Srushti Shinde
Roll No: 71

Experiment no 8

AIM:-Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars

Requirements Required: command prompt, printout pages,printer

Theory:-

Network reconnaissance is the process through which threat actors collect information about target networks before mounting an attack. It typically involves the use of techniques such as networking scanning and probing to identify potentially exploitable vulnerabilities.

Network Reconnaissance involves identifying and mapping network assets to locate potential entry points. It is often the first stage in Automated Penetration Testing scenarios.

Network reconnaissance is important because it provides actionable information on network vulnerabilities and security posture.

For threat actors, this is essential as it enables them to establish a plan of attack.

For defenders, understanding these methods is equally important because it enables them to identify and mitigate exploitable vulnerabilities through vulnerability management practices, which systematically prioritize and address network weaknesses.

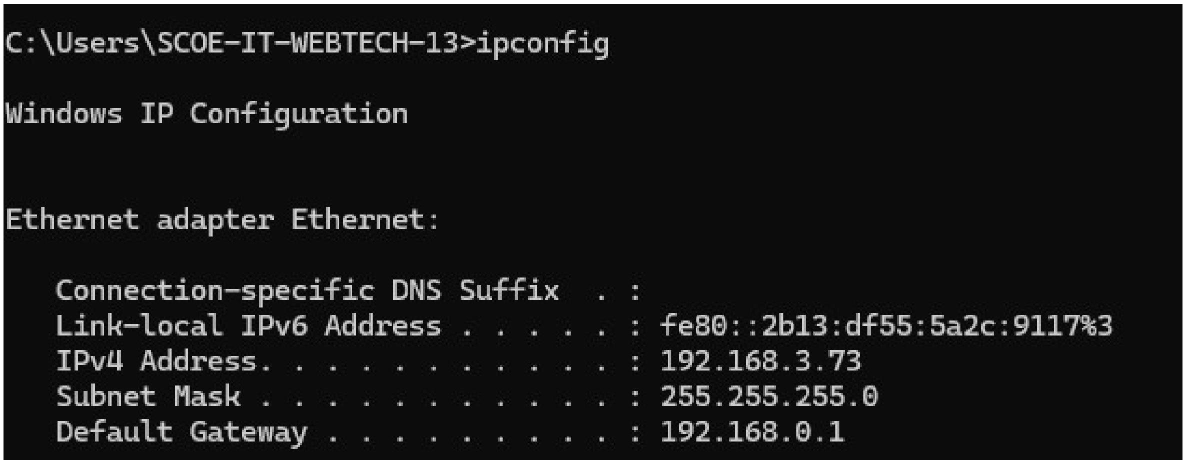
The purpose of network reconnaissance is to learn technical details about open ports, IPs, security, active services, security mechanisms, and more. This information helps threat actors establish a clear understanding of IT infrastructure and network topology so as to map out potential entry points and attack paths. For defenders, this information enables the anticipation of certain attack vectors so that defenses can be strengthened preemptively through automated penetration testing methods.

During this process, threat actors employ a variety of different techniques to help them uncover network vulnerabilities. These include the following:

(1) ipconfig:

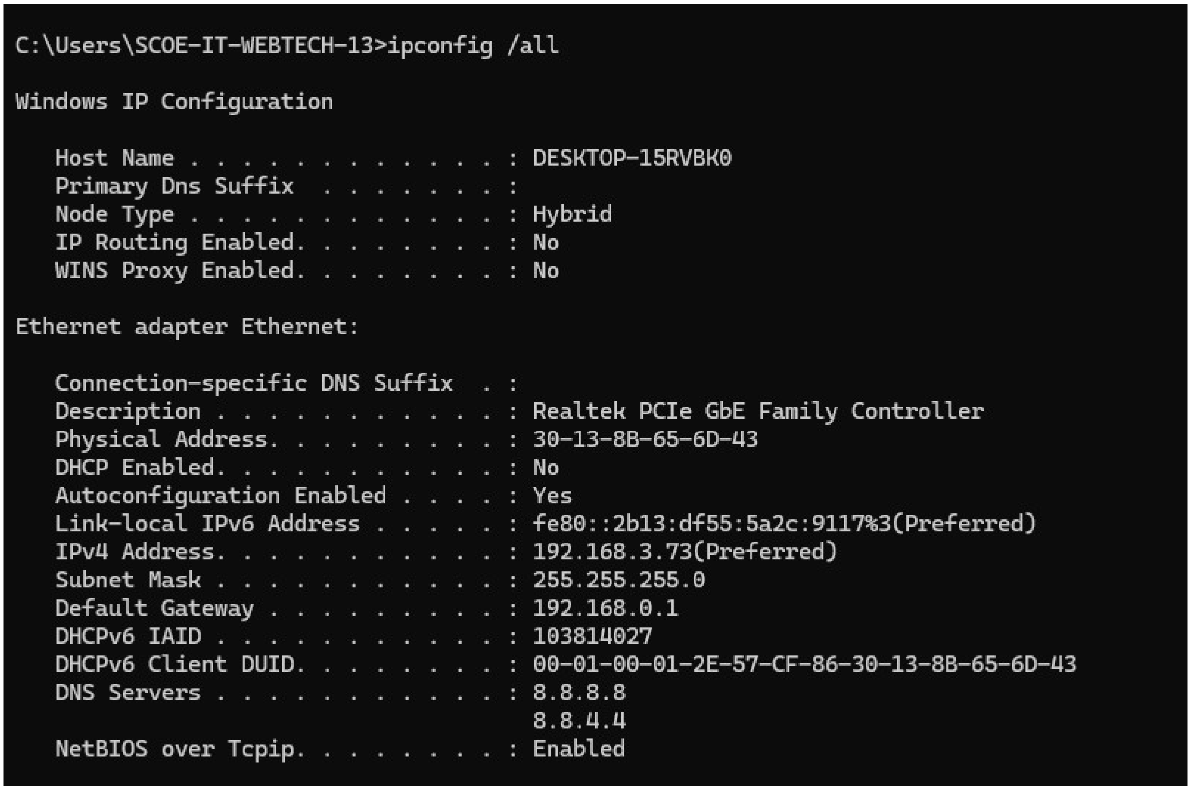
Displays current IP address, subnet mask, default gateway, and other network configuration details. Using ipconfig /all provides more comprehensive information including MAC address and DHCP status.

- ipconfig:



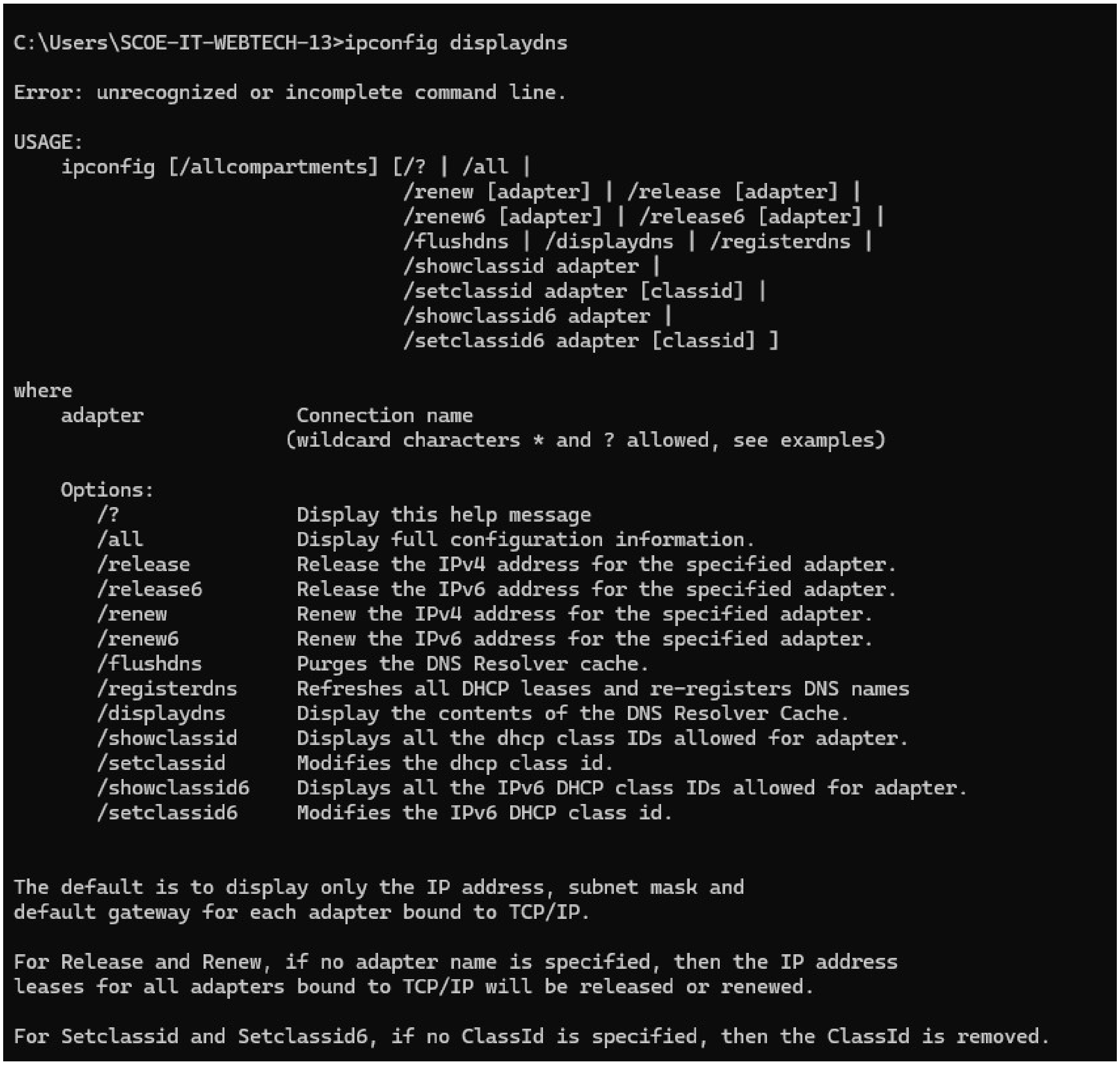
```
C:\Users\SCOE-IT-WEBTECH-13>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2b13:df55:5a2c:9117%3
   IPv4 Address. . . . . . . . . . . : 192.168.3.73
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

- ipconfig/all:



```
C:\Users\SCOE-IT-WEBTECH-13>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-15RVBK0
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 30-13-8B-65-6D-43
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2b13:df55:5a2c:9117%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.3.73(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 103814027
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-57-CF-86-30-13-8B-65-6D-43
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- ipconfig displaydns

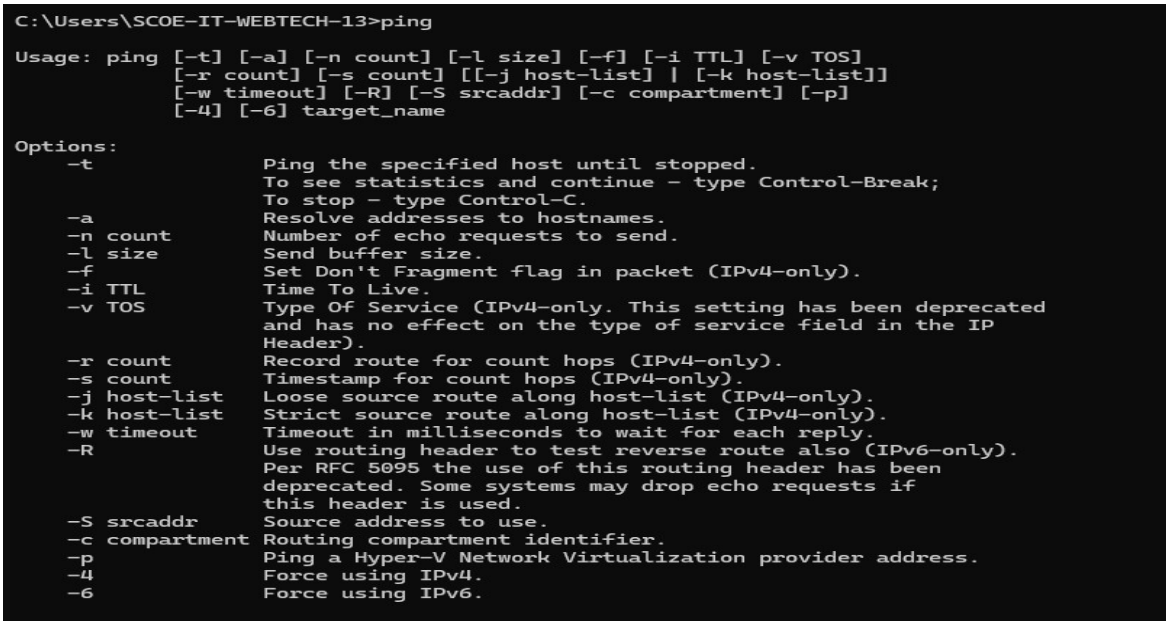


```
C:\Users\SCOE-IT-WEBTECH-13>ipconfig displaydns

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.
```

(2)ping:

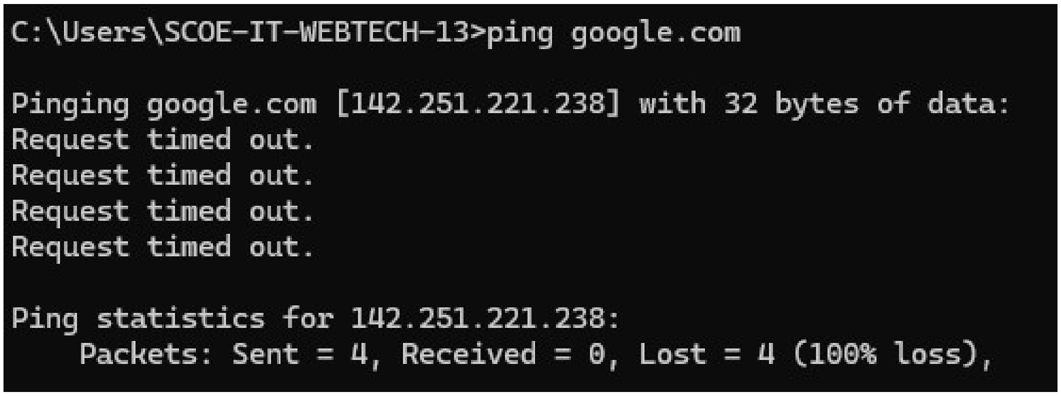
Verifies connectivity to a target host by sending ICMP echo requests and measuring response times.

- Ping:



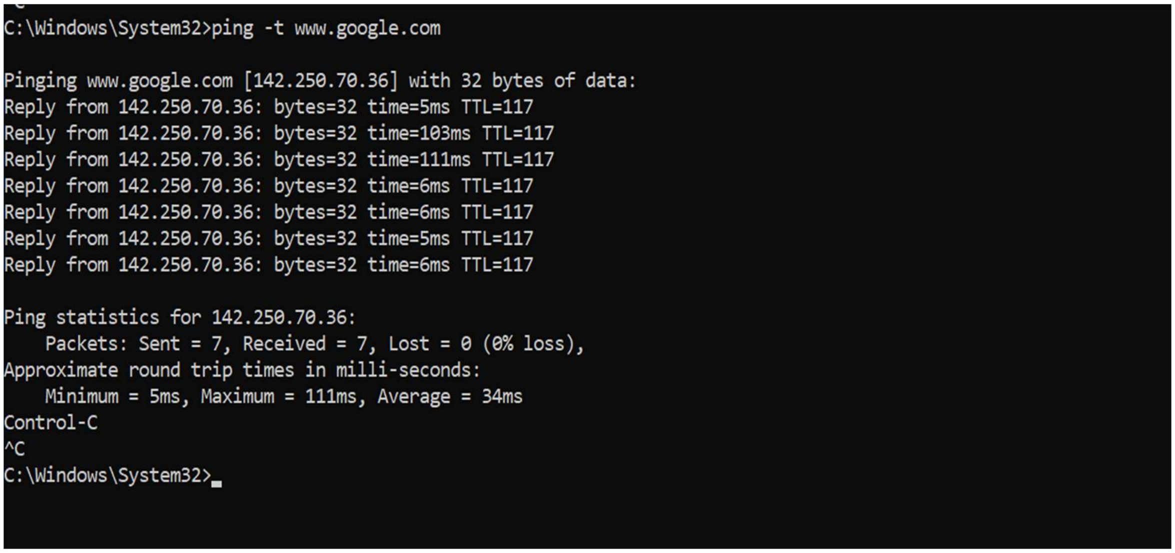
```
C:\Users\SCOE-IT-WEBTECH-13>ping

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.
```

- Ping destination:



```
C:\Users\SCOE-IT-WEBTECH-13>ping google.com

Pinging google.com [142.251.221.238] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.251.221.238:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Ping -t destination :

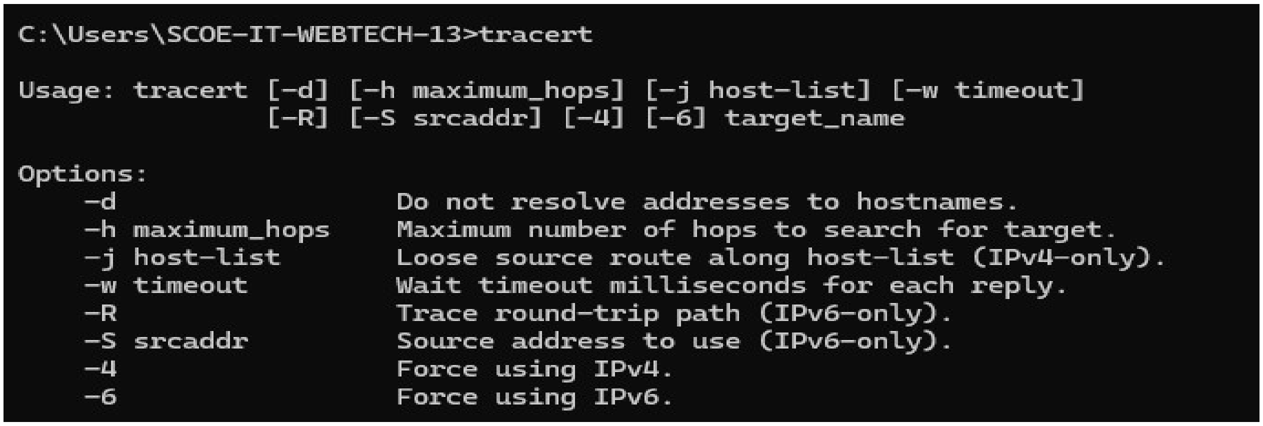


```
C:\Windows\System32>ping -t www.google.com

Pinging www.google.com [142.250.70.36] with 32 bytes of data:
Reply from 142.250.70.36: bytes=32 time=5ms TTL=117
Reply from 142.250.70.36: bytes=32 time=103ms TTL=117
Reply from 142.250.70.36: bytes=32 time=111ms TTL=117
Reply from 142.250.70.36: bytes=32 time=6ms TTL=117
Reply from 142.250.70.36: bytes=32 time=6ms TTL=117
Reply from 142.250.70.36: bytes=32 time=5ms TTL=117
Reply from 142.250.70.36: bytes=32 time=6ms TTL=117

Ping statistics for 142.250.70.36:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 111ms, Average = 34ms
Control-C
^C
C:\Windows\System32>
```

(3) tracert:

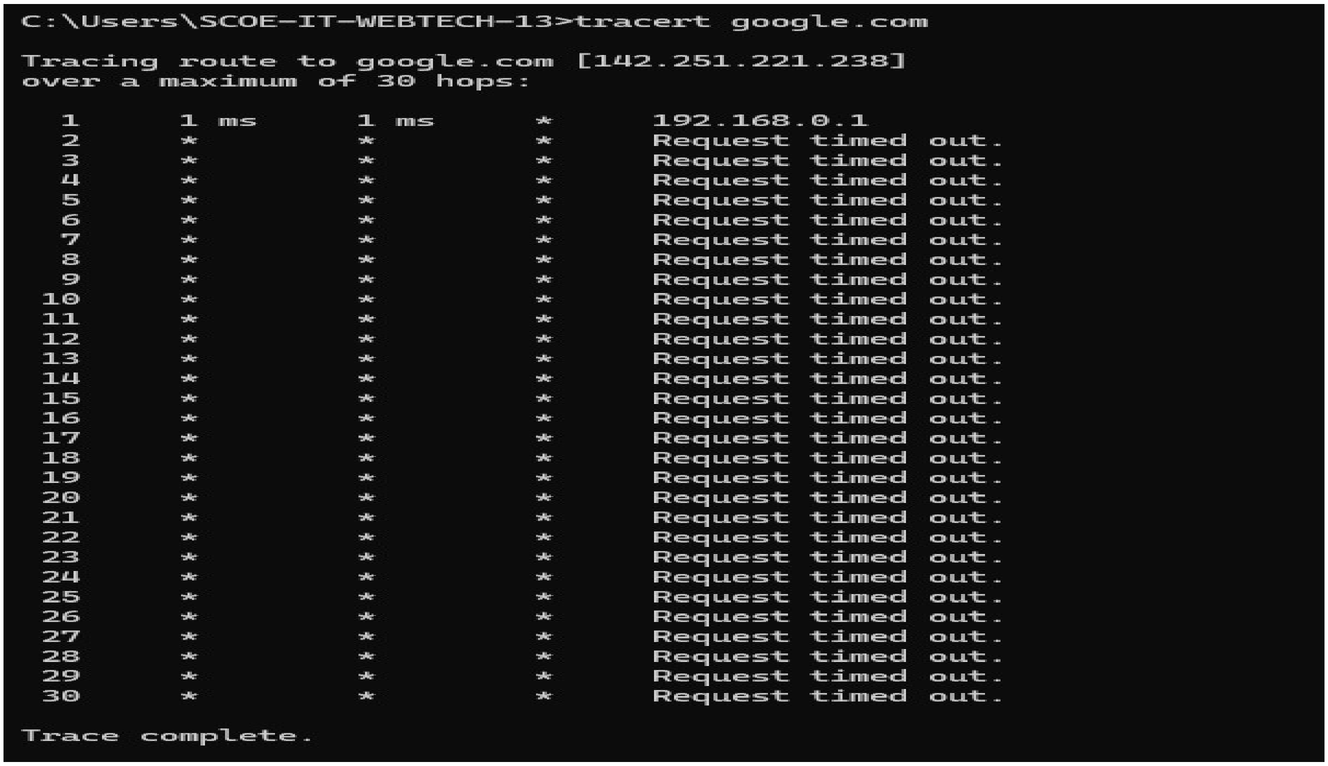
Maps the route packets take to reach a destination, showing the hops (routers) involved and their respective response times

- tracert:



```
C:\Users\SCOE-IT-WEBTECH-13>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

- tracert : tracert destination



```
C:\Users\SCOE-IT-WEBTECH-13>tracert google.com

Tracing route to google.com [142.251.221.238]
over a maximum of 30 hops:

  1     1 ms     1 ms     *     192.168.0.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 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     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

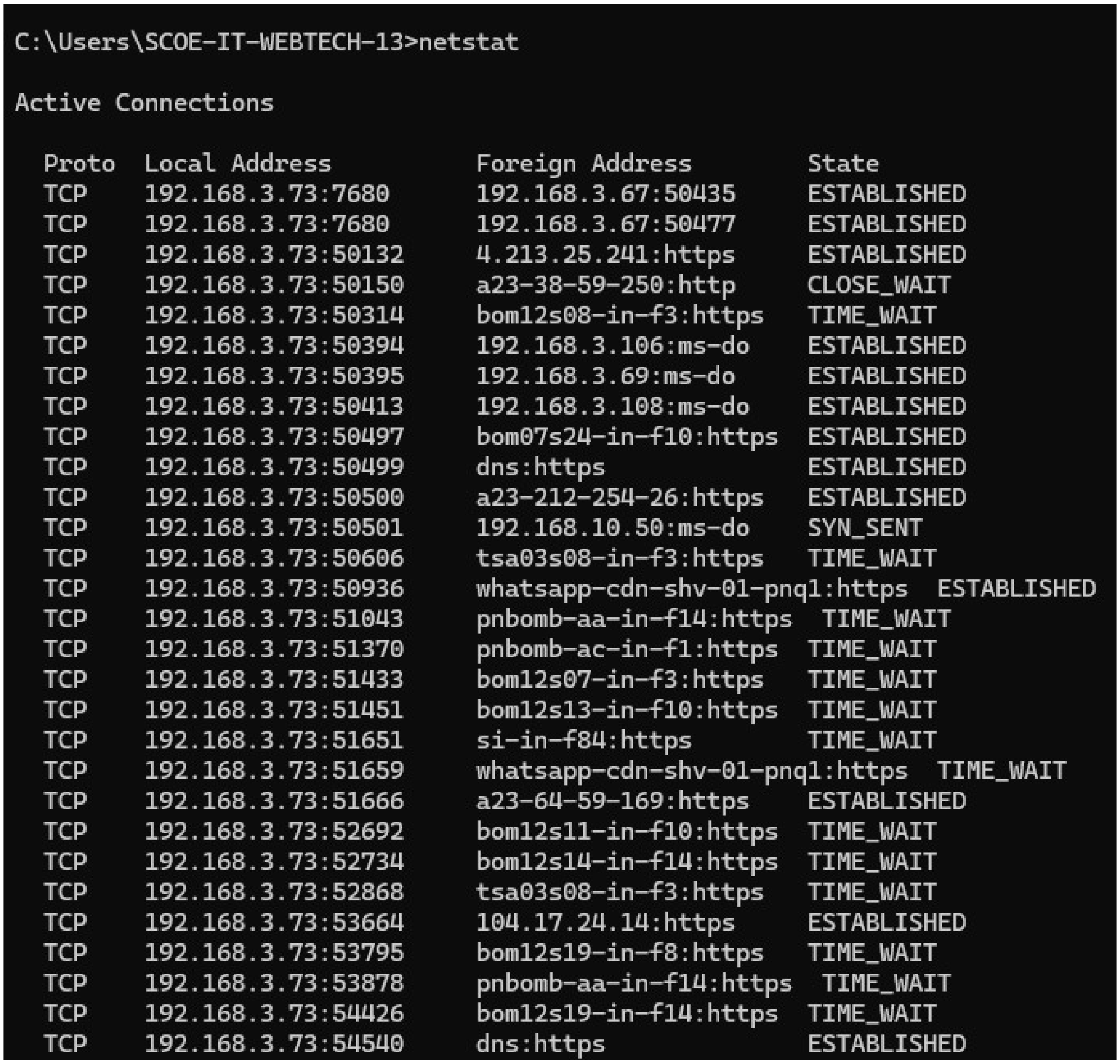
Srushti Shinde
Roll No: 71

Srushti Shinde
Roll No: 71

Srushti Shinde
Roll No: 71

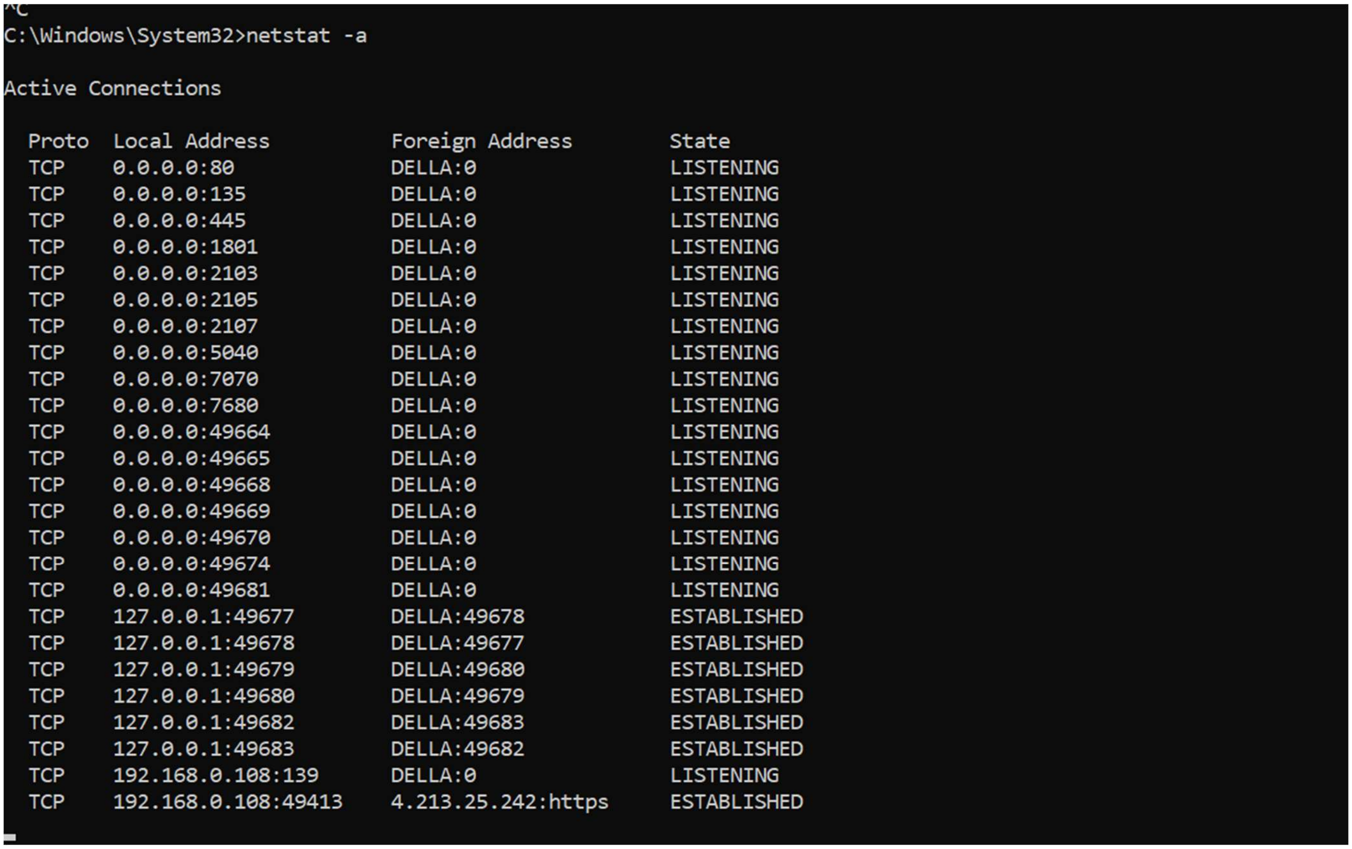
4t) netstat:

Displays active network connections, listening ports, routing tables, and network interface statistics. Options like netstat -a show all connections, netstat -b (requires administrator privileges) shows associated executables, and netstat -n displays numerical addresses without name resolution.



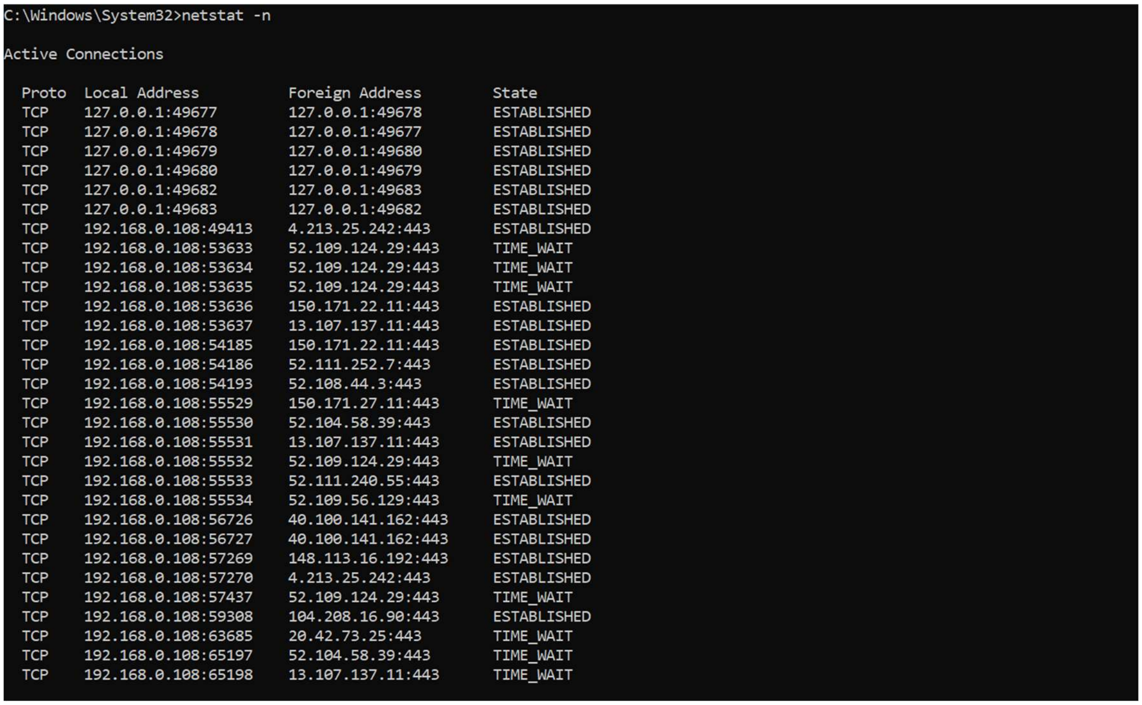
```
C:\Users\SCOE-IT-WEBTECH-13>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.3.73:7680      192.168.3.67:50435     ESTABLISHED
  TCP    192.168.3.73:7680      192.168.3.67:50477     ESTABLISHED
  TCP    192.168.3.73:50132     4.213.25.241:https     ESTABLISHED
  TCP    192.168.3.73:50150     a23-38-59-250:http     CLOSE_WAIT
  TCP    192.168.3.73:50314     bom12s08-in-f3:https   TIME_WAIT
  TCP    192.168.3.73:50394     192.168.3.106:ms-do    ESTABLISHED
  TCP    192.168.3.73:50395     192.168.3.69:ms-do     ESTABLISHED
  TCP    192.168.3.73:50413     192.168.3.108:ms-do    ESTABLISHED
  TCP    192.168.3.73:50497     bom07s24-in-f10:https  ESTABLISHED
  TCP    192.168.3.73:50499     dns:https              ESTABLISHED
  TCP    192.168.3.73:50500     a23-212-254-26:https   ESTABLISHED
  TCP    192.168.3.73:50501     192.168.10.50:ms-do    SYN_SENT
  TCP    192.168.3.73:50606     tsa03s08-in-f3:https   TIME_WAIT
  TCP    192.168.3.73:50936     whatsapp-cdn-shv-01-pnq1:https  ESTABLISHED
  TCP    192.168.3.73:51043     pnbomb-aa-in-f14:https  TIME_WAIT
  TCP    192.168.3.73:51370     pnbomb-ac-in-f1:https  TIME_WAIT
  TCP    192.168.3.73:51433     bom12s07-in-f3:https   TIME_WAIT
  TCP    192.168.3.73:51451     bom12s13-in-f10:https  TIME_WAIT
  TCP    192.168.3.73:51651     si-in-f84:https        TIME_WAIT
  TCP    192.168.3.73:51659     whatsapp-cdn-shv-01-pnq1:https  TIME_WAIT
  TCP    192.168.3.73:51666     a23-64-59-169:https    ESTABLISHED
  TCP    192.168.3.73:52692     bom12s11-in-f10:https  TIME_WAIT
  TCP    192.168.3.73:52734     bom12s14-in-f14:https  TIME_WAIT
  TCP    192.168.3.73:52868     tsa03s08-in-f3:https   TIME_WAIT
  TCP    192.168.3.73:53664     104.17.24.14:https     ESTABLISHED
  TCP    192.168.3.73:53795     bom12s19-in-f8:https   TIME_WAIT
  TCP    192.168.3.73:53878     pnbomb-aa-in-f14:https  TIME_WAIT
  TCP    192.168.3.73:54426     bom12s19-in-f14:https  TIME_WAIT
  TCP    192.168.3.73:54540     dns:https              ESTABLISHED
```

- netstat -a



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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             DELLA:0                LISTENING
  TCP    0.0.0.0:135            DELLA:0                LISTENING
  TCP    0.0.0.0:445            DELLA:0                LISTENING
  TCP    0.0.0.0:1801           DELLA:0                LISTENING
  TCP    0.0.0.0:2103           DELLA:0                LISTENING
  TCP    0.0.0.0:2105           DELLA:0                LISTENING
  TCP    0.0.0.0:2107           DELLA:0                LISTENING
  TCP    0.0.0.0:5040           DELLA:0                LISTENING
  TCP    0.0.0.0:7070           DELLA:0                LISTENING
  TCP    0.0.0.0:7680           DELLA:0                LISTENING
  TCP    0.0.0.0:49664          DELLA:0                LISTENING
  TCP    0.0.0.0:49665          DELLA:0                LISTENING
  TCP    0.0.0.0:49668          DELLA:0                LISTENING
  TCP    0.0.0.0:49669          DELLA:0                LISTENING
  TCP    0.0.0.0:49670          DELLA:0                LISTENING
  TCP    0.0.0.0:49674          DELLA:0                LISTENING
  TCP    0.0.0.0:49681          DELLA:0                LISTENING
  TCP    127.0.0.1:49677        DELLA:49678            ESTABLISHED
  TCP    127.0.0.1:49678        DELLA:49677            ESTABLISHED
  TCP    127.0.0.1:49679        DELLA:49680            ESTABLISHED
  TCP    127.0.0.1:49680        DELLA:49679            ESTABLISHED
  TCP    127.0.0.1:49682        DELLA:49683            ESTABLISHED
  TCP    127.0.0.1:49683        DELLA:49682            ESTABLISHED
  TCP    192.168.0.108:139      DELLA:0                LISTENING
  TCP    192.168.0.108:49413    4.213.25.242:https     ESTABLISHED
```

- netstat -n

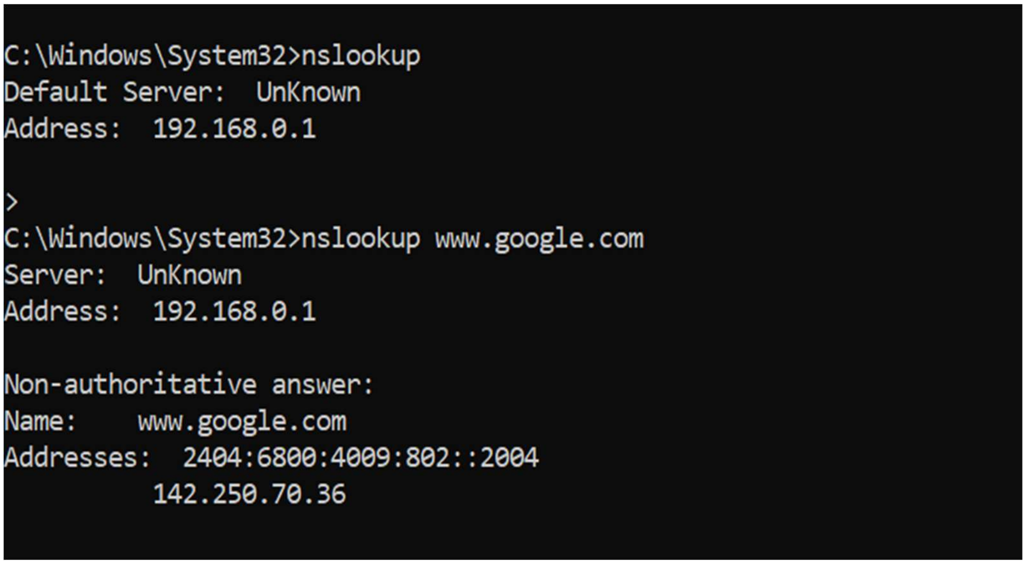


```
C:\Windows\System32>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49677        127.0.0.1:49678        ESTABLISHED
  TCP    127.0.0.1:49678        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:49679        127.0.0.1:49680        ESTABLISHED
  TCP    127.0.0.1:49680        127.0.0.1:49679        ESTABLISHED
  TCP    127.0.0.1:49682        127.0.0.1:49683        ESTABLISHED
  TCP    127.0.0.1:49683        127.0.0.1:49682        ESTABLISHED
  TCP    192.168.0.108:49413    4.213.25.242:443       ESTABLISHED
  TCP    192.168.0.108:53633    52.109.124.29:443      TIME_WAIT
  TCP    192.168.0.108:53634    52.109.124.29:443      TIME_WAIT
  TCP    192.168.0.108:53635    52.109.124.29:443      TIME_WAIT
  TCP    192.168.0.108:53636    150.171.22.11:443      ESTABLISHED
  TCP    192.168.0.108:53637    13.107.137.11:443      ESTABLISHED
  TCP    192.168.0.108:54185    150.171.22.11:443      ESTABLISHED
  TCP    192.168.0.108:54186    52.111.252.7:443       ESTABLISHED
  TCP    192.168.0.108:54193    52.108.44.3:443        ESTABLISHED
  TCP    192.168.0.108:55529    150.171.27.11:443      TIME_WAIT
  TCP    192.168.0.108:55530    52.104.58.39:443       ESTABLISHED
  TCP    192.168.0.108:55531    13.107.137.11:443      ESTABLISHED
  TCP    192.168.0.108:55532    52.109.124.29:443      TIME_WAIT
  TCP    192.168.0.108:55533    52.111.240.55:443      ESTABLISHED
  TCP    192.168.0.108:55534    52.109.56.129:443      TIME_WAIT
  TCP    192.168.0.108:56726    40.100.141.162:443     ESTABLISHED
  TCP    192.168.0.108:56727    40.100.141.162:443     ESTABLISHED
  TCP    192.168.0.108:57269    148.113.16.192:443     ESTABLISHED
  TCP    192.168.0.108:57270    4.213.25.242:443       ESTABLISHED
  TCP    192.168.0.108:57437    52.109.124.29:443      TIME_WAIT
  TCP    192.168.0.108:59308    104.208.16.90:443      ESTABLISHED
  TCP    192.168.0.108:63685    20.42.73.25:443        TIME_WAIT
  TCP    192.168.0.108:65197    52.104.58.39:443       TIME_WAIT
  TCP    192.168.0.108:65198    13.107.137.11:443      TIME_WAIT
```

(5)nslookup:

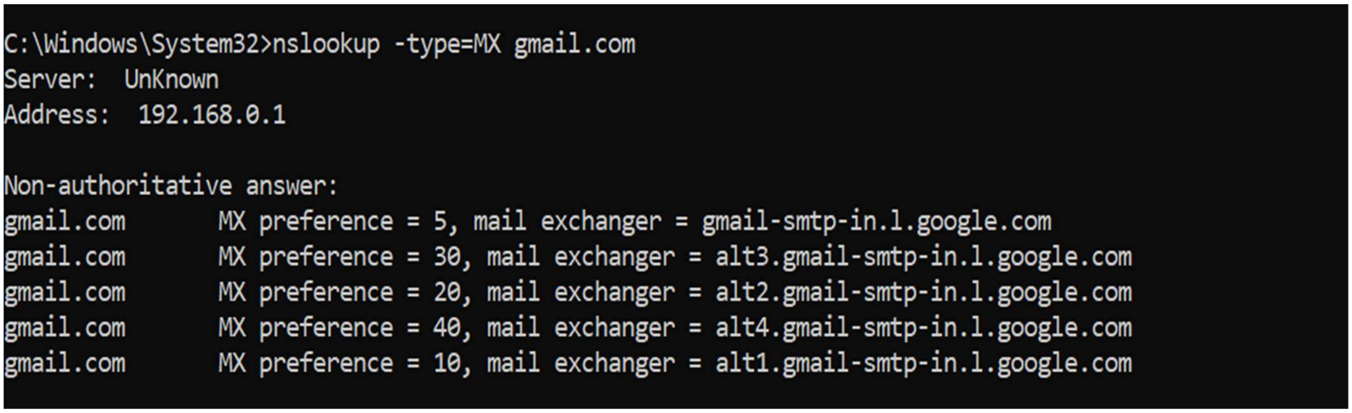
Queries DNS servers to resolve hostnames to IP addresses and vice versa, and to retrieve other DNS records.

- nslookup



```
C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

>
C:\Windows\System32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:802::2004
          142.250.70.36
```

- nslookup -type=MX gmail.com

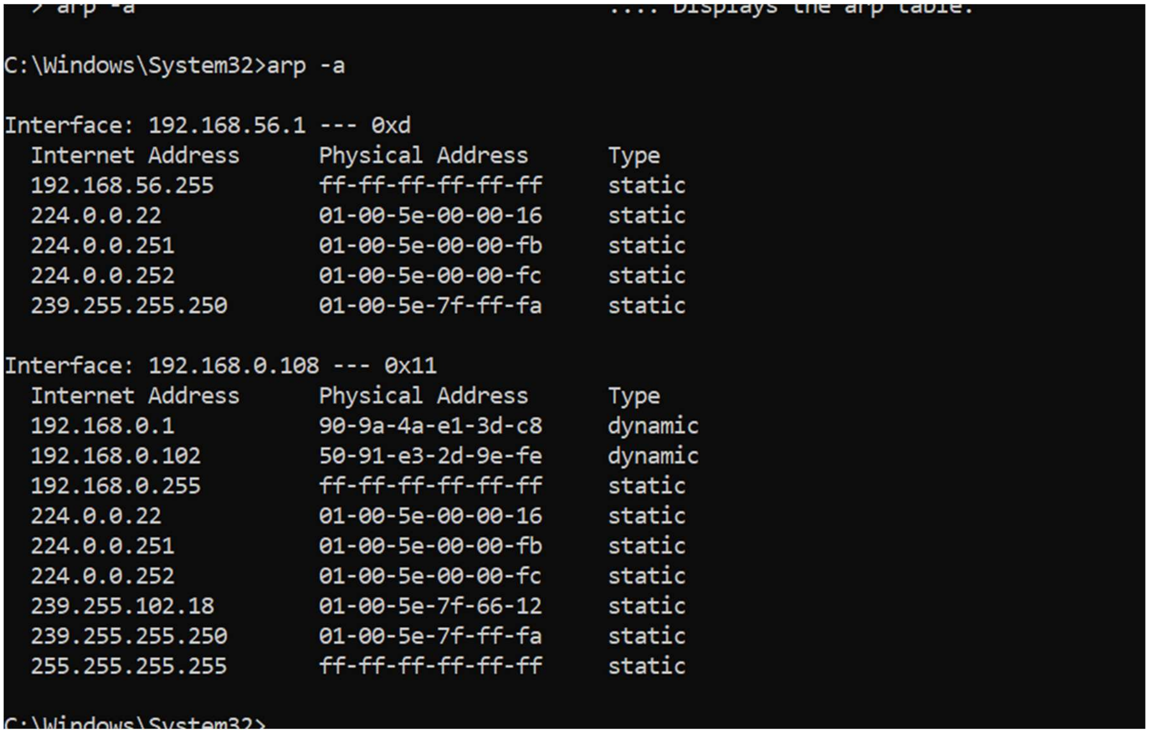


```
C:\Windows\System32>nslookup -type=MX gmail.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
```

(6)arp:

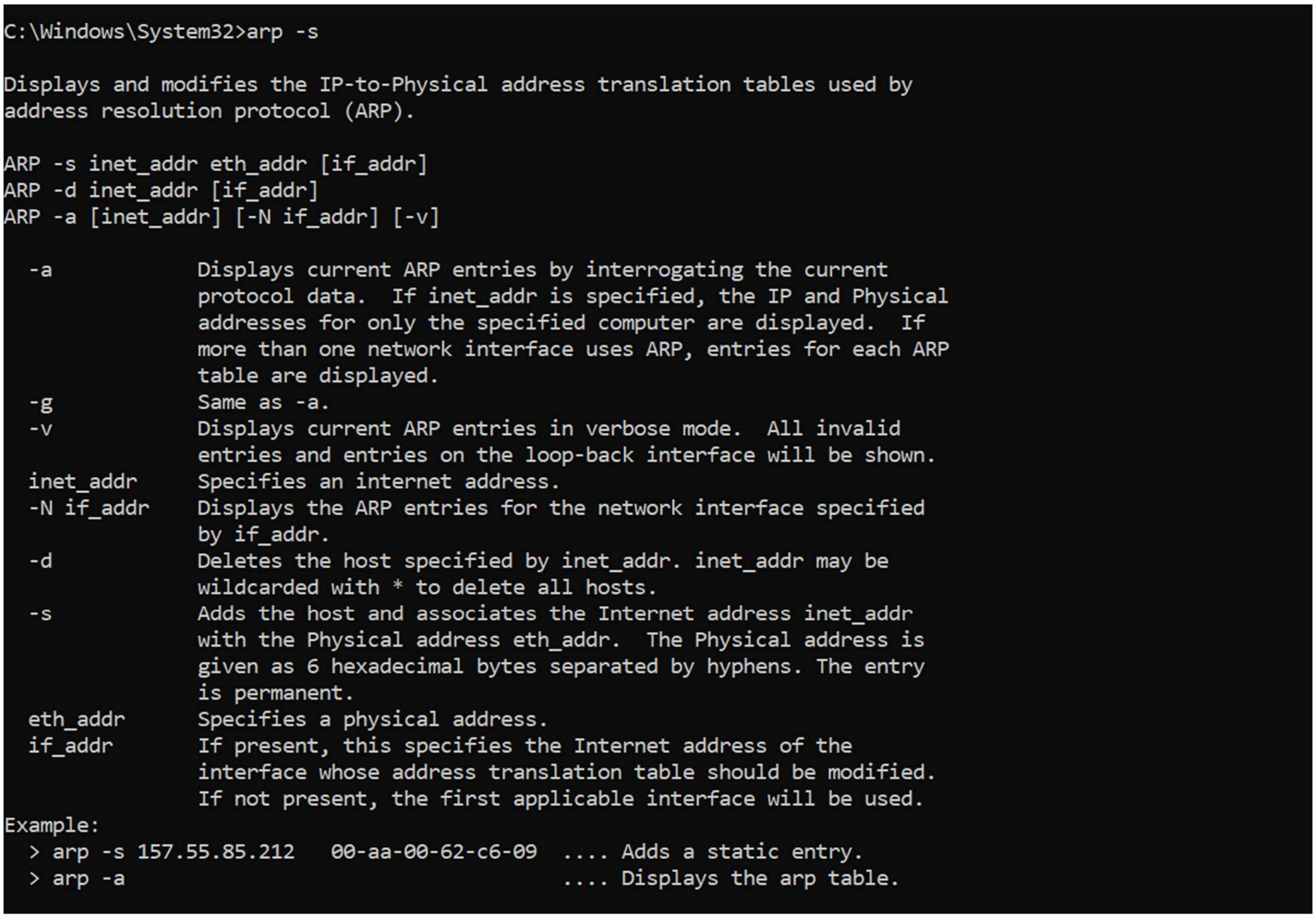
Displays and modifies the Address Resolution Protocol (ARP) cache, showing the mapping between IP addresses and MAC addresses of devices on the local network.

- arp -a



```
  > arp -a                                    .... Displays the arp table.

C:\Windows\System32>arp -a

Interface: 192.168.56.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     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: 192.168.0.108 --- 0x11
  Internet Address      Physical Address      Type
  192.168.0.1           90-9a-4a-e1-3d-c8     dynamic
  192.168.0.102         50-91-e3-2d-9e-fe     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     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
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\System32>
```

- arp -s

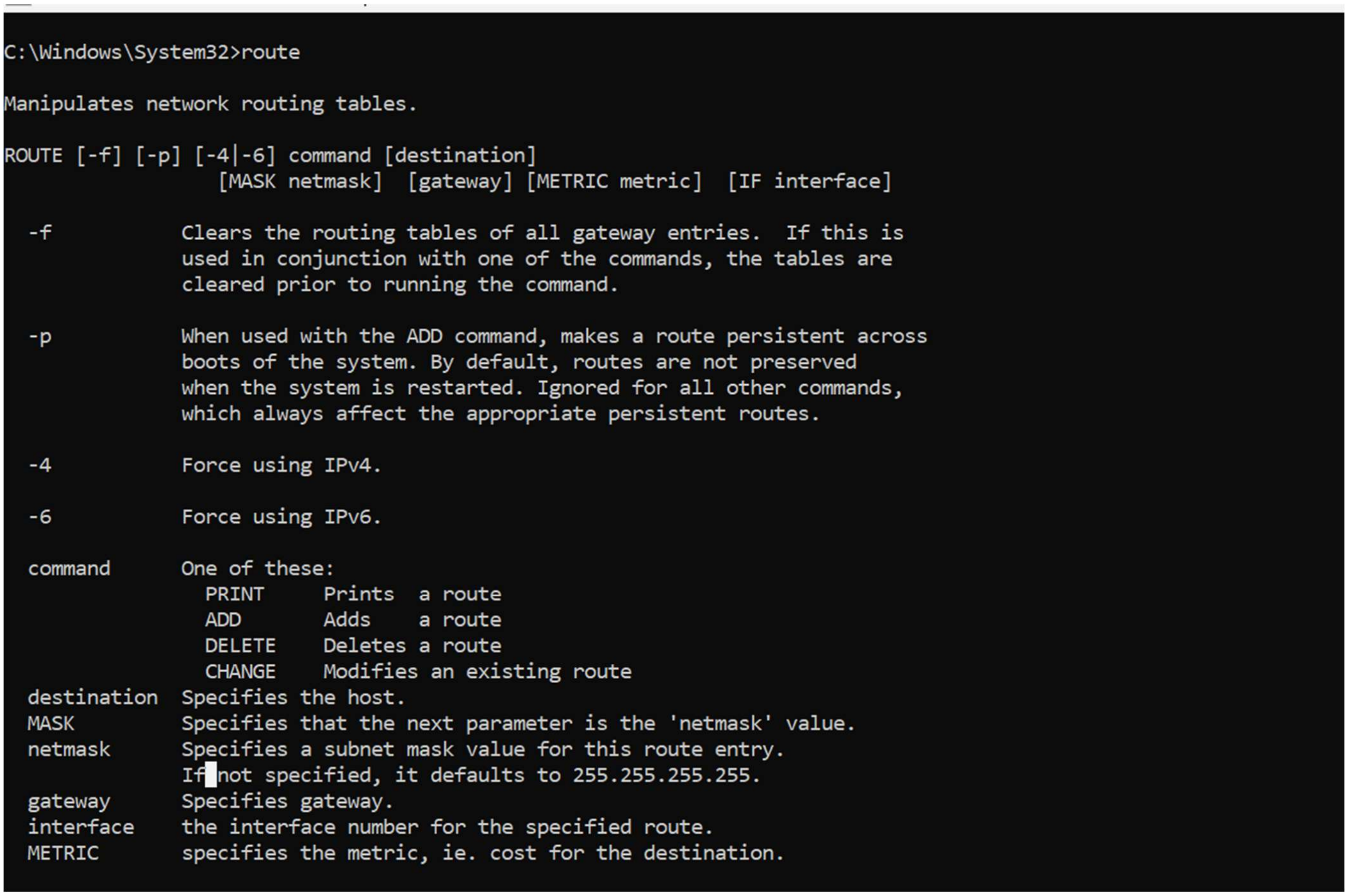


```
C:\Windows\System32>arp -s

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

(7)route:

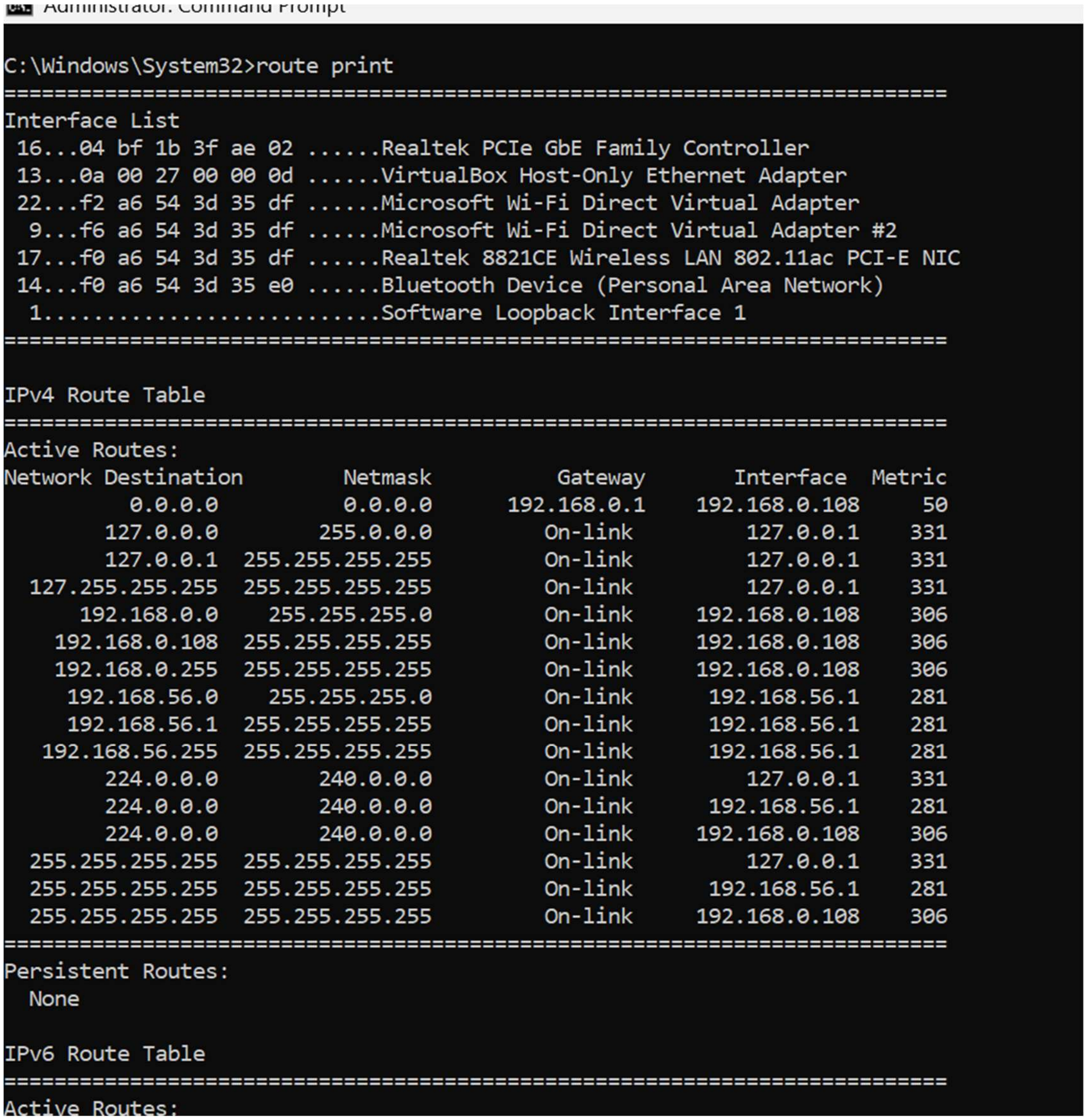
Manages network routing tables, allowing display and modification of routes.

- route



```
C:\Windows\System32>route

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.
```

- route print



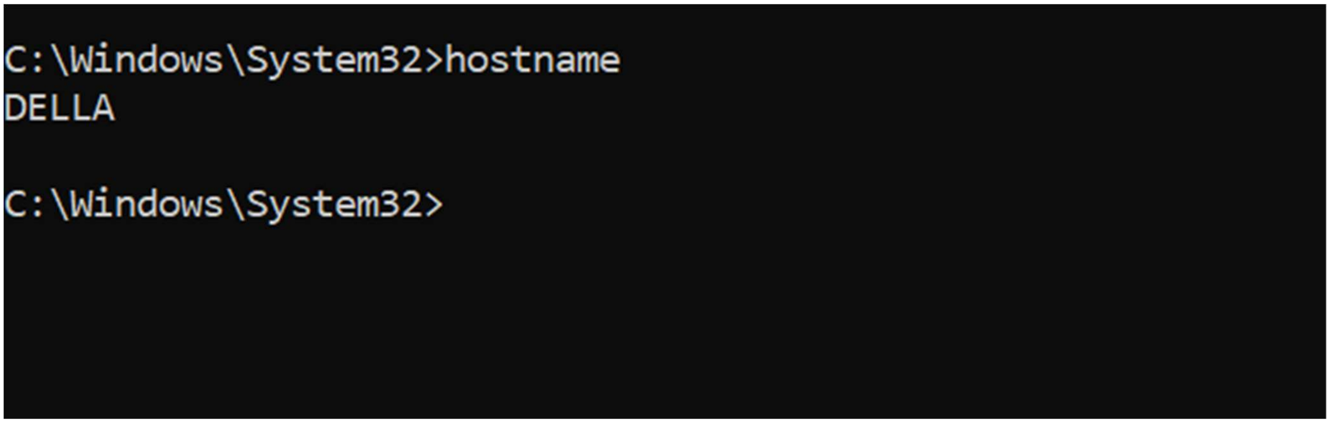
Administrator: Command Prompt

```
C:\Windows\System32>route print
===========================================================================
Interface List
 16...04 bf 1b 3f ae 02 ......Realtek PCIe GbE Family Controller
 13...0a 00 27 00 00 0d ......VirtualBox Host-Only Ethernet Adapter
 22...f2 a6 54 3d 35 df ......Microsoft Wi-Fi Direct Virtual Adapter
  9...f6 a6 54 3d 35 df ......Microsoft Wi-Fi Direct Virtual Adapter #2
 17...f0 a6 54 3d 35 df ......Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
 14...f0 a6 54 3d 35 e0 ......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      192.168.0.1    192.168.0.108     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
      192.168.0.0    255.255.255.0         On-link     192.168.0.108    306
    192.168.0.108  255.255.255.255         On-link     192.168.0.108    306
    192.168.0.255  255.255.255.255         On-link     192.168.0.108    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     192.168.0.108    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     192.168.0.108    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
```

(8)hostname

Shows the Hostname of the current computer system.

- hostname

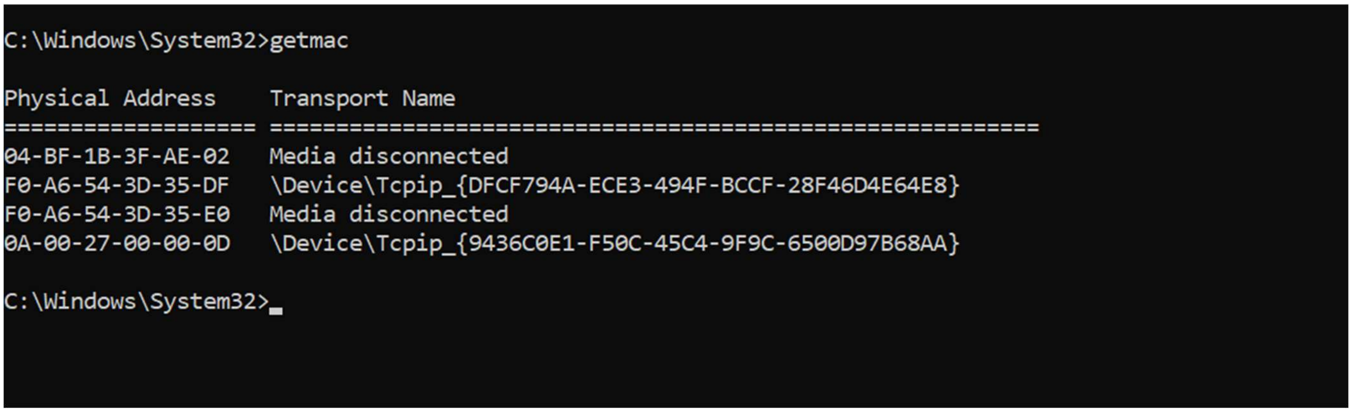


```
C:\Windows\System32>hostname
DELLA

C:\Windows\System32>
```

(9)getmac

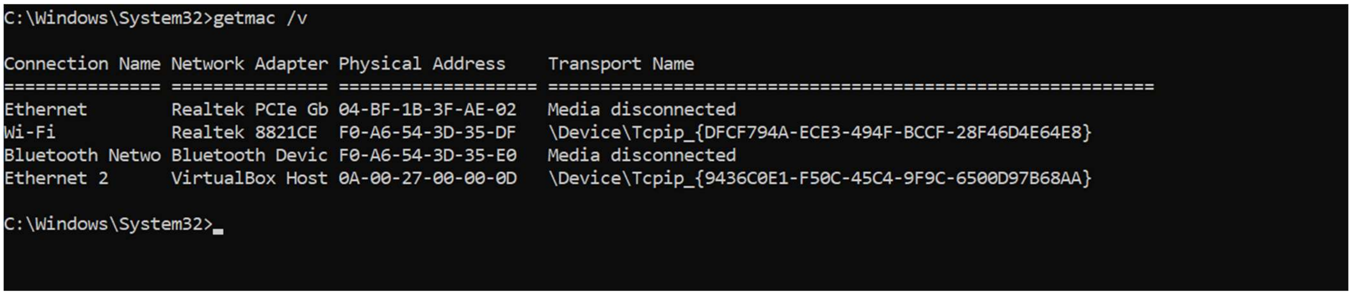
he getmac command in Windows is used to display the MAC addresses of your network adapters. It’s helpful for identifying hardware addresses for network troubleshooting or configuration.

- getmac



```
C:\Windows\System32>getmac

Physical Address    Transport Name
=================== ==========================================================
04-BF-1B-3F-AE-02   Media disconnected
F0-A6-54-3D-35-DF   \Device\Tcpip_{DFCF794A-ECE3-494F-BCCF-28F46D4E64E8}
F0-A6-54-3D-35-E0   Media disconnected
0A-00-27-00-00-0D   \Device\Tcpip_{9436C0E1-F50C-45C4-9F9C-6500D97B68AA}

C:\Windows\System32>
```

- getmac /v - Verbose output (shows connection name, status, transport name)

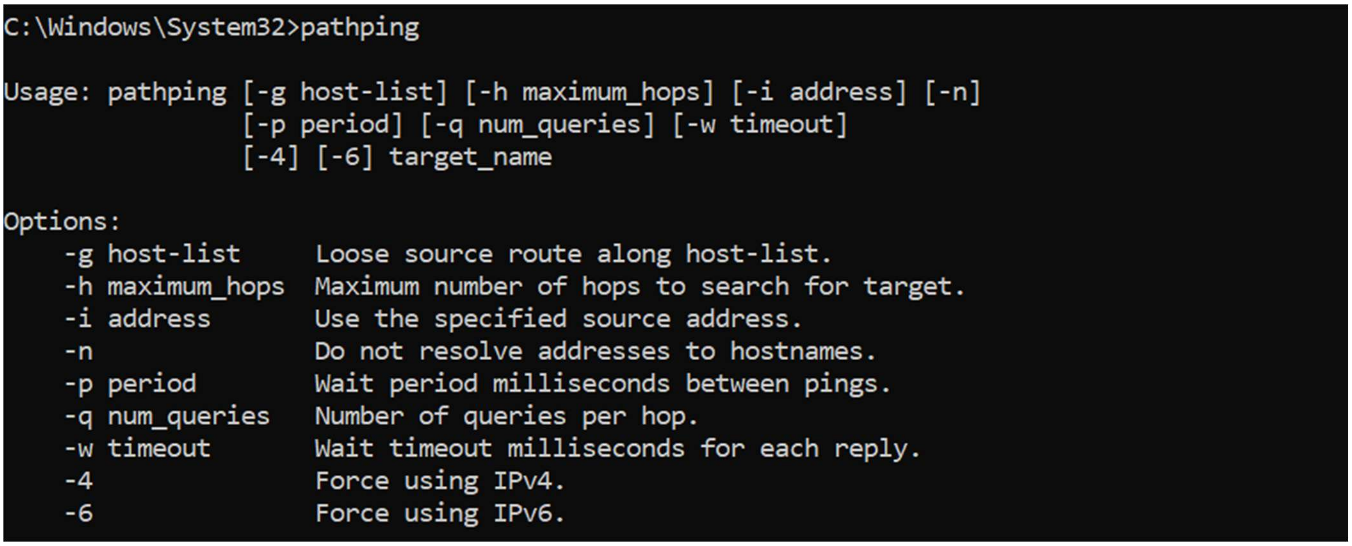


```
C:\Windows\System32>getmac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
Ethernet        Realtek PCIe Gb 04-BF-1B-3F-AE-02   Media disconnected
Wi-Fi           Realtek 8821CE  F0-A6-54-3D-35-DF   \Device\Tcpip_{DFCF794A-ECE3-494F-BCCF-28F46D4E64E8}
Bluetooth Netwo Bluetooth Devic F0-A6-54-3D-35-E0   Media disconnected
Ethernet 2      VirtualBox Host 0A-00-27-00-00-0D   \Device\Tcpip_{9436C0E1-F50C-45C4-9F9C-6500D97B68AA}

C:\Windows\System32>
```

(10) pathping

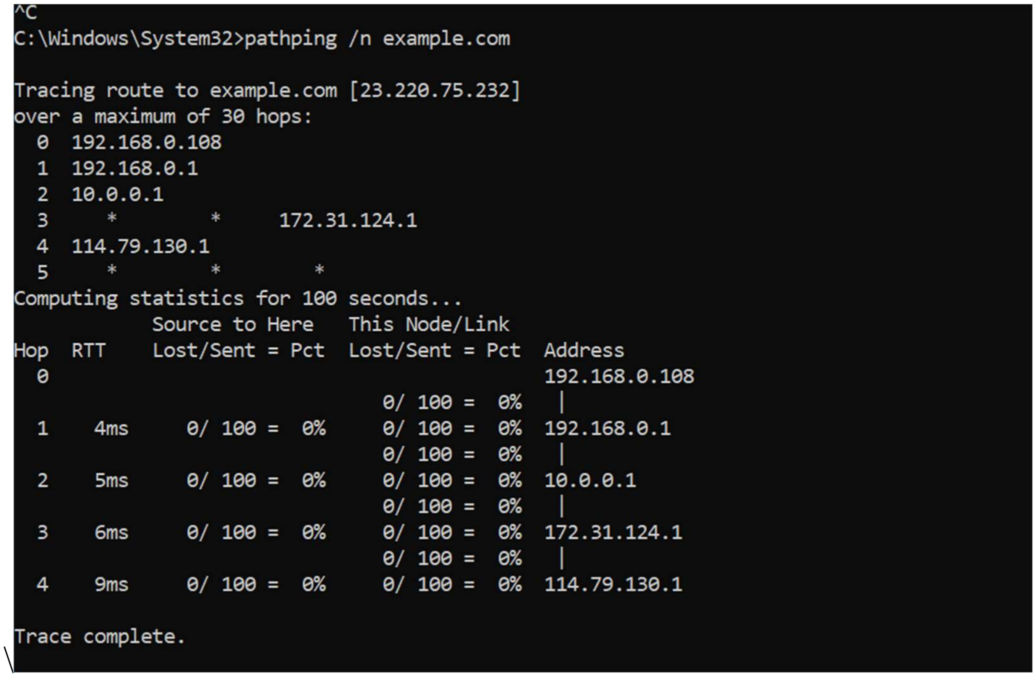
The pathping command in Windows is a network diagnostic tool that combines the functionality of ping and tracert. It helps you trace the route to a host and measure packet loss and latency at each hop along the way.

- pathping



```
C:\Windows\System32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.
```

- pathping /n example.com - Do not resolve IP addresses to hostname



```
^C
C:\Windows\System32>pathping /n example.com

Tracing route to example.com [23.220.75.232]
over a maximum of 30 hops:
  0  192.168.0.108
  1  192.168.0.1
  2  10.0.0.1
  3     *        *     172.31.124.1
  4  114.79.130.1
  5     *        *        *
Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           192.168.0.108
                                0/ 100 =  0%   |
  1    4ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                0/ 100 =  0%   |
  2    5ms     0/ 100 =  0%     0/ 100 =  0%  10.0.0.1
                                0/ 100 =  0%   |
  3    6ms     0/ 100 =  0%     0/ 100 =  0%  172.31.124.1
                                0/ 100 =  0%   |
  4    9ms     0/ 100 =  0%     0/ 100 =  0%  114.79.130.1

Trace complete.
```

\

Srushti Shinde
Roll No: 71

CONCLUSION:

We have successfully studied and implemented networking commands such as ifconfig, netstat, ping, arp, tracert, etc. in above experiment.