UNITECH
TIC-HAITI-BRH

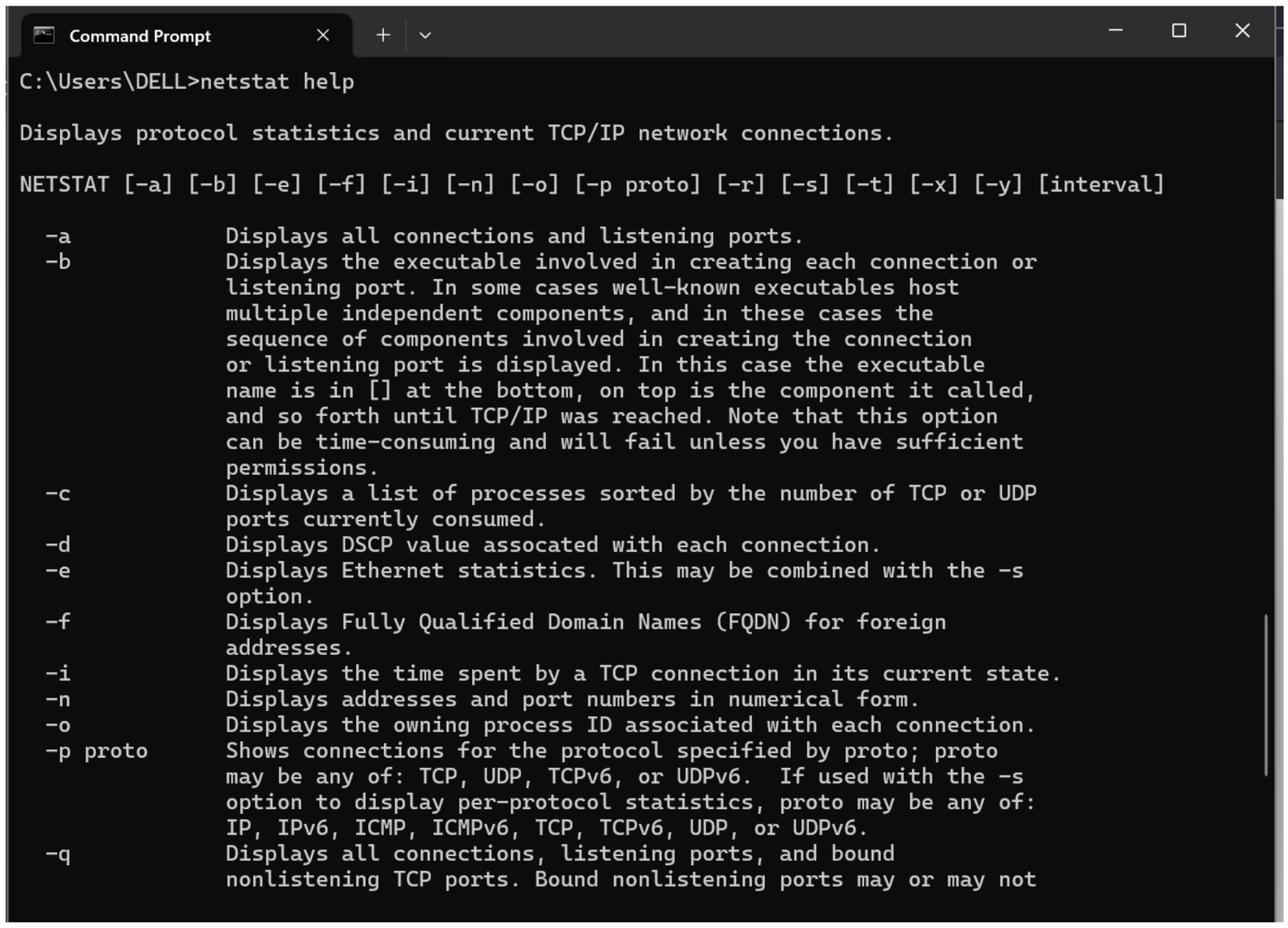
Gestion de Risques Informatiques

Austin Waffo Kouhoué

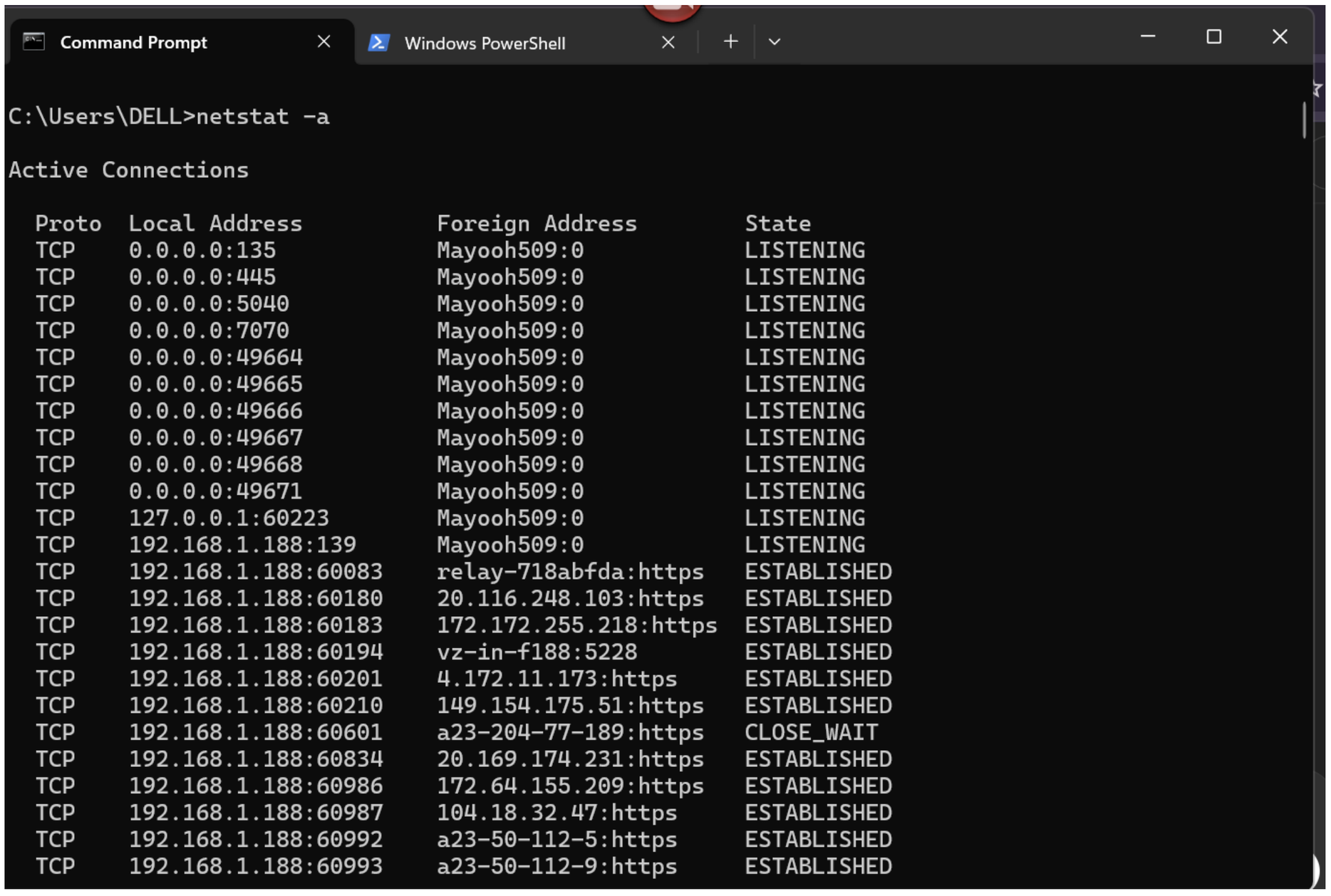
Marie France Logea DORCIN
logeadorcinmf@gmail.com

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

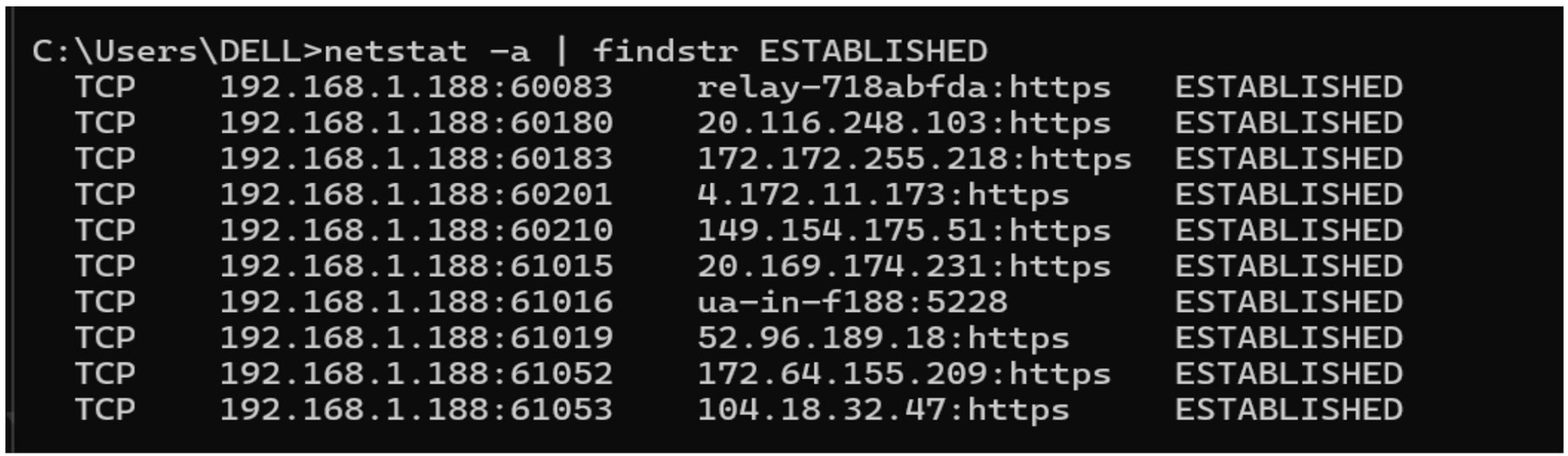
netstat help



1. Lister toutes les connexions réseau actives



2. Identifier les connexions établies



3. Identifier les ports en écoute

```
C:\Users\DELL>netstat -a | findstr LISTENING
  TCP    0.0.0.0:135            Mayooh509:0            LISTENING
  TCP    0.0.0.0:445            Mayooh509:0            LISTENING
  TCP    0.0.0.0:5040           Mayooh509:0            LISTENING
  TCP    0.0.0.0:7070           Mayooh509:0            LISTENING
  TCP    0.0.0.0:7680           Mayooh509:0            LISTENING
  TCP    0.0.0.0:49664          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49665          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49666          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49667          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49668          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49671          Mayooh509:0            LISTENING
  TCP    127.0.0.1:60223        Mayooh509:0            LISTENING
  TCP    192.168.1.188:139      Mayooh509:0            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

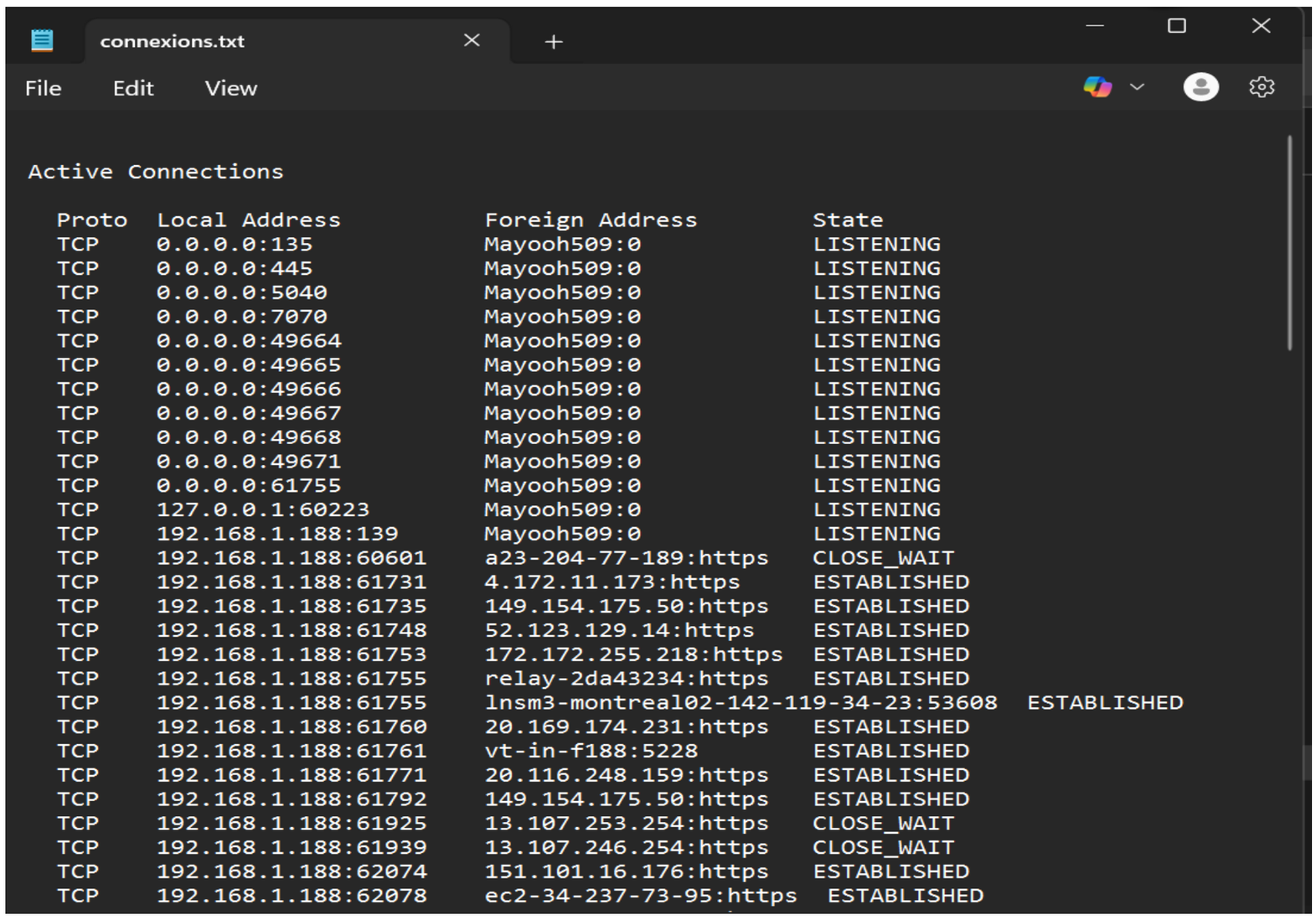
Voir les routes utilisées par mon PC pour communiquer avec d'autres réseaux.

```
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.. [redacted] .....Microsoft Wi-Fi Direct Virtual Adapter
  8.. [redacted] .....Microsoft Wi-Fi Direct Virtual Adapter #2
 17.. [redacted] .....Intel(R) Wireless-AC 9560
 19.. [redacted] .....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
```

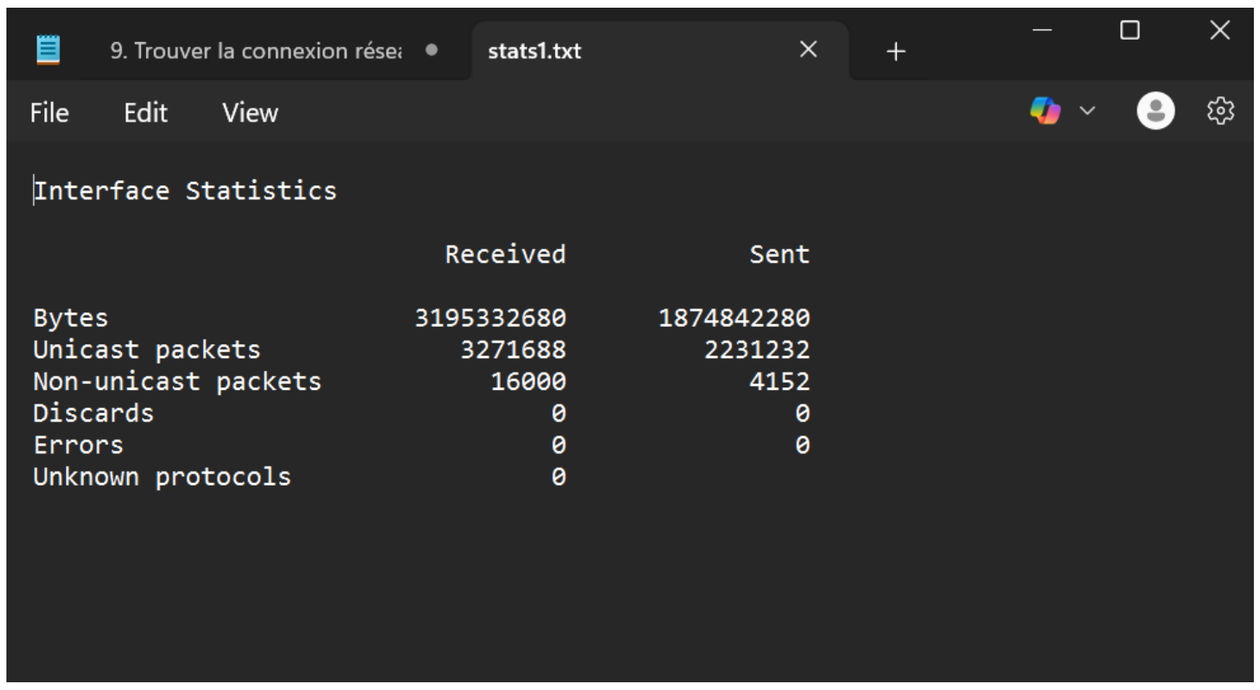
7 Actualiser l'affichage en temps réel

```
Command Prompt    Windows PowerShell

C:\Users\DELL>netstat -a 5

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Mayooh509:0            LISTENING
  TCP    0.0.0.0:445            Mayooh509:0            LISTENING
  TCP    0.0.0.0:5040           Mayooh509:0            LISTENING
  TCP    0.0.0.0:7070           Mayooh509:0            LISTENING
  TCP    0.0.0.0:7680           Mayooh509:0            LISTENING
  TCP    0.0.0.0:49664          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49665          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49666          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49667          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49668          Mayooh509:0            LISTENING
  TCP    0.0.0.0:49671          Mayooh509:0            LISTENING
  TCP    127.0.0.1:60223        Mayooh509:0            LISTENING
  TCP    192.168.1.188:139      Mayooh509:0            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
^C
```

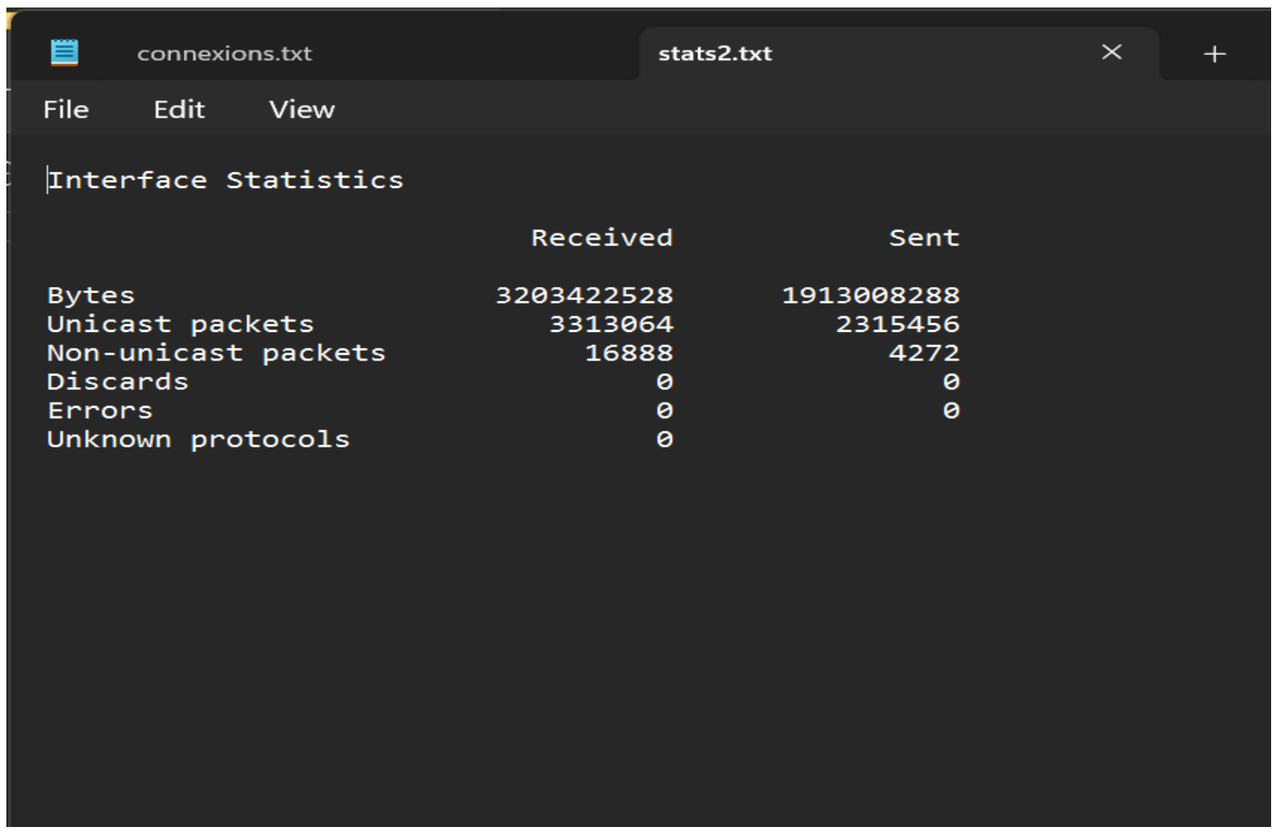
8. Lister les connexions réseau et exporter les résultats
netstat -a > connexions.txt



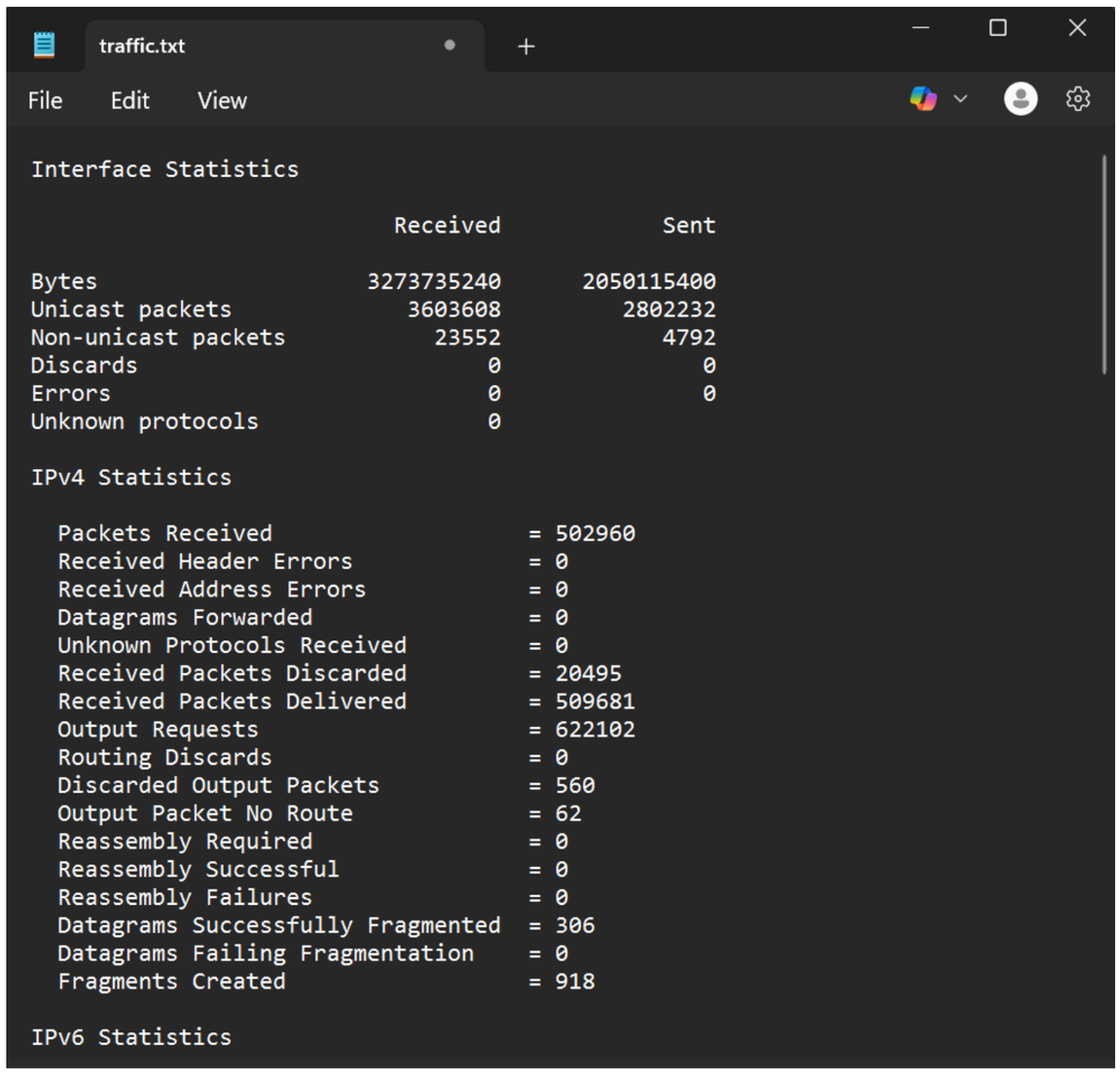
9. Trouver la connexion réseau la plus active
a) netstat -e > stats1.txt



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

```
C:\Users\DELL>netstat -n | findstr ESTABLISHED
  TCP    192.168.1.188:61731    4.172.11.173:443       ESTABLISHED
  TCP    192.168.1.188:61735    149.154.175.50:443     ESTABLISHED
  TCP    192.168.1.188:61753    172.172.255.218:443    ESTABLISHED
  TCP    192.168.1.188:61755    92.223.66.31:443       ESTABLISHED
  TCP    192.168.1.188:61755    142.119.34.23:53608    ESTABLISHED
  TCP    192.168.1.188:61771    20.116.248.159:443     ESTABLISHED
  TCP    192.168.1.188:61792    149.154.175.50:443     ESTABLISHED
  TCP    192.168.1.188:62078    34.237.73.95:443       ESTABLISHED
  TCP    192.168.1.188:62140    173.194.217.188:5228   ESTABLISHED
  TCP    192.168.1.188:62625    172.64.155.209:443     ESTABLISHED
  TCP    192.168.1.188:62626    104.18.32.47:443       ESTABLISHED
  TCP    192.168.1.188:62627    13.54.184.52:443       ESTABLISHED
  TCP    192.168.1.188:62628    13.54.184.52:443       ESTABLISHED
```

```
C:\Users\DELL>netstat -n | findstr ESTABLISHED | findstr :443
  TCP    192.168.1.188:61731    4.172.11.173:443       ESTABLISHED
  TCP    192.168.1.188:61735    149.154.175.50:443     ESTABLISHED
  TCP    192.168.1.188:61753    172.172.255.218:443    ESTABLISHED
  TCP    192.168.1.188:61755    92.223.66.31:443       ESTABLISHED
  TCP    192.168.1.188:61771    20.116.248.159:443     ESTABLISHED
  TCP    192.168.1.188:61792    149.154.175.50:443     ESTABLISHED
  TCP    192.168.1.188:62078    34.237.73.95:443       ESTABLISHED
  TCP    192.168.1.188:62642    172.64.155.209:443     ESTABLISHED
  TCP    192.168.1.188:62643    172.64.155.209:443     ESTABLISHED
```

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.