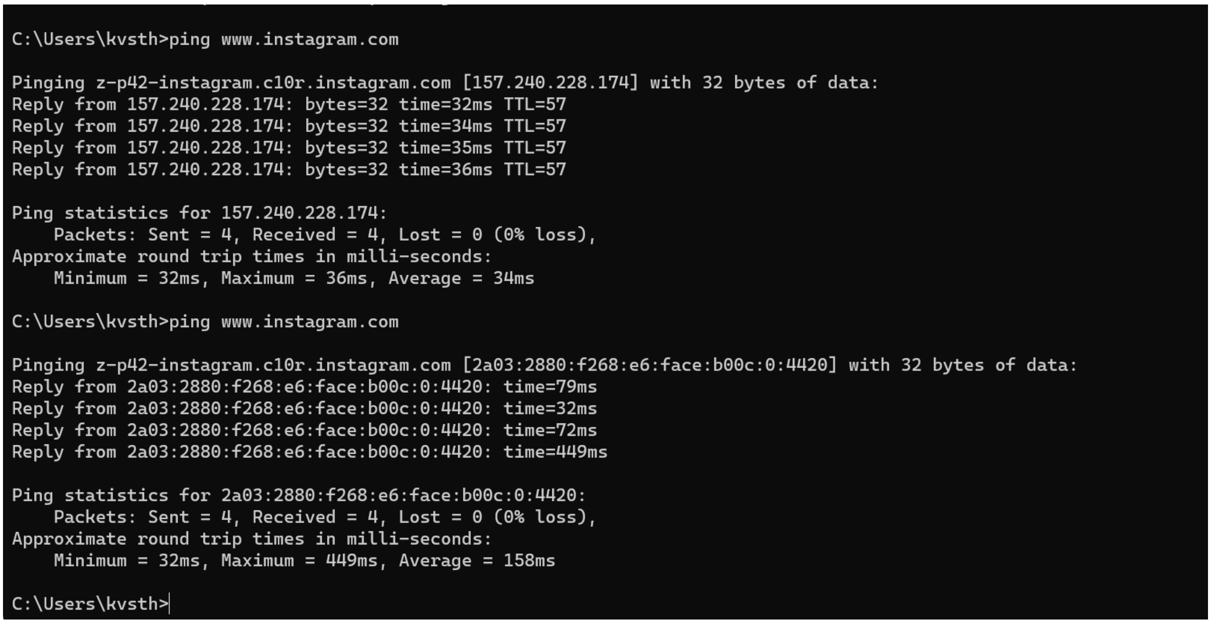
COMPUTER NETWORKS

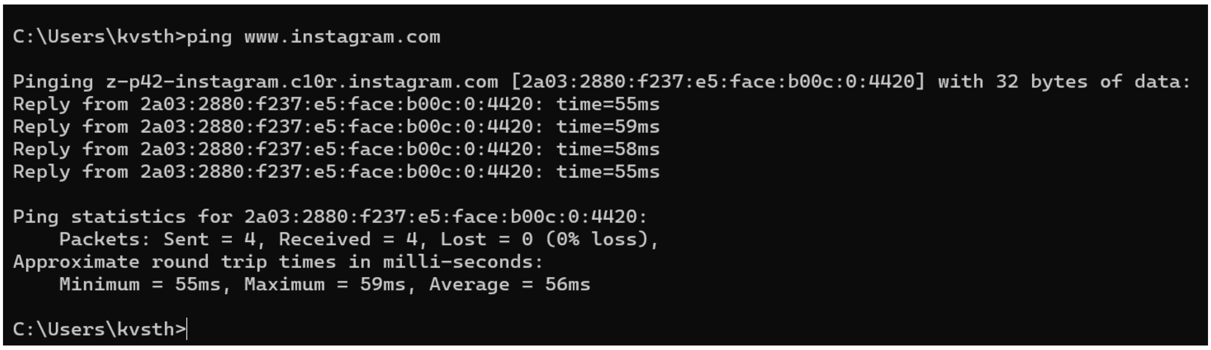
NAME - KAPAROTU VENKATA SURYA THARANI
USN - 22BTRAD018
BRANCH - AIDE

Experiment 1: Ping

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: ping www.example.com.
3. Observe the output and record the following information:
   Response time of each ping
   Number of packets sent and received
   Any packet loss or errors encountered
   The IP address of the target



```
C:\Users\kvsth>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [157.240.228.174] with 32 bytes of data:
Reply from 157.240.228.174: bytes=32 time=32ms TTL=57
Reply from 157.240.228.174: bytes=32 time=34ms TTL=57
Reply from 157.240.228.174: bytes=32 time=35ms TTL=57
Reply from 157.240.228.174: bytes=32 time=36ms TTL=57

Ping statistics for 157.240.228.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 36ms, Average = 34ms

C:\Users\kvsth>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [2a03:2880:f268:e6:face:b00c:0:4420] with 32 bytes of data:
Reply from 2a03:2880:f268:e6:face:b00c:0:4420: time=79ms
Reply from 2a03:2880:f268:e6:face:b00c:0:4420: time=32ms
Reply from 2a03:2880:f268:e6:face:b00c:0:4420: time=72ms
Reply from 2a03:2880:f268:e6:face:b00c:0:4420: time=449ms

Ping statistics for 2a03:2880:f268:e6:face:b00c:0:4420:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 449ms, Average = 158ms

C:\Users\kvsth>
```

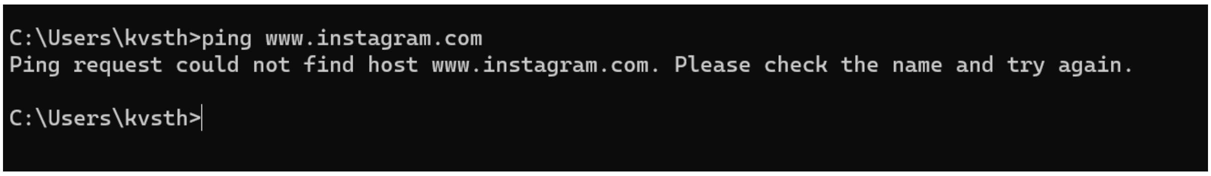


```
C:\Users\kvsth>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [2a03:2880:f237:e5:face:b00c:0:4420] with 32 bytes of data:
Reply from 2a03:2880:f237:e5:face:b00c:0:4420: time=55ms
Reply from 2a03:2880:f237:e5:face:b00c:0:4420: time=59ms
Reply from 2a03:2880:f237:e5:face:b00c:0:4420: time=58ms
Reply from 2a03:2880:f237:e5:face:b00c:0:4420: time=55ms

Ping statistics for 2a03:2880:f237:e5:face:b00c:0:4420:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 59ms, Average = 56ms

C:\Users\kvsth>
```

Used three different networks and used the ping cmd to execute www.instagram.com.

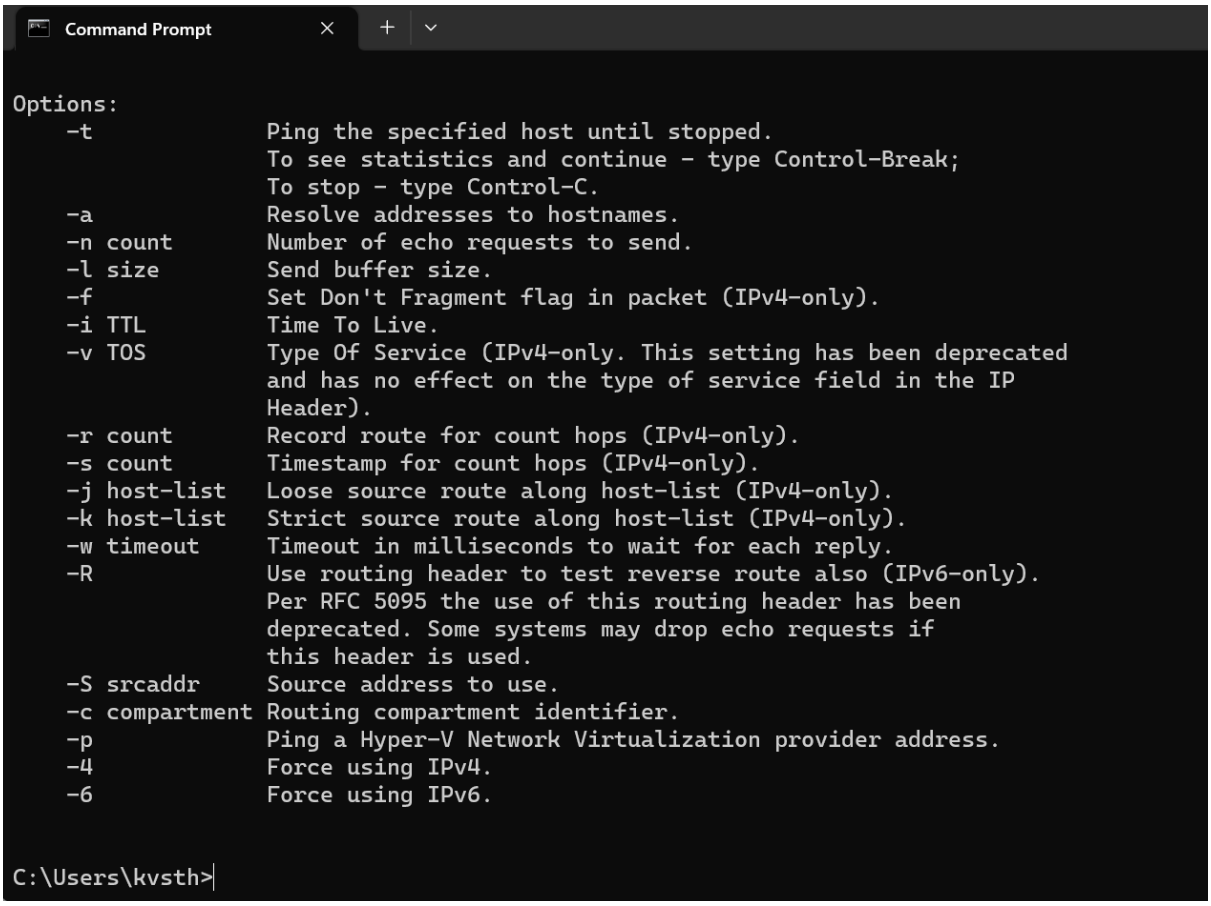
ping command is used to check whether the device is connected to a network connection or not.

If you are not connected to a network then it will show like this:

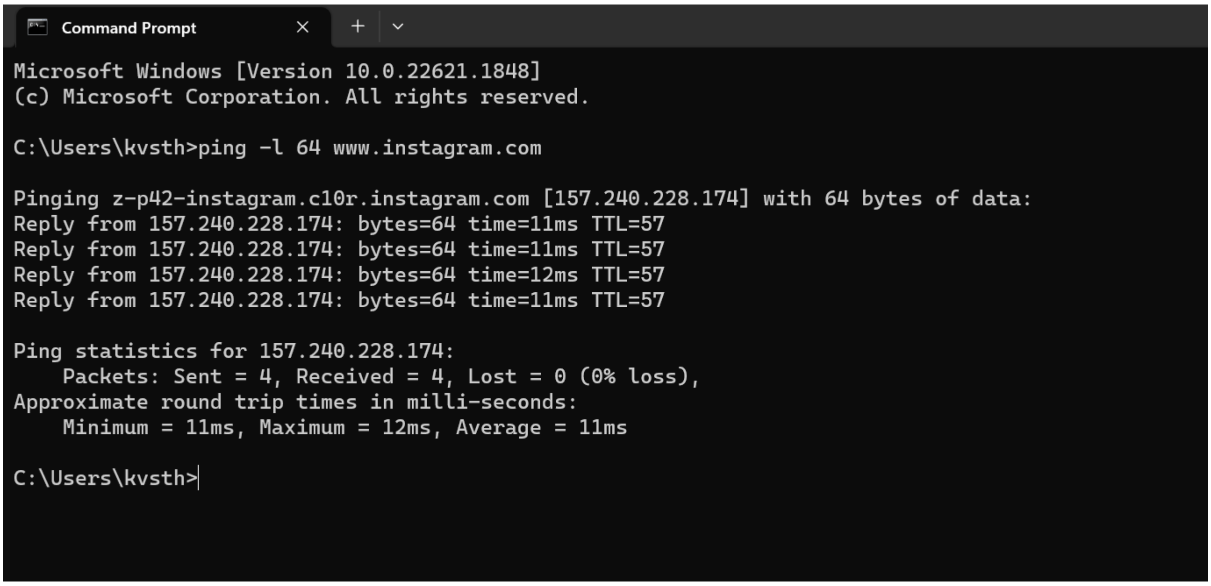


```
C:\Users\kvsth>ping www.instagram.com
Ping request could not find host www.instagram.com. Please check the name and try again.

C:\Users\kvsth>
```

Various options available in ping command are:

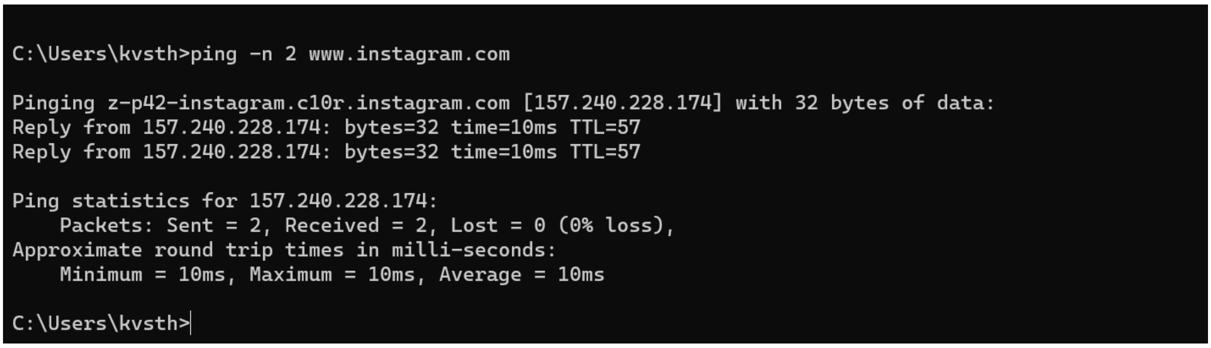


```
Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        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:\Users\kvsth>
```



```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>ping -l 64 www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [157.240.228.174] with 64 bytes of data:
Reply from 157.240.228.174: bytes=64 time=11ms TTL=57
Reply from 157.240.228.174: bytes=64 time=11ms TTL=57
Reply from 157.240.228.174: bytes=64 time=12ms TTL=57
Reply from 157.240.228.174: bytes=64 time=11ms TTL=57

Ping statistics for 157.240.228.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\Users\kvsth>
```

ping -l cmd is used to change the bytes for eg - 32 to 64 bytes of data.

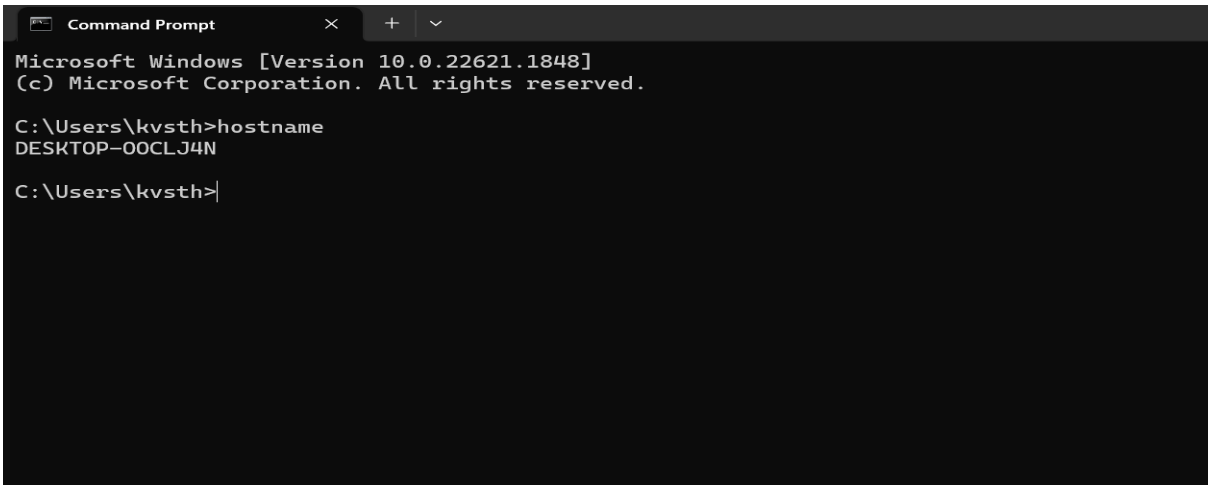


```
C:\Users\kvsth>ping -n 2 www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [157.240.228.174] with 32 bytes of data:
Reply from 157.240.228.174: bytes=32 time=10ms TTL=57
Reply from 157.240.228.174: bytes=32 time=10ms TTL=57

Ping statistics for 157.240.228.174:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\Users\kvsth>
```

ping -n count command is used to get the number of packets we want.

Experiment 2: Hostname

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: hostname.
3. Record the output, which will display the hostname of your computer.



```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>hostname
DESKTOP-OOCLJ4N

C:\Users\kvsth>
```

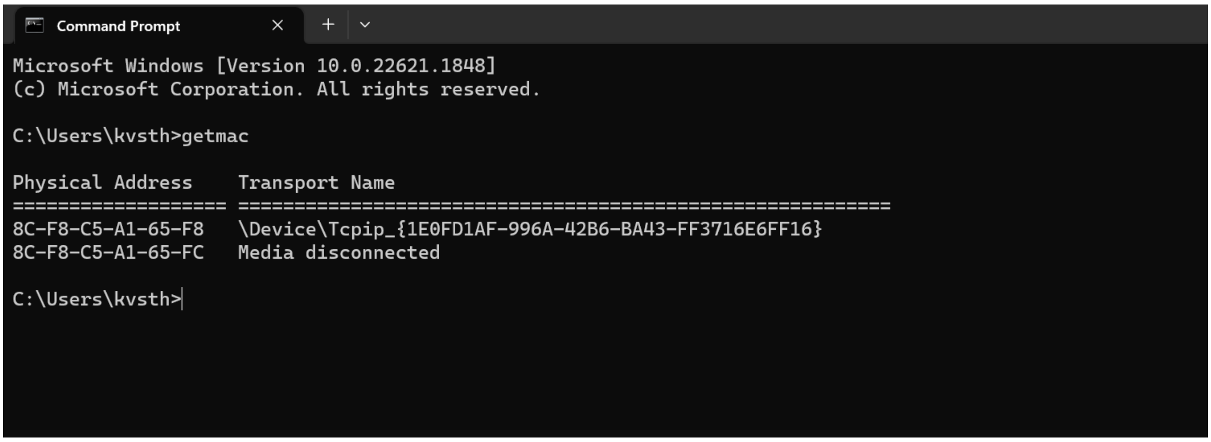
Using the ‘hostname’ command we can get the hostname i.e. the name of the device present in the network.

Experiment 3: Getmac

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: getmac.
3. Observe the output and record the following information:

    a. MAC (Media Access Control) address of each network adapter on your computer

    b. Connection type (wired or wireless).

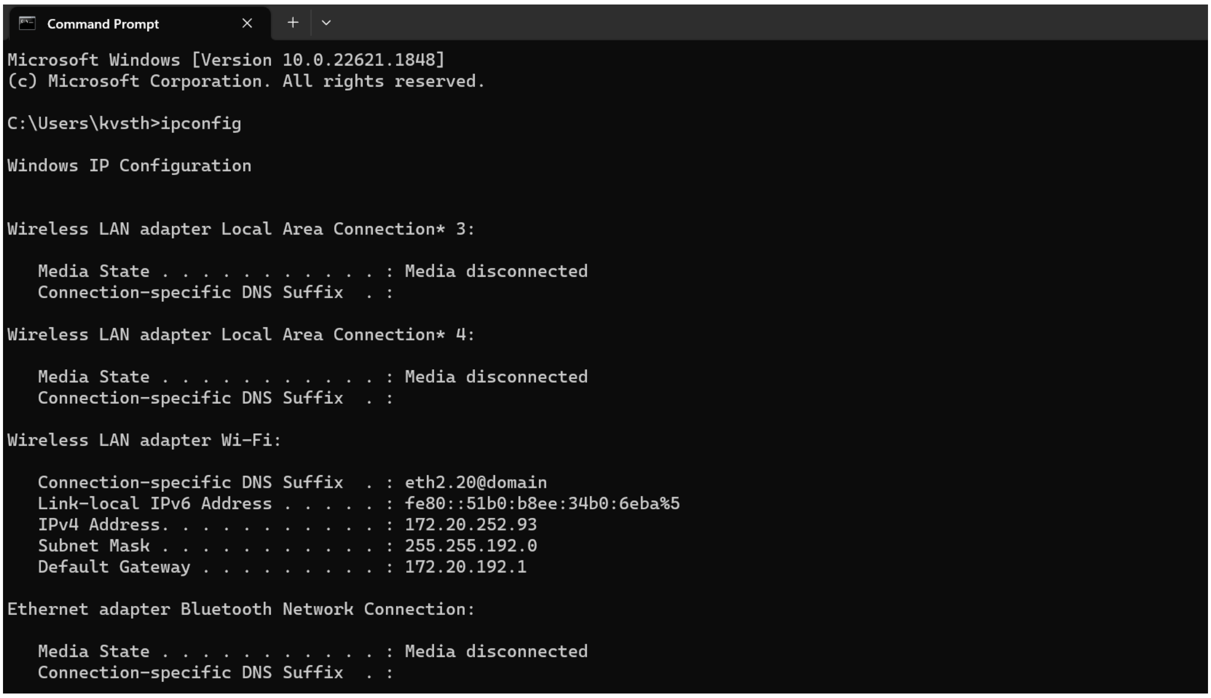


```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>getmac

Physical Address    Transport Name
=================== ==========================================================
8C-F8-C5-A1-65-F8   \Device\Tcpip_{1E0FD1AF-996A-42B6-BA43-FF3716E6FF16}
8C-F8-C5-A1-65-FC   Media disconnected

C:\Users\kvsth>
```

‘getmac’ cmd is used to get the Media Access Control(MAC) address of the device connected to a network that is unique to every device.
The device can be identified by looking at its mac address.
The connection type is wireless between the device and the network.

Experiment 4: Ipconfig

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: ipconfig.
3. Observe the output and record the following information:
   a. IP address, subnet mask, and default gateway of each network adapter on your computer
   b. DNS (Domain Name System) server information
   c. Any active network connections and their configurations.



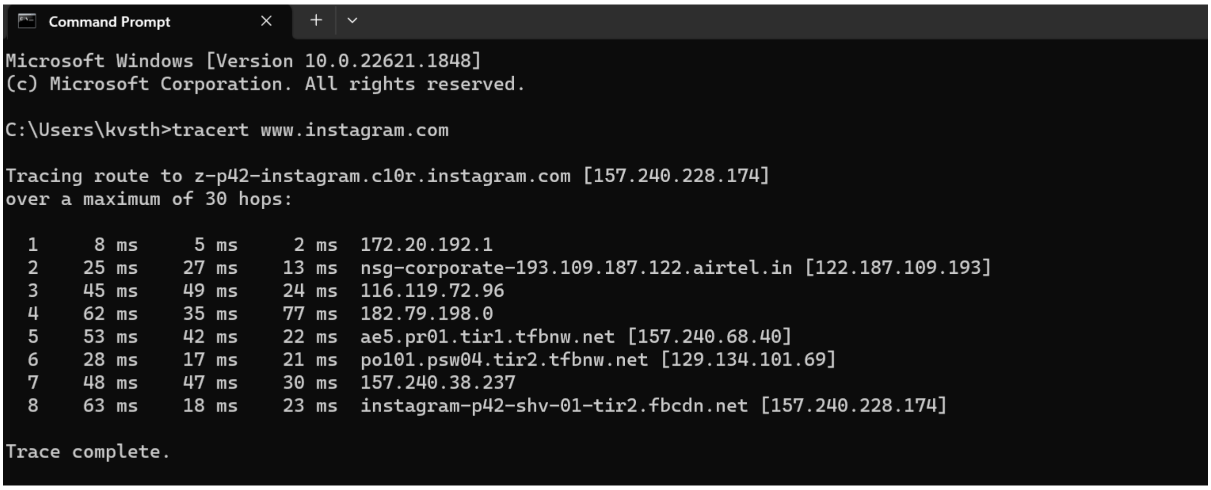
```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : eth2.20@domain
   Link-local IPv6 Address . . . . . : fe80::51b0:b8ee:34b0:6eba%5
   IPv4 Address. . . . . . . . . . . : 172.20.252.93
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Default Gateway . . . . . . . . . : 172.20.192.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

IP address gives the address of the network to which the device is connected. Mac address gives the address of the device in the network whereas IP address gives the address of the network to which it is connected.

Experiment 5: Tracert

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: tracert www.example.com.
3. Observe the output and record the following information:

   List of hops (routers) between your computer and the target
   Response time of each hop
   IP addresses of intermediate routers

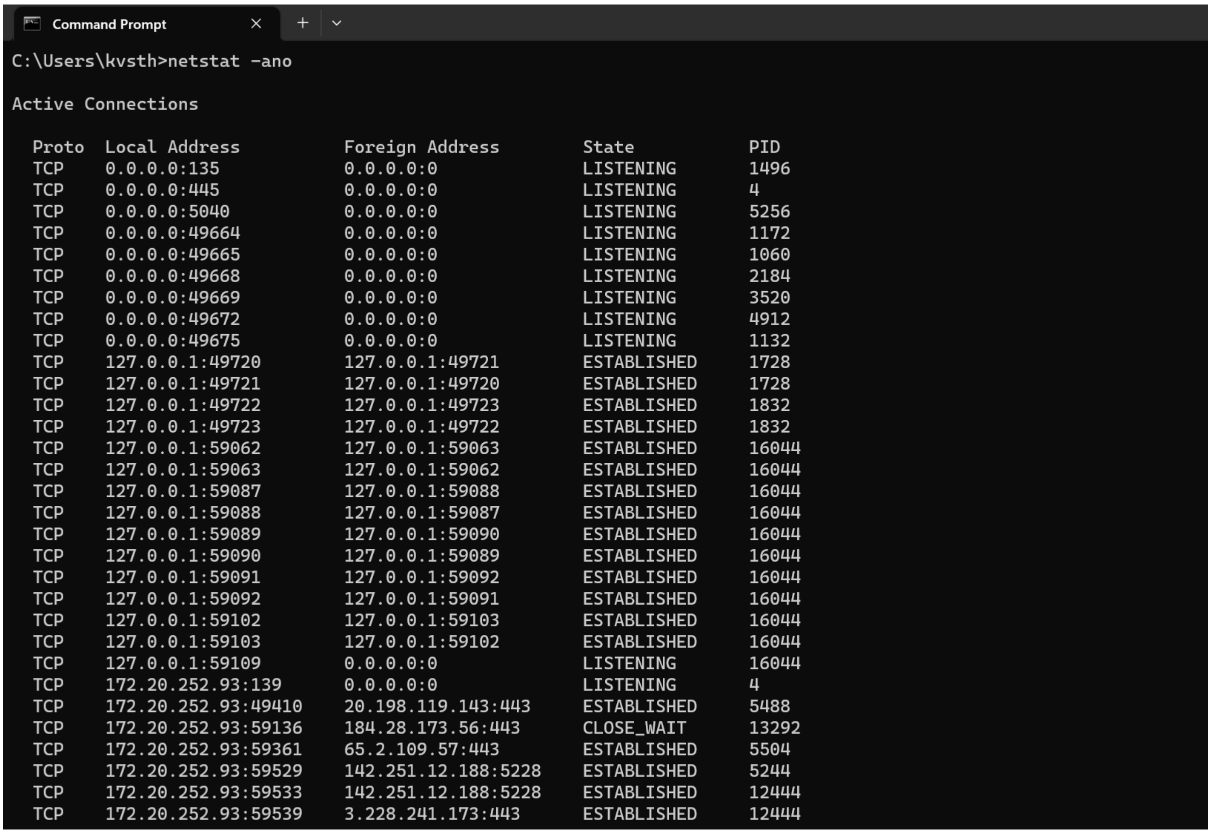


```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>tracert www.instagram.com

Tracing route to z-p42-instagram.c10r.instagram.com [157.240.228.174]
over a maximum of 30 hops:

  1     8 ms     5 ms     2 ms  172.20.192.1
  2    25 ms    27 ms    13 ms  nsg-corporate-193.109.187.122.airtel.in [122.187.109.193]
  3    45 ms    49 ms    24 ms  116.119.72.96
  4    62 ms    35 ms    77 ms  182.79.198.0
  5    53 ms    42 ms    22 ms  ae5.pr01.tir1.tfbnw.net [157.240.68.40]
  6    28 ms    17 ms    21 ms  po101.psw04.tir2.tfbnw.net [129.134.101.69]
  7    48 ms    47 ms    30 ms  157.240.38.237
  8    63 ms    18 ms    23 ms  instagram-p42-shv-01-tir2.fbcdn.net [157.240.228.174]

Trace complete.
```

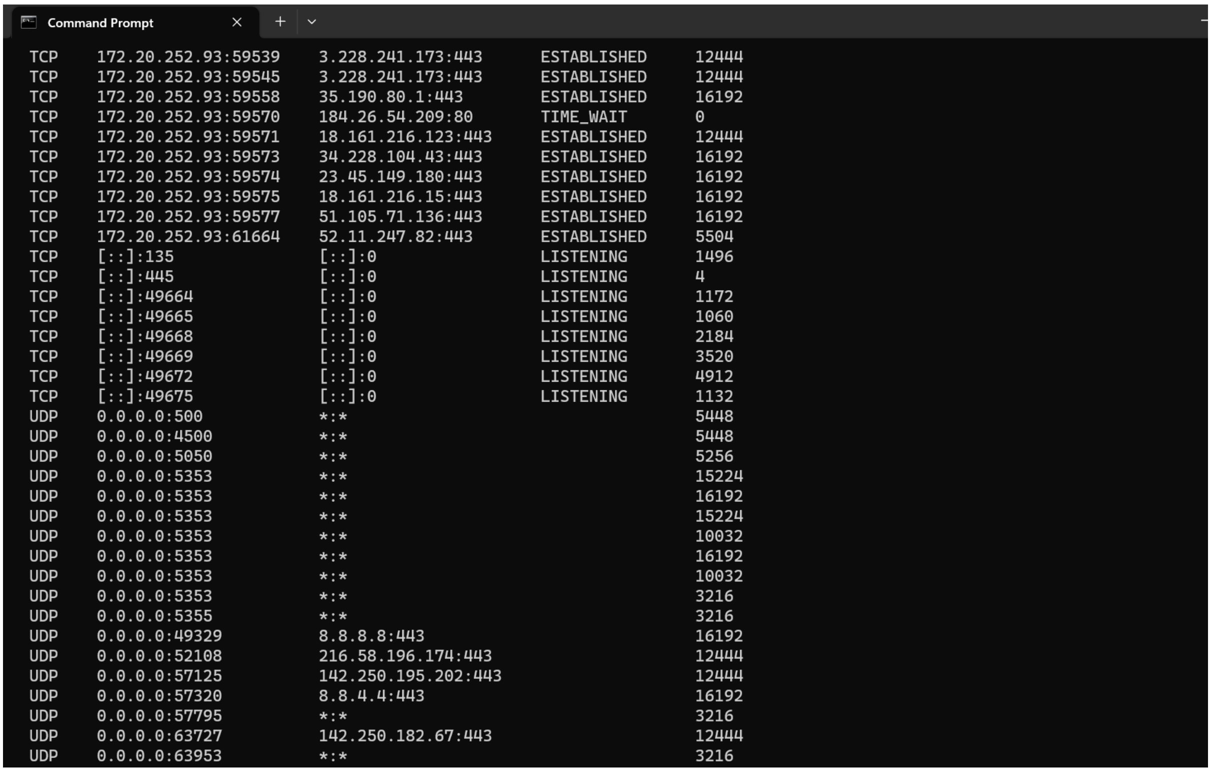
The Tracert command is used to trace the routes taken by the packets to go to their destination IP address.
It will give a list of hops (routers), response time that is how much time they took to transfer, and the IP address of the corresponding routers, that help in the transmission of the packets from the source IP address to the destination IP.

Experiment 6: Netstat

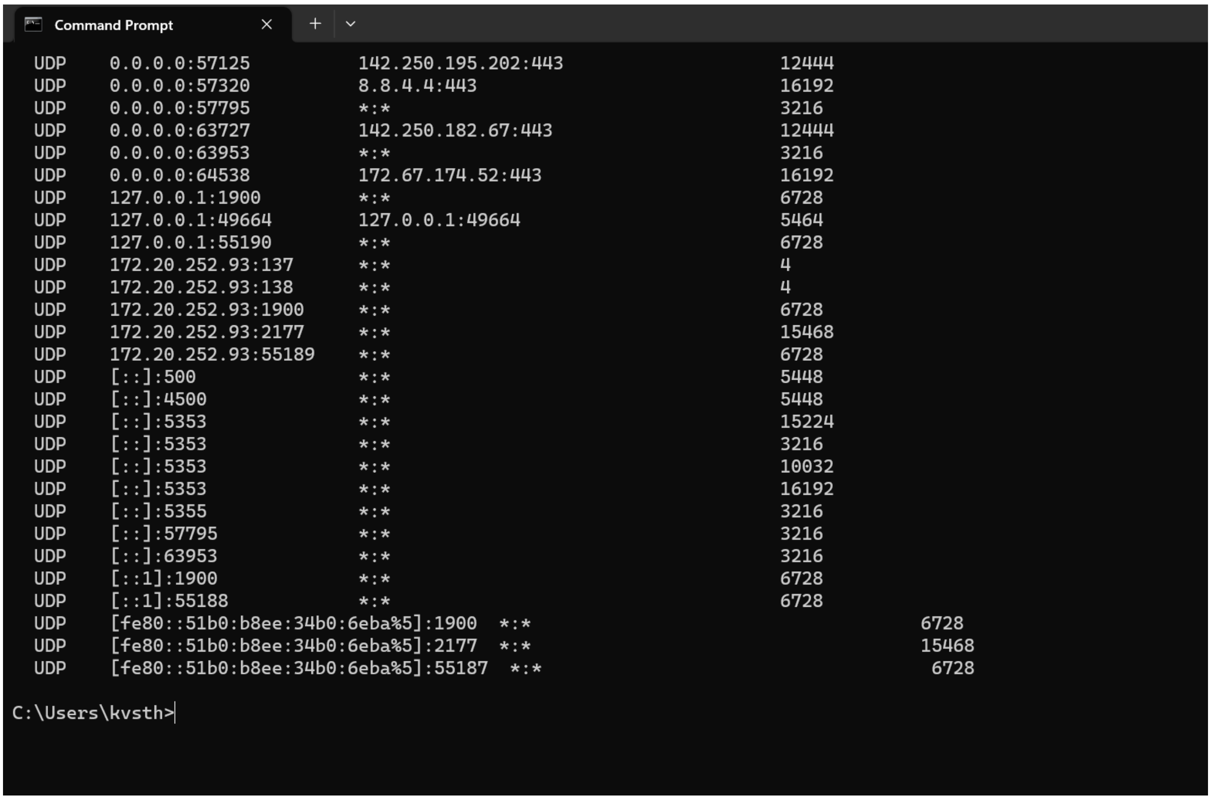
1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: netstat -ano.
3. Observe the output and record the following information:
   List of active network connections on your computer
   Local and remote IP addresses and port numbers
   Protocol used (TCP or UDP)
   State of each connection (established, listening, etc.)



```
C:\Users\kvsth>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1496
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5256
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1172
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1060
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2184
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       3520
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       4912
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING       1132
  TCP    127.0.0.1:49720        127.0.0.1:49721        ESTABLISHED     1728
  TCP    127.0.0.1:49721        127.0.0.1:49720        ESTABLISHED     1728
  TCP    127.0.0.1:49722        127.0.0.1:49723        ESTABLISHED     1832
  TCP    127.0.0.1:49723        127.0.0.1:49722        ESTABLISHED     1832
  TCP    127.0.0.1:59062        127.0.0.1:59063        ESTABLISHED     16044
  TCP    127.0.0.1:59063        127.0.0.1:59062        ESTABLISHED     16044
  TCP    127.0.0.1:59087        127.0.0.1:59088        ESTABLISHED     16044
  TCP    127.0.0.1:59088        127.0.0.1:59087        ESTABLISHED     16044
  TCP    127.0.0.1:59089        127.0.0.1:59090        ESTABLISHED     16044
  TCP    127.0.0.1:59090        127.0.0.1:59089        ESTABLISHED     16044
  TCP    127.0.0.1:59091        127.0.0.1:59092        ESTABLISHED     16044
  TCP    127.0.0.1:59092        127.0.0.1:59091        ESTABLISHED     16044
  TCP    127.0.0.1:59102        127.0.0.1:59103        ESTABLISHED     16044
  TCP    127.0.0.1:59103        127.0.0.1:59102        ESTABLISHED     16044
  TCP    127.0.0.1:59109        0.0.0.0:0              LISTENING       16044
  TCP    172.20.252.93:139      0.0.0.0:0              LISTENING       4
  TCP    172.20.252.93:49410    20.198.119.143:443     ESTABLISHED     5488
  TCP    172.20.252.93:59136    184.28.173.56:443      CLOSE_WAIT      13292
  TCP    172.20.252.93:59361    65.2.109.57:443        ESTABLISHED     5504
  TCP    172.20.252.93:59529    142.251.12.188:5228    ESTABLISHED     5244
  TCP    172.20.252.93:59533    142.251.12.188:5228    ESTABLISHED     12444
  TCP    172.20.252.93:59539    3.228.241.173:443      ESTABLISHED     12444
```



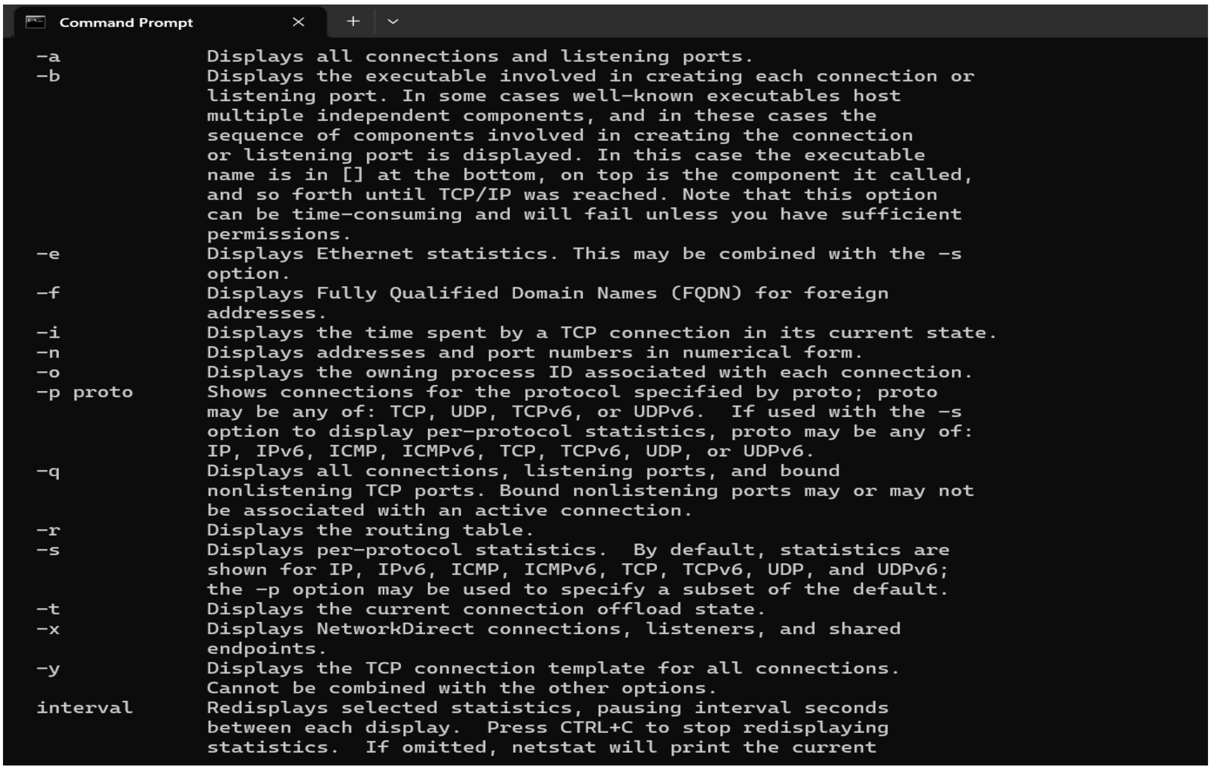
```
  TCP    172.20.252.93:59539    3.228.241.173:443      ESTABLISHED     12444
  TCP    172.20.252.93:59545    3.228.241.173:443      ESTABLISHED     12444
  TCP    172.20.252.93:59558    35.190.80.1:443        ESTABLISHED     16192
  TCP    172.20.252.93:59570    184.26.54.209:80       TIME_WAIT       0
  TCP    172.20.252.93:59571    18.161.216.123:443     ESTABLISHED     12444
  TCP    172.20.252.93:59573    34.228.104.43:443      ESTABLISHED     16192
  TCP    172.20.252.93:59574    23.45.149.180:443      ESTABLISHED     16192
  TCP    172.20.252.93:59575    18.161.216.15:443      ESTABLISHED     16192
  TCP    172.20.252.93:59577    51.105.71.136:443      ESTABLISHED     16192
  TCP    172.20.252.93:61664    52.11.247.82:443       ESTABLISHED     5504
  TCP    [::]:135               [::]:0                 LISTENING       1496
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       1172
  TCP    [::]:49665             [::]:0                 LISTENING       1060
  TCP    [::]:49668             [::]:0                 LISTENING       2184
  TCP    [::]:49669             [::]:0                 LISTENING       3520
  TCP    [::]:49672             [::]:0                 LISTENING       4912
  TCP    [::]:49675             [::]:0                 LISTENING       1132
  UDP    0.0.0.0:500            *:*                                    5448
  UDP    0.0.0.0:4500           *:*                                    5448
  UDP    0.0.0.0:5050           *:*                                    5256
  UDP    0.0.0.0:5353           *:*                                    15224
  UDP    0.0.0.0:5353           *:*                                    16192
  UDP    0.0.0.0:5353           *:*                                    15224
  UDP    0.0.0.0:5353           *:*                                    10032
  UDP    0.0.0.0:5353           *:*                                    16192
  UDP    0.0.0.0:5353           *:*                                    10032
  UDP    0.0.0.0:5353           *:*                                    3216
  UDP    0.0.0.0:5355           *:*                                    3216
  UDP    0.0.0.0:49329          8.8.8.8:443                            16192
  UDP    0.0.0.0:52108          216.58.196.174:443                     12444
  UDP    0.0.0.0:57125          142.250.195.202:443                    12444
  UDP    0.0.0.0:57320          8.8.4.4:443                            16192
  UDP    0.0.0.0:57795          *:*                                    3216
  UDP    0.0.0.0:63727          142.250.182.67:443                     12444
  UDP    0.0.0.0:63953          *:*                                    3216
```



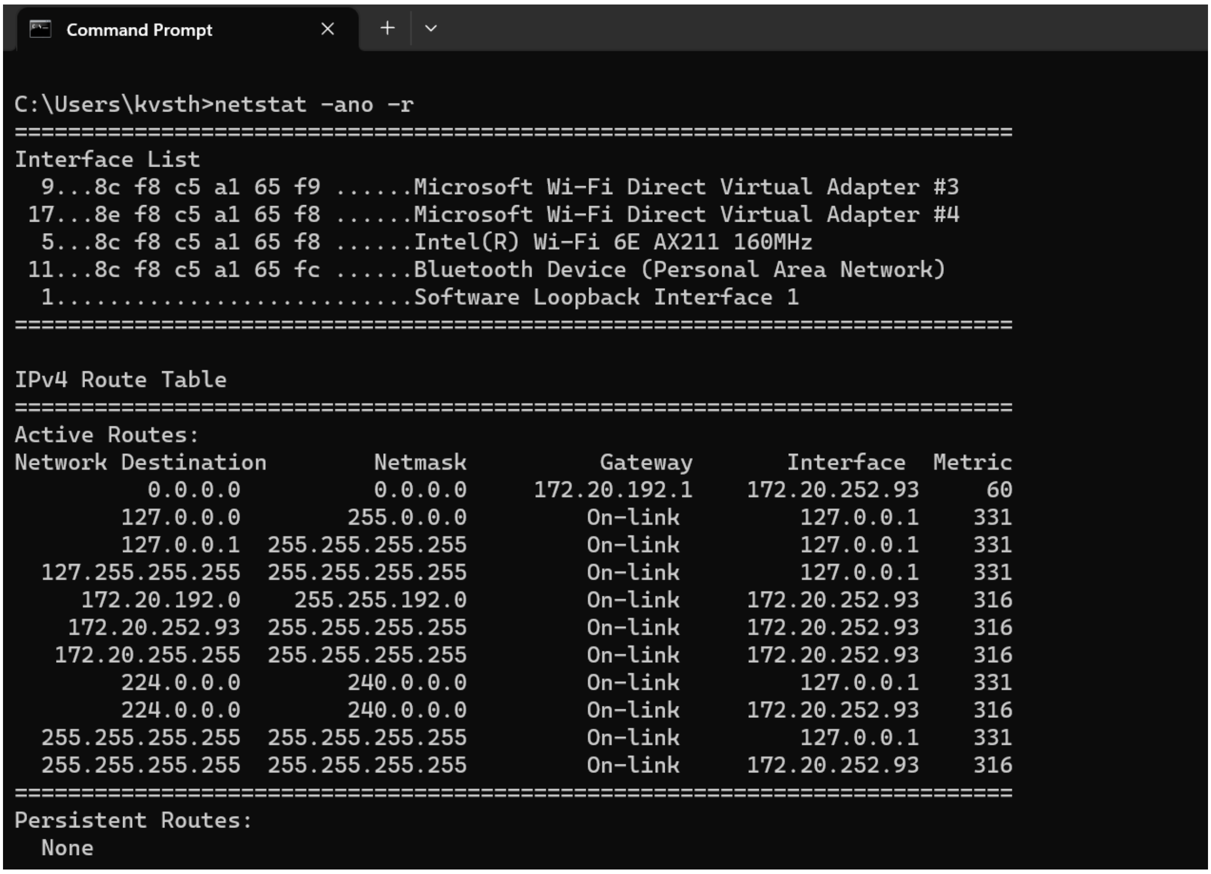
```
  UDP    0.0.0.0:57125          142.250.195.202:443                    12444
  UDP    0.0.0.0:57320          8.8.4.4:443                            16192
  UDP    0.0.0.0:57795          *:*                                    3216
  UDP    0.0.0.0:63727          142.250.182.67:443                     12444
  UDP    0.0.0.0:63953          *:*                                    3216
  UDP    0.0.0.0:64538          172.67.174.52:443                      16192
  UDP    127.0.0.1:1900         *:*                                    6728
  UDP    127.0.0.1:49664        127.0.0.1:49664                        5464
  UDP    127.0.0.1:55190        *:*                                    6728
  UDP    172.20.252.93:137      *:*                                    4
  UDP    172.20.252.93:138      *:*                                    4
  UDP    172.20.252.93:1900     *:*                                    6728
  UDP    172.20.252.93:2177     *:*                                    15468
  UDP    172.20.252.93:55189    *:*                                    6728
  UDP    [::]:500               *:*                                    5448
  UDP    [::]:4500              *:*                                    5448
  UDP    [::]:5353              *:*                                    15224
  UDP    [::]:5353              *:*                                    3216
  UDP    [::]:5353              *:*                                    10032
  UDP    [::]:5353              *:*                                    16192
  UDP    [::]:5355              *:*                                    3216
  UDP    [::]:57795             *:*                                    3216
  UDP    [::]:63953             *:*                                    3216
  UDP    [::1]:1900             *:*                                    6728
  UDP    [::1]:55188            *:*                                    6728
  UDP    [fe80::51b0:b8ee:34b0:6eba%5]:1900  *:*                                    6728
  UDP    [fe80::51b0:b8ee:34b0:6eba%5]:2177  *:*                                    15468
  UDP    [fe80::51b0:b8ee:34b0:6eba%5]:55187  *:*                                    6728

C:\Users\kvsth>
```

netstat -ano command is used to display active network connections in your device, id of the associated processes. This cmd is helpful in various ways identifying which processes are using which network connection or ports, and investigating network performance issues.

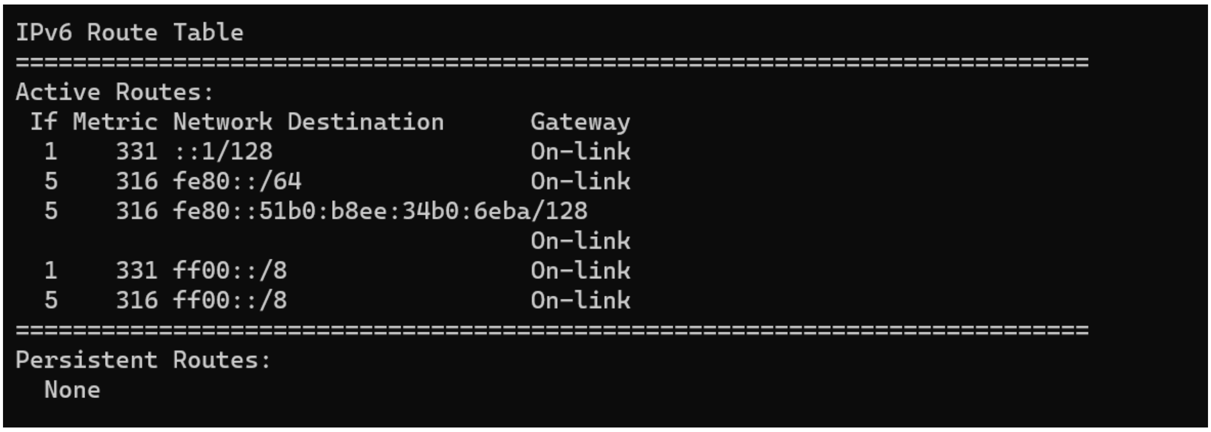
Various options are available in the netstat -ano command:



```
  -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
```



```
C:\Users\kvsth>netstat -ano -r
===========================================================================
Interface List
  9...8c f8 c5 a1 65 f9 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 17...8e f8 c5 a1 65 f8 ......Microsoft Wi-Fi Direct Virtual Adapter #4
  5...8c f8 c5 a1 65 f8 ......Intel(R) Wi-Fi 6E AX211 160MHz
 11...8c f8 c5 a1 65 fc ......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     172.20.192.1    172.20.252.93     60
        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
     172.20.192.0    255.255.192.0         On-link     172.20.252.93    316
    172.20.252.93  255.255.255.255         On-link     172.20.252.93    316
   172.20.255.255  255.255.255.255         On-link     172.20.252.93    316
        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     172.20.252.93    316
  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     172.20.252.93    316
===========================================================================
Persistent Routes:
  None
```

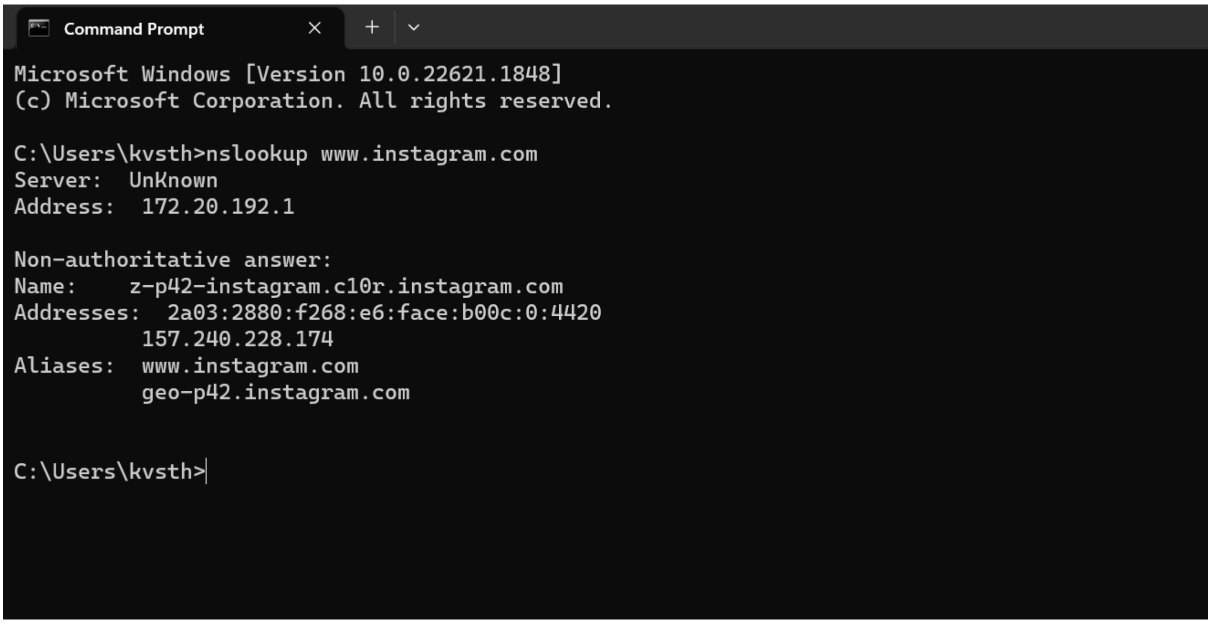


```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  5    316 fe80::/64                On-link
  5    316 fe80::51b0:b8ee:34b0:6eba/128
                                    On-link
  1    331 ff00::/8                 On-link
  5    316 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

netstat -ano -r command gives us the routing table. The routing table is used to determine the best path for forwarding packets of data from the source to the destination. The routing table contains information about the network destinations, next-hop routers, and associated metrics or preferences.

Experiment 7: Nslookup

1. Open the Command Prompt or PowerShell on your computer.
2. Execute the following command: nslookup www.example.com.
3. Observe the output and record the following information:
   IP address(es) associated with the given domain name
   DNS server(s) used for the lookup
   Additional details such as the TTL (Time to Live) value



```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kvsth>nslookup www.instagram.com
Server:  UnKnown
Address:  172.20.192.1

Non-authoritative answer:
Name:    z-p42-instagram.c10r.instagram.com
Addresses:  2a03:2880:f268:e6:face:b00c:0:4420
          157.240.228.174
Aliases:  www.instagram.com
          geo-p42.instagram.com


C:\Users\kvsth>
```

The "nslookup" command is a network administration tool used to query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and related DNS records.