INGENIERÍA EN SOFTWARE

Jessica Mariel Márquez Rodríguez

Ismael Jimenez Sanchez

7mo cuatrimestre

25BV

Sistema Operativos

ACTIVIDAD 987: Comando CMS2

1. Obtener la ayuda del comando ping:

```
C:\Windows\System32>ping -?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Windows\System32>2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parametro

```
C:\Windows\System32>ping -t -l 1000 -n 10 127.0.0.1

Pinging 127.0.0.1 with 1000 bytes of data:
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=1000 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

3- Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones

```
C:\Windows\System32>ping google.com

Pinging google.com [142.250.217.238] with 32 bytes of data:
Reply from 142.250.217.238: bytes=32 time=91ms TTL=118
Reply from 142.250.217.238: bytes=32 time=22ms TTL=118
Reply from 142.250.217.238: bytes=32 time=34ms TTL=118
Reply from 142.250.217.238: bytes=32 time=99ms TTL=118

Ping statistics for 142.250.217.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 99ms, Average = 61ms
```

4.- Obtener la ayuda del comando nslookup

```
C:\Windows\System32>nslookup -?
Usage:
  nslookup [-opt ...]             # interactive mode using default server
  nslookup [-opt ...] - server    # interactive mode using 'server'
  nslookup [-opt ...] host        # just look up 'host' using default server
  nslookup [-opt ...] host server # just look up 'host' using 'server'
```

5.-Resolver la direccion ip de https://upqroo.edu.mx/ usando nslookup

```
C:\Windows\System32>nslookup upqroo.edu.mx
Server:  b.resolvers.level3.net
Address:  4.2.2.2

Non-authoritative answer:
Name:    upqroo.edu.mx
Address:  77.68.126.20
```

6.- Hacer ping a la ip obtenida en el paso anterior, anotar conclusiones

```
C:\Windows\System32>ping 77.68.126.20

Pinging 77.68.126.20 with 32 bytes of data:
Reply from 77.68.126.20: bytes=32 time=119ms TTL=50
Reply from 77.68.126.20: bytes=32 time=120ms TTL=50
Reply from 77.68.126.20: bytes=32 time=132ms TTL=50
Reply from 77.68.126.20: bytes=32 time=118ms TTL=50

Ping statistics for 77.68.126.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 118ms, Maximum = 132ms, Average = 122ms
```

7.- Obtener la ayuda del comando netstat

```
C:\Windows\System32>netstat -?

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.
  -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
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

8.- Mostrar todas las conexiones y puertos de escucha

```
C:\Windows\System32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             Breney:0               LISTENING
  TCP    0.0.0.0:80             Breney:0               LISTENING
  TCP    0.0.0.0:135            Breney:0               LISTENING
  TCP    0.0.0.0:442            Breney:0               LISTENING
  TCP    0.0.0.0:443            Breney:0               LISTENING
  TCP    0.0.0.0:445            Breney:0               LISTENING
  TCP    0.0.0.0:3306           Breney:0               LISTENING
  TCP    0.0.0.0:5040           Breney:0               LISTENING
  TCP    0.0.0.0:8080           Breney:0               LISTENING
  TCP    0.0.0.0:49664          Breney:0               LISTENING
  TCP    0.0.0.0:49665          Breney:0               LISTENING
  TCP    0.0.0.0:49666          Breney:0               LISTENING
  TCP    0.0.0.0:49667          Breney:0               LISTENING
  TCP    0.0.0.0:49668          Breney:0               LISTENING
  TCP    0.0.0.0:49669          Breney:0               LISTENING
  TCP    127.0.0.1:1434         Breney:0               LISTENING
  TCP    127.0.0.1:14147        Breney:0               LISTENING
  TCP    172.16.129.150:139     Breney:0               LISTENING
```

9.- Ejecutar netstat sin resolver nombres de dominio o puertos.

```
C:\Windows\System32>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.129.150:49410   52.159.126.152:443     ESTABLISHED
  TCP    172.16.129.150:57856   104.210.1.187:443      ESTABLISHED
  TCP    172.16.129.150:57857   103.41.69.207:443      ESTABLISHED
  TCP    172.16.129.150:57858   23.54.200.10:443       CLOSE_WAIT
  TCP    172.16.129.150:57861   192.229.211.108:80     CLOSE_WAIT
  TCP    172.16.129.150:57862   192.229.211.108:80     CLOSE_WAIT
  TCP    172.16.129.150:57879   104.210.1.187:443      ESTABLISHED
  TCP    172.16.129.150:57880   103.41.69.207:443      ESTABLISHED
  TCP    172.16.129.150:57882   23.54.200.10:443       CLOSE_WAIT
  TCP    172.16.129.150:57883   192.229.211.108:80     CLOSE_WAIT
  TCP    172.16.129.150:57884   192.229.211.108:80     CLOSE_WAIT
  TCP    172.16.129.150:58083   142.250.9.188:5228     ESTABLISHED
  TCP    172.16.129.150:58084   108.177.122.190:443    ESTABLISHED
  TCP    172.16.129.150:58089   172.217.30.195:443     ESTABLISHED
  TCP    172.16.129.150:58160   142.251.15.113:443     ESTABLISHED
  TCP    172.16.129.150:58161   172.217.215.138:443    ESTABLISHED
  TCP    172.16.129.150:58162   192.178.49.3:443       ESTABLISHED
  TCP    172.16.129.150:58199   64.233.176.100:443     ESTABLISHED
  TCP    172.16.129.150:58202   142.251.15.147:443     ESTABLISHED
  TCP    172.16.129.150:58203   64.233.185.119:443     ESTABLISHED
  TCP    172.16.129.150:58208   172.253.124.156:443    ESTABLISHED
  TCP    172.16.129.150:58209   64.233.185.94:443      ESTABLISHED
  TCP    172.16.129.150:58267   31.13.67.52:443        ESTABLISHED
  TCP    172.16.129.150:58302   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58303   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58304   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58305   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58306   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58307   23.218.93.201:443      CLOSE_WAIT
  TCP    172.16.129.150:58311   52.96.173.226:443      ESTABLISHED
  TCP    172.16.129.150:58312   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58313   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58314   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58315   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58316   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58317   23.218.93.137:443      CLOSE_WAIT
  TCP    172.16.129.150:58327   108.177.122.113:443    TIME_WAIT
  TCP    172.16.129.150:58328   64.233.177.94:443      TIME_WAIT
  TCP    172.16.129.150:58331   72.21.81.200:80        TIME_WAIT
  TCP    172.16.129.150:58333   187.190.14.108:443     ESTABLISHED
  TCP    172.16.129.150:58334   64.233.176.132:443     ESTABLISHED
  TCP    172.16.129.150:58339   20.69.136.49:443       ESTABLISHED
```

```
TCP    172.16.129.150:58339   20.69.136.49:443       ESTABLISHED
TCP    172.16.129.150:58340   20.69.136.49:443       ESTABLISHED
TCP    172.16.129.150:58342   20.69.136.49:443       ESTABLISHED
TCP    172.16.129.150:58343   20.69.136.49:443       ESTABLISHED
TCP    172.16.129.150:58347   52.140.118.28:443      TIME_WAIT
TCP    172.16.129.150:58348   74.125.138.113:443     ESTABLISHED
TCP    172.16.129.150:58352   64.233.176.101:443     ESTABLISHED
TCP    172.16.129.150:58355   13.78.111.198:443      TIME_WAIT
TCP    172.16.129.150:58357   20.242.39.171:443      TIME_WAIT
TCP    172.16.129.150:58364   23.46.202.178:443      ESTABLISHED
TCP    172.16.129.150:58366   23.46.200.15:443       ESTABLISHED
TCP    172.16.129.150:58368   23.46.200.15:443       ESTABLISHED
TCP    172.16.129.150:58369   23.46.200.15:443       ESTABLISHED
TCP    172.16.129.150:58372   208.111.136.128:80     TIME_WAIT
TCP    172.16.129.150:58373   208.111.136.0:80       TIME_WAIT
TCP    172.16.129.150:58376   208.111.136.0:80       TIME_WAIT
TCP    172.16.129.150:58377   208.111.136.128:80     TIME_WAIT
TCP    172.16.129.150:58383   20.242.39.171:443      TIME_WAIT
TCP    172.16.129.150:58392   72.21.81.240:80        TIME_WAIT
TCP    172.16.129.150:58395   72.21.81.240:80        TIME_WAIT
TCP    172.16.129.150:58430   23.46.200.15:443       ESTABLISHED
TCP    172.16.129.150:58431   72.21.81.240:80        TIME_WAIT
TCP    172.16.129.150:58432   142.250.9.102:443      ESTABLISHED
TCP    172.16.129.150:58433   108.177.122.113:443    ESTABLISHED
TCP    172.16.129.150:58435   51.132.193.104:443     TIME_WAIT
TCP    172.16.129.150:58436   20.44.229.112:443      ESTABLISHED
TCP    172.16.129.150:58437   216.239.32.116:443     ESTABLISHED
TCP    172.16.129.150:58438   20.44.229.112:443      ESTABLISHED
TCP    172.16.129.150:58439   52.96.40.114:443       ESTABLISHED

:\Windows\System32>
```

10.- Mostrar las conexiones TCP

```
C:\Windows\System32>netstat -t

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    172.16.129.150:49410   52.159.126.152:https   ESTABLISHED     InHost
  TCP    172.16.129.150:57856   104.210.1.187:https    ESTABLISHED     InHost
  TCP    172.16.129.150:57857   103.41.69.207:https    ESTABLISHED     InHost
  TCP    172.16.129.150:57858   a23-54-200-10:https    CLOSE_WAIT      InHost
  TCP    172.16.129.150:57861   192.229.211.108:http   CLOSE_WAIT      InHost
  TCP    172.16.129.150:57862   192.229.211.108:http   CLOSE_WAIT      InHost
  TCP    172.16.129.150:57879   104.210.1.187:https    ESTABLISHED     InHost
  TCP    172.16.129.150:57880   103.41.69.207:https    ESTABLISHED     InHost
  TCP    172.16.129.150:57882   a23-54-200-10:https    CLOSE_WAIT      InHost
  TCP    172.16.129.150:57883   192.229.211.108:http   CLOSE_WAIT      InHost
  TCP    172.16.129.150:57884   192.229.211.108:http   CLOSE_WAIT      InHost
  TCP    172.16.129.150:58083   yq-in-f188:5228        ESTABLISHED     InHost
  TCP    172.16.129.150:58084   ym-in-f190:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58089   bog02s08-in-f3:https   ESTABLISHED     InHost
  TCP    172.16.129.150:58160   yl-in-f113:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58161   yo-in-f138:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58162   phx18s08-in-f3:https   ESTABLISHED     InHost
  TCP    172.16.129.150:58199   yw-in-f100:https       TIME_WAIT       InHost
  TCP    172.16.129.150:58202   yl-in-f147:https       TIME_WAIT       InHost
  TCP    172.16.129.150:58203   yb-in-f119:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58208   ys-in-f156:https       TIME_WAIT       InHost
  TCP    172.16.129.150:58209   yb-in-f94:https        TIME_WAIT       InHost
  TCP    172.16.129.150:58267   whatsapp-cdn-shv-01-mia3:https  ESTABLISHED     InHost
  TCP    172.16.129.150:58334   yw-in-f132:https       TIME_WAIT       InHost
  TCP    172.16.129.150:58348   yi-in-f113:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58352   yw-in-f101:https       TIME_WAIT       InHost
  TCP    172.16.129.150:58432   yq-in-f102:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58433   ym-in-f113:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58437   e2a:https              ESTABLISHED     InHost
  TCP    172.16.129.150:58440   yl-in-f94:https        ESTABLISHED     InHost
  TCP    172.16.129.150:58446   13.107.21.200:https    ESTABLISHED     InHost
  TCP    172.16.129.150:58447   a23-218-93-137:https   CLOSE_WAIT      InHost
  TCP    172.16.129.150:58452   204.79.197.222:https   ESTABLISHED     InHost
  TCP    172.16.129.150:58455   192.229.211.108:http   ESTABLISHED     InHost
  TCP    172.16.129.150:58458   a-0003:https           TIME_WAIT       InHost
  TCP    172.16.129.150:58472   72.21.81.200:http      TIME_WAIT       InHost
  TCP    172.16.129.150:58474   yt-in-f101:https       ESTABLISHED     InHost
  TCP    172.16.129.150:58475   yr-in-f95:https        ESTABLISHED     InHost
  TCP    172.16.129.150:58476   52.123.128.254:https   ESTABLISHED     InHost
  TCP    172.16.129.150:58477   13.107.3.254:https     ESTABLISHED     InHost
  TCP    172.16.129.150:58478   152.199.24.163:https   ESTABLISHED     InHost
  TCP    172.16.129.150:58480   20.44.229.112:https    ESTABLISHED     InHost
  TCP    172.16.129.150:58481   fixed-187-190-14-109:https  ESTABLISHED     InHost
```

11.- Mostrar las conexiones UDP

```
C:\Windows\System32>netstat -a -p UDP -n

Active Connections

  Proto  Local Address          Foreign Address        State
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:64711          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:55448        *:*
  UDP    127.0.0.1:61687        127.0.0.1:61687
  UDP    172.16.129.150:137     *:*
  UDP    172.16.129.150:138     *:*
  UDP    172.16.129.150:1900    *:*
  UDP    172.16.129.150:55447   *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:55446     *:*
```

12. Utilizar el comando tasklist

```
C:\Windows\System32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        148 K
Secure System                  140 Services                   0     47,452 K
Registry                       180 Services                   0     30,704 K
smss.exe                       616 Services                   0      1,140 K
csrss.exe                      944 Services                   0      5,076 K
wininit.exe                    544 Services                   0      6,012 K
csrss.exe                      772                            1      5,620 K
services.exe                  1072 Services                   0     10,540 K
LsaIso.exe                    1100 Services                   0      3,584 K
lsass.exe                     1116 Services                   0     29,912 K
winlogon.exe                  1180                            1     14,412 K
svchost.exe                   1304 Services                   0     38,136 K
fontdrvhost.exe               1352                            1      7,268 K
fontdrvhost.exe               1360 Services                   0      2,456 K
svchost.exe                   1420 Services                   0     20,052 K
svchost.exe                   1492 Services                   0      9,084 K
dwm.exe                       1580                            1     64,340 K
svchost.exe                   1672 Services                   0     10,380 K
svchost.exe                   1668 Services                   0      4,976 K
svchost.exe                   1704 Services                   0     11,532 K
svchost.exe                   1824 Services                   0     10,720 K
svchost.exe                   1832 Services                   0     10,360 K
svchost.exe                   1844 Services                   0      9,704 K
svchost.exe                   1892 Services                   0     16,292 K
svchost.exe                   1972 Services                   0      6,100 K
svchost.exe                   2012 Services                   0     15,868 K
svchost.exe                   2032 Services                   0      8,820 K
svchost.exe                   1800 Services                   0     17,936 K
svchost.exe                   2060 Services                   0      8,092 K
svchost.exe                   2120 Services                   0     16,120 K
svchost.exe                   2336 Services                   0      7,408 K
svchost.exe                   2368 Services                   0      8,712 K
svchost.exe                   2568 Services                   0     17,500 K
svchost.exe                   2584 Services                   0      6,120 K
svchost.exe                   2956 Services                   0     36,112 K
svchost.exe                   2980 Services                   0     18,632 K
NetworkCap.exe                2988 Services                   0     11,616 K
AppHelperCap.exe              2992 Services                   0     19,828 K
DiagsCap.exe                  3008 Services                   0     13,652 K
SysInfoCap.exe                3016 Services                   0     26,556 K
TouchpointAnalyticsClient     2560 Services                   0     57,852 K
svchost.exe                   2432 Services                   0     15,848 K
svchost.exe                   3196 Services                   0      7,516 K
WmiPrvSE.exe                  3304 Services                   0     21,584 K
```

```
WmiPrvSE.exe                  3684 Services                   0     53,892 K
svchost.exe                   3752 Services                   0      8,480 K
svchost.exe                   3760 Services                   0     10,624 K
Memory Compression            3772 Services                   0    431,288 K
svchost.exe                   3988 Services                   0     21,396 K
svchost.exe                   3100 Services                   0     16,056 K
svchost.exe                   3292 Services                   0     15,904 K
svchost.exe                   4144 Services                   0      6,864 K
svchost.exe                   4292 Services                   0      9,976 K
svchost.exe                   4464 Services                   0     19,840 K
svchost.exe                   4492 Services                   0      9,240 K
sihost.exe                    4508                            1     32,608 K
svchost.exe                   4564 Services                   0     13,868 K
svchost.exe                   4572                            1     27,684 K
svchost.exe                   4648                            1      8,540 K
svchost.exe                   4720                            1     32,792 K
svchost.exe                   4828 Services                   0     21,148 K
AUEPMaster.exe                4852                            1     10,028 K
taskhostw.exe                 4884                            1     19,124 K
spoolsv.exe                   4800 Services                   0     14,288 K
svchost.exe                   5464 Services                   0      7,832 K
httpd.exe                     5708 Services                   0     16,740 K
svchost.exe                   5716 Services                   0     43,444 K
FileZillaServer.exe           5724 Services                   0      6,904 K
ETDService.exe                5732 Services                   0      6,076 K
svchost.exe                   5740 Services                   0      9,168 K
svchost.exe                   5764 Services                   0     29,940 K
OfficeClickToRun.exe          5780 Services                   0     56,388 K
svchost.exe                   5836 Services                   0     11,048 K
ETDCtrl.exe                   5940                            1     13,304 K
mysqld.exe                    5948 Services                   0     33,800 K
RtkBtManServ.exe              6016 Services                   0      7,860 K
SECOMN64.exe                  6056 Services                   0     14,260 K
sqlwriter.exe                 6072 Services                   0      8,208 K
svchost.exe                   6140 Services                   0      8,628 K
svchost.exe                   6148 Services                   0     10,184 K
sqlceip.exe                   6156 Services                   0     54,140 K
svchost.exe                   6168 Services                   0     19,124 K
MsMpEng.exe                   6180 Services                   0    208,296 K
svchost.exe                   6248 Services                   0      9,164 K
svchost.exe                   6288 Services                   0      5,720 K
sqlservr.exe                  6340 Services                   0    133,308 K
explorer.exe                  6768                            1    181,276 K
RtkAudUService64.exe          7048                            1     12,772 K
svchost.exe                   5428 Services                   0     20,504 K
svchost.exe                   7400 Services                   0      8,744 K
svchost.exe                   7796 Services                   0      9,740 K
svchost.exe                   7932 Services                   0     14,256 K
AggregatorHost.exe            6892 Services                   0     10,284 K
```

AggregatorHost.exe	6892	Services	0	10,284 K
svchost.exe	5048		1	16,688 K
svchost.exe	6724	Services	0	12,544 K
httpd.exe	7960	Services	0	16,148 K
StartMenuExperienceHost.e	7812		1	74,616 K
Widgets.exe	5856		1	12,888 K
RuntimeBroker.exe	7984		1	25,544 K
RuntimeBroker.exe	8280		1	45,976 K
ctfmon.exe	8352		1	25,996 K
svchost.exe	8444		1	9,404 K
svchost.exe	8836	Services	0	17,296 K
dllhost.exe	9548		1	13,856 K
backgroundTaskHost.exe	10164		1	2,248 K
LocationNotificationWindo	10540		1	3,072 K
PhoneExperienceHost.exe	11384		1	134,748 K
svchost.exe	11576	Services	0	27,028 K
SearchIndexer.exe	11644	Services	0	35,464 K
SecurityHealthSystray.exe	11732		1	9,976 K
SecurityHealthService.exe	11756	Services	0	18,092 K
GoogleCrashHandler.exe	11864	Services	0	1,096 K
GoogleCrashHandler64.exe	11880	Services	0	1,060 K
WidgetService.exe	11928		1	22,396 K
RuntimeBroker.exe	12244		1	12,844 K
RtkAudUService64.exe	12276		1	15,004 K
NisSrv.exe	12388	Services	0	9,560 K
backgroundTaskHost.exe	13144		1	2,188 K
ShellExperienceHost.exe	8500		1	56,320 K
TextInputHost.exe	11372		1	63,668 K
RuntimeBroker.exe	9500		1	27,724 K
RuntimeBroker.exe	12832		1	7,388 K
RadeonSoftware.exe	13428		1	38,208 K
svchost.exe	13496	Services	0	22,684 K
svchost.exe	13536	Services	0	7,456 K
svchost.exe	13572		1	11,452 K
SystemSettingsBroker.exe	13648		1	32,016 K
svchost.exe	13804	Services	0	6,620 K
svchost.exe	13896		1	8,876 K
svchost.exe	13924	Services	0	7,524 K
svchost.exe	14056	Services	0	13,612 K
cncmd.exe	1576		1	6,068 K
AMDRSServ.exe	12920		1	88,076 K
svchost.exe	6828	Services	0	12,632 K
WmiPrvSE.exe	12620	Services	0	13,676 K
SearchHost.exe	10520		1	88,776 K
ApplicationFrameHost.exe	248		1	31,220 K
WWAHost.exe	11224		1	75,484 K
RuntimeBroker.exe	7156		1	18,192 K
svchost.exe	6280	Services	0	15,892 K
WhatsApp.exe	1368		1	42,676 K

```
WhatsApp.exe                  1368                            1     42,676 K
svchost.exe                  11960 Services                   0     22,024 K
svchost.exe                  12688                            1     25,940 K
RuntimeBroker.exe             8784                            1     21,540 K
OMENOverlay.exe              15064                            1     65,040 K
AUEPDU.exe                   14928 Services                   0     15,508 K
svchost.exe                   8216 Services                   0     19,536 K
svchost.exe                  14704 Services                   0     14,544 K
svchost.exe                   7252 Services                   0     13,484 K
svchost.exe                  12512 Services                   0     10,352 K
SystemSettings.exe            8456                            1      2,136 K
svchost.exe                   3980 Services                   0     13,640 K
UserOOBEBroker.exe            7956                            1      8,808 K
LogonUI.exe                   2828                            1     36,576 K
csrss.exe                     7356 Console                    3     12,092 K
winlogon.exe                  2076 Console                    3     11,216 K
fontdrvhost.exe               3484 Console                    3      7,996 K
dwm.exe                      11992 Console                    3    119,664 K
atieclxx.exe                  7580 Console                    3     15,284 K
ETDCtrl.exe                   7688 Console                    3     13,832 K
RtkAudUService64.exe         16312 Console                    3     13,244 K
sihost.exe                   16224 Console                    3     35,652 K
svchost.exe                  16096 Console                    3     31,184 K
svchost.exe                  17272 Console                    3      8,312 K
SECOCL64.exe                  6748 Console                    3     10,920 K
svchost.exe                   4008 Console                    3     37,588 K
conhost.exe                   3504 Console                    3      5,808 K
taskhostw.exe                15588 Console                    3     20,432 K
explorer.exe                 16432 Console                    3    306,932 K
ctfmon.exe                   16528 Console                    3     30,320 K
svchost.exe                  15676 Console                    3     26,816 K
OverlayHelper.exe             1552 Console                    3    686,848 K
OverlayHelper.exe             8952                            1    784,724 K
Widgets.exe                  11612 Console                    3     53,052 K
msteams.exe                  14728 Console                    3     21,448 K
StartMenuExperienceHost.e    13352 Console                    3    114,188 K
SearchHost.exe                1880 Console                    3    267,324 K
RuntimeBroker.exe             4256 Console                    3     56,028 K
WWAHost.exe                   6276 Console                    3     65,316 K
RuntimeBroker.exe             9772 Console                    3     28,752 K
RuntimeBroker.exe            10020 Console                    3     27,288 K
RuntimeBroker.exe            15448 Console                    3     10,768 K
svchost.exe                   8696 Console                    3     13,652 K
msedgewebview2.exe            7160 Console                    3     44,388 K
msedgewebview2.exe           17264 Console                    3      7,616 K
msedgewebview2.exe           15996 Console                    3      9,104 K
msedgewebview2.exe           15988 Console                    3     18,652 K
msedgewebview2.exe           17160 Console                    3      5,952 K
msedgewebview2.exe            3204 Console                    3     43,600 K
```

13.- Utilizar el comando taskkill

```
C:\Windows\System32>taskkill /pid 1368
ERROR: The process with PID 1368 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
```

14.- Utilizar el comando tracert.

```
C:\Windows\System32> tracert google.com

Tracing route to google.com [172.253.124.139]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  172.16.128.1
  2     1 ms     1 ms     1 ms  192.168.109.1
  3     6 ms    10 ms     4 ms  fixed-187-188-58-130.totalplay.net [187.188.58.130]
  4     4 ms     9 ms     5 ms  10.180.58.1
  5    18 ms    20 ms    17 ms  72.14.242.148
  6    18 ms    20 ms    17 ms  209.85.253.117
  7    20 ms    18 ms    18 ms  108.170.253.18
  8    31 ms    23 ms    20 ms  142.250.212.10
  9    32 ms    34 ms    32 ms  142.250.237.154
 10    32 ms    32 ms    32 ms  108.170.232.7
 11    34 ms    32 ms    32 ms  209.85.242.161
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21    31 ms    31 ms    31 ms  ys-in-f139.1e100.net [172.253.124.139]

Trace complete.
```

15. Utilizar el comando ARP

```
C:\Windows\System32> arp -a

Interface: 192.168.56.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.16.129.150 --- 0xf
  Internet Address      Physical Address      Type
  172.16.128.1          00-0c-e6-f5-d8-73     dynamic
  172.16.143.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

B) Contesta con tus propias palabras las siguientes preguntas:

1.- ¿Para qué sirve el comando ping?

Desde mi punto de vista, la función del comando 'ping' es realizar un análisis de la red del dispositivo con el fin de identificar posibles inconvenientes que puedan surgir durante la transferencia de datos o paquetes y encontrar soluciones a dichos problemas.

2.- ¿Para qué sirve el comando nslookup?

Es una herramienta útil para administradores de sistemas y redes, ya que les permite obtener información sobre la resolución de nombres de dominio y diagnosticar problemas relacionados con la resolución DNS.

3.- ¿Para qué sirve el comando netstat?

El comando 'netstat' proporciona datos estadísticos relativos a la red y las conexiones en curso en un sistema, brindando información detallada sobre los puertos, las comunicaciones de red, las rutas de enrutamiento y otros aspectos. Su utilidad reside en la vigilancia del flujo de datos en la red y la identificación de posibles dificultades en la conectividad.

4-¿Para qué sirve el comando tasklist?

Se emplea para enlistar los procesos en curso en un sistema Windows, proporcionando información acerca de las aplicaciones y servicios actualmente en funcionamiento.

5.- ¿Para qué sirve el comando taskkill?

Se emplea para terminar procesos en un sistema Windows. Puedes utilizarlo para detener aplicaciones o procesos que no responden, así como para cerrar procesos no deseados.

6.- ¿Para qué sirve el comando tracert?

El comando "tracert" o "traceroute" generalmente se ejecuta desde la línea de comandos en sistemas como Windows (donde se usa "tracert") o sistemas basados en Unix (donde se usa "traceroute").

7-¿Cómo ayudan los primeros tres comandos para detectar problemas en la red?

Estos 3 combinados nos ayudan a tener toda la información completa de las conexiones de nuestra computadora por lo que tenemos acceso a la información completa y un diagnóstico más detallado.