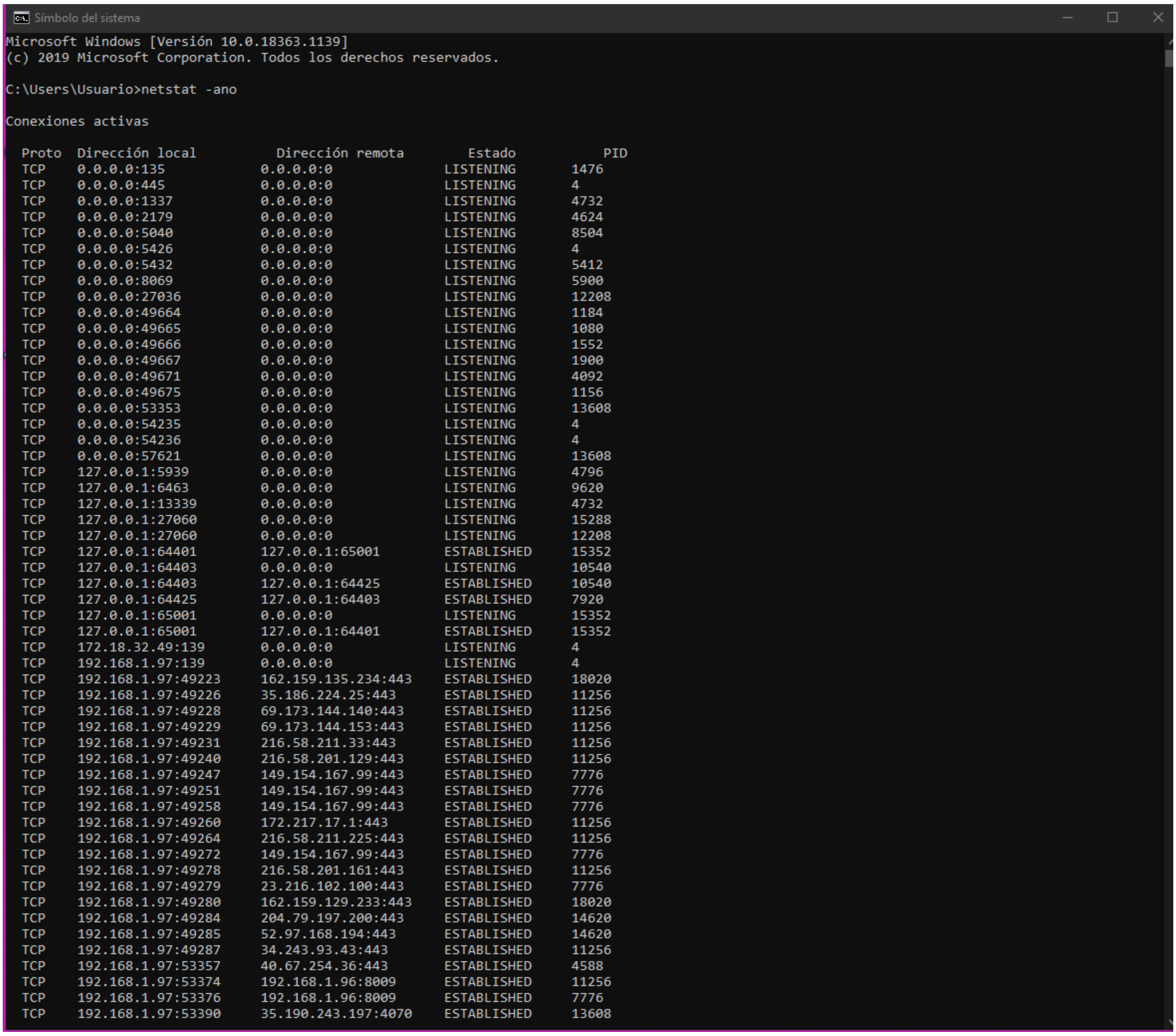
HLC TAREA 4B

1- En la consola de windows y escribimos “netstat -ano” y nos aparecen las conexiones activas:

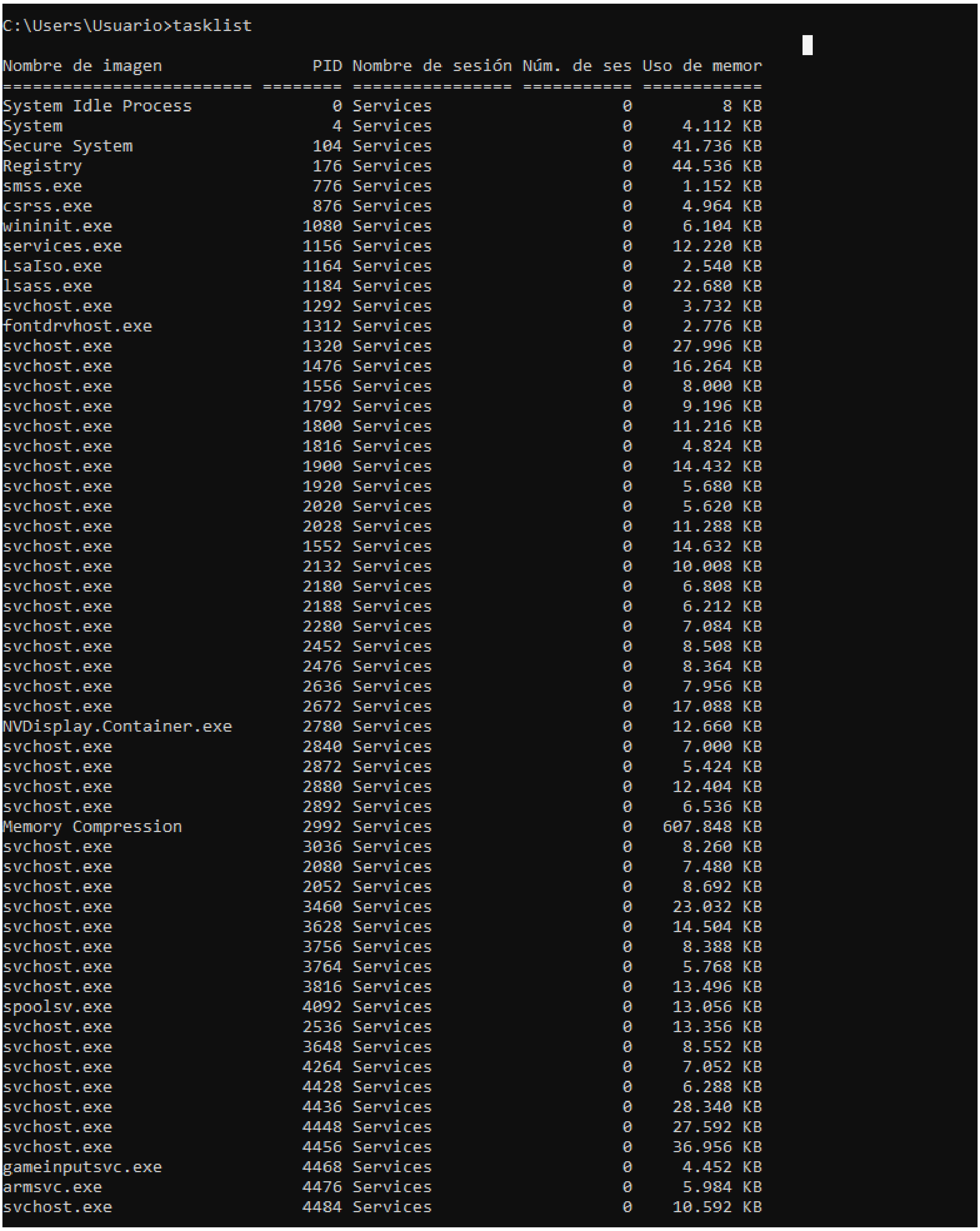


```
Microsoft Windows [Versión 10.0.18363.1139]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>netstat -ano

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1476
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1337           0.0.0.0:0              LISTENING       4732
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING       4624
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8504
  TCP    0.0.0.0:5426           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING       5412
  TCP    0.0.0.0:8069           0.0.0.0:0              LISTENING       5900
  TCP    0.0.0.0:27036          0.0.0.0:0              LISTENING       12208
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1184
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1080
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1552
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1900
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       4092
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING       1156
  TCP    0.0.0.0:53353          0.0.0.0:0              LISTENING       13608
  TCP    0.0.0.0:54235          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:54236          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:57621          0.0.0.0:0              LISTENING       13608
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       4796
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING       9620
  TCP    127.0.0.1:13339        0.0.0.0:0              LISTENING       4732
  TCP    127.0.0.1:27060        0.0.0.0:0              LISTENING       15288
  TCP    127.0.0.1:27060        0.0.0.0:0              LISTENING       12208
  TCP    127.0.0.1:64401        127.0.0.1:65001        ESTABLISHED     15352
  TCP    127.0.0.1:64403        0.0.0.0:0              LISTENING       10540
  TCP    127.0.0.1:64403        127.0.0.1:64425        ESTABLISHED     10540
  TCP    127.0.0.1:64425        127.0.0.1:64403        ESTABLISHED     7920
  TCP    127.0.0.1:65001        0.0.0.0:0              LISTENING       15352
  TCP    127.0.0.1:65001        127.0.0.1:64401        ESTABLISHED     15352
  TCP    172.18.32.49:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.1.97:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.1.97:49223     162.159.135.234:443    ESTABLISHED     18020
  TCP    192.168.1.97:49226     35.186.224.25:443      ESTABLISHED     11256
  TCP    192.168.1.97:49228     69.173.144.140:443     ESTABLISHED     11256
  TCP    192.168.1.97:49229     69.173.144.153:443     ESTABLISHED     11256
  TCP    192.168.1.97:49231     216.58.211.33:443      ESTABLISHED     11256
  TCP    192.168.1.97:49240     216.58.201.129:443     ESTABLISHED     11256
  TCP    192.168.1.97:49247     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49251     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49258     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49260     172.217.17.1:443       ESTABLISHED     11256
  TCP    192.168.1.97:49264     216.58.211.225:443     ESTABLISHED     11256
  TCP    192.168.1.97:49272     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49278     216.58.201.161:443     ESTABLISHED     11256
  TCP    192.168.1.97:49279     23.216.102.100:443     ESTABLISHED     7776
  TCP    192.168.1.97:49280     162.159.129.233:443    ESTABLISHED     18020
  TCP    192.168.1.97:49284     204.79.197.200:443     ESTABLISHED     14620
  TCP    192.168.1.97:49285     52.97.168.194:443      ESTABLISHED     14620
  TCP    192.168.1.97:49287     34.243.93.43:443       ESTABLISHED     11256
  TCP    192.168.1.97:53357     40.67.254.36:443       ESTABLISHED     4588
  TCP    192.168.1.97:53374     192.168.1.96:8009      ESTABLISHED     11256
  TCP    192.168.1.97:53376     192.168.1.96:8009      ESTABLISHED     7776
  TCP    192.168.1.97:53390     35.190.243.197:4070    ESTABLISHED     13608
```

2- Observamos el PID de esas conexiones y nos fijamos en donde ponga “ESTABLISHED”, yo he apuntado la información de todos los que tienen puesto eso:

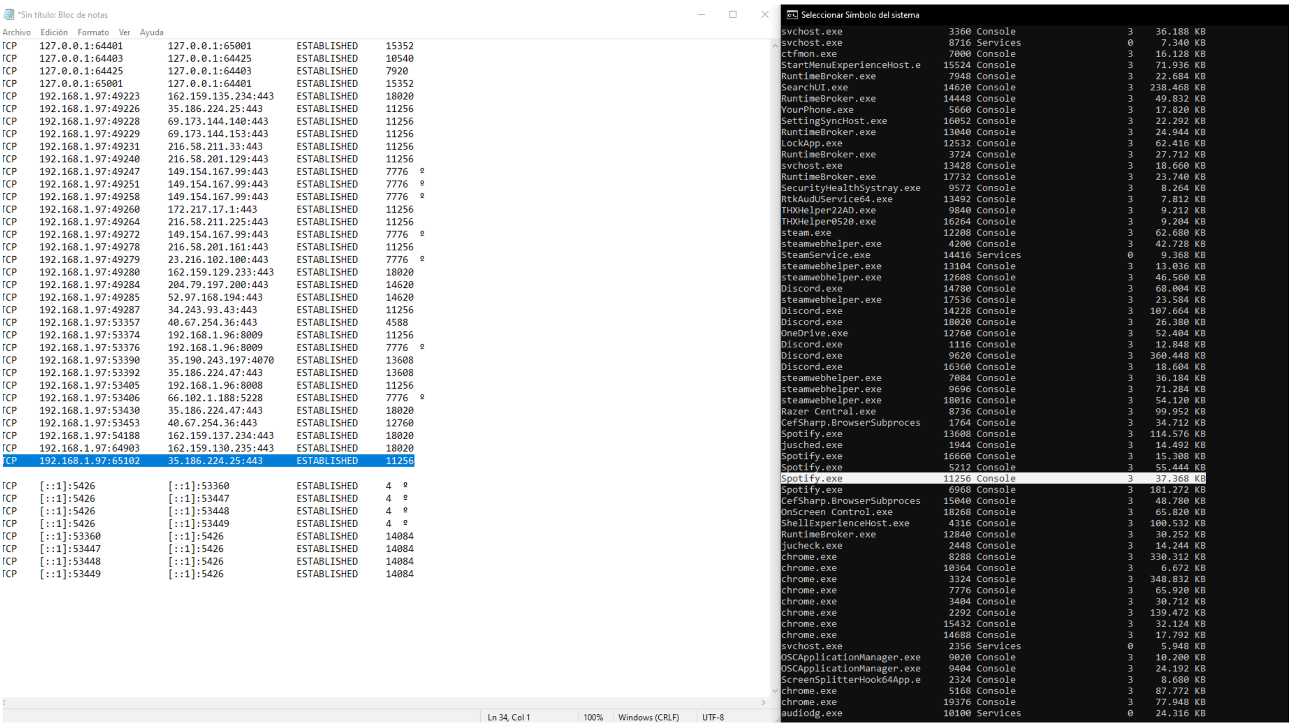
```
  TCP    127.0.0.1:64401        127.0.0.1:65001        ESTABLISHED     15352
  TCP    127.0.0.1:64403        127.0.0.1:64425        ESTABLISHED     10540
  TCP    127.0.0.1:64425        127.0.0.1:64403        ESTABLISHED     7920
  TCP    127.0.0.1:65001        127.0.0.1:64401        ESTABLISHED     15352
  TCP    192.168.1.97:49223     162.159.135.234:443    ESTABLISHED     18020
  TCP    192.168.1.97:49226     35.186.224.25:443      ESTABLISHED     11256
  TCP    192.168.1.97:49228     69.173.144.140:443     ESTABLISHED     11256
  TCP    192.168.1.97:49229     69.173.144.153:443     ESTABLISHED     11256
  TCP    192.168.1.97:49231     216.58.211.33:443      ESTABLISHED     11256
  TCP    192.168.1.97:49240     216.58.201.129:443     ESTABLISHED     11256
  TCP    192.168.1.97:49247     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49251     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49258     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49260     172.217.17.1:443       ESTABLISHED     11256
  TCP    192.168.1.97:49264     216.58.211.225:443     ESTABLISHED     11256
  TCP    192.168.1.97:49272     149.154.167.99:443     ESTABLISHED     7776
  TCP    192.168.1.97:49278     216.58.201.161:443     ESTABLISHED     11256
  TCP    192.168.1.97:49279     23.216.102.100:443     ESTABLISHED     7776
  TCP    192.168.1.97:49280     162.159.129.233:443    ESTABLISHED     18020
  TCP    192.168.1.97:49284     204.79.197.200:443     ESTABLISHED     14620
  TCP    192.168.1.97:49285     52.97.168.194:443      ESTABLISHED     14620
  TCP    192.168.1.97:49287     34.243.93.43:443       ESTABLISHED     11256
  TCP    192.168.1.97:53357     40.67.254.36:443       ESTABLISHED     4588
  TCP    192.168.1.97:53374     192.168.1.96:8009      ESTABLISHED     11256
  TCP    192.168.1.97:53376     192.168.1.96:8009      ESTABLISHED     7776
  TCP    192.168.1.97:53390     35.190.243.197:4070    ESTABLISHED     13608
  TCP    192.168.1.97:53392     35.186.224.47:443      ESTABLISHED     13608
  TCP    192.168.1.97:53405     192.168.1.96:8008      ESTABLISHED     11256
  TCP    192.168.1.97:53406     66.102.1.188:5228      ESTABLISHED     7776
  TCP    192.168.1.97:53430     35.186.224.47:443      ESTABLISHED     18020
  TCP    192.168.1.97:53453     40.67.254.36:443       ESTABLISHED     12760
  TCP    192.168.1.97:54188     162.159.137.234:443    ESTABLISHED     18020
  TCP    192.168.1.97:64903     162.159.130.235:443    ESTABLISHED     18020
  TCP    192.168.1.97:65102     35.186.224.25:443      ESTABLISHED     11256
```

3- escribimos “tasklist” en la consola y aparecen todos los programas activos:



```
C:\Users\Usuario>tasklist

Nombre de imagen               PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 KB
System                           4 Services                   0      4.112 KB
Secure System                  104 Services                   0     41.736 KB
Registry                       176 Services                   0     44.536 KB
smss.exe                       776 Services                   0      1.152 KB
csrss.exe                      876 Services                   0      4.964 KB
wininit.exe                   1080 Services                   0      6.104 KB
services.exe                  1156 Services                   0     12.220 KB
LsaIso.exe                    1164 Services                   0      2.540 KB
lsass.exe                     1184 Services                   0     22.680 KB
svchost.exe                   1292 Services                   0      3.732 KB
fontdrvhost.exe               1312 Services                   0      2.776 KB
svchost.exe                   1320 Services                   0     27.996 KB
svchost.exe                   1476 Services                   0     16.264 KB
svchost.exe                   1556 Services                   0      8.000 KB
svchost.exe                   1792 Services                   0      9.196 KB
svchost.exe                   1800 Services                   0     11.216 KB
svchost.exe                   1816 Services                   0      4.824 KB
svchost.exe                   1900 Services                   0     14.432 KB
svchost.exe                   1920 Services                   0      5.680 KB
svchost.exe                   2020 Services                   0      5.620 KB
svchost.exe                   2028 Services                   0     11.288 KB
svchost.exe                   1552 Services                   0     14.632 KB
svchost.exe                   2132 Services                   0     10.008 KB
svchost.exe                   2180 Services                   0      6.808 KB
svchost.exe                   2188 Services                   0      6.212 KB
svchost.exe                   2280 Services                   0      7.084 KB
svchost.exe                   2452 Services                   0      8.508 KB
svchost.exe                   2476 Services                   0      8.364 KB
svchost.exe                   2636 Services                   0      7.956 KB
svchost.exe                   2672 Services                   0     17.088 KB
NVDisplay.Container.exe       2780 Services                   0     12.660 KB
svchost.exe                   2840 Services                   0      7.000 KB
svchost.exe                   2872 Services                   0      5.424 KB
svchost.exe                   2880 Services                   0     12.404 KB
svchost.exe                   2892 Services                   0      6.536 KB
Memory Compression            2992 Services                   0    607.848 KB
svchost.exe                   3036 Services                   0      8.260 KB
svchost.exe                   2080 Services                   0      7.480 KB
svchost.exe                   2052 Services                   0      8.692 KB
svchost.exe                   3460 Services                   0     23.032 KB
svchost.exe                   3628 Services                   0     14.504 KB
svchost.exe                   3756 Services                   0      8.388 KB
svchost.exe                   3764 Services                   0      5.768 KB
svchost.exe                   3816 Services                   0     13.496 KB
spoolsv.exe                   4092 Services                   0     13.056 KB
svchost.exe                   2536 Services                   0     13.356 KB
svchost.exe                   3648 Services                   0      8.552 KB
svchost.exe                   4264 Services                   0      7.052 KB
svchost.exe                   4428 Services                   0      6.288 KB
svchost.exe                   4436 Services                   0     28.340 KB
svchost.exe                   4448 Services                   0     27.592 KB
svchost.exe                   4456 Services                   0     36.956 KB
gameinputsvc.exe              4468 Services                   0      4.452 KB
armsvc.exe                    4476 Services                   0      5.984 KB
svchost.exe                   4484 Services                   0     10.592 KB
```

4- Buscamos el PID que habíamos apuntado para ver de que aplicación se trata como se puede ver en la imagen de abajo:


*Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda
Ln 34, Col 1
100%
Windows (CRLF)
UTF-8
Seleccionar Símbolo del sistema

```
TCP    127.0.0.1:64401        127.0.0.1:65001        ESTABLISHED     15352
TCP    127.0.0.1:64403        127.0.0.1:64425        ESTABLISHED     10540
TCP    127.0.0.1:64425        127.0.0.1:64403        ESTABLISHED     7920
TCP    127.0.0.1:65001        127.0.0.1:64401        ESTABLISHED     15352
TCP    192.168.1.97:49223     162.159.135.234:443    ESTABLISHED     18020
TCP    192.168.1.97:49226     35.186.224.25:443      ESTABLISHED     11256
TCP    192.168.1.97:49228     69.173.144.140:443     ESTABLISHED     11256
TCP    192.168.1.97:49229     69.173.144.153:443     ESTABLISHED     11256
TCP    192.168.1.97:49231     216.58.211.33:443      ESTABLISHED     11256
TCP    192.168.1.97:49240     216.58.201.129:443     ESTABLISHED     11256
TCP    192.168.1.97:49247     149.154.167.99:443     ESTABLISHED     7776  º
TCP    192.168.1.97:49251     149.154.167.99:443     ESTABLISHED     7776  º
TCP    192.168.1.97:49258     149.154.167.99:443     ESTABLISHED     7776  º
TCP    192.168.1.97:49260     172.217.17.1:443       ESTABLISHED     11256
TCP    192.168.1.97:49264     216.58.211.225:443     ESTABLISHED     11256
TCP    192.168.1.97:49272     149.154.167.99:443     ESTABLISHED     7776  º
TCP    192.168.1.97:49278     216.58.201.161:443     ESTABLISHED     11256
TCP    192.168.1.97:49279     23.216.102.100:443     ESTABLISHED     7776  º
TCP    192.168.1.97:49280     162.159.129.233:443    ESTABLISHED     18020
TCP    192.168.1.97:49284     204.79.197.200:443     ESTABLISHED     14620
TCP    192.168.1.97:49285     52.97.168.194:443      ESTABLISHED     14620
TCP    192.168.1.97:49287     34.243.93.43:443       ESTABLISHED     11256
TCP    192.168.1.97:53357     40.67.254.36:443       ESTABLISHED     4588
TCP    192.168.1.97:53374     192.168.1.96:8009      ESTABLISHED     11256
TCP    192.168.1.97:53376     192.168.1.96:8009      ESTABLISHED     7776  º
TCP    192.168.1.97:53390     35.190.243.197:4070    ESTABLISHED     13608
TCP    192.168.1.97:53392     35.186.224.47:443      ESTABLISHED     13608
TCP    192.168.1.97:53405     192.168.1.96:8008      ESTABLISHED     11256
TCP    192.168.1.97:53406     66.102.1.188:5228      ESTABLISHED     7776  º
TCP    192.168.1.97:53430     35.186.224.47:443      ESTABLISHED     18020
TCP    192.168.1.97:53453     40.67.254.36:443       ESTABLISHED     12760
TCP    192.168.1.97:54188     162.159.137.234:443    ESTABLISHED     18020
TCP    192.168.1.97:64903     162.159.130.235:443    ESTABLISHED     18020
TCP    192.168.1.97:65102     35.186.224.25:443      ESTABLISHED     11256

TCP    [::1]:5426             [::1]:53360            ESTABLISHED     4  º
TCP    [::1]:5426             [::1]:53447            ESTABLISHED     4  º
TCP    [::1]:5426             [::1]:53448            ESTABLISHED     4  º
TCP    [::1]:5426             [::1]:53449            ESTABLISHED     4  º
TCP    [::1]:53360            [::1]:5426             ESTABLISHED     14084
TCP    [::1]:53447            [::1]:5426             ESTABLISHED     14084
TCP    [::1]:53448            [::1]:5426             ESTABLISHED     14084
TCP    [::1]:53449            [::1]:5426             ESTABLISHED     14084
```

```
svchost.exe                   3360 Console                    3     36.188 KB
svchost.exe                   8716 Services                   0      7.340 KB
ctfmon.exe                    7000 Console                    3     16.128 KB
StartMenuExperienceHost.e    15524 Console                    3     71.936 KB
RuntimeBroker.exe             7948 Console                    3     22.684 KB
SearchUI.exe                 14620 Console                    3    238.468 KB
RuntimeBroker.exe            14448 Console                    3     49.832 KB
YourPhone.exe                 5660 Console                    3     17.820 KB
SettingSyncHost.exe          16052 Console                    3     22.292 KB
RuntimeBroker.exe            13040 Console                    3     24.944 KB
LockApp.exe                  12532 Console                    3     62.416 KB
RuntimeBroker.exe             3724 Console                    3     27.712 KB
svchost.exe                  13428 Console                    3     18.660 KB
RuntimeBroker.exe            17732 Console                    3     23.740 KB
SecurityHealthSystray.exe     9572 Console                    3      8.264 KB
RtkAudUService64.exe         13492 Console                    3      7.812 KB
THXHelper22AD.exe             9840 Console                    3      9.212 KB
THXHelper0520.exe            16264 Console                    3      9.204 KB
steam.exe                    12208 Console                    3     62.680 KB
steamwebhelper.exe            4200 Console                    3     42.728 KB
SteamService.exe             14416 Services                   0      9.368 KB
steamwebhelper.exe           13104 Console                    3     13.036 KB
steamwebhelper.exe           12608 Console                    3     46.560 KB
Discord.exe                  14780 Console                    3     68.004 KB
steamwebhelper.exe           17536 Console                    3     23.584 KB
Discord.exe                  14228 Console                    3    107.664 KB
Discord.exe                  18020 Console                    3     26.380 KB
OneDrive.exe                 12760 Console                    3     52.404 KB
Discord.exe                   1116 Console                    3     12.848 KB
Discord.exe                   9620 Console                    3    360.448 KB
Discord.exe                  16360 Console                    3     18.604 KB
steamwebhelper.exe            7084 Console                    3     36.184 KB
steamwebhelper.exe            9696 Console                    3     71.284 KB
steamwebhelper.exe           18016 Console                    3     54.120 KB
Razer Central.exe             8736 Console                    3     99.952 KB
CefSharp.BrowserSubproces     1764 Console                    3     34.712 KB
Spotify.exe                  13608 Console                    3    114.576 KB
jusched.exe                   1944 Console                    3     14.492 KB
Spotify.exe                  16660 Console                    3     15.308 KB
Spotify.exe                   5212 Console                    3     55.444 KB
Spotify.exe                  11256 Console                    3     37.368 KB
Spotify.exe                   6968 Console                    3    181.272 KB
CefSharp.BrowserSubproces    15040 Console                    3     48.780 KB
OnScreen Control.exe         18268 Console                    3     65.820 KB
ShellExperienceHost.exe       4316 Console                    3    100.532 KB
RuntimeBroker.exe            12840 Console                    3     30.252 KB
jucheck.exe                   2448 Console                    3     14.244 KB
chrome.exe                    8288 Console                    3    330.312 KB
chrome.exe                   10364 Console                    3      6.672 KB
chrome.exe                    3324 Console                    3    348.832 KB
chrome.exe                    7776 Console                    3     65.920 KB
chrome.exe                    3404 Console                    3     30.712 KB
chrome.exe                    2292 Console                    3    139.472 KB
chrome.exe                   15432 Console                    3     32.124 KB
chrome.exe                   14688 Console                    3     17.792 KB
svchost.exe                   2356 Services                   0      5.948 KB
OSCApplicationManager.exe     9020 Console                    3     10.200 KB
OSCApplicationManager.exe     9404 Console                    3     24.192 KB
ScreenSplitterHook64App.e     2324 Console                    3      8.680 KB
chrome.exe                    5168 Console                    3     87.772 KB
chrome.exe                   19376 Console                    3     77.948 KB
audiodg.exe                  10100 Services                   0     24.316 KB
```

Mis PIDS serían de las siguientes aplicaciones, todas reconocidas:

```
  TCP    127.0.0.1:64401        127.0.0.1:65001        ESTABLISHED     15352   -> nvcontainer.exe
  TCP    127.0.0.1:64403        127.0.0.1:64425        ESTABLISHED     10540   -> NVIDIA Web Helper.exe
  TCP    127.0.0.1:64425        127.0.0.1:64403        ESTABLISHED     7920   -> NVIDIA Share.exe
  TCP    127.0.0.1:65001        127.0.0.1:64401        ESTABLISHED     15352   -> nvcontainer.exe
  TCP    192.168.1.97:49223     162.159.135.234:443    ESTABLISHED     18020   -> Discord.exe
  TCP    192.168.1.97:49226     35.186.224.25:443      ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49228     69.173.144.140:443     ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49229     69.173.144.153:443     ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49231     216.58.211.33:443      ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49240     216.58.201.129:443     ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49247     149.154.167.99:443     ESTABLISHED     7776   -> chrome.exe
  TCP    192.168.1.97:49251     149.154.167.99:443     ESTABLISHED     7776   -> chrome.exe
  TCP    192.168.1.97:49258     149.154.167.99:443     ESTABLISHED     7776   -> chrome.exe
  TCP    192.168.1.97:49260     172.217.17.1:443       ESTABLISHED     11256   -> Spotify.exe
  TCP    192.168.1.97:49264     216.58.211.225:443     ESTABLISHED     11256   ->
Spotify.exe
  TCP    192.168.1.97:49272     149.154.167.99:443     ESTABLISHED     7776   ->
chrome.exe
  TCP    192.168.1.97:49278     216.58.201.161:443     ESTABLISHED     11256   ->
Spotify.exe
  TCP    192.168.1.97:49279     23.216.102.100:443     ESTABLISHED     7776   ->
Spotify.exe
  TCP    192.168.1.97:49280     162.159.129.233:443    ESTABLISHED     18020   ->
Discord.exe
  TCP    192.168.1.97:49284     204.79.197.200:443     ESTABLISHED     14620   ->
SearchUI.exe
  TCP    192.168.1.97:49285     52.97.168.194:443      ESTABLISHED     14620   ->
SearchUI.exe
  TCP    192.168.1.97:49287     34.243.93.43:443       ESTABLISHED     11256   ->
Spotify.exe
  TCP    192.168.1.97:53357     40.67.254.36:443       ESTABLISHED     4588   ->
svchost.exe
  TCP    192.168.1.97:53374     192.168.1.96:8009      ESTABLISHED     11256   ->
Spotify.exe
  TCP    192.168.1.97:53376     192.168.1.96:8009      ESTABLISHED     7776   ->
Spotify.exe
  TCP    192.168.1.97:53390     35.190.243.197:4070    ESTABLISHED     13608   ->
Spotify.exe
  TCP    192.168.1.97:53392     35.186.224.47:443      ESTABLISHED     13608   ->
Spotify.exe
  TCP    192.168.1.97:53405     192.168.1.96:8008      ESTABLISHED     11256   ->
Spotify.exe
  TCP    192.168.1.97:53406     66.102.1.188:5228      ESTABLISHED     7776   ->
Spotify.exe
  TCP    192.168.1.97:53430     35.186.224.47:443      ESTABLISHED     18020   ->
Discord.exe
  TCP    192.168.1.97:53453     40.67.254.36:443       ESTABLISHED     12760   ->
OneDrive.exe
  TCP    192.168.1.97:54188     162.159.137.234:443    ESTABLISHED     18020   ->
Discord.exe
  TCP    192.168.1.97:64903     162.159.130.235:443    ESTABLISHED     18020   ->
Discord.exe
  TCP    192.168.1.97:65102     35.186.224.25:443      ESTABLISHED     11256   ->
Spotify.exe
```

5- Yo no tengo ningún virus, pero si necesitáramos eliminar un virus al no reconocer una aplicación, se debería usar el comando: “taskkil /PID(numerodelpid) /F”