EX NO:	**Learn to use commands like tcpdump, netstat, ifconfig, nslookup and traceroute. Capture ping and traceroute PDUs using a network protocol analyzer and examine.**
Date:	

AIM:

To Learn to use commands like tcpdump, netstat, ifconfig, nslookup and traceroute ping

COMMANDS

1. Tcpdump:

Display traffic between 2 hosts:

To display all traffic between two hosts (represented by variables host1and host2):

```
tcpdump host host1 and host2
```

Display traffic from a source or destination host only:

To display traffic from only a source (src) or destination (dst) host: #tcpdump

src host

```
tcpdump dst host
```

Display traffic for a specific protocol

Provide the protocol as an argument to display only traffic for a specificprotocol, for example tcp, udp, icmp, arp

```
tcpdump protocol
```

For example to display traffic only for the tcp traffic :

```
tcpdump tcp
```

Filtering based on source or destination port To filter based on a source ordestination port:

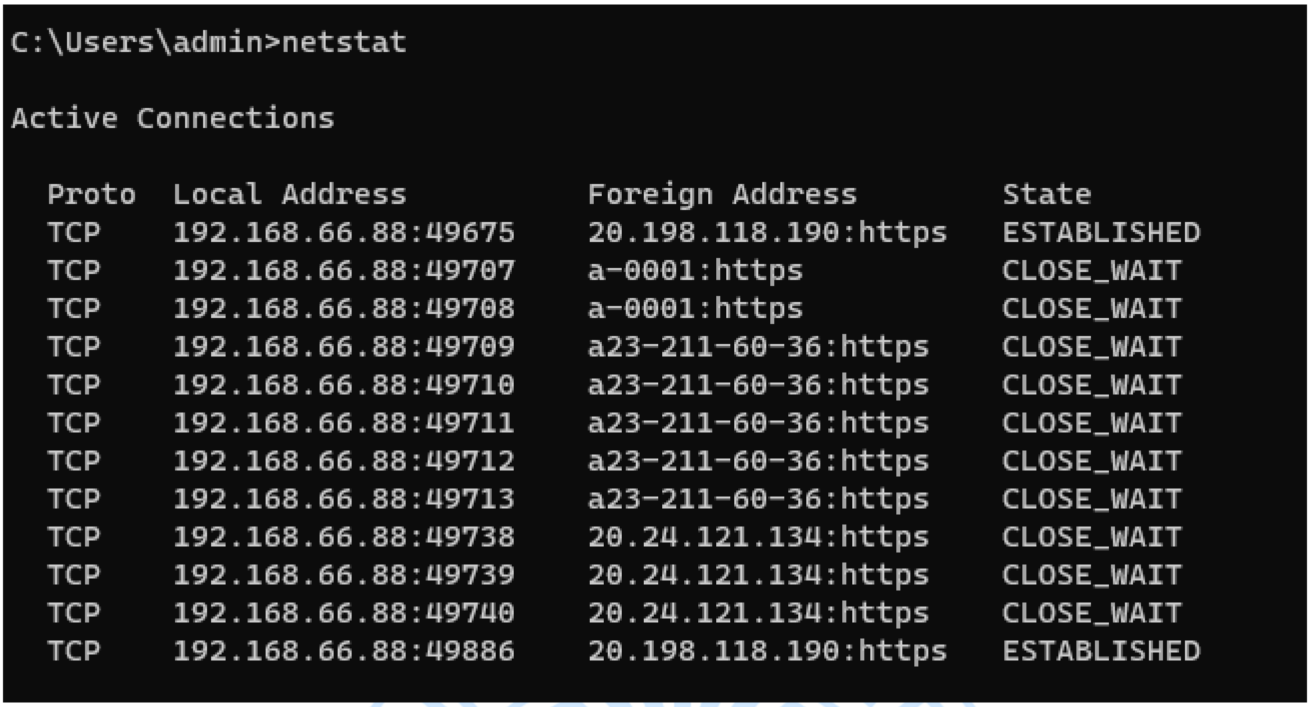
```
tcpdump src port ftp
tcpdump dst port http
```

2. Netstat

Netstat is a common command line TCP/IP networking available in most versions ofWindows, Linux, UNIX and other operating systems. Netstat providesinformation and statistics about protocols in use and current TCP/IP network connections. The Windowshelp screen (analogous to a Linux or UNIX for netstatreads as follows:
displays protocol statistics and current TCP/IP network connections.

Example:

```
>netstat
```



```
C:\Users\admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.66.88:49675    20.198.118.190:https   ESTABLISHED
  TCP    192.168.66.88:49707    a-0001:https           CLOSE_WAIT
  TCP    192.168.66.88:49708    a-0001:https           CLOSE_WAIT
  TCP    192.168.66.88:49709    a23-211-60-36:https    CLOSE_WAIT
  TCP    192.168.66.88:49710    a23-211-60-36:https    CLOSE_WAIT
  TCP    192.168.66.88:49711    a23-211-60-36:https    CLOSE_WAIT
  TCP    192.168.66.88:49712    a23-211-60-36:https    CLOSE_WAIT
  TCP    192.168.66.88:49713    a23-211-60-36:https    CLOSE_WAIT
  TCP    192.168.66.88:49738    20.24.121.134:https    CLOSE_WAIT
  TCP    192.168.66.88:49739    20.24.121.134:https    CLOSE_WAIT
  TCP    192.168.66.88:49740    20.24.121.134:https    CLOSE_WAIT
  TCP    192.168.66.88:49886    20.198.118.190:https   ESTABLISHED
```

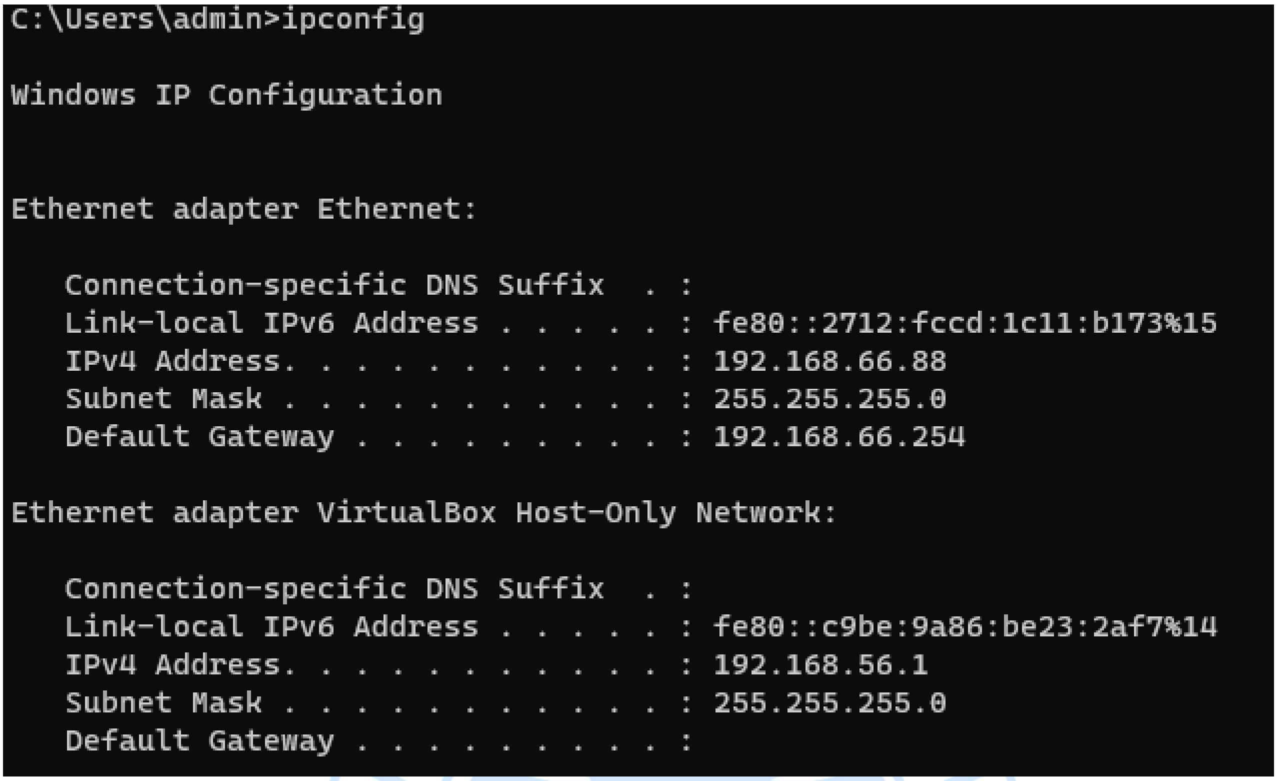
3.ipconfig

In Windows, ipconfig is a console application designed to run from the Windows command prompt. This utility allows you to get the IP address information of a Windowscomputer

From the command prompt, type ipconfig to run the utility with default options. The output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapter.

Example:

>ipconfig



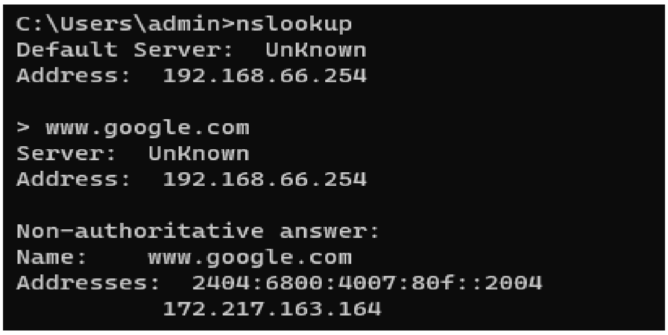
```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2712:fccd:1c11:b173%15
   IPv4 Address. . . . . . . . . . . : 192.168.66.88
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.66.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c9be:9a86:be23:2af7%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

4.nslookup

The nslookup (which stands for name server lookup) command is a networkutility program used to obtain information about internet servers. It finds name server information for domains by querying the Domain Name System. The nslookup commandis a powerful tool for diagnosing DNS problems. You knowyou're experiencing a DNS problem when you can access a resource by specifying its IP address but not its DNS name.

Example

>nslookup



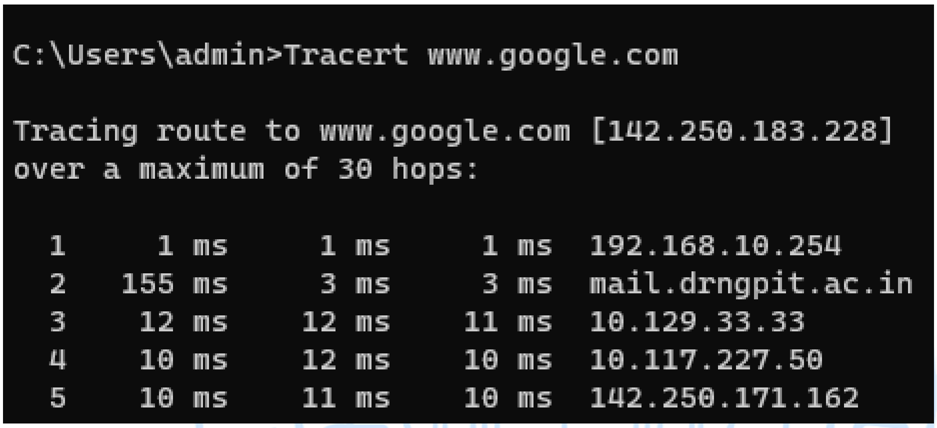
```
C:\Users\admin>nslookup
Default Server:  UnKnown
Address:  192.168.66.254

> www.google.com
Server:  UnKnown
Address:  192.168.66.254

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4007:80f::2004
          172.217.163.164
```

5.Trace route:

Traceroute uses Internet Control Message Protocol (ICMP) echo packetswith variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. Traceroute sends packets with TTL values that gradually increase from packet to packet, starting with TTL value of one.

Example:

>tracert google.com



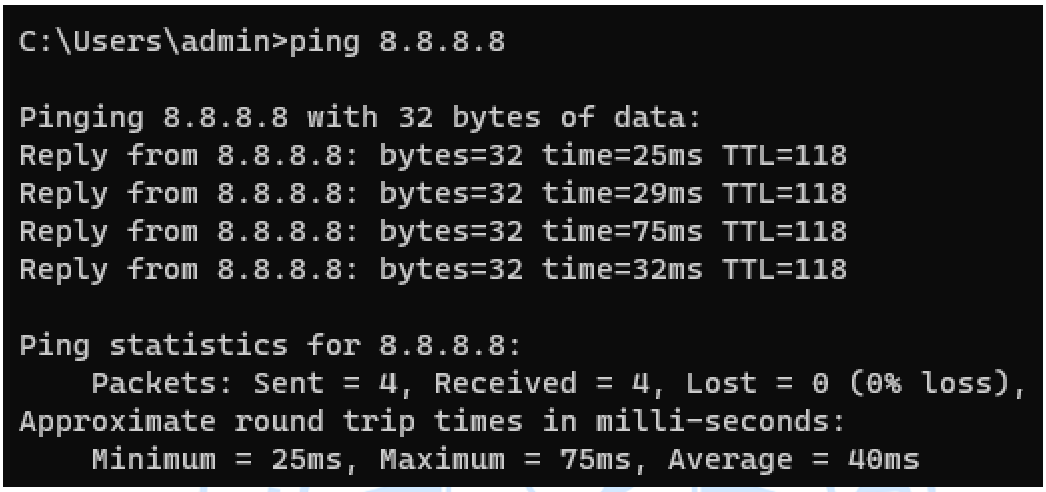
```
C:\Users\admin>Tracert www.google.com

Tracing route to www.google.com [142.250.183.228]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.10.254
  2   155 ms     3 ms     3 ms  mail.drngpit.ac.in
  3    12 ms    12 ms    11 ms  10.129.33.33
  4    10 ms    12 ms    10 ms  10.117.227.50
  5    10 ms    11 ms    10 ms  142.250.171.162
```

6.Ping:

The ping command sends an echo request to a host available on thenetwork. Using this command, you can check if your remote host is responding well or not. Tracking and isolating hardware and software problems. Determining the status of the network and various foreign hosts.The ping command is usually used as a simple way to verify that a computer can communicate over 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.

Example:

>ping 8.8.8.8



```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=118
Reply from 8.8.8.8: bytes=32 time=29ms TTL=118
Reply from 8.8.8.8: bytes=32 time=75ms TTL=118
Reply from 8.8.8.8: bytes=32 time=32ms TTL=118

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 75ms, Average = 40ms
```

RESULT

Thus the various networks commands like tcpdump, netstat, ifconfig, nslookupand traceroute ping are executed successfully.