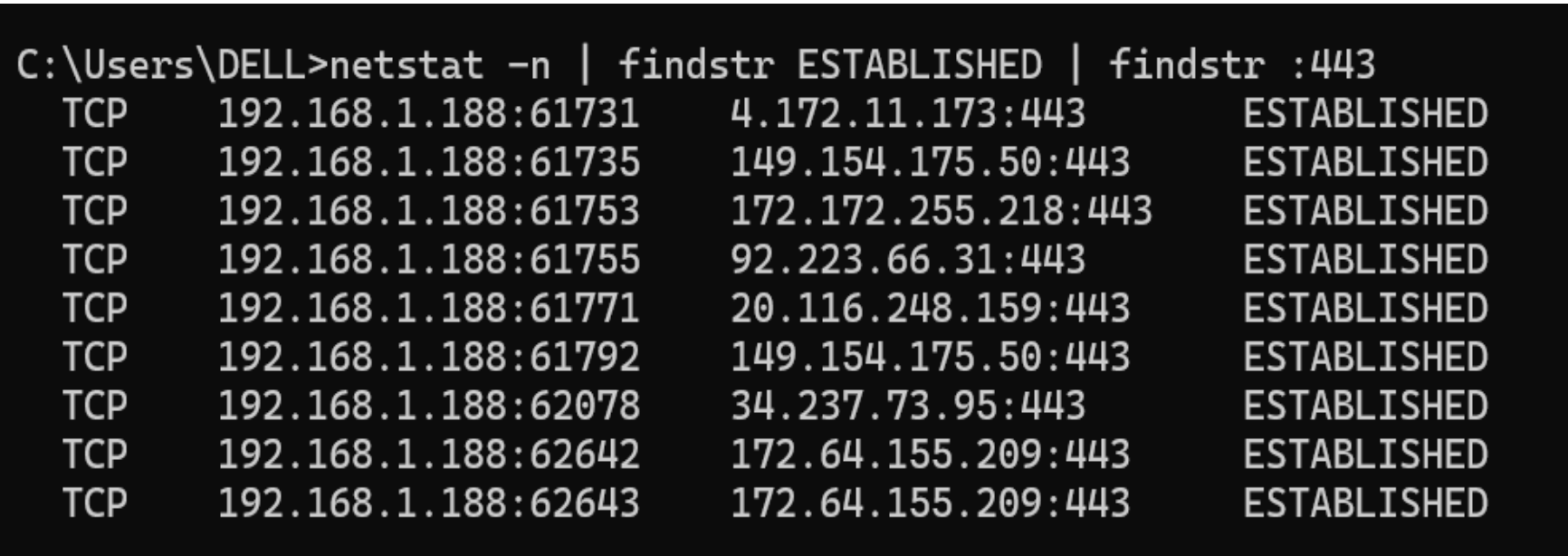
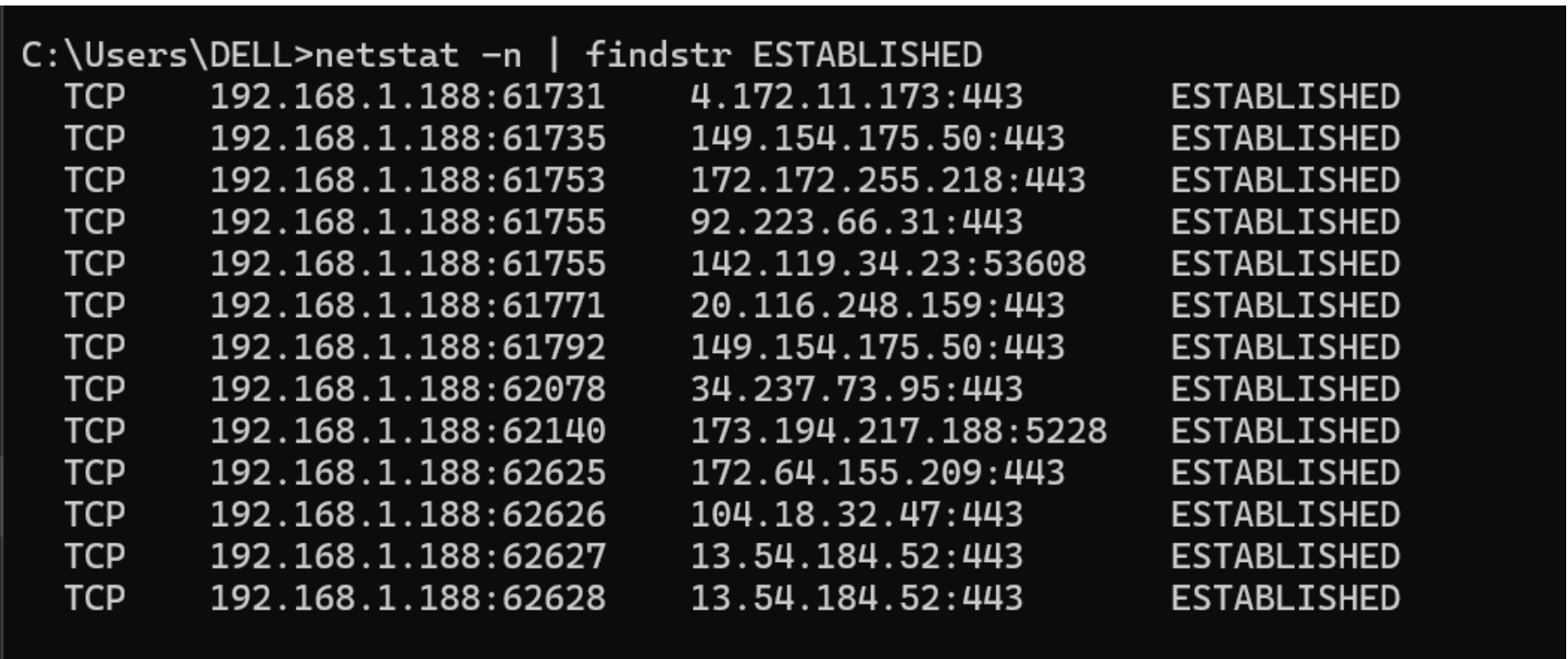
b) netstat -e > stats2.txt



Identifier connexion génère le plus de trafic
c) netstat -e -s > traffic.txt



10. Trouver si une machine du réseau envoie trop de requêtes



Je peux conclure que ce devoir sur les commandes de netstat démontre l'importance cruciale de la surveillance réseau dans un contexte de sécurité informatique.