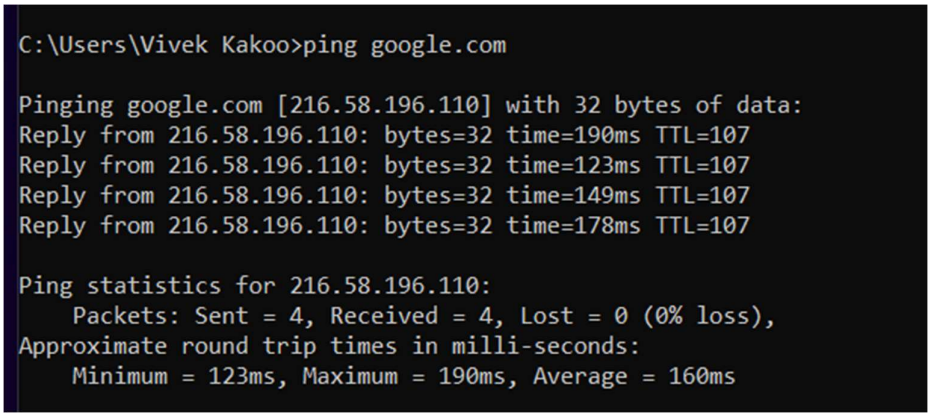
PRACTICAL – 1

Execute Basic TCP/IP utilities and commands. (eg: ping, ipconfig, tracert, arp, tcpdump, whois, host, netsat, nslookup, ftp, telnet etc...)

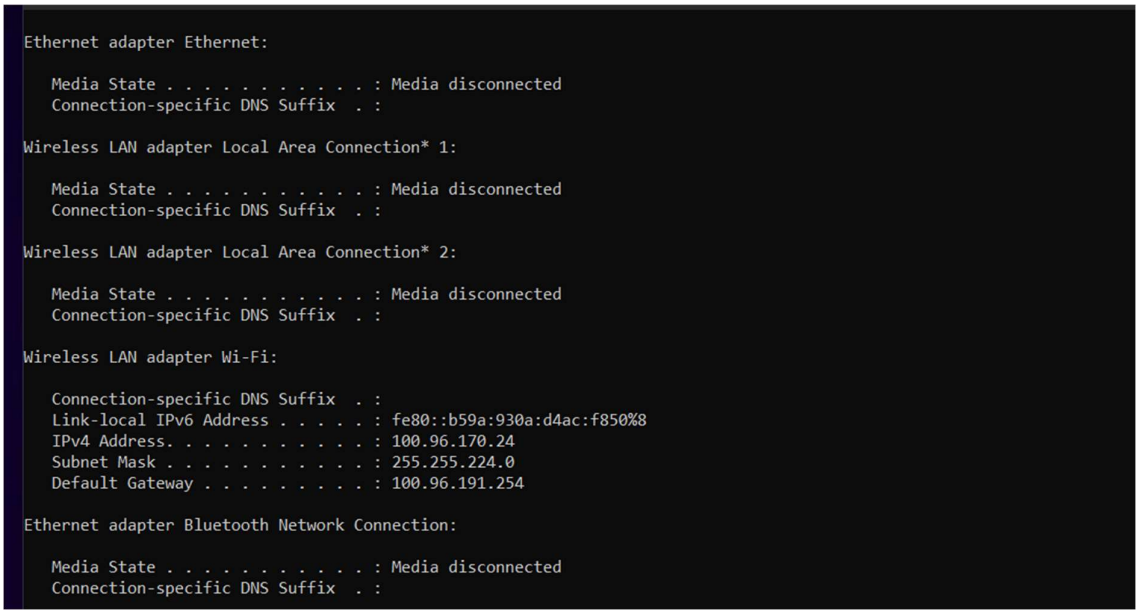
Ping:

- The ping command is used to test the ability of the source computer to reach a specified destination computer.
- The ping command is usually used as a simple way verify that a computer can communicate over the network with another computer or network device.
- The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response.
- For example: ping 10.9.39.60 (It will check that our system is communicate with the system which has IP address 10.9.39.60).



Ipconfig:

- ipconfig is a MS-DOS utility that can be used from MS-DOS and a MS-DOS shell to display the network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your network settings.



Tracert:

- A tracert is the tracking of a packet sent to a server. During its route, this packet goes through several network devices (routers, firewalls etc.) and then goes finally at the server.
- With the tracert, you can see the IP as well as the response time between each barrier (router, firewall…). We use then the tracert to check the problem between your computer and the server. We can see quickly where the problem is and fix it.

```
C:\Users\hh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.7.27:1037      a23-34-252-10:https    CLOSE_WAIT
  TCP    192.168.7.27:1042      104.18.24.243:http     CLOSE_WAIT
  TCP    192.168.7.27:17405     13.107.5.88:https      CLOSE_WAIT
  TCP    192.168.7.27:17407     117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.7.27:17423     20.198.162.78:https    ESTABLISHED
  TCP    192.168.7.27:17424     5.62.54.29:https       ESTABLISHED
  TCP    192.168.7.27:17427     104.22.0.235:https     ESTABLISHED
  TCP    192.168.7.27:17428     117.18.237.29:http     ESTABLISHED
  TCP    192.168.7.27:17429     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17430     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17431     117.18.237.29:http     ESTABLISHED
  TCP    192.168.7.27:17432     a-0001:https           ESTABLISHED
  TCP    192.168.7.27:17433     a-0001:https           ESTABLISHED
  TCP    192.168.7.27:17434     fra02-008:http         ESTABLISHED
  TCP    192.168.7.27:17436     204.79.197.222:https   ESTABLISHED
  TCP    192.168.7.27:17437     13.107.4.254:https     ESTABLISHED
  TCP    192.168.7.27:17438     13.107.246.58:https    ESTABLISHED
  TCP    192.168.7.27:17439     117.18.232.200:https   ESTABLISHED
  TCP    192.168.7.27:17440     a23-65-111-20:http     ESTABLISHED
  TCP    192.168.7.27:17441     104.18.31.182:http     ESTABLISHED
  TCP    192.168.7.27:17442     104.18.31.182:http     ESTABLISHED
  TCP    192.168.7.27:17443     104.18.31.182:http     ESTABLISHED
  TCP    192.168.7.27:17444     104.18.31.182:http     ESTABLISHED
  TCP    192.168.7.27:17445     104.18.31.182:http     ESTABLISHED
  TCP    192.168.7.27:17448     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17449     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17450     117.18.237.29:http     ESTABLISHED
  TCP    192.168.7.27:17451     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17452     a23-15-155-27:http     ESTABLISHED
  TCP    192.168.7.27:17458     5.62.40.178:https      TIME_WAIT
  TCP    192.168.7.27:17459     143.166.199.30:https   ESTABLISHED
  TCP    192.168.7.27:25117     192.168.2.1:8090       ESTABLISHED
  TCP    [::1]:1748             DESKTOP-FP51MKA:1750   ESTABLISHED
  TCP    [::1]:1750             DESKTOP-FP51MKA:1748   ESTABLISHED
```

Arp:

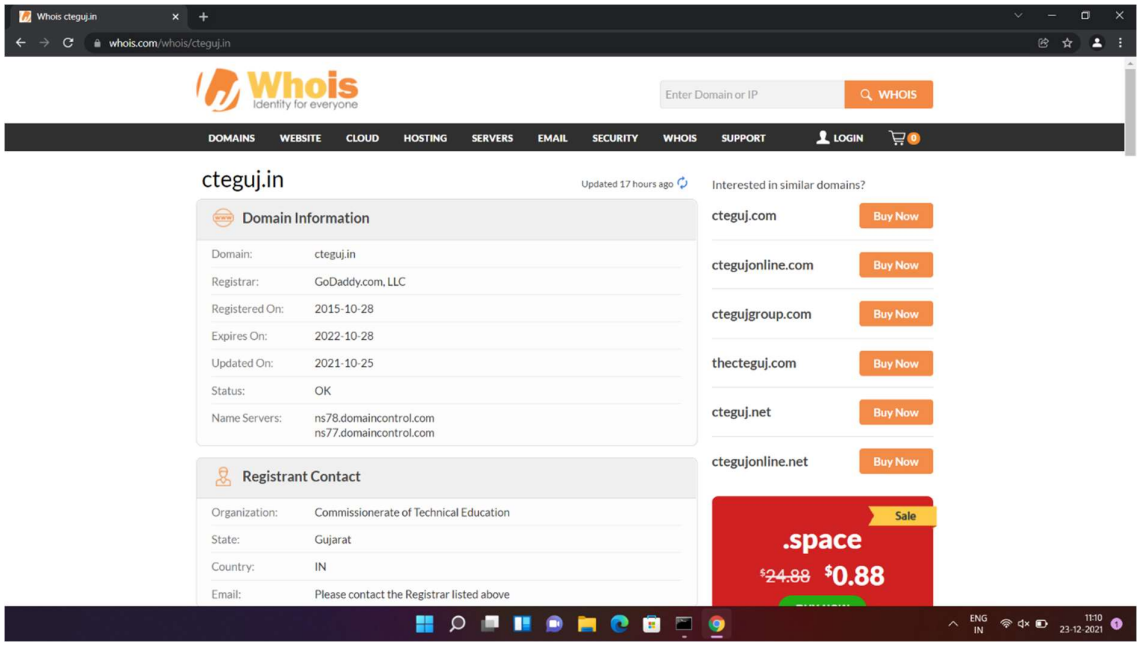
- Display or manipulate the ARP information on a network device or computer.
- The Physical Address or MAC address as shown is the unique manufacturer identification number. This number should always be an unique address.

```
C:\Users\Vivek Kakoo>arp -a

Interface: 100.96.170.24 --- 0x8
  Internet Address      Physical Address      Type
  100.96.176.62         88-53-2e-5d-03-2c     dynamic
  100.96.179.163        dc-fb-48-39-ab-43     dynamic
  100.96.181.79         d4-6a-6a-d9-67-89     dynamic
  100.96.191.253        00-a6-ca-f6-61-7f     dynamic
  100.96.191.254        00-00-5e-00-01-a0     dynamic
  100.96.191.255        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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

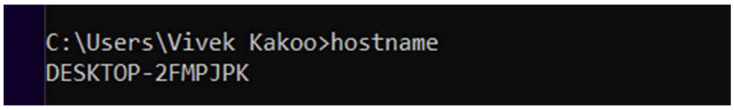
Whois:

- The whois command available in Unix and Linux variants helps allow a user to identify a domain name.
- This command provides information about a domain name. Whois searches for an object in a WHOIS database.
- WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block.
- Example: whois google.com (It performs a whois query for the domain name google.com.)



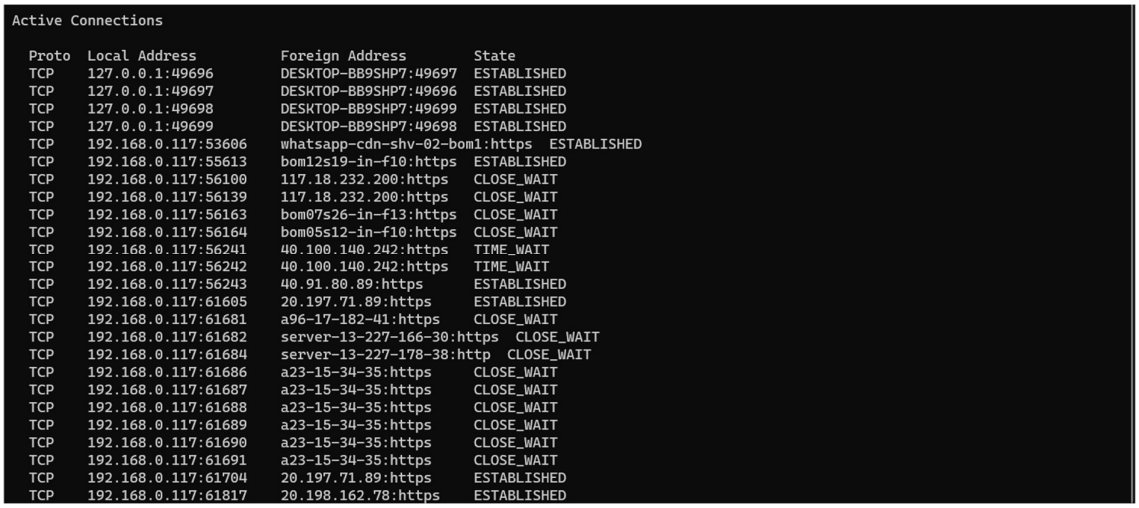
Hostname:

- The hostname command displays the host name of the windows computer currently logged into.
- Examples: hostname (Running the command would display the hostname for the computer.)



Netstat:

- Abbreviation of network statistics, the netstat command is a command found in almost all command line environments that allow you to view the statistics of the network.
- The netstat command is used to display the TCP/IP network protocol statistics and information.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49696        DESKTOP-BB9SHP7:49697  ESTABLISHED
  TCP    127.0.0.1:49697        DESKTOP-BB9SHP7:49696  ESTABLISHED
  TCP    127.0.0.1:49698        DESKTOP-BB9SHP7:49699  ESTABLISHED
  TCP    127.0.0.1:49699        DESKTOP-BB9SHP7:49698  ESTABLISHED
  TCP    192.168.0.117:53606    whatsapp-cdn-shv-02-bom1:https  ESTABLISHED
  TCP    192.168.0.117:55613    bom12s19-in-f10:https  ESTABLISHED
  TCP    192.168.0.117:56100    117.18.232.200:https   CLOSE_WAIT
  TCP    192.168.0.117:56139    117.18.232.200:https   CLOSE_WAIT
  TCP    192.168.0.117:56163    bom07s26-in-f13:https  CLOSE_WAIT
  TCP    192.168.0.117:56164    bom05s12-in-f10:https  CLOSE_WAIT
  TCP    192.168.0.117:56241    40.100.140.242:https   TIME_WAIT
  TCP    192.168.0.117:56242    40.100.140.242:https   TIME_WAIT
  TCP    192.168.0.117:56243    40.91.80.89:https      ESTABLISHED
  TCP    192.168.0.117:61605    20.197.71.89:https     ESTABLISHED
  TCP    192.168.0.117:61681    a96-17-182-41:https    CLOSE_WAIT
  TCP    192.168.0.117:61682    server-13-227-166-30:https  CLOSE_WAIT
  TCP    192.168.0.117:61684    server-13-227-178-38:http  CLOSE_WAIT
  TCP    192.168.0.117:61686    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61687    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61688    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61689    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61690    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61691    a23-15-34-35:https     CLOSE_WAIT
  TCP    192.168.0.117:61704    20.197.71.89:https     ESTABLISHED
  TCP    192.168.0.117:61817    20.198.162.78:https    ESTABLISHED
```

Nslookup:

- nslookup is a command line tool included with most operating systems that allows a user to look up a network name server, as well as return IP addresses and domain names for a network server.