Date: 25/07/2024

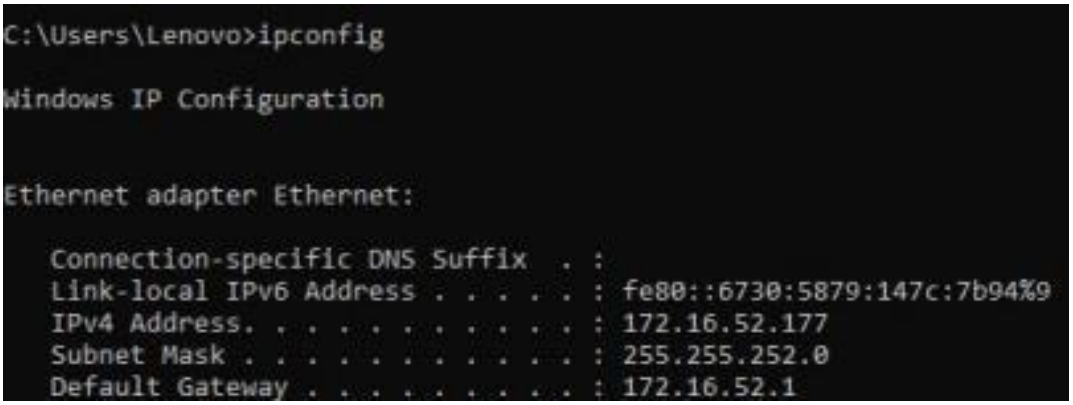
Exp. No.:1A

Janit B 231901013
CSE(CYBER SECURITY)

BASIC NETWORKING COMMAND IN WINDOWS.

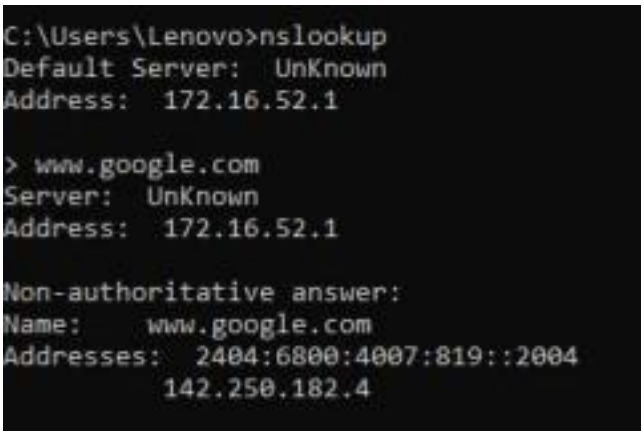
1. IPCONFIG

The IPCONFIG network command provides a comprehensive view of information regarding the IP address configuration of the device we are currently working on. Command to enter in Prompt – ipconfig



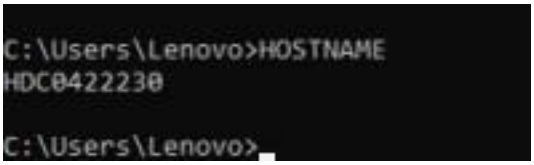
2. NSLOOKUP

The NSLOOKUP command is used to troubleshoot network connectivity issues in the system. Using the nslookup command, we can access the information related to our system's DNS server, i.e., domain name and IP address.
Command to enter in Prompt – nslookup



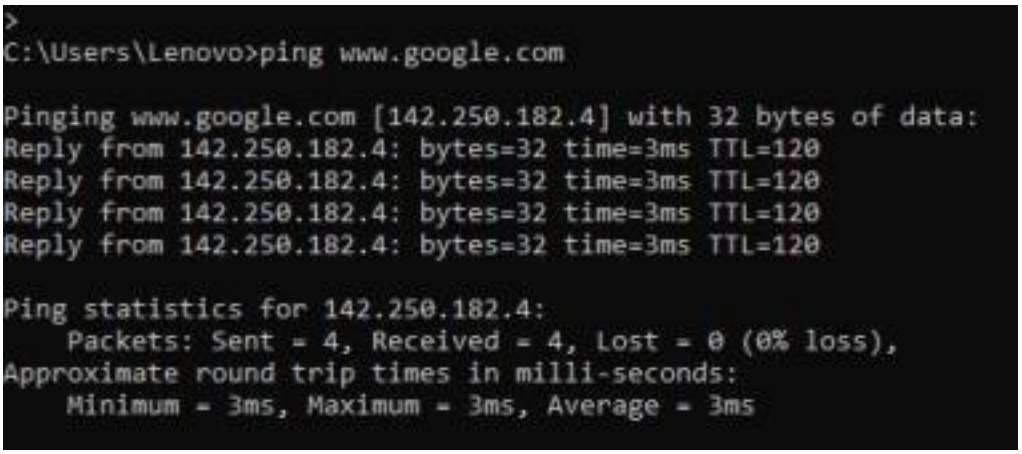
3. HOSTNAME

The HOSTNAME command displays the system's hostname. The hostname command ismuch easier to use than going into the system settings to search for it. Command to enter in Prompt – hostname



4. PING

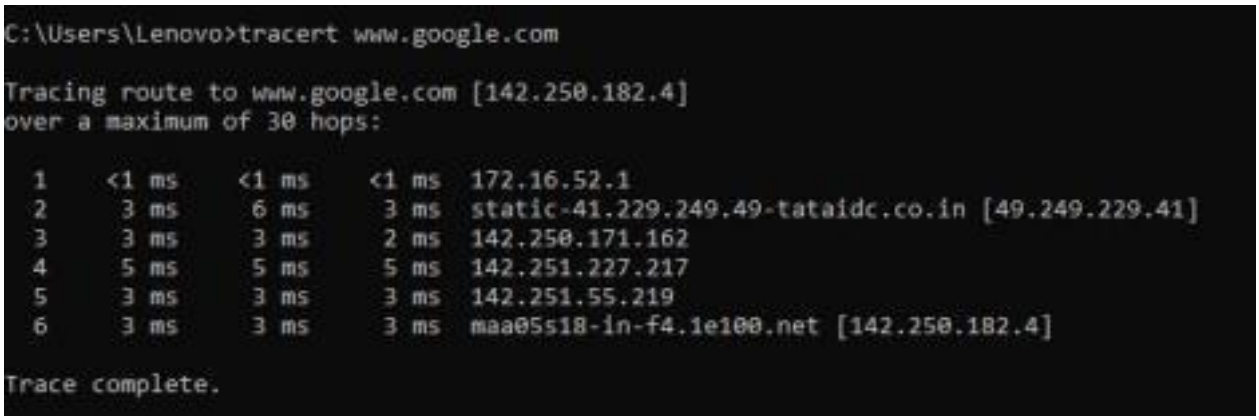
The Ping command is one of the most widely used commands in the prompt tool, as it allows theuser to check the connectivity of our system to another host. Command to enter in Prompt - ping www.destination_host_name.com



5. TRACERT

The TRACERT command is used to trace the route during the transmission of the data packet over to the destination host and also provides us with the “hop” count during transmission.

Using the number of hops and the hop IP address, we can troubleshoot network issues and identify the point of the problem during the transmission of the data packet. Command to enter in Prompt- tracert IP-address OR tracert www.destination_host_name.com



6. NETSTAT

The Netstat command as the name suggests displays an overview of all the network connections in the device. The table shows details about the connection protocol, address, and the current state of the network. Command to enter in Prompt - netstat

```
C:\Users\Lenovo>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49684        HDC0422230:49685       ESTABLISHED
  TCP    127.0.0.1:49685        HDC0422230:49684       ESTABLISHED
  TCP    127.0.0.1:49686        HDC0422230:49687       ESTABLISHED
  TCP    127.0.0.1:49687        HDC0422230:49686       ESTABLISHED
  TCP    172.16.52.177:23635    20.24.249.45:https     CLOSE_WAIT
  TCP    172.16.52.177:23636    152.195.38.76:http     CLOSE_WAIT
  TCP    172.16.52.177:24089    20.198.119.143:https   ESTABLISHED
  TCP    172.16.52.177:24424    server-108-158-46-66:https  ESTABLISHED
  TCP    172.16.52.177:24427    172.64.155.61:https    ESTABLISHED
  TCP    172.16.52.177:24428    a23-201-220-154:https  ESTABLISHED
  TCP    172.16.52.177:24429    a23-201-220-154:https  ESTABLISHED
  TCP    172.16.52.177:24430    172.64.155.61:https    ESTABLISHED
  TCP    172.16.52.177:24432    server-18-66-41-102:https  ESTABLISHED
  TCP    172.16.52.177:24433    server-52-84-12-2:https  ESTABLISHED
  TCP    172.16.52.177:24434    server-108-158-251-26:https  ESTABLISHED
  TCP    172.16.52.177:24440    172.66.0.163:https     ESTABLISHED
  TCP    172.16.52.177:24445    104.18.32.77:https     ESTABLISHED
  TCP    172.16.52.177:24448    151.101.193.138:https  ESTABLISHED
  TCP    172.16.52.177:24450    a23-223-244-177:https  CLOSE_WAIT
  TCP    172.16.52.177:24451    a23-223-244-177:https  CLOSE_WAIT
  TCP    172.16.52.177:24452    a23-223-244-177:https  CLOSE_WAIT
  TCP    172.16.52.177:24453    a23-223-244-177:https  CLOSE_WAIT
  TCP    172.16.52.177:24454    13.107.226.58:https    CLOSE_WAIT
  TCP    172.16.52.177:24455    52.108.8.254:https     CLOSE_WAIT
  TCP    172.16.52.177:24456    52.123.128.254:https   CLOSE_WAIT
  TCP    172.16.52.177:24457    204.79.197.222:https   CLOSE_WAIT
  TCP    172.16.52.177:24458    52.182.143.208:https   CLOSE_WAIT
  TCP    172.16.52.177:24459    a23-223-244-88:https   CLOSE_WAIT
  TCP    172.16.52.177:24460    a23-223-244-88:https   CLOSE_WAIT
  TCP    172.16.52.177:24461    a23-223-244-88:https   CLOSE_WAIT
  TCP    172.16.52.177:24462    a23-223-244-88:https   CLOSE_WAIT
  TCP    172.16.52.177:24463    a23-223-244-88:https   CLOSE_WAIT
  TCP    172.16.52.177:24465    a104-114-94-26:https   ESTABLISHED
  TCP    172.16.52.177:24466    204.79.197.239:https   ESTABLISHED
  TCP    172.16.52.177:24469    20.198.118.190:https   ESTABLISHED
  TCP    [fe80::6730:5879:147c:7b94%9]:1521  HDC0422230:49688       ESTABLISHED
  TCP    [fe80::6730:5879:147c:7b94%9]:49688  HDC0422230:1521       ESTABLISHED
```

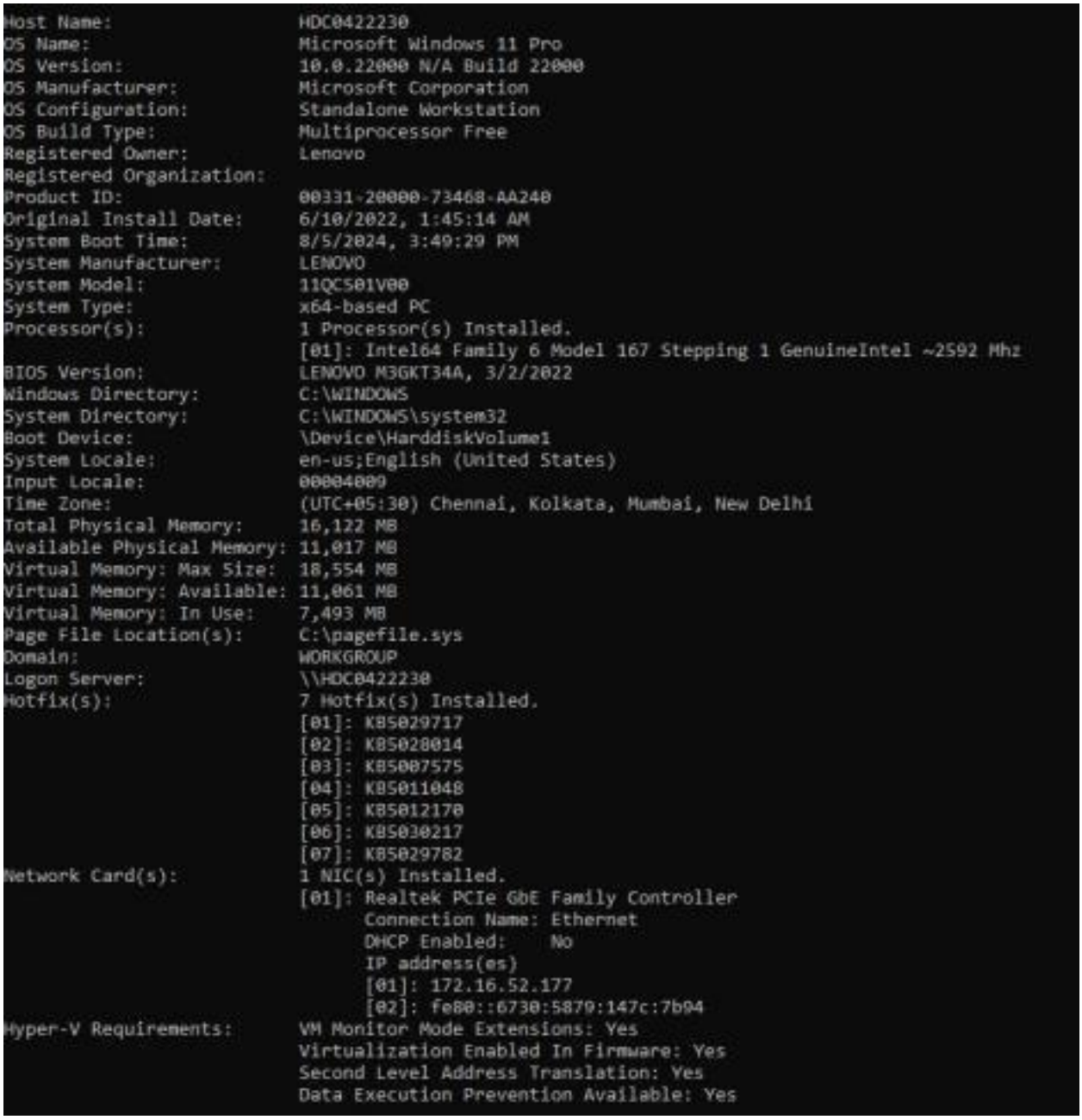
7. ARP(Address Resolution Protocol)

The ARP command is used to access the mapping structure of IP addresses to the MAC address. This provides us with a better understanding of the transmission of packets in the network channel.
Command to enter in Prompt – arp

```
C:\Users\Lenovo>arp

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.
```

8. SYSTEMINFO

Using the SYSTEMINFO command, we can access the system's hardware and software details,such as processor data, booting data, Windows version, etc.
Command to enter in Prompt – systeminfo



9. ROUTE

Provides the data of routing data packets in the system over the communication channel. Command to enter in Prompt – route print

```
C:\Users\Lenovo>route print
===========================================================================
Interface List
  9...88 ae dd 12 c7 fc ......Realtek PCIe GbE 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      172.16.52.1    172.16.52.177    281
        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
      172.16.52.0    255.255.252.0         On-link     172.16.52.177    281
    172.16.52.177  255.255.255.255         On-link     172.16.52.177    281
    172.16.55.255  255.255.255.255         On-link     172.16.52.177    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     172.16.52.177    281
  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     172.16.52.177    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      172.16.52.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  9    281 fe80::/64                On-link
  9    281 fe80::6730:5879:147c:7b94/128
                                    On-link
  1    331 ff00::/8                 On-link
  9    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```