Experiment 5

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

Windows Commands:

1.Ping:

```
C:\Windows\System32>ping google.com

Pinging google.com [142.250.192.14] with 32 bytes of data:
Reply from 142.250.192.14: bytes=32 time=5ms TTL=118
Reply from 142.250.192.14: bytes=32 time=4ms TTL=118
Reply from 142.250.192.14: bytes=32 time=6ms TTL=118
Reply from 142.250.192.14: bytes=32 time=4ms TTL=118

Ping statistics for 142.250.192.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 4ms
```

2.Tracert:

```
C:\Windows\System32>tracert google.com

Tracing route to google.com [142.250.183.110]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     3 ms     3 ms     1 ms  103.29.116.3
  3     3 ms     5 ms     3 ms  103.29.116.1
  4     4 ms     7 ms     8 ms  10.10.200.2
  5     6 ms     6 ms     7 ms  103.29.116.69
  6     4 ms     4 ms     4 ms  74.125.37.7
  7     4 ms     7 ms     7 ms  72.14.233.59
  8     4 ms     3 ms     5 ms  bom12s13-in-f14.1e100.net
[142.250.183.110]

Trace complete.
```

3.Ip config:

```
C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . :
fe80::d34c:5238:e1c0:8e3d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 3:

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

```
Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . :
fe80::5fb6:a16b:eb17:3706%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

4.Netstat:

```
C:\Windows\System32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:3000         MyLove:64361
ESTABLISHED
  TCP    127.0.0.1:5141         MyLove:50036
ESTABLISHED
  TCP    127.0.0.1:50026        MyLove:6742
ESTABLISHED
  TCP    127.0.0.1:50035        MyLove:63467
ESTABLISHED
  TCP    127.0.0.1:50036        MyLove:5141
ESTABLISHED
  TCP    127.0.0.1:50094        MyLove:46933
ESTABLISHED
```

```
  TCP    127.0.0.1:50096        MyLove:51779
ESTABLISHED
  TCP    127.0.0.1:51779        MyLove:50096
ESTABLISHED
  TCP    127.0.0.1:59300        MyLove:64501
ESTABLISHED
  TCP    127.0.0.1:59350        MyLove:64502
ESTABLISHED
  TCP    127.0.0.1:64502        MyLove:59350
ESTABLISHED
  TCP    127.0.0.1:65001        MyLove:63456
ESTABLISHED
  TCP    192.168.0.104:15101    DESKTOP-64QST15:64651
ESTABLISHED
  TCP    192.168.0.104:50247    20.198.118.190:https
ESTABLISHED
  TCP    192.168.0.104:50336    sh-in-f188:5228
ESTABLISHED
  TCP    192.168.0.104:52675    91.108.56.131:https
ESTABLISHED
  TCP    192.168.0.104:55238    DESKTOP-64QST15:15101
ESTABLISHED
  TCP    192.168.0.104:59018    91.108.23.100:https
ESTABLISHED
  TCP    192.168.0.104:59552    91.108.23.100:https
ESTABLISHED
  TCP    192.168.0.104:60013
whatsapp-chatd-edge-shv-02-bom2:5222  ESTABLISHED
  TCP    192.168.0.104:60028    13.107.226.254:https
CLOSE_WAIT
  TCP    192.168.0.104:61113    162.159.135.234:https
ESTABLISHED
```

```
  TCP    192.168.0.104:61588    sb-in-f188:5228
ESTABLISHED
  TCP    192.168.0.104:62260    150.171.27.254:https
ESTABLISHED
  TCP    192.168.0.104:62261    DESKTOP-64QST15:15101
ESTABLISHED
  TCP    192.168.0.104:62262    204.79.197.222:https
ESTABLISHED
  TCP    [::1]:4343             MyLove:63457           ESTABLISHED
  TCP    [::1]:4449             MyLove:63482           ESTABLISHED
  TCP    [::1]:5141             MyLove:63459           ESTABLISHED
  TCP    [::1]:15150            MyLove:50097           ESTABLISHED
  TCP    [::1]:15150            MyLove:63473           ESTABLISHED
  TCP    [::1]:50097            MyLove:15150           ESTABLISHED
  TCP    [::1]:63457            MyLove:4343            ESTABLISHED
  TCP    [::1]:63459            MyLove:5141            ESTABLISHED
  TCP    [::1]:63473            MyLove:15150           ESTABLISHED
```

5.Nslookup:

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

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:827::200e
          142.250.192.14
```

6.Netsh:

```
C:\Windows\System32>netsh interface ip show config
```

```
Configuration for interface "Ethernet"
    DHCP enabled:                         Yes
    InterfaceMetric:                      5
    DNS servers configured through DHCP:  10.0.1.21
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Ethernet 2"
    DHCP enabled:                         No
    IP Address:                           192.168.56.1
    Subnet Prefix:                        192.168.56.0/24 (mask
255.255.255.0)
    InterfaceMetric:                      25
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
    Statically Configured WINS Servers:   None

Configuration for interface "Local Area Connection* 3"
    DHCP enabled:                         Yes
    InterfaceMetric:                      25
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Local Area Connection* 4"
    DHCP enabled:                         Yes
    InterfaceMetric:                      25
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.0.104
    Subnet Prefix:                         192.168.0.0/24 (mask
255.255.255.0)
    Default Gateway:                        192.168.0.1
    Gateway Metric:                        0
    InterfaceMetric:                      35
    DNS servers configured through DHCP:  192.168.0.1
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                          No
    IP Address:                           127.0.0.1
    Subnet Prefix:                         127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
    Statically Configured WINS Servers:   None
```

7.Arp:

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

Interface: 192.168.56.1 --- 0xb
  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: 192.168.0.104 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           14-eb-b6-6b-cf-2d     dynamic
  192.168.0.100         b2-1b-de-f9-e4-d0     dynamic
  192.168.0.101         ae-d5-7b-01-a9-6c     dynamic
  192.168.0.102         fa-83-22-63-cf-0c     dynamic
  192.168.0.103         b2-f4-75-92-90-27     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

8.Route:

```
C:\Windows\System32>route print
===========================================================================
Interface List
 19...74 d4 dd 26 5d 1f ......Killer E2600 Gigabit Ethernet Controller
 11...0a 00 27 00 00 0b ......VirtualBox Host-Only Ethernet Adapter
 12...b0 dc ef dd 9b 46 ......Microsoft Wi-Fi Direct Virtual Adapter #3
  7...b2 dc ef dd 9b 45 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 14...b0 dc ef dd 9b 45 ......Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
  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    192.168.0.104
35
        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     192.168.0.104
291
    192.168.0.104  255.255.255.255         On-link
192.168.0.104    291
    192.168.0.255  255.255.255.255         On-link
192.168.0.104    291
     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     192.168.0.104
291
  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
192.168.0.104    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 11    281 fe80::/64                On-link
 14    291 fe80::/64                On-link
 14    291 fe80::5fb6:a16b:eb17:3706/128
                                    On-link
 11    281 fe80::d34c:5238:e1c0:8e3d/128
                                    On-link
  1    331 ff00::/8                 On-link
 11    281 ff00::/8                 On-link
 14    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Linux Commands:

1.Ping:

```
surya@surya-VirtualBox:~$ ping youtube.com
PING youtube.com (142.250.182.238) 56(84) bytes of data.
```

```
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=1 ttl=117 time=4.83 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=2 ttl=117 time=5.00 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=3 ttl=117 time=8.90 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=4 ttl=117 time=5.35 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=5 ttl=117 time=6.85 ms
64 bytes from bom07s29-in-f14.1e100.net (142.250.182.238):
icmp_seq=6 ttl=117 time=4.66 ms
^Z
[2]+  Stopped                 ping youtube.com
```

2.Traceroute:

```
surya@surya-VirtualBox:~$ traceroute youtube.com
traceroute to youtube.com (142.250.182.238), 30 hops max, 60
byte packets
 1  _gateway (10.0.2.2)  0.929 ms  0.867 ms  0.840 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
```

```
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

3.Ifconfig:

```
surya@surya-VirtualBox:~$ ifconfig
enp0s3:
flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu
1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast
10.0.2.255
        inet6 fe80::a00:27ff:feb1:f0e8  prefixlen 64  scopeid
0x20<link>
        ether 08:00:27:b1:f0:e8  txqueuelen 1000  (Ethernet)
        RX packets 2325  bytes 3166013 (3.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1363  bytes 120208 (120.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 111  bytes 12167 (12.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 111  bytes 12167 (12.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4.Dig:

```
surya@surya-VirtualBox:~$ dig google.com

; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
10314
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN    A

;; ANSWER SECTION:
google.com.        204  IN    A     142.250.192.142

;; Query time: 11 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Sep 29 03:26:23 IST 2024
;; MSG SIZE  rcvd: 55
```

5.Nslookup:

```
surya@surya-VirtualBox:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.14
Name:   google.com
Address: 2404:6800:4009:827::200e
```