National Forensics Sciences University

School of Cyber Security and Digital Forensics

M.Tech Artificial Intelligence and Data Science (Specialization in Cyber Security)

Network Security and Forensics

Practical 1

Session 2024-25

Semester 1

Submitted To:-

Dr. Vijeta Khare

Submitted By:-

Pratham Badge

0. Prerequisite

- Search Command Prompt or cmd in windows search and open it.

or

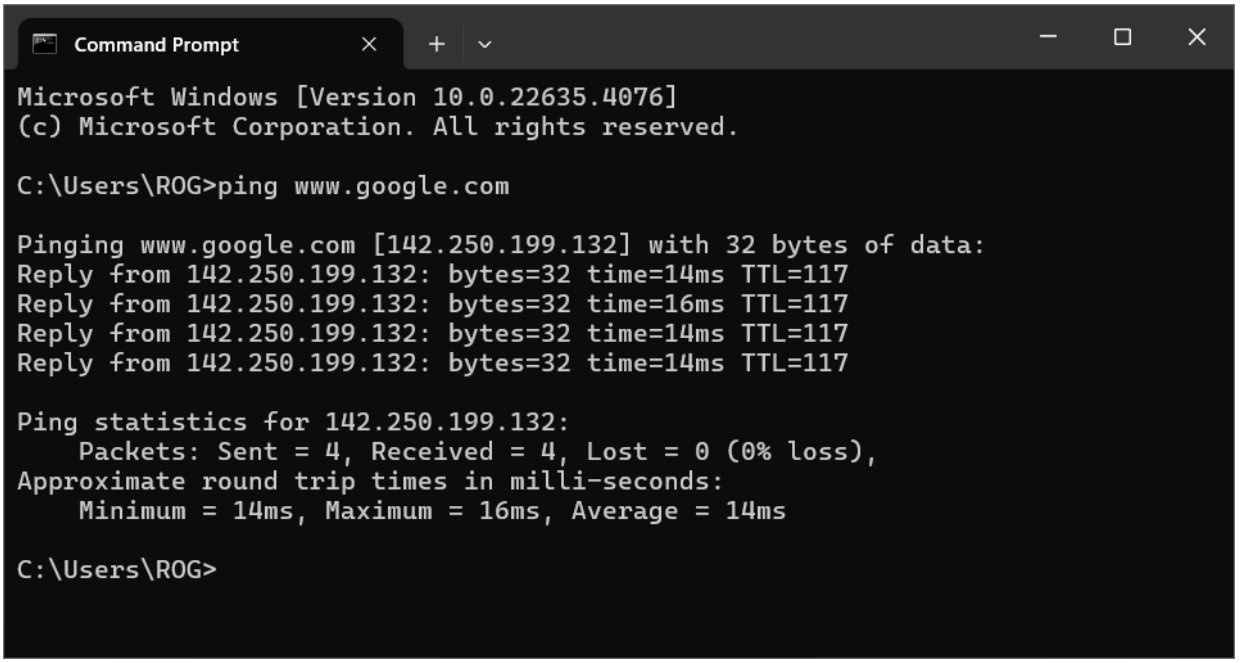
- Press Windows + R Keys Run will pop-up then type cmd and press ok

1. How do you check the network connectivity between host and server/host.

To check the network connectivity between host and server/host:

We can use **ping** command :

syntax: **ping [options] [hostname/IP address]**



```
Command Prompt

Microsoft Windows [Version 10.0.22635.4076]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ROG>ping www.google.com

Pinging www.google.com [142.250.199.132] with 32 bytes of data:
Reply from 142.250.199.132: bytes=32 time=14ms TTL=117
Reply from 142.250.199.132: bytes=32 time=16ms TTL=117
Reply from 142.250.199.132: bytes=32 time=14ms TTL=117
Reply from 142.250.199.132: bytes=32 time=14ms TTL=117

Ping statistics for 142.250.199.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 16ms, Average = 14ms

C:\Users\ROG>
```

Output Explained:

It shows

i) IP Address/Domain
ii) Packet Size of ping
iii) Reply Time from IP and
iv) Time to live of packet
v) No. of packets sent, received and lost(if any)
vi) Max, Min and Avg Times to send and receive packets

2. How to find the IP Address of your system.

To find IP Address of our system:
We can use **ipconfig** command:

```
Command Prompt

C:\Users\ROG>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a1d6:f39:9c97:c956%22
   IPv4 Address. . . . . . . . . . . : 192.168.233.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::447c:9ce4:3de9:8148%15
   IPv4 Address. . . . . . . . . . . : 192.168.116.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::12b1:6c7c:8ab7:3a3f%2
   IPv4 Address. . . . . . . . . . . : 192.168.0.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Ethernet:

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

Output Explained:

It shows

i) Interface Names and their status if disconnected
ii) IPv4 and IPv6 Addresses
iii) Subnet Mask
iv) Default Gateway

3. Find MAC address from all the network cards on a system

To find MAC Address from all the network cards on a system:
We can use **getmac** command:

syntax: **getmac [/s system [/u username [/p [password]]]] [/fo format] [/nh] [/v]**

```
Command Prompt                                   Windows PowerShell

C:\Users\ROG>getmac

Physical Address    Transport Name
=================== ==========================================================
50-EB-F6-D4-9C-46   Media disconnected
50-C2-E8-33-D5-4B   \Device\Tcpip_{00C803F7-FDE2-418E-8E77-F883723AE259}
50-C2-E8-33-D5-4C   Media disconnected
00-50-56-C0-00-01   \Device\Tcpip_{F13CEE98-CDAA-47FB-9AC1-01F9B50752CA}
00-50-56-C0-00-08   \Device\Tcpip_{8F694F71-8437-482A-967D-6F6EB8F541CF}

C:\Users\ROG>getmac /v /fo list

Connection Name:  Ethernet
Network Adapter:  Realtek Gaming 2.5GbE Family Controller
Physical Address: 50-EB-F6-D4-9C-46
Transport Name:   Media disconnected

Connection Name:  Wi-Fi
Network Adapter:  MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
Physical Address: 50-C2-E8-33-D5-4B
Transport Name:   Media disconnected

Connection Name:  Bluetooth Network Connection
Network Adapter:  Bluetooth Device (Personal Area Network)
Physical Address: 50-C2-E8-33-D5-4C
Transport Name:   Media disconnected

Connection Name:  VMware Network Adapter VMnet1
Network Adapter:  VMware Virtual Ethernet Adapter for VMnet1
Physical Address: 00-50-56-C0-00-01
Transport Name:   \Device\Tcpip_{F13CEE98-CDAA-47FB-9AC1-01F9B50752CA}

Connection Name:  VMware Network Adapter VMnet8
Network Adapter:  VMware Virtual Ethernet Adapter for VMnet8
Physical Address: 00-50-56-C0-00-08
Transport Name:   \Device\Tcpip_{8F694F71-8437-482A-967D-6F6EB8F541CF}

C:\Users\ROG>
```

Output Explained:

It shows

i) NIC Details
ii) MAC/Physical Address of the NIC attached to the device

4. How to find specification of your own system.

To find specification of your own system:

We can use **systeminfo** command:

```
Windows PowerShell    Command Prompt

Microsoft Windows [Version 10.0.22635.4076]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ROG>systeminfo

Host Name:                 PRATHAM-ROG-STR
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22635 N/A Build 22635
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          ROG
Registered Organization:   N/A
Product ID:                00330-80000-00000-AA824
Original Install Date:     26-07-2023, 05:00:06 PM
System Boot Time:          26-08-2024, 02:58:18 PM
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              ROG Strix G513RC_G513RC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 68 Stepping 1 AuthenticAMD ~3201 Mhz
BIOS Version:              American Megatrends International, LLC. G513RC.327, 16-02-2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             4009
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     15,629 MB
Available Physical Memory: 8,274 MB
Virtual Memory: Max Size:  27,917 MB
Virtual Memory: Available: 17,856 MB
Virtual Memory: In Use:    10,061 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\PRATHAM-ROG-STR
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5042099
                           [02]: KB5027397
                           [03]: KB5031483
                           [04]: KB5041873
                           [05]: KB5041874
Network Card(s):           5 NIC(s) Installed.
                           [01]: Realtek Gaming 2.5GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [02]: MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.0.1
                                 IP address(es)
                                 [01]: 192.168.0.131
                                 [02]: fe80::12b1:6c7c:8ab7:3a3f
                           [03]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection
                                 Status:          Media disconnected
                           [04]: VMware Virtual Ethernet Adapter for VMnet1
                                 Connection Name: VMware Network Adapter VMnet1
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.233.1
                                 [02]: fe80::a1d6:f39:9c97:c956
                           [05]: VMware Virtual Ethernet Adapter for VMnet8
                                 Connection Name: VMware Network Adapter VMnet8
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.116.1
                                 [02]: fe80::447c:9ce4:3de9:8148
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

C:\Users\ROG>
```

Output Explained:

It shows

i) All the system information/specs of the device

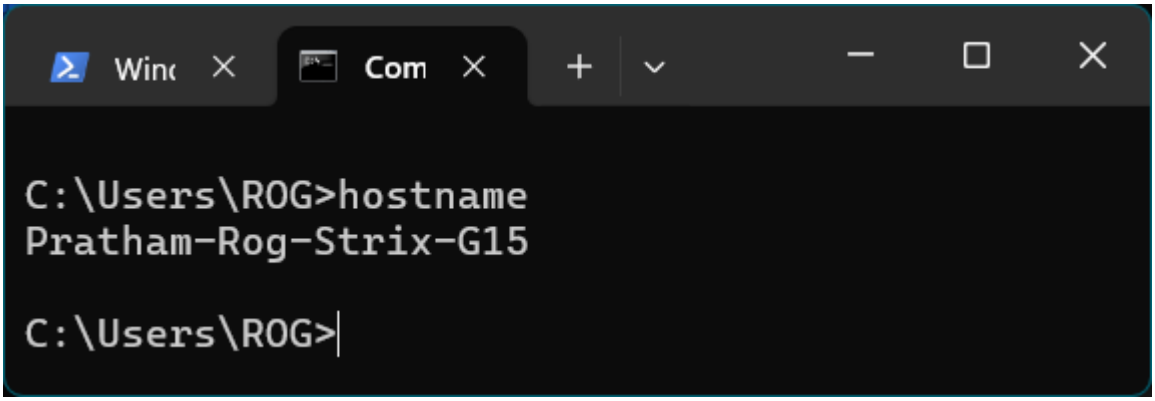
ii) NIC attached to the device

iii) Details about Patch and Hotfixes

5. **How to find host name of your system, and what do you understand by hostname.**

   To find host name of your system:

   We can use **hostname** command and by hostname we understand the name of host device in the network:



Output Explained:

It shows the host/current computer unique device identifier name

6. **How do you find network statistics?**

To find network statistics:

We can use **netstat** command:

syntax: **netstat [-a] [-b] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<interval>]**

```
C:\Users\ROG>netstat -e -s
Interface Statistics

                           Received            Sent

Bytes                       1795437          481683
Unicast packets                3150            2408
Non-unicast packets             826           27471
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                   = 910979
  Received Header Errors             = 0
  Received Address Errors            = 9803
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 8
  Received Packets Discarded         = 25977
  Received Packets Delivered         = 931943
  Output Requests                    = 891789
  Routing Discards                   = 0
  Discarded Output Packets           = 3145
  Output Packet No Route             = 211
  Reassembly Required                = 1074
  Reassembly Successful              = 495
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 5
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 10
```

Output Explained:

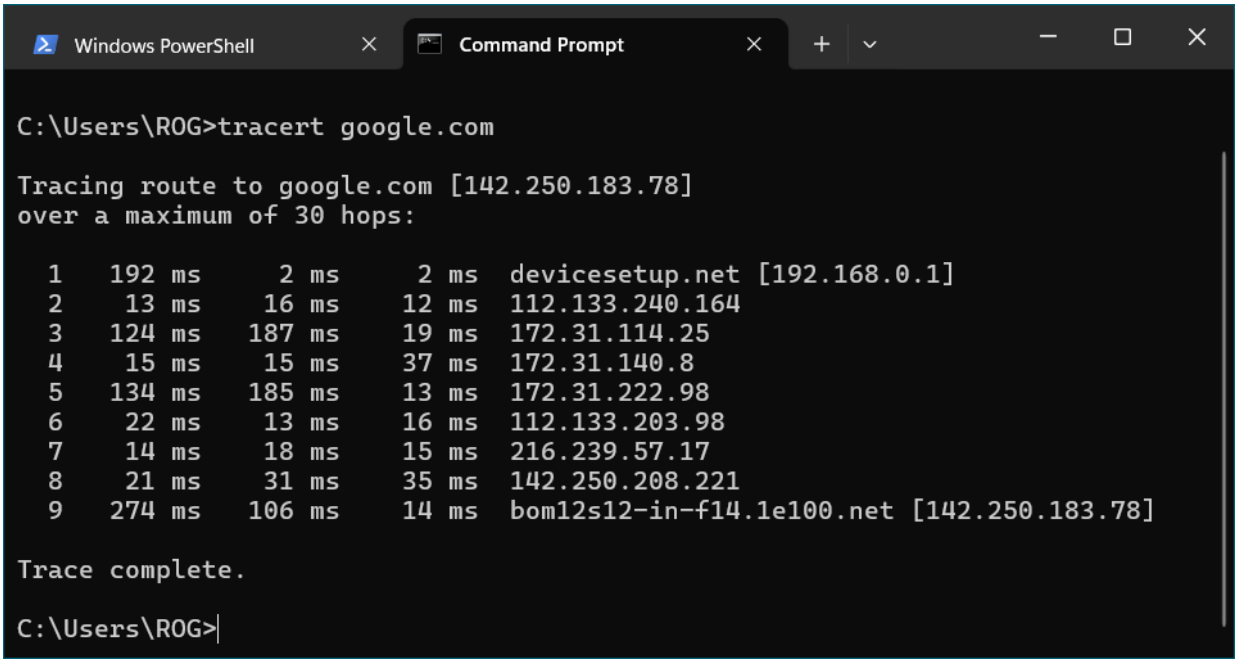
It shows

i) Stats about network – Send Receive with type of protocol

ii) IPv4 Stats

7. **How do you trace the route that your packet has taken to reach google.com. Describe the response.**
   To trace the route that your packet has taken to reach google.com:
   We can use **tracert** command:

   syntax: **tracert -d -h maximum_hops -j host-list -w timeout target_host**



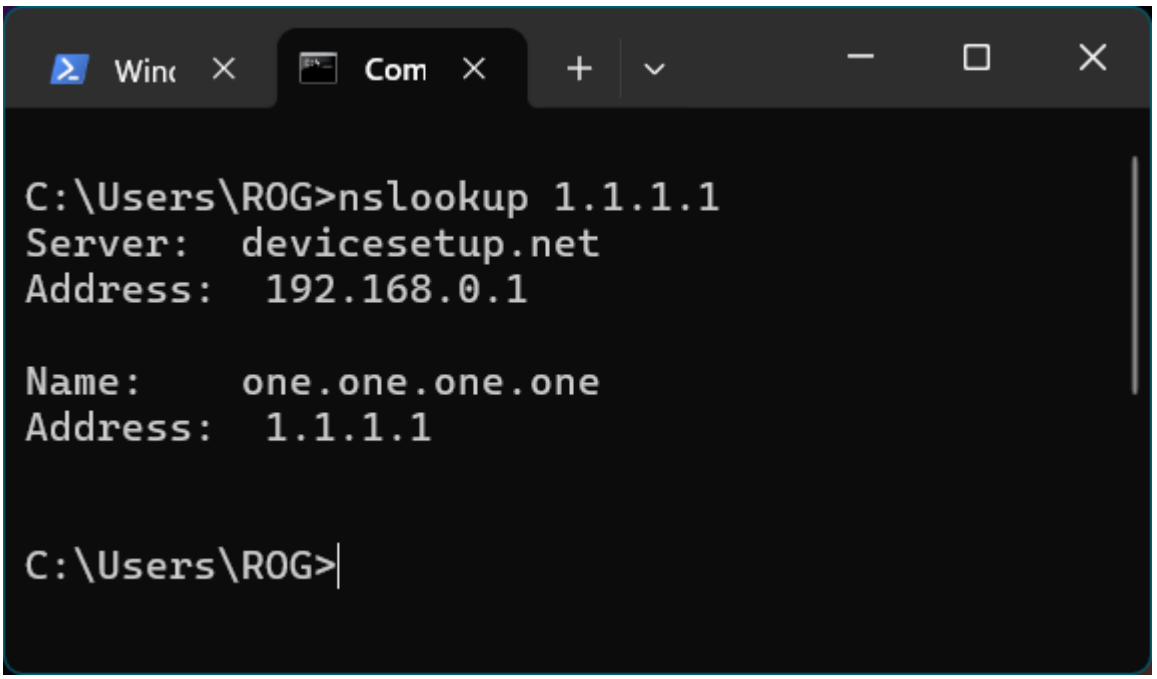
```
C:\Users\ROG>tracert google.com

Tracing route to google.com [142.250.183.78]
over a maximum of 30 hops:

  1   192 ms     2 ms     2 ms  devicesetup.net [192.168.0.1]
  2    13 ms    16 ms    12 ms  112.133.240.164
  3   124 ms   187 ms    19 ms  172.31.114.25
  4    15 ms    15 ms    37 ms  172.31.140.8
  5   134 ms   185 ms    13 ms  172.31.222.98
  6    22 ms    13 ms    16 ms  112.133.203.98
  7    14 ms    18 ms    15 ms  216.239.57.17
  8    21 ms    31 ms    35 ms  142.250.208.221
  9   274 ms   106 ms    14 ms  bom12s12-in-f14.1e100.net [142.250.183.78]

Trace complete.

C:\Users\ROG>
```

Output Explained:

It shows

i) No. of hopes to travel the destination Domain/IP
ii) 3 RTT to check consistency
iii) Domain/IP of the destination or the hop

8. **How do you find ip address associated with domain name?**
   To find IP Address associated with domain name:
   We can use **nslookup** command:



Output Explained:

It shows the Domain Name to which the specific IP address is assigned to.

9. **How do you access the mapping structure of IP addresses to the MAC address.**

To access the mapping structure of IP addresses to the MAC address: We can use **arp** command:

syntax: **arp [-v] [-i if] [-H type] -a [hostname]**

```
Command Prompt

C:\Users\ROG>arp -a

Interface: 192.168.0.131 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1           bc-22-28-c0-1c-02     dynamic
  192.168.0.101         c0-35-32-43-99-cb     dynamic
  192.168.0.169         f8-54-f6-1a-fc-dd     dynamic
  192.168.0.179         c8-94-02-83-68-1d     dynamic
  192.168.0.212         50-a6-d8-be-b6-f6     dynamic
  192.168.0.222         a6-de-33-97-98-8a     dynamic
  192.168.0.223         1c-ce-51-b5-52-f0     dynamic
  192.168.0.255         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
  224.77.77.77          01-00-5e-4d-4d-4d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.116.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.116.255       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
  224.77.77.77          01-00-5e-4d-4d-4d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.233.1 --- 0x16
  Internet Address      Physical Address      Type
  192.168.233.255       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
  224.77.77.77          01-00-5e-4d-4d-4d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\ROG>
```

Output Explained:

It shows

i) Local IP Address

ii) Device MAC

iii) Type of connection

10. How to view and manipulate the IP routing table.

To view and manipulate the IP routing table:
We can use **route** command:

syntax: **route [/f] [/p] [<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.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
   Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
   Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
         The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

   > route PRINT
   > route PRINT -4
   > route PRINT -6
   > route PRINT 157*        .... Only prints those matching 157*

   > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
         destination^     ^mask     ^gateway    metric^    ^
                                        Interface^
    If IF is not given, it tries to find the best interface for a given
    gateway.
   > route ADD 3ffe::/32 3ffe::1

   > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

    CHANGE is used to modify gateway and/or metric only.

   > route DELETE 157.0.0.0
   > route DELETE 3ffe::/32
```

```
Administrator: Windows Powe

PS C:\Users\ROG> route PRINT
===========================================================================
Interface List
 15...52 c2 e8 33 f5 6b ......Microsoft Wi-Fi Direct Virtual Adapter
  5...52 c2 e8 33 e5 7b ......Microsoft Wi-Fi Direct Virtual Adapter #2
 23...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 16...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  2...50 c2 e8 33 d5 4b ......MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
 13...50 c2 e8 33 d5 4c ......Bluetooth Device (Personal Area Network)
  7...50 eb f6 d4 9c 46 ......Realtek Gaming 2.5GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.19.0.1     172.19.2.176     55
        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
       172.19.0.0    255.255.248.0         On-link      172.19.2.176    311
     172.19.2.176  255.255.255.255         On-link      172.19.2.176    311
     172.19.7.255  255.255.255.255         On-link      172.19.2.176    311
    192.168.116.0    255.255.255.0         On-link     192.168.116.1    291
    192.168.116.1  255.255.255.255         On-link     192.168.116.1    291
  192.168.116.255  255.255.255.255         On-link     192.168.116.1    291
    192.168.233.0    255.255.255.0         On-link     192.168.233.1    291
    192.168.233.1  255.255.255.255         On-link     192.168.233.1    291
  192.168.233.255  255.255.255.255         On-link     192.168.233.1    291
        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     192.168.233.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.116.1    291
        224.0.0.0        240.0.0.0         On-link      172.19.2.176    311
  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     192.168.233.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.116.1    291
  255.255.255.255  255.255.255.255         On-link      172.19.2.176    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  2    311 fe80::/64                On-link
 16    291 fe80::/64                On-link
 23    291 fe80::/64                On-link
  2    311 fe80::12b1:6c7c:8ab7:3a3f/128
                                    On-link
 16    291 fe80::447c:9ce4:3de9:8148/128
                                    On-link
 23    291 fe80::a1d6:f39:9c97:c956/128
                                    On-link
  1    331 ff00::/8                 On-link
  2    311 ff00::/8                 On-link
 16    291 ff00::/8                 On-link
 23    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Output Explained:

It shows

i) List of NIC attached to the device

ii) IPv4 & IPv6 Route Tables