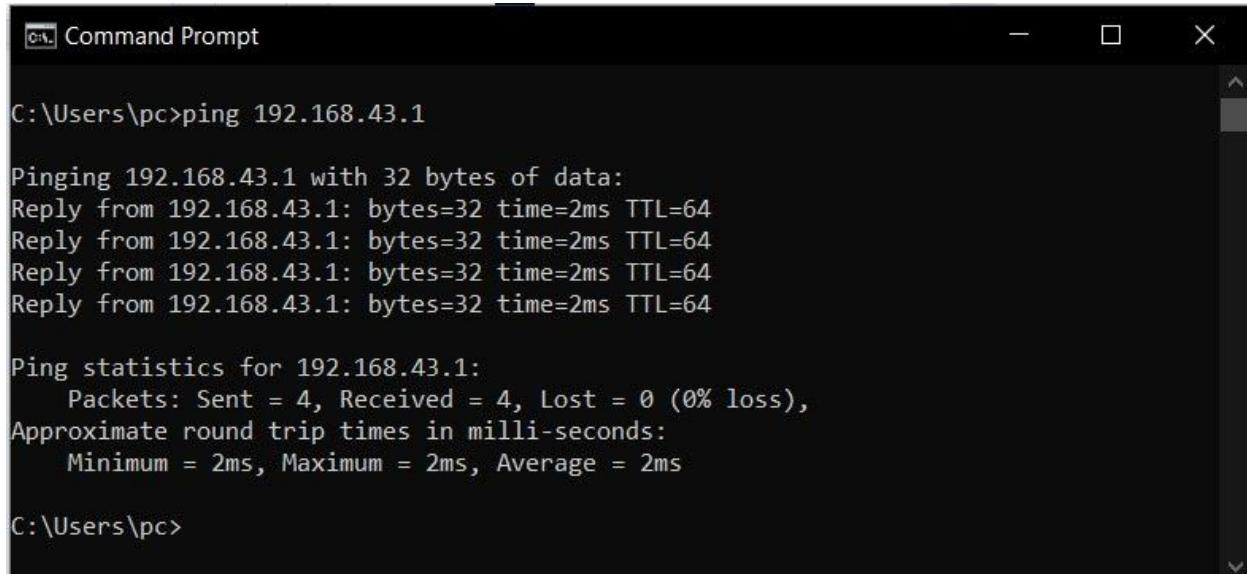

EXPERIMENT - 1

NETWORKS LAB

**Submitted by
Mohammed Ismail C
B180437CS
B Batch**

1.ping

The Ping network command uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. When a ping command is issued, an echo request packet is sent to the address specified. When the remote host receives the echo request, it responds with an echo reply packet.



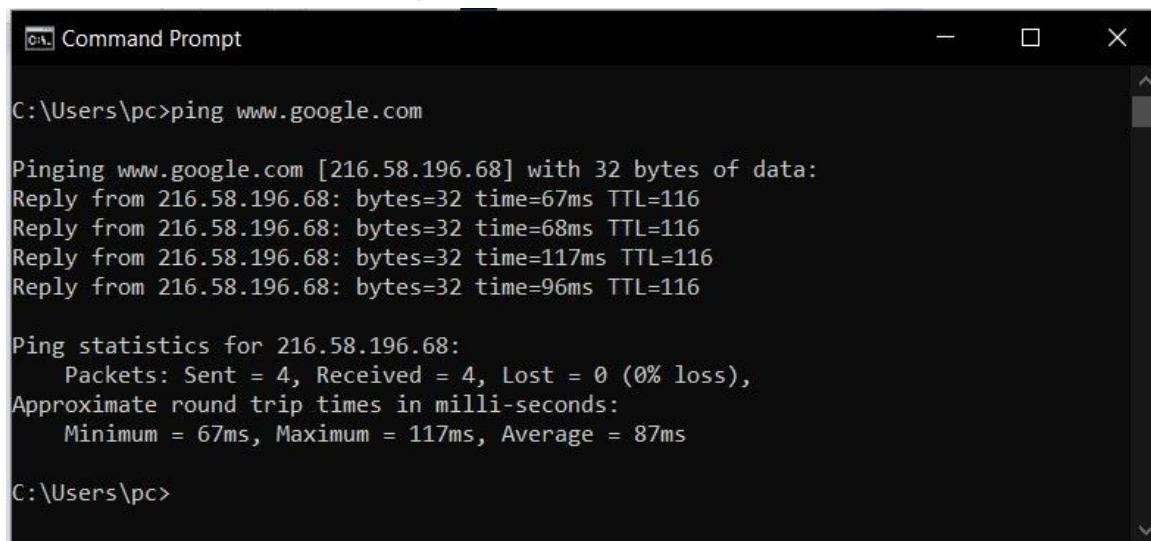
```
Command Prompt
C:\Users\pc>ping 192.168.43.1

Pinging 192.168.43.1 with 32 bytes of data:
Reply from 192.168.43.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.43.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\pc>
```

My home router IP address is 192.168.43.1 .We are sending 4 ICMP data packets and upon receiving it sends back same packets as response. You can see in summary, data packet lost is 0%. So there is a successful connection with remote system.



```
Command Prompt
C:\Users\pc>ping www.google.com

Pinging www.google.com [216.58.196.68] with 32 bytes of data:
Reply from 216.58.196.68: bytes=32 time=67ms TTL=116
Reply from 216.58.196.68: bytes=32 time=68ms TTL=116
Reply from 216.58.196.68: bytes=32 time=117ms TTL=116
Reply from 216.58.196.68: bytes=32 time=96ms TTL=116

Ping statistics for 216.58.196.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 67ms, Maximum = 117ms, Average = 87ms

C:\Users\pc>
```

We can also ping using domain name as shown above.

1.1 controlling the number of pings

```
ismail@ismail-VirtualBox:~$ ping -c 5 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.017 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.018 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.017/0.022/0.040/0.008 ms
```

Here 5 packets will be send to the destination address.

1.2 Controlling the size of packets send

```
ismail@ismail-VirtualBox:~$ ping -s 40 -c 5 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 40(68) bytes of data.
48 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.016 ms
48 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.039 ms
48 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.035 ms
48 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.048 ms
48 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.024 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4103ms
rtt min/avg/max/mdev = 0.016/0.032/0.048/0.011 ms
ismail@ismail-VirtualBox:~$
```

1.3 Changing the time interval:

```
ismail@ismail-VirtualBox:~$ ping -i 2 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.020 ms
^C
--- 10.0.2.15 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 10095ms
rtt min/avg/max/mdev = 0.018/0.022/0.036/0.006 ms
ismail@ismail-VirtualBox:~$
```

By default ping wait for 1 sec to send next packet, Now it will wait for 2 seconds.

1.4 To get only summary

```
ismail@ismail-VirtualBox:~$ ping -c 5 -q 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 0.015/0.021/0.035/0.007 ms
ismail@ismail-VirtualBox:~$
```

1.5 To timeout ping

```
ismail@ismail-VirtualBox:~$ ping -w 3 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.019 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.012/0.017/0.022/0.004 ms
```

Pinging stopped after 3 seconds.

1.6 To add timestamp only

```
ismail@ismail-VirtualBox:~$ ping -T tsonly -c 2 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(124) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.012 ms
TS: 18379867 absolute
0
0
0

64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.024 ms
TS: 18380878 absolute
0
0
0

--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.012/0.018/0.024/0.006 ms
```

1.7 To add timestamp and address

```
ismail@ismail-VirtualBox:~$ ping -c 2 -T tsandaddr 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(124) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.012 ms
TS: 10.0.2.15 18513509 absolute
    10.0.2.15 0
    10.0.2.15 0
    10.0.2.15 0

64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.040 ms
TS: 10.0.2.15 18514548 absolute
    10.0.2.15 0
    10.0.2.15 0
    10.0.2.15 0

--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1039ms
rtt min/avg/max/mdev = 0.012/0.026/0.040/0.014 ms
```

1.8 To fill packet with data

```
ismail@ismail-VirtualBox:~$ ping -c 5 -p ff 10.0.2.15
PATTERN: 0xff
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.017 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.018 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4097ms
rtt min/avg/max/mdev = 0.017/0.018/0.019/0.000 ms
```

We can fill data in packet using **-p** option. Like **-p ff** will fill packet with ones.

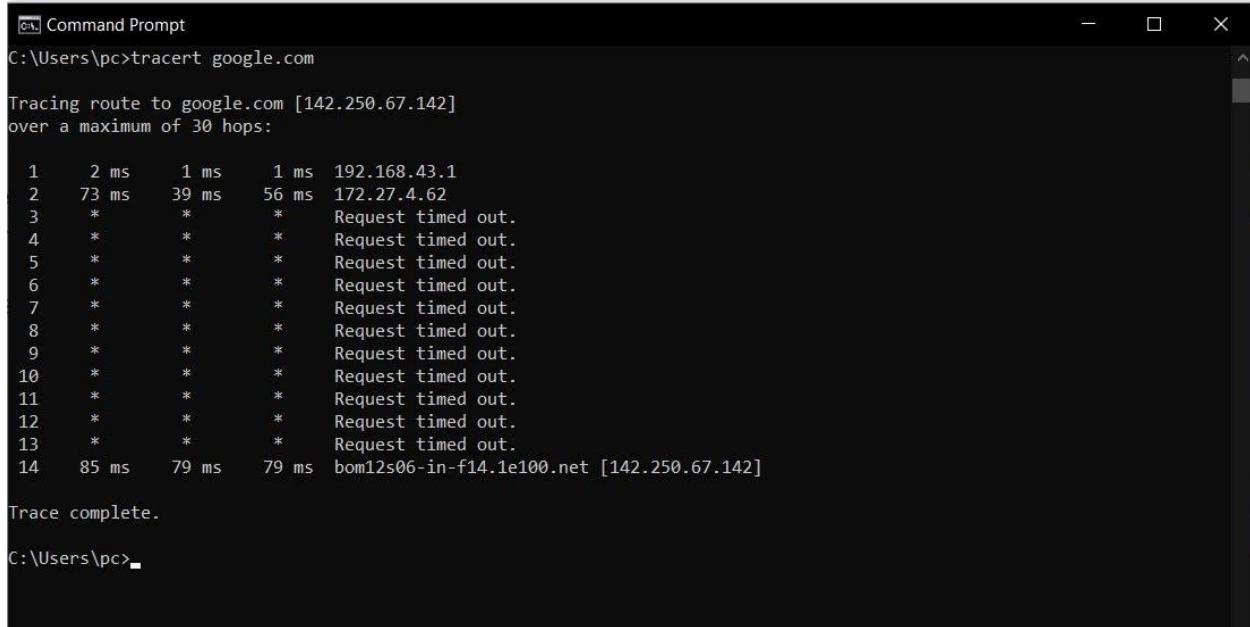
1.9 Specify Time to Live(TTL)

```
ismail@ismail-VirtualBox:~$ ping -c 5 -t 64 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.017 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.019 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.017/0.021/0.025/0.003 ms
```

2.tracert

The tracert command used to show several details about the path that a packet takes from the computer to whatever destination you specify.



```
Command Prompt
C:\Users\pc>tracert google.com

Tracing route to google.com [142.250.67.142]
over a maximum of 30 hops:

 1   2 ms    1 ms    1 ms 192.168.43.1
 2   73 ms   39 ms   56 ms 172.27.4.62
 3   *        *        * Request timed out.
 4   *        *        * Request timed out.
 5   *        *        * Request timed out.
 6   *        *        * Request timed out.
 7   *        *        * Request timed out.
 8   *        *        * Request timed out.
 9   *        *        * Request timed out.
10   *        *        * Request timed out.
11   *        *        * Request timed out.
12   *        *        * Request timed out.
13   *        *        * Request timed out.
14   85 ms   79 ms   79 ms bom12s06-in-f14.1e100.net [142.250.67.142]

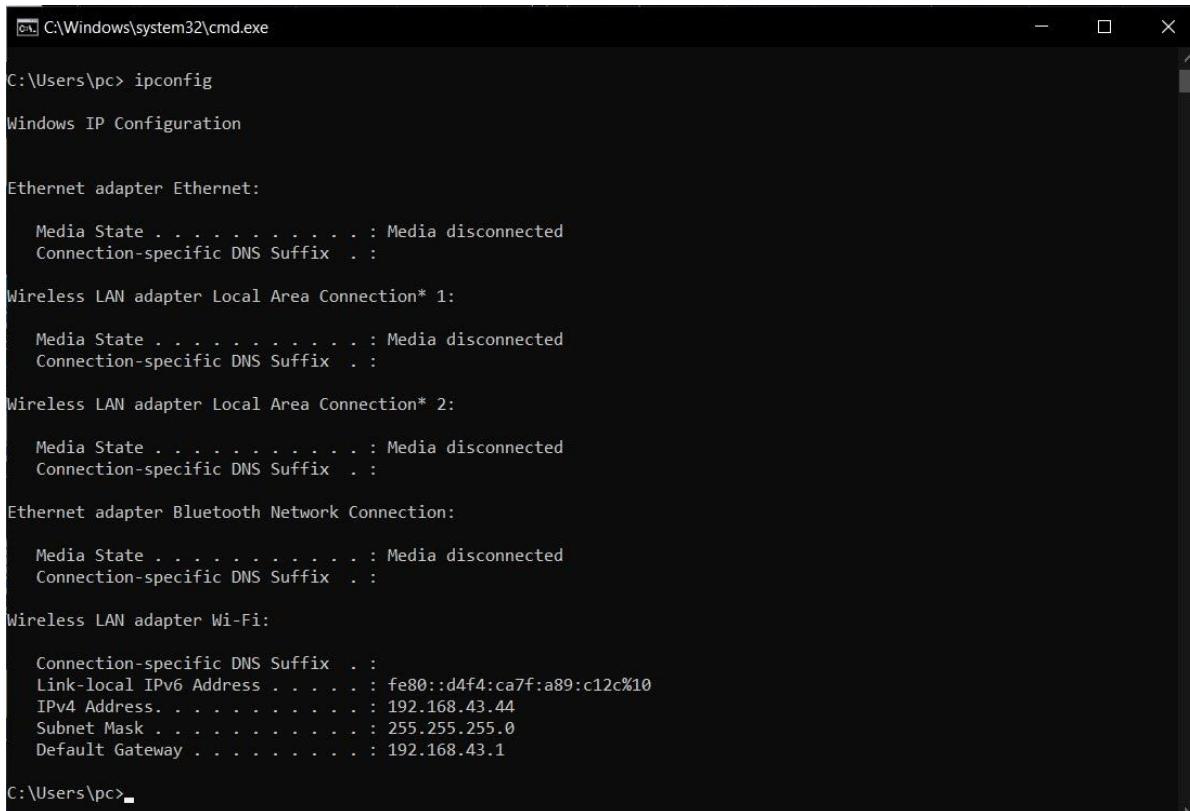
Trace complete.

C:\Users\pc>
```

we can see here that tracert identified 14 network devices including my router(mobile hotspot) at 192.168.43.1 and all the way through to the target of www.google.com, which we now know uses the public IP address of 142.250.67.142, one of Google's many IP addresses. Here some router details are displayed as “*” because many router intentionally discard ping commands.

3.ipconfig/ifconfig

ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.



```
C:\Windows\system32\cmd.exe
C:\Users\pc> ipconfig
Windows IP Configuration

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

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

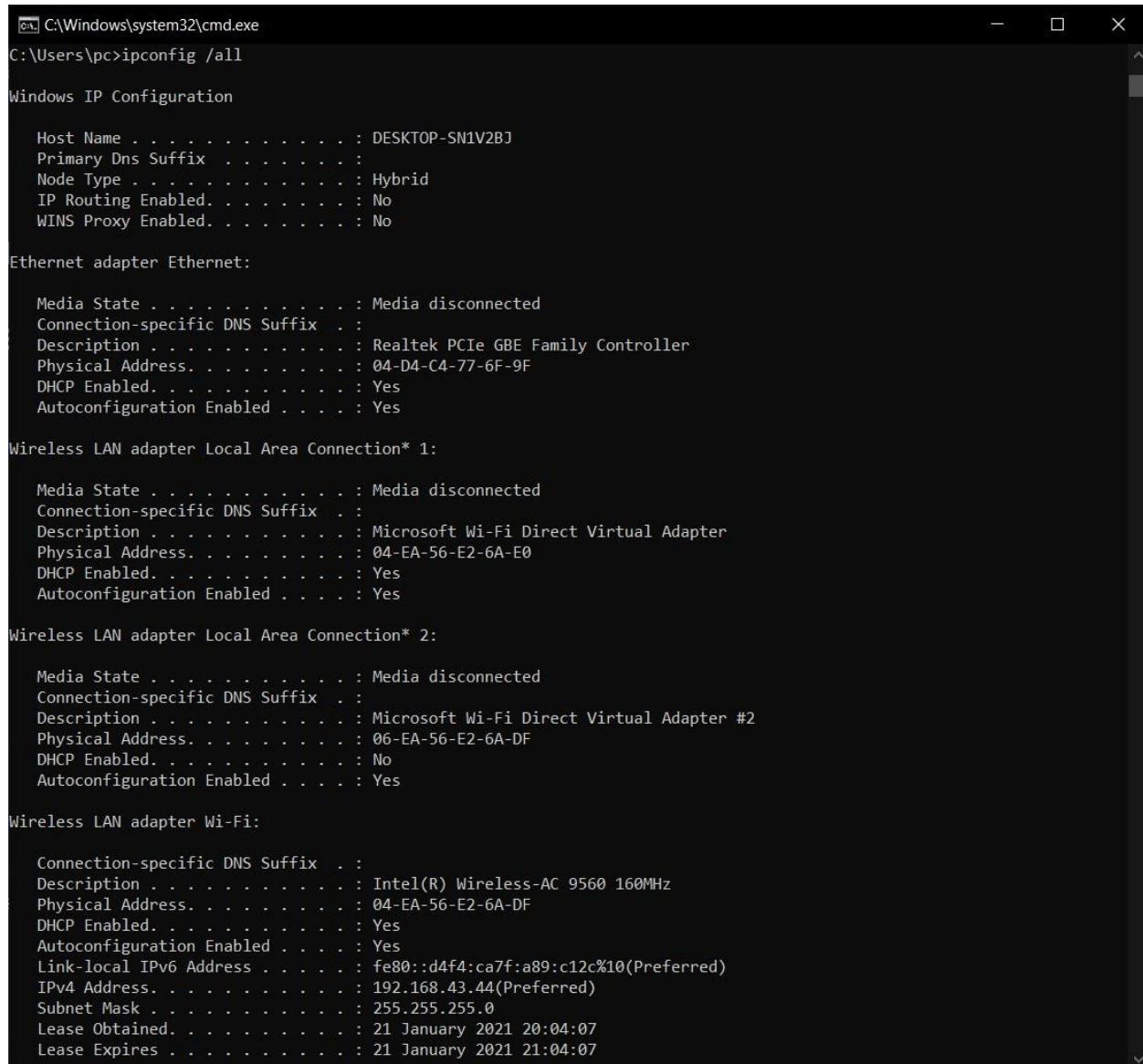
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::d4f4:ca7f:a89:c12c%10
  IPv4 Address . . . . . : 192.168.43.44
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.43.1

C:\Users\pc>
```

My computer is connected to internet through the wireless LAN adapter or Wi-Fi whose IP address is 192.168.43.1.

3.1 ipconfig/all

Displays the full TCP/IP configuration for all adapters.



```
C:\Windows\system32\cmd.exe
C:\Users\pc>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-SN1V2BJ
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 04-D4-C4-77-6F-9F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 04-EA-56-E2-6A-E0
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 06-EA-56-E2-6A-DF
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
    Physical Address. . . . . : 04-EA-56-E2-6A-DF
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d4f4:ca7f:a89:c12c%10(Preferred)
    IPv4 Address . . . . . : 192.168.43.44(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 21 January 2021 20:04:07
    Lease Expires . . . . . : 21 January 2021 21:04:07
```

3.2 ipconfig/displaydns

Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer.

```
C:\Windows\system32\cmd.exe
C:\Users\pc>ipconfig /displaydns
Windows IP Configuration

t.kite.com
-----
Record Name . . . . . : t.kite.com
Record Type . . . . . : 1
Time To Live . . . . . : 23
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 3.82.182.124

Record Name . . . . . : t.kite.com
Record Type . . . . . : 1
Time To Live . . . . . : 23
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 52.5.201.89

eduserver.nitc.ac.in
-----
Record Name . . . . . : eduserver.nitc.ac.in
Record Type . . . . . : 1
Time To Live . . . . . : 3591
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 103.241.136.151

28.137.168.192.in-addr.arpa
-----
Record Name . . . . . : 28.137.168.192.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 68981
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : android-8b79d97bd3882695.mshome.net
```

3.3 ipconfig/release

Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the adapter parameter is included.

```
C:\Windows\system32\cmd.exe
C:\Users\pc>ipconfig /release
Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.

Ethernet adapter Ethernet:

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

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 . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::d4f4:ca7f:a89:c12c%10
    Default Gateway . . . . . :
```

3.4 display all the interfaces available

```
ismail@ismail-VirtualBox:~$ ifconfig -a
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::bc3f:b4c8:e1b7:6548  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:3b:62:e0  txqueuelen 1000  (Ethernet)
            RX packets 36895  bytes 21354278 (21.3 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 33632  bytes 5233973 (5.2 MB)
            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 8555  bytes 954924 (954.9 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 8555  bytes 954924 (954.9 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

ismail@ismail-VirtualBox:~$ █
```

3.5 display a shortlist instead of all information

```
ismail@ismail-VirtualBox:~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500    37620     0     0 0      34402     0     0     0 BMRU
lo       65536    8700     0     0 0      8700     0     0     0 LRU
ismail@ismail-VirtualBox:~$ █
```

3.6 Activating and deactivating driver for a given interface

```
ismail@ismail-VirtualBox:~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500    38789     0     0 0      35536     0     0     0 BMRU
lo       65536    9017     0     0 0      9017     0     0     0 LRU
ismail@ismail-VirtualBox:~$ 
ismail@ismail-VirtualBox:~$ sudo ifconfig enp0s3 down
[sudo] password for ismail:
ismail@ismail-VirtualBox:~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
lo       65536    9129     0     0 0      9129     0     0     0 LRU
ismail@ismail-VirtualBox:~$ 
ismail@ismail-VirtualBox:~$ sudo ifconfig enp0s3 up
ismail@ismail-VirtualBox:~$ 
ismail@ismail-VirtualBox:~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500    38913     0     0 0      35683     0     0     0 BMRU
lo       65536    9918     0     0 0      9918     0     0     0 LRU
ismail@ismail-VirtualBox:~$ █
```

3.7 View network setting for specific interface

```
ismail@ismail-VirtualBox:~$ ifconfig enp0s3
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::bc3f:b4c8:e1b7:6548 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:3b:62:e0 txqueuelen 1000 (Ethernet)
            RX packets 43714 bytes 24689447 (24.6 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 40136 bytes 6246051 (6.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3.8 Assign IP address to a network interface

```
ismail@ismail-VirtualBox:~$ sudo ifconfig lo 192.168.1.1
ismail@ismail-VirtualBox:~$
ismail@ismail-VirtualBox:~$ ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 192.168.1.1 netmask 255.255.255.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 11120 bytes 1216978 (1.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11120 bytes 1216978 (1.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ismail@ismail-VirtualBox:~$ █
```

3.9 Assign netmask to a network interface

```
ismail@ismail-VirtualBox:~$ sudo ifconfig lo netmask 255.255.255.224
ismail@ismail-VirtualBox:~$
ismail@ismail-VirtualBox:~$ ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.255.255.224
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 11243 bytes 1231138 (1.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11243 bytes 1231138 (1.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ismail@ismail-VirtualBox:~$ █
```

4.nslookup

nslookup is a command-line administrative tool for testing and troubleshooting DNS servers (Domain Name Server). It is used to query specific DNS resource records (RR) as well.

4.1 display IP address of domain

```
ismail@ismail-VirtualBox:~$ nslookup yahoo.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:  yahoo.com
Address: 74.6.143.25
Name:  yahoo.com
Address: 74.6.143.26
Name:  yahoo.com
Address: 98.137.11.163
Name:  yahoo.com
Address: 74.6.231.21
Name:  yahoo.com
Address: 74.6.231.20
Name:  yahoo.com
Address: 98.137.11.164
Name:  yahoo.com
Address: 2001:4998:24:120d::1:0
Name:  yahoo.com
Address: 2001:4998:44:3507::8000
Name:  yahoo.com
Address: 2001:4998:44:3507::8001
Name:  yahoo.com
Address: 2001:4998:124:1507::f000
Name:  yahoo.com
Address: 2001:4998:24:120d::1:1
Name:  yahoo.com
Address: 2001:4998:124:1507::f001
```

4.2 Reverse domain lookup

```
ismail@ismail-VirtualBox:~$ nslookup 209.191.122.70
70.122.191.209.in-addr.arpa      name = unknown.yahoo.com.

Authoritative answers can be found from:

ismail@ismail-VirtualBox:~$
```

4.3 To query Mail Exchange(MX) record

```
ismail@ismail-VirtualBox:~$ nslookup -query=mx www.yahoo.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.yahoo.com  canonical name = new-fp-shed.wg1.b.yahoo.com.

Authoritative answers can be found from:
```

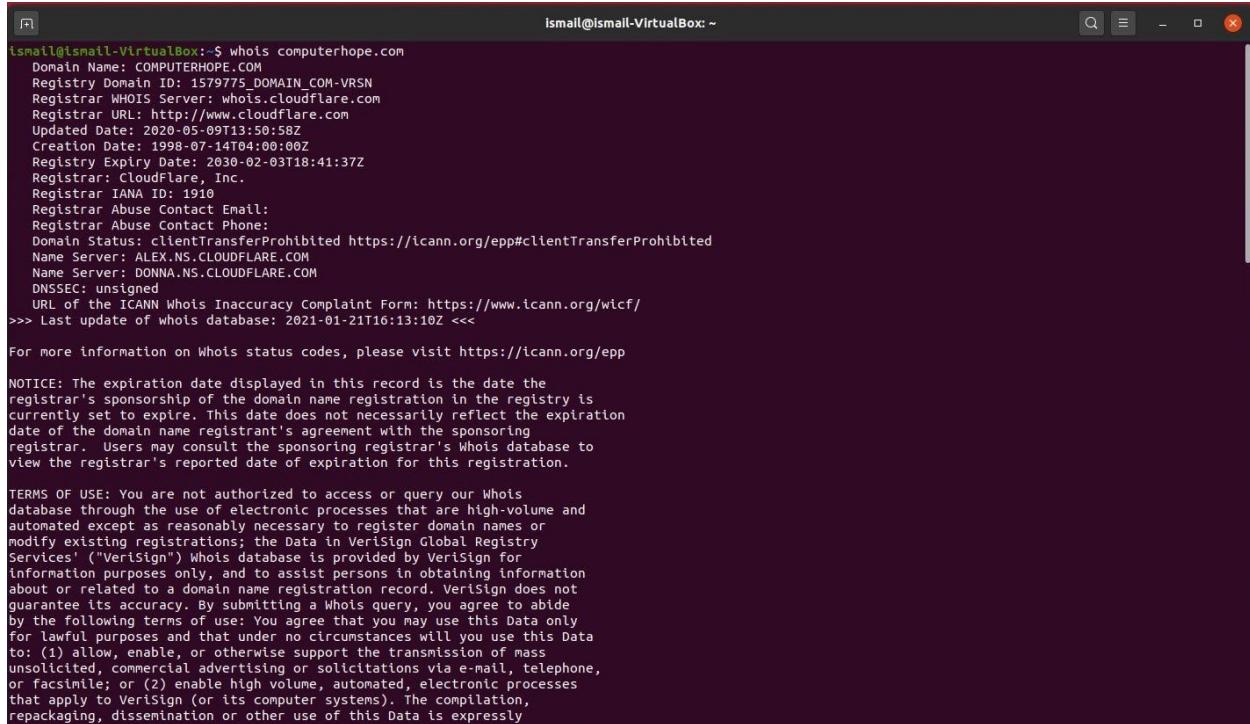
4.4 To enable debug mode

```
ismail@ismail-VirtualBox:~$ nslookup -debug yahoo.com
Server:      127.0.0.53
Address:     127.0.0.53#53

-----
QUESTIONS:
  yahoo.com, type = A, class = IN
ANSWERS:
->  yahoo.com
    internet address = 98.137.11.164
    ttl = 1017
->  yahoo.com
    internet address = 74.6.231.20
    ttl = 1017
->  yahoo.com
    internet address = 74.6.231.21
    ttl = 1017
->  yahoo.com
    internet address = 98.137.11.163
    ttl = 1017
->  yahoo.com
    internet address = 74.6.143.26
    ttl = 1017
->  yahoo.com
    internet address = 74.6.143.25
    ttl = 1017
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
```

5.whois

whois is a TCP-based query and response protocol that is commonly used to provide information services to Internet users. It returns information about the registered Domain Names, an IP address block, Name Servers and a much wider range of information services.



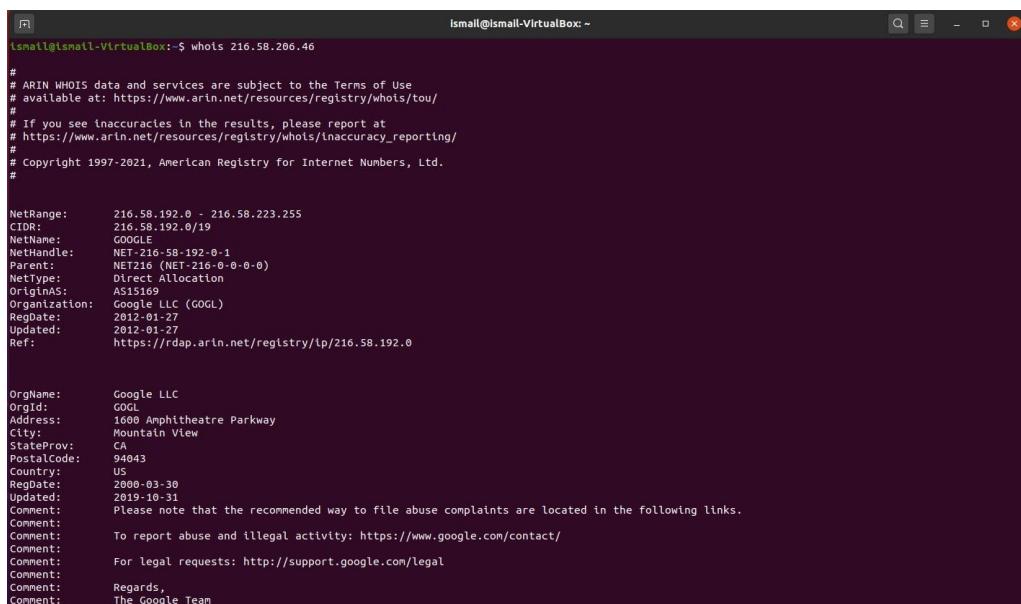
```
ismail@ismall-VirtualBox:~$ whois computerhope.com
Domain Name: COMPUTERHOPE.COM
Registry Domain ID: 1579775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: http://www.cloudflare.com
Updated Date: 2020-05-09T13:50:58Z
Creation Date: 1998-07-14T04:00:00Z
Registry Expiry Date: 2030-02-03T18:41:37Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ALEX.NS.CLOUDFLARE.COM
Name Server: DONNA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-01-21T16:13:10Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign.
```

Whois can be used to get the information about specific IP Address issue the command as shown in the below screenshot.



```
ismail@ismall-VirtualBox:~$ whois 216.58.206.46
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#

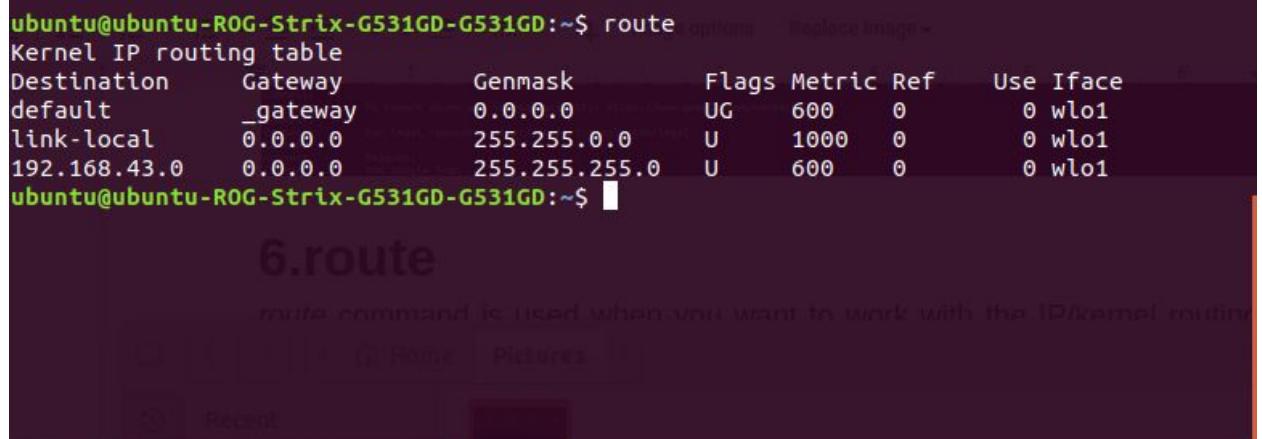
NetRange:      216.58.192.0 - 216.58.223.255
CIDR:          216.58.192.0/19
NetName:        GOOGLE
NetHandle:      NET-216-58-192-0-1
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS15169
Organization:   Google LLC (GOGL)
RegDate:        2012-01-27
Updated:        2012-01-27
Ref:            https://rdap.arin.net/registry/lp/216.58.192.0

OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2008-03-30
UpdateDate:    2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:        For legal requests: http://support.google.com/legal
Comment:        Regards,
Comment:        The Google Team
```

6.route

route command is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.

6.1 To display the IP/kernel routing table.



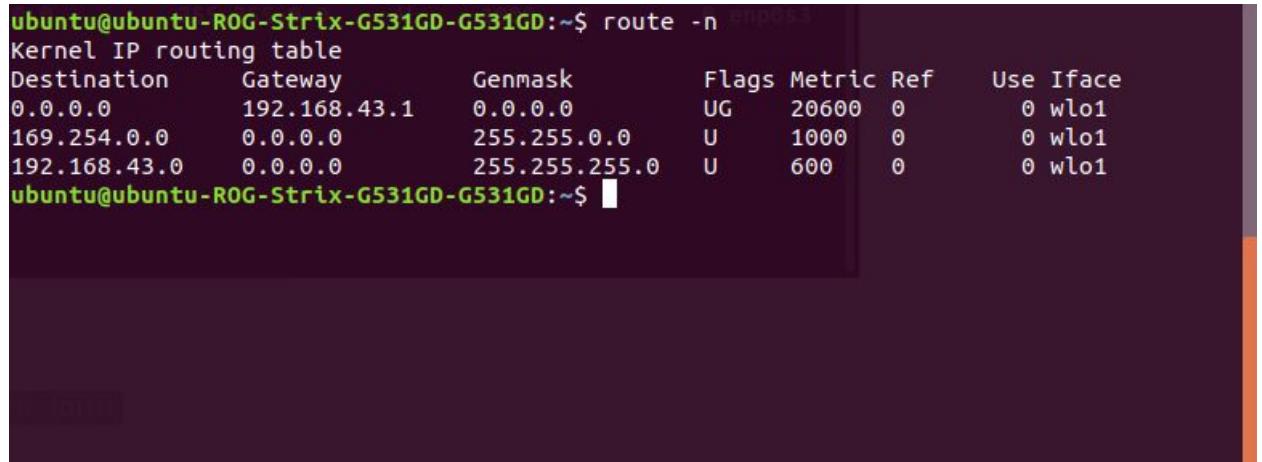
The screenshot shows a terminal window with the following content:

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         _gateway       0.0.0.0        UG    600    0        0 wlo1
link-local      0.0.0.0        255.255.0.0   U     1000   0        0 wlo1
192.168.43.0   0.0.0.0        255.255.255.0 U     600    0        0 wlo1
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

The terminal window has a dark background and light-colored text. The title bar says "6.route". Below the title bar, there is a status bar with the text "route command is used when you want to work with the IP/kernel routing table". The desktop environment visible behind the terminal window includes icons for Home, Pictures, and Recent.

It displays the routing table entries.

6.2 To display routing table in full numeric form



The screenshot shows a terminal window with the following content:

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.1  0.0.0.0        UG    20600  0        0 wlo1
169.254.0.0     0.0.0.0       255.255.0.0   U     1000   0        0 wlo1
192.168.43.0   0.0.0.0       255.255.255.0 U     600    0        0 wlo1
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

The terminal window has a dark background and light-colored text. The title bar says "6.route". Below the title bar, there is a status bar with the text "route command is used when you want to work with the IP/kernel routing table". The desktop environment visible behind the terminal window includes icons for Home, Pictures, and Recent.

It is even useful when you have to determine why the route to nameserver has even vanished.

6.3 To add a default gateway

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo route add default gw 169.254.0.0
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
default        169.254.0.0     0.0.0.0         UG    0      0        0 wlo1
default        _gateway        0.0.0.0         UG    20600   0        0 wlo1
link-local     0.0.0.0         255.255.0.0    U     1000   0        0 wlo1
192.168.43.0   0.0.0.0         255.255.255.0   U     600    0        0 wlo1
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

This assigns a gateway address on which all the packets that do not belong to the network are forwarded.

6.4 To get details of the kernel/IP routing table using ip command

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ip route
default via 192.168.43.1 dev wlo1 proto dhcp metric 20600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.43.0/24 dev wlo1 proto kernel scope link src 192.168.43.44 metric 600
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

This will give the details of the kernel/IP routing table and in this case, we have used IP command.

6.5 To get output related to IPv4

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ip -4 route
default via 192.168.43.1 dev wlo1 proto dhcp metric 20600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.43.0/24 dev wlo1 proto kernel scope link src 192.168.43.44 metric 600
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

This will only display the entries with ipv4.

6.6 To get output related to IPv6

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ip -6 route  
fe80::/64 dev wlo1 proto kernel metric 256 pref medium  
fe80::/64 dev wlo1 proto kernel metric 600 pref medium  
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ █
```

This will only display the entries with ipv6.

7.tcpdump

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well.

7.1 To capture the packets of current network interface

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes  
08:51:56.603055 IP ubuntu-ROG-Strix-G531GD-44810 > a184-29-25-201.deploy.static.akamaitechnologies.com  
.https: Flags [.], ack 2161489509, win 336, options [nop,nop,TS val 1631179307 ecr 2798866284], length 0  
08:51:56.603084 IP ubuntu-ROG-Strix-G531GD-G531GD.36346 > 216.52.2.48.https: Flags [S], seq 980087995, win 29  
200, options [mss 1460,sackOK,TS val 1511765110 ecr 0,nop,wscale 7], length 0  
08:51:56.603094 IP ubuntu-ROG-Strix-G531GD-G531GD.52578 > 69.173.159.50.https: Flags [S], seq 903862319, win  
29200, options [mss 1460,sackOK,TS val 2785019945 ecr 0,nop,wscale 7], length 0  
08:51:56.603582 IP ubuntu-ROG-Strix-G531GD-G531GD.57071 > _gateway.domain: 35302+ PTR? 201.25.29.184.in-addr.  
arpa. (44)  
08:51:56.677370 IP a184-29-25-201.deploy.static.akamaitechnologies.com.https > ubuntu-ROG-Strix-G531GD-G531GD  
.44810: Flags [.], ack 1, win 501, options [nop,nop,TS val 2798876524 ecr 1631148578], length 0  
08:51:56.918915 IP _gateway.domain > ubuntu-ROG-Strix-G531GD-G531GD.57071: 35302 1/0/0 PTR a184-29-25-201.dep  
loy.static.akamaitechnologies.com. (109)  
08:51:56.919515 IP ubuntu-ROG-Strix-G531GD-G531GD.60791 > _gateway.domain: 9773+ PTR? 44.43.168.192.in-addr.a  
rpa. (44)  
08:51:56.922292 IP ubuntu-ROG-Strix-G531GD-G531GD.34541 > _gateway.domain: 31148+ PTR? 48.2.52.216.in-addr.ar  
pa. (42)  
08:52:06.933505 IP ubuntu-ROG-Strix-G531GD-G531GD.56155 > _gateway.domain: 14939+ PTR? 50.159.173.69.in-addr.  
arpa. (44)  
08:52:08.058683 ARP, Request who-has ubuntu-ROG-Strix-G531GD-G531GD tell _gateway, length 28  
08:52:08.058697 ARP, Reply ubuntu-ROG-Strix-G531GD-G531GD is-at 04:ea:56:e2:6a:df (oui Unknown), length 28  
08:52:08.072597 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28  
08:52:08.092441 IP ubuntu-ROG-Strix-G531GD-G531GD.56778 > ec2-52-203-62-154.compute-1.amazonaws.com.https: Fl  
ags [P.], seq 1196253537:1196253583, ack 908478590, win 355, options [nop,nop,TS val 597821081 ecr 1919396274  
, length 46  
08:52:08.093048 IP ubuntu-ROG-Strix-G531GD-G531GD.35622 > _gateway.domain: 46575+ PTR? 154.62.203.52.in-addr.  
arpa. (44)  
08:52:08.379055 IP ubuntu-ROG-Strix-G531GD-G531GD.39978 > 74.118.186.210.https: Flags [.], ack 1354732310, wi  
n 35376, options [nop,nop,TS val 1193313883 ecr 759314221], length 0  
08:52:08.380760 IP ec2-52-203-62-154.compute-1.amazonaws.com.https > ubuntu-ROG-Strix-G531GD-G531GD.56778: Fl  
ags [P.], seq 1:47, ack 46, win 118, options [nop,nop,TS val 1919410854 ecr 597821081], length 46  
08:52:08.380772 IP ubuntu-ROG-Strix-G531GD-G531GD.56778 > ec2-52-203-62-154.compute-1.amazonaws.com.https: Fl  
ags [.], ack 47, win 355, options [nop,nop,TS val 597821369 ecr 1919410854], length 0  
08:52:08.635062 IP ubuntu-ROG-Strix-G531GD-G531GD.46870 > 117.18.237.29.http: Flags [.], ack 254144806, win 2  
41, options [nop,nop,TS val 10796868 ecr 773539944], length 0
```

This will capture the packets from the current interface of the network through which the system is connected to the internet. i.e., `wlo1`

7.2 To capture packets from a specific network interface

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
08:59:50.112043 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
08:59:53.275216 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
08:59:55.418443 IP ubuntu-ROG-Strix-G531GD-G531GD.55105 > alphyn.canonical.com.ntp: NTPv4, Client, length 48
08:59:55.418999 IP ubuntu-ROG-Strix-G531GD-G531GD.56443 > _gateway.domain: 32598+ PTR? 157.91.189.91.in-addr.
arpa. (44)
08:59:56.347078 IP ubuntu-ROG-Strix-G531GD-G531GD.34870 > 69.173.159.63.https: Flags [S], seq 1587827175, win
29200, options [mss 1460,sackOK,TS val 3645453875 ecr 0,nop,wscale 7], length 0
08:59:56.418478 IP ubuntu-ROG-Strix-G531GD-G531GD.56443 > _gateway.domain: 32598+ PTR? 157.91.189.91.in-addr.
arpa. (44)
08:59:56.501362 IP _gateway.domain > ubuntu-ROG-Strix-G531GD-G531GD.56443: 32598 1/0/0 PTR alphyn.canonical.c
om. (78)
08:59:56.502090 IP ubuntu-ROG-Strix-G531GD-G531GD.37544 > _gateway.domain: 4296+ PTR? 44.43.168.192.in-addr.a
rpa. (44)
08:59:56.505262 IP _gateway.domain > ubuntu-ROG-Strix-G531GD-G531GD.37544: 4296* 1/0/0 PTR ubuntu-ROG-Strix-G
531GD-G531GD. (88)
08:59:56.542091 IP ubuntu-ROG-Strix-G531GD-G531GD.42741 > _gateway.domain: 50209+ PTR? 63.159.173.69.in-addr.
arpa. (44)
08:59:56.550488 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
08:59:59.937974 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
09:00:01.071755 IP ubuntu-ROG-Strix-G531GD-G531GD.60406 > bom12s03-in-f10.1e100.net.https: Flags [P.], seq 41
17815717:4117815756, ack 2733820992, win 291, options [nop,nop,TS val 3892024829 ecr 711991561], length 39
09:00:01.071910 IP ubuntu-ROG-Strix-G531GD-G531GD.47786 > bom07s28-in-f10.1e100.net.https: Flags [P.], seq 36
36379402:3636379441, ack 1474789905, win 361, options [nop,nop,TS val 4060754702 ecr 3127810543], length 39
09:00:01.072454 IP ubuntu-ROG-Strix-G531GD-G531GD.39371 > _gateway.domain: 51299+ PTR? 234.174.217.172.in-add
r.arpa. (46)
09:00:01.072672 IP ubuntu-ROG-Strix-G531GD-G531GD.60406 > bom12s03-in-f10.1e100.net.https: Flags [FP.], seq 3
9:63, ack 1, win 291, options [nop,nop,TS val 3892024830 ecr 711991561], length 24
09:00:01.072922 IP ubuntu-ROG-Strix-G531GD-G531GD.47786 > bom07s28-in-f10.1e100.net.https: Flags [FP.], seq 3
9:63, ack 1, win 361, options [nop,nop,TS val 4060754703 ecr 3127810543], length 24
09:00:01.268583 IP bom07s28-in-f10.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.47786: Flags [.], ack 39,
win 351, options [nop,nop,TS val 3127863428 ecr 4060754702], length 0
09:00:01.268584 IP _gateway.domain > ubuntu-ROG-Strix-G531GD-G531GD.39371: 51299 1/0/0 PTR bom12s03-in-f10.1e
100.net. (85)
```

This command will now capture the packets from `wlo1` network interface.

7.3 Packet Analysing from a given source and destination IP

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump -i wlo1 src 14.139.185.121 and dst 192.168.43.44
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:19:09.170567 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [S.], seq 761673300,
ack 516282997, win 16060, options [mss 1360,nop,nop,sackOK,nop,wscale 1], length 0
09:19:09.427006 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], ack 330, win 80
30, length 0
09:19:13.114985 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 1361:4081,
ack 330, win 8030, length 2720: HTTP
09:19:13.115070 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 12241:13601
, ack 330, win 8030, length 1360: HTTP
09:19:13.115094 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 8161:9521,
ack 330, win 8030, length 1360: HTTP
09:19:13.115111 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 6801:8161,
ack 330, win 8030, length 1360: HTTP
09:19:13.115126 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 5441:6801,
ack 330, win 8030, length 1360: HTTP
09:19:13.115681 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 1:1361, ack
330, win 8030, length 1360: HTTP: HTTP/1.1 200 OK
09:19:13.115765 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 4081:5441,
ack 330, win 8030, length 1360: HTTP
09:19:13.115804 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 9521:12241,
ack 330, win 8030, length 2720: HTTP
09:19:13.251904 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 13601:14961
, ack 330, win 8030, length 1360: HTTP
09:19:13.252785 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 16321:17681
, ack 330, win 8030, length 1360: HTTP
09:19:13.253479 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 19041:20401
, ack 330, win 8030, length 1360: HTTP
09:19:13.253491 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 17681:19041
, ack 330, win 8030, length 1360: HTTP
09:19:13.253496 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 14961:16321
, ack 330, win 8030, length 1360: HTTP
09:19:13.259844 IP 14.139.185.121.http > ubuntu-ROG-Strix-G531GD-G531GD.50816: Flags [.], seq 23121:24481
```

Here the source IP is 14.139.185.121 which is the IP address of nitc server and source IP is 192.168.43.44 which is my system IP address. So whenever i access www.nitc.ac.in , all packets that i receive to my system from that particular server is displayed.

7.4 To save captured packets into a file

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump -w captured_packets.pcap -i wlo1
[sudo] password for ubuntu:
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C3354 packets captured
3354 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

This command will now output all the captures packets in a file named as captured_packets.pcap.

7.5 To read captured packets from a file

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump -r captured_packets.pcap
reading from file captured_packets.pcap, link-type EN10MB (Ethernet)
09:39:16.171937 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
09:39:17.179143 IP ubuntu-ROG-Strix-G531GD-G531GD.46150 > ec2-44-240-93-245.us-west-2.compute.amazonaws.com.h
    ttps: Flags [S], seq 2517212871, win 29200, options [mss 1460,sackOK,TS val 325880858 ecr 0,nop,wscale 7], le
    ngt 0
09:39:17.179177 IP ubuntu-ROG-Strix-G531GD-G531GD.47300 > a184-29-25-201.deploy.static.akamaitechnologies.com
    .https: Flags [.], ack 2178566681, win 353, options [nop,nop,TS val 1634019792 ecr 2801706761], length 0
09:39:17.252023 IP a184-29-25-201.deploy.static.akamaitechnologies.com.https > ubuntu-ROG-Strix-G531GD-G531GD
    .47300: Flags [.], ack 1, win 501, options [nop,nop,TS val 2801717021 ecr 1633968511], length 0
09:39:17.947109 IP ubuntu-ROG-Strix-G531GD-G531GD.36212 > bom07s31-in-f14.1e100.net.https: Flags [S], seq 352
    21923, win 29200, options [mss 1460,sackOK,TS val 3002498773 ecr 0,nop,wscale 7], length 0
09:39:17.950468 ARP, Request who-has ubuntu-ROG-Strix-G531GD-G531GD tell _gateway, length 28
09:39:17.950490 ARP, Reply ubuntu-ROG-Strix-G531GD-G531GD is-at 04:ea:56:e2:6a:df (oui Unknown), length 28
09:39:18.203077 IP ubuntu-ROG-Strix-G531GD-G531GD.36214 > bom07s31-in-f14.1e100.net.https: Flags [S], seq 196
    8082206, win 29200, options [mss 1460,sackOK,TS val 3002499030 ecr 0,nop,wscale 7], length 0
09:39:19.441126 ARP, Reply _gateway is-at e6:c4:83:bb:6d:65 (oui Unknown), length 28
09:39:19.668481 IP ubuntu-ROG-Strix-G531GD-G531GD.35787 > _gateway.domain: 15583+ AAAA? ib.sin1.geoadnxs.com.
    (38)
09:39:19.995097 IP ubuntu-ROG-Strix-G531GD-G531GD.60664 > bom05s12-in-f14.1e100.net.https: Flags [S], seq 274
    9277502, win 29200, options [mss 1460,sackOK,TS val 3279448490 ecr 0,nop,wscale 7], length 0
09:39:20.352581 IP ubuntu-ROG-Strix-G531GD-G531GD.57600 > bom12s08-in-f3.1e100.net.https: Flags [P.], seq 109
    6381787:1096381826, ack 2704220483, win 291, options [nop,nop,TS val 1934951443 ecr 980988573], length 39
09:39:20.439589 IP bom12s08-in-f3.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.57600: Flags [.], ack 39,
    win 271, options [nop,nop,TS val 981047104 ecr 1934951443], length 0
09:39:20.439617 IP bom12s08-in-f3.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.57600: Flags [P.], seq 1:4
    0, ack 39, win 271, options [nop,nop,TS val 981047104 ecr 1934951443], length 39
09:39:20.483151 IP ubuntu-ROG-Strix-G531GD-G531GD.57600 > bom12s08-in-f3.1e100.net.https: Flags [.], ack 40,
    win 291, options [nop,nop,TS val 1934951574 ecr 981047104], length 0
09:39:20.896032 IP ubuntu-ROG-Strix-G531GD-G531GD.43156 > maa05s13-in-f2.1e100.net.https: Flags [P.], seq 351
    2861950:3512861989, ack 761560252, win 355, options [nop,nop,TS val 3204624795 ecr 3703742951], length 39
09:39:20.896165 IP ubuntu-ROG-Strix-G531GD-G531GD.43154 > maa05s13-in-f2.1e100.net.https: Flags [P.], seq 117
    3797457:1173797496, ack 1866289901, win 352, options [nop,nop,TS val 3204624795 ecr 1518670058], length 39
09:39:20.896646 IP ubuntu-ROG-Strix-G531GD-G531GD.43154 > maa05s13-in-f2.1e100.net.https: Flags [FP.], seq 39
    :63, ack 1, win 352, options [nop,nop,TS val 3204624796 ecr 1518670058], length 24
09:39:20.896873 IP ubuntu-ROG-Strix-G531GD-G531GD.43156 > maa05s13-in-f2.1e100.net.https: Flags [FP.], seq 39
    :63, ack 1, win 355, options [nop,nop,TS val 3204624796 ecr 3703742951], length 24
```

This command will now read the captured packets from the captured_packets.pcap file.

7.6 To capture only TCP packets

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ sudo tcpdump -i wlo1 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:44:25.465270 IP ubuntu-ROG-Strix-G531GD-G531GD.40638 > maa05s12-in-f2.1e100.net.https: Flags [P.], seq 308
    5957581:3085957620, ack 1578784187, win 1444, options [nop,nop,TS val 1278619412 ecr 1188174331], length 39
09:44:25.539154 IP maa05s12-in-f2.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.40638: Flags [.], ack 39,
    win 698, options [nop,nop,TS val 1188233001 ecr 1278619412], length 0
09:44:25.539193 IP maa05s12-in-f2.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.40638: Flags [P.], seq 1:4
    0, ack 39, win 698, options [nop,nop,TS val 1188233001 ecr 1278619412], length 39
09:44:25.583119 IP ubuntu-ROG-Strix-G531GD-G531GD.40638 > maa05s12-in-f2.1e100.net.https: Flags [.], ack 40,
    win 1444, options [nop,nop,TS val 1278619529 ecr 1188233001], length 0
09:44:26.427694 IP ubuntu-ROG-Strix-G531GD-G531GD.48022 > a184-29-25-201.deploy.static.akamaitechnologies.com
    .https: Flags [.], ack 2166040396, win 254, options [nop,nop,TS val 1634329221 ecr 2802016211], length 0
09:44:26.427732 IP ubuntu-ROG-Strix-G531GD-G531GD.48022 > a184-29-25-201.deploy.static.akamaitechnologies.com
    .https: Flags [.], ack 2165942046, win 254, options [nop,nop,TS val 1634329221 ecr 2802016213], length 0
09:44:26.499786 IP a184-29-25-201.deploy.static.akamaitechnologies.com.https > ubuntu-ROG-Strix-G531GD-G531GD
    .48022: Flags [.], ack 1, win 501, options [nop,nop,TS val 2802026451 ecr 1634278355], length 0
09:44:26.512048 IP a184-29-25-201.deploy.static.akamaitechnologies.com.https > ubuntu-ROG-Strix-G531GD-G531GD
    .48022: Flags [.], ack 1, win 501, options [nop,nop,TS val 2802026463 ecr 1634278251], length 0
09:44:27.466236 IP ubuntu-ROG-Strix-G531GD-G531GD.47998 > bom07s15-in-f1.1e100.net.https: Flags [P.], seq 321
    0852524:3210852563, ack 3066962796, win 1444, options [nop,nop,TS val 3139690544 ecr 118439286], length 39
09:44:27.555181 IP bom07s15-in-f1.1e100.net.https > ubuntu-ROG-Strix-G531GD-G531GD.47998: Flags [P.], seq 1:4
    0, ack 39, win 287, options [nop,nop,TS val 118498326 ecr 3139690544], length 39
09:44:27.555227 IP ubuntu-ROG-Strix-G531GD-G531GD.47998 > bom07s15-in-f1.1e100.net.https: Flags [.], ack 40,
    win 1444, options [nop,nop,TS val 3139690632 ecr 118498326], length 0
^C
11 packets captured
11 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

7.6 To capture only TCP packets

This command will now capture only TCP packets from wlo1.

8. Netstat

Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp    0      0  ubuntu-ROG-Strix-:40638  maa05s12-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:50396  117.18.237.29:http   TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:51460  172.217.194.157:https ESTABLISHED
tcp    0      1  ubuntu-ROG-Strix-:44252  69.173.159.49:https SYN_SENT
tcp    0      0  ubuntu-ROG-Strix-:50158  server-54-182-0-1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:45550  205.180.87.210:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:56454  bom12s10-in-f3.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:51818  218.64.98.34.bc.g:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:48012  a184-29-25-201.de:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:60074  bom12s06-in-f14.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:44086  bom12s10-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:56560  103.231.98.193:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:51814  bom12s01-in-f14.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:42370  bom12s01-in-f10.1:https TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:45158  37.212.186.35.bc.:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:60102  bom07s26-in-f14.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:48022  a184-29-25-201.de:https ESTABLISHED
tcp    0      1  ubuntu-ROG-Strix-:53666  bom05s15-in-f1.1e:https SYN_SENT
tcp    0      0  ubuntu-ROG-Strix-:51370  ec2-34-214-241-12:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:53382  bom05s15-in-f1.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:49566  bom07s25-in-f10.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:40830  ip184.208.100.17.:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:50250  103.229.10.173:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:49878  maa05s01-in-f4.1e:https TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:36792  a104-94-18-218.dep:http  TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:37462  bom05s08-in-f3.1e:https TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:44270  69.173.159.49:https   TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:44784  bom07s16-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:40362  ec2-52-74-154-26.:https ESTABLISHED
```

8.1 Show both listening and non-listening sockets

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp    0      0  0.0.0.0:netbios-ssn       0.0.0.0:*
tcp    0      0  localhost:domain         0.0.0.0:*
tcp    0      0  0.0.0.0:ssh             0.0.0.0:*
tcp    0      0  localhost:ipp           0.0.0.0:*
tcp    0      0  0.0.0.0:microsoft-ds   0.0.0.0:*
tcp    0      0  ubuntu-ROG-Strix-:57254  a23-57-196-79.dep:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:54206  bom05s15-in-f1.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:50134  bom07s15-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:59064  bom12s08-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:51818  218.64.98.34.bc.g:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:49118  a184-29-25-201.de:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:52784  bom12s01-in-f14.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:60074  bom12s06-in-f14.1:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:56194  bom07s30-in-f3.1e1:http  TIME_WAIT
tcp    0      0  ubuntu-ROG-Strix-:35376  159.127.41.210:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:44514  ads.us.e-planning:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:43234  bom07s20-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:51370  ec2-34-214-241-12:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:48352  mil04s43-in-f3.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:53340  216.52.2.39:https   ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:58464  103.231.98.193:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:44784  bom07s16-in-f2.1e:https ESTABLISHED
tcp    0      1  ubuntu-ROG-Strix-:57252  a23-57-196-79.dep:https SYN_SENT
tcp    0      0  ubuntu-ROG-Strix-:43264  bom07s20-in-f2.1e:https ESTABLISHED
tcp    0      0  ubuntu-ROG-Strix-:52786  bom12s01-in-f14.1:https ESTABLISHED
```

8.2 List all tcp ports

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 0.0.0.0:netbios-ssn       0.0.0.0:*
tcp     0      0 localhost:domain         0.0.0.0:*
tcp     0      0 0.0.0.0:ssh             0.0.0.0:*
tcp     0      0 localhost:ipp           0.0.0.0:*
tcp     0      0 0.0.0.0:microsoft-ds    0.0.0.0:*
tcp     0      0 ubuntu-ROG-Strix-:50134  bom07s15-in-f2.1e:https TIME_WAIT
tcp     0      0 ubuntu-ROG-Strix-:59064  bom12s08-in-f2.1e:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:51818  218.64.98.34.bc.g:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:52784  bom12s01-in-f14.1:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:60074  bom12s06-in-f14.1:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:35376  159.127.41.210:https TIME_WAIT
tcp     0      0 ubuntu-ROG-Strix-:43234  bom07s20-in-f2.1e:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:51370  ec2-34-214-241-12:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:48352  mil04s43-in-f3.1e:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:44784  bom07s16-in-f2.1e:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:52786  bom12s01-in-f14.1:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:59230  kul01s09-in-f74.1:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:59226  kul01s09-in-f74.1:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:52278  172.217.194.157:https TIME_WAIT
tcp     0      0 ubuntu-ROG-Strix-:59050  bom12s08-in-f2.1e:https ESTABLISHED
tcp     0      0 ubuntu-ROG-Strix-:53636  bom07s25-in-f2.1e:https ESTABLISHED

```

8.3 List only listening ports

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 0.0.0.0:netbios-ssn       0.0.0.0:*
tcp     0      0 localhost:domain         0.0.0.0:*
tcp     0      0 0.0.0.0:ssh             0.0.0.0:*
tcp     0      0 localhost:ipp           0.0.0.0:*
tcp     0      0 0.0.0.0:microsoft-ds    0.0.0.0:*
tcp6    0      0 [::]:netbios-ssn        [::]:*
tcp6    0      0 [::]:1716              [::]:*
tcp6    0      0 [::]:ssh               [::]:*
tcp6    0      0 ip6-localhost:ipp      [::]:*
tcp6    0      0 [::]:microsoft-ds      [::]:*
udp     0      0 0.0.0.0:51862         0.0.0.0:*
udp     0      0 localhost:domain       0.0.0.0:*
udp     0      0 0.0.0.0:bootpc        0.0.0.0:*
udp     0      0 0.0.0.0:ipp          0.0.0.0:*
udp     0      0 0.0.0.0:mdns          0.0.0.0:*
udp6   0      0 [::]:34896            [::]:*
udp6   0      0 [::]:mdns             [::]:*
udp6   0      0 [::]:1716             [::]:*
raw6   0      0 [::]:ipv6-icmp        [::]:*          7

Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type      State      I-Node  Path
unix  2      [ ACC ]     STREAM    LISTENING  26521   @/tmp/.ICE-unix/1286
unix  2      [ ACC ]     SEQPACKET  LISTENING  1401    /run/udev/control
unix  2      [ ACC ]     STREAM    LISTENING  22020   /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING  22024   /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM    LISTENING  22025   /run/user/1000/gnupg/S.dirmgr
unix  2      [ ACC ]     STREAM    LISTENING  22026   /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING  22027   /run/user/1000/bus
unix  2      [ ACC ]     STREAM    LISTENING  22028   /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM    LISTENING  22029   /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM    LISTENING  21784   @irqbalance854.sock
unix  2      [ ACC ]     STREAM    LISTENING  38756   /run/NetworkManager/private-dhcp
unix  2      [ ACC ]     STREAM    LISTENING  21944   @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM    LISTENING  19139   /run/uuidd/request
```

8.4 List all udp ports

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 0.0.0.0:51862           0.0.0.0:*
udp      0      0 localhost:domain        0.0.0.0:*
udp      0      0 0.0.0.0:bootpc         0.0.0.0:*
udp      0      0 0.0.0.0:ipp            0.0.0.0:*
udp      0      0 0.0.0.0:mdns           0.0.0.0:*
udp      0      0 ubuntu-ROG-Strix-:38215 _gateway:domain
udp6     0      0 [::]:34896             [::]:*
udp6     0      0 [::]:mdns              [::]:*
udp6     0      0 [::]:1716              [::]:*                                         Types of Transmission Media
                                         TCP Server-Client implementa
                                         RSA Algorithm in Cryptograph
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

8.5 List the statistics for all ports

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -s
Ip:
Forwarding: 2
141154 total packets received
3 with invalid addresses
0 forwarded
0 incoming packets discarded
141149 incoming packets delivered
142888 requests sent out
9 dropped because of missing route
Icmp:
277 ICMP messages received
0 input ICMP message failed
ICMP input histogram:
destination unreachable: 277
369 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
destination unreachable: 352
echo requests: 17
IcmpMsg:
InType3: 277
OutType3: 352
OutType8: 17
Tcp:
2931 active connection openings
0 passive connection openings
5 failed connection attempts
17 connection resets received
23 connections established
117691 segments received
116596 segments sent out
5991 segments retransmitted
33 bad segments received
1487 resets sent
```

CoolGeeks

NOT
AN AD.

Just to remind you
that the placements
are nearby.



Start Preparing

8.6 Display PID and program names in the output

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -pt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 ubuntu-ROG-Strix-:58566  103.231.98.193:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:41260  bom05s11-in-f2.1e:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:51818  218.64.98.34.bc.g:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:47226  bom07s16-in-f2.1e:https TIME_WAIT -
tcp      0      0 ubuntu-ROG-Strix-:52784  bom12s01-in-f14.1:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:60074  bom12s06-in-f14.1:https ESTABLISHED 2339/firefox
tcp      0      1 ubuntu-ROG-Strix-:51884  a104-96-204-135.d:https SYN_SENT    2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:43234  bom07s20-in-f2.1e:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:51370  ec2-34-214-241-12:https ESTABLISHED 2339/firefox
tcp      0      0 ubuntu-ROG-Strix-:51264  maa05s01-in-f4.1e:https ESTABLISHED 2339/firefox
^C
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

8.7 The kernel routing information

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -r -t -n -x
Kernel IP routing table
Destination      Gateway        Genmask        Flags   MSS Window irtt Iface
default         _gateway       0.0.0.0        UG        0 0          0 wlo1
link-local      0.0.0.0        255.255.0.0    U         0 0          0 wlo1
192.168.43.0   0.0.0.0        255.255.255.0  U         0 0          0 wlo1
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

8.8 Which process is using a particular port

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -an | grep ':443'
tcp        0      0 192.168.43.44:52000   104.96.204.135:443      ESTABLISHED
tcp        0      0 192.168.43.44:51818   34.98.64.218:443      ESTABLISHED
tcp        0      1 192.168.43.44:45340   142.250.76.194:443     SYN_SENT
tcp        0      0 192.168.43.44:52784   172.217.167.174:443     ESTABLISHED
tcp        0      0 192.168.43.44:60074   142.250.67.142:443     ESTABLISHED
tcp        0      0 192.168.43.44:49720   216.52.2.19:443      ESTABLISHED
tcp        0      0 192.168.43.44:51370   34.214.241.122:443     ESTABLISHED
tcp        0     39 192.168.43.44:44784   172.217.160.194:443     ESTABLISHED
tcp        0      0 192.168.43.44:52786   172.217.167.174:443     ESTABLISHED
tcp        0      0 192.168.43.44:59230   216.58.196.74:443      ESTABLISHED
tcp        0      0 192.168.43.44:59226   216.58.196.74:443      ESTABLISHED
tcp        0      0 192.168.43.44:46520   103.43.90.19:443      ESTABLISHED
tcp        0      0 192.168.43.44:56774   172.217.166.34:443      ESTABLISHED
tcp        0      0 192.168.43.44:56778   172.217.166.34:443      ESTABLISHED
tcp        0      1 192.168.43.44:46528   103.43.90.19:443      SYN_SENT
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

8.9 List of network interfaces

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ netstat -i
Kernel Interface table
Iface      MTU   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno2      1500      0      0      0 0          0      0      0 0      BMU
lo       65536  21592      0      0 0          21592      0      0 0      LRU
wlo1      1500 137741      0      0 0          131145      0      0 0      BMRU
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

9.dstat

dstat is a tool that is used to retrieve information or statistics from components of the system such as network connections, IO devices, or CPU, etc. It is generally used by system administrators to retrieve a handful of information about the above-mentioned components of the system. By using this tool one can even see the throughput for block devices that make up a single filesystem or storage system.

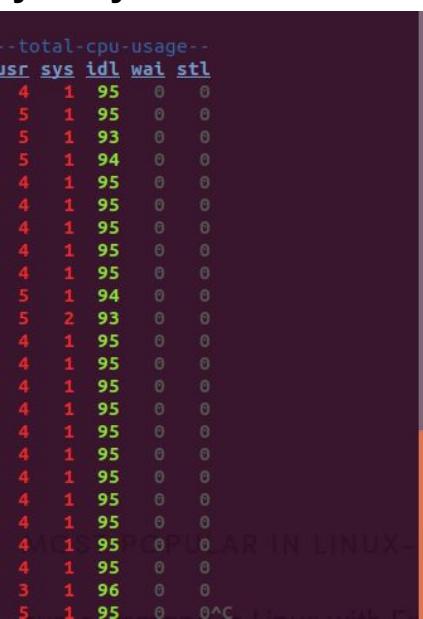
9.1 To display statistics of major OS components



dstat													
You did not select any stats, using -cdngy by default.													
--total-cpu-usage--			-dsk/total-		-net/total-		---paging---		---system---				
usr	sys	idl	wai	stl	read	writ	recv	send	in	out	int	csw	
4	1	95	0	0	198k	137k	0	0	0	0	971	4153	
4	2	93	0	0	0	240k	1568	2788	0	0	675	3291	
4	1	95	0	0	0	80k	6418	6708	0	0	588	2818	
5	1	94	0	0	0	0	42B	2048	0	0	572	2821	
5	1	94	0	0	0	0	474B	959B	0	0	887	3206	
5	1	94	0	0	0	0	384B	400B	0	0	838	3536	
4	1	95	0	0	0	0	0	1028	0	0	575	2879	
4	1	94	0	0	0	400k	318B	518B	0	0	520	2876	
5	1	94	0	0	0	72k	1035B	3919B	0	0	553	3107	
5	1	94	0	0	0	0	0	2028	0	0	608	2984	
5	1	94	0	0	0	212k	108B	0	0	0	639	2957	
5	1	94	0	0	0	52k	42B	70B	0	0	626	3081	
5	1	94	0	0	0	0	0	0	0	0	538	2903	
5	1	94	0	0	0	12k	42B	2048	0	0	690	3125	
5	1	94	0	0	0	0	0	210B	0	0	713	3167	
4	1	95	0	0	0	0	66B	94B	0	0	501	2867	^C

This command will display CPU, Disk, Network, Paging and System stats.

9.2 To display information that was to be displayed by vmstat tool



dstat																	
You did not select any stats, using -cdngy by default.																	
--procs--			-memory-usage--		-dsk/total-		---paging---		---system---								
run	blk	new	used	free	buff	cach	in	out	read	writ	int	csw	usr	sys	idl	wai	stl
2.0	0	5.1	2241M	3617M	249M	1858M	0	0	195k	136k	971	4159	4	1	95	0	0
0	0	0	2241M	3616M	249M	1858M	0	0	0	0	688	3009	5	1	95	0	0
1.0	0	0	2242M	3616M	249M	1858M	0	0	0	0	755	3239	5	1	93	0	0
0	0	0	2237M	3621M	249M	1858M	0	0	0	0	1085	3437	5	1	94	0	0
0	0	0	2237M	3621M	249M	1858M	0	0	0	0	523	2777	4	1	95	0	0
0	0	0	2237M	3621M	249M	1858M	0	0	0	24k	502	2859	4	1	95	0	0
0	0	0	2237M	3620M	249M	1858M	0	0	0	0	539	2691	4	1	95	0	0
1.0	0	0	2238M	3620M	249M	1858M	0	0	0	0	517	2792	4	1	95	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	0	484	2809	4	1	95	0	0
0	0	0	2237M	3620M	249M	1858M	0	0	0	12k	678	2888	5	1	94	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	0	1175	3827	5	2	93	0	0
2.0	0	0	2238M	3620M	249M	1858M	0	0	0	0	479	2750	4	1	95	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	0	476	2711	4	1	95	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	0	511	2815	4	1	95	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	76k	485	2820	4	1	95	0	0
0	0	0	2238M	3619M	249M	1858M	0	0	0	0	494	2856	4	1	95	0	0
0	0	0	2238M	3620M	249M	1858M	0	0	0	0	665	2794	4	1	95	0	0
1.0	0	0	2239M	3619M	249M	1858M	0	0	0	0	551	2804	4	1	95	0	0
0	0	0	2239M	3619M	249M	1858M	0	0	0	0	487	2772	4	1	95	0	0
0	0	0	2239M	3619M	249M	1858M	0	0	0	68k	505	2770	4	1	95	0	0
0	0	0	2240M	3618M	249M	1858M	0	0	0	0	500	2688	4	1	95	0	0
0	0	0	2240M	3618M	249M	1858M	0	0	0	0	490	2759	4	1	95	0	0
1.0	0	0	2240M	3617M	249M	1858M	0	0	0	0	484	2697	3	1	96	0	0
0	0	0	2242M	3616M	249M	1858M	0	0	0	0	544	2826	5	1	95	0	^C

The above command results in the process and memory stats.

9.3 To display stats of process using most of the CPU

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ dstat -c --top-cpu
--total-cpu-usage-- -most-expensive-
usr sys idl wai stl | _cpu_process_
 4 1 95 0 0 |MainThread 1.7
 0 0 100 0 0 |kworker/3:0 0.1
 0 0 99 0 0 |gnome-terminal 0.1
 2 1 98 0 0 |MainThread 0.9
 4 1 94 0 0 |MainThread 2.9
 8 2 90 0 0 |MainThread 4.2
 3 1 96 0 0 |MainThread 3.0
 7 2 91 0 0 |MainThread 4.8
 6 1 93 0 0 |MainThread 3.2
 4 1 94 0 0 |Xorg 2.4
 1 0 98 0 0 |Xorg 0.6
 0 0 99 0 0 |Xorg 0.2
 1 0 99 0 0 |We 0.2 Screenshot Screenshot Screenshot Screenshot Screenshot
 1 0 99 0 0 |MainThread 0.2 From 2021-01-22 22:00:00 From 2021-01-22 22:00:00 From 2021-01-22 22:00:00 From 2021-01-22 22:00:00 From 2021-01-22 22:00:00
 1 0 99 0 0 |gnome-terminal 0.2
 2 1 98 0 0 |We 1.6
 0 0 99 0 0 |gnome-flashback 0.1
 0 0 100 0 0 |We 0.1
 0 0 100 0 0 |gnome-terminal 0.1^C
```

This will display the stats of the process which is consuming most of the CPU.

9.4 To display stats of process using most of the memory

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ dstat -d --top-mem
-dsk/total- -most-expensive-
read writ | _memory_process_
190k 133k |We 12.0T
 0 100k |We 12.0T
 0 0 |We 12.0T
 0 708k |We 12.0T
 0 0 |We 12.0T
 0 176k |We 12.0T
 0 0 |We 12.0T
 0 416k |We 12.0T In the process and memory stats.
 0 0 |We 12.0T
 0 0 |We 12.0T
 0 176k |We 12.0T
 0 0 |We 12.0T
 0 0 |We 12.0T
 0 28k |We 12.0T
 0 56k |We 12.0T
 0 52k |We 12.0T^C
```

This will display the stats of the process which is consuming most of the memory.

9.5 To display the list of all plugins

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ dstat --list
internal:
    aio, cpu, cpu-adv, cpu-use, cpu24, disk, disk24, disk24-old, epoch, fs, int, int24, io, ipc, load,
    lock, mem, mem-adv, net, page, page24, proc, raw, socket, swap, swap-old, sys, tcp, time, udp,
    unix, vm, vm-adv, zones
/usr/share/dstat:
    battery, battery-remain, condor-queue, cpufreq, dbus, disk-avgqu, disk-avgrq, disk-svctm, disk-tps,
    disk-util, disk-wait, dstat, dstat-cpu, dstat-ctxt, dstat-mem, fan, freespace, fuse, gpfs,
    gpfs-ops, helloworld, innodb-buffer, innodb-io, innodb-ops, lustre, md-status, memcache-hits,
    mysql-io, mysql-keys, mysql5-cmds, mysql5-conn, mysql5-innodb, mysql5-innodb-basic,
    mysql5-innodb-extra, mysql5-io, mysql5-keys, net-packets, nfs3, nfs3-ops, nfsd3, nfsd3-ops,
    nfsd4-ops, nfsstat4, ntp, postfix, power, proc-count, qmail, redis, rpc, rcpd, sendmail, snmp-cpu,
    snmp-load, snmp-mem, snmp-net, snmp-net-err, snmp-sys, snooze, squid, test, thermal, top-bio,
    top-bio-adv, top-childwait, top-cpu, top-cpu-adv, top-cputime, top-cputime-avg, top-int, top-io,
    top-io-adv, top-latency, top-latency-avg, top-mem, top-oom, utmp, vm-cpu, vm-mem, vm-mem-adv,
    vmk-hba, vmk-int, vmk-nic, vz-cpu, vz-io, vz-ubc, wifi, zfs-arc, zfs-l2arc, zfs-ziling online ?
```

9.6 To get all stats of the processes

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ dstat -a
--total-cpu-usage-- -disk-total- -net-total- ---paging-- ---system--
usr sys idl wai stl| read writ| recv send| in out| int csw
 4  1 95  0  0 | 184k 133k|   0   0 |   0   0 | 969 4177
 1  1 98  0  0 |     0   0 | 408B 10C|   0   0 | 318 1413
 2  1 98  0  0 |     0   0 | 1306B 227B|   0   0 | 353 1495
 2  0 98  0  0 |     0   0 | 56k 42B|   0   0 | 335 1310
 2  1 97  0  0 |     0   0 | 330B 451B|   0   0 | 767 1883
 1  0 98  0  0 |     0   0 |     0   0 |   0   0 | 276 1469
 2  1 98  0  0 |     0   0 | 656k 487B| 465B|   0   0 | 308 1244
 2  0 97  0  0 |     0   0 |     0   0 |   0   0 | 317 1421
 2  0 98  0  0 |     0   0 |     0   0 |   0   0 | 256 1587
 2  0 98  0  0 |     0   0 |     0   0 | 42B   0 |   0   0 | 232 1195
 2  0 98  0  0 |     0   0 |     0   0 | 108B 164B|   0   0 | 225 1133
 4  1 95  0  0 |     0   0 |     0   0 |     0   0 |   0   0 | 1206 1989
 2  0 98  0  0 |     0   0 | 4096B 337B| 419B|   0   0 | 267 1392
 2  1 98  0  0 |     0   0 |     0   0 | 42B   0 |   0   0 | 305 1407
 2  1 98  0  0 |     0   0 |     0   0 | 74B 807B|   0   0 | 293 1182
 2  1 98  0  0 |     0   0 |     0   0 | 4442B 506B|   0   0 | 326 1358
 2  0 98  0  0 |     0   0 |     0   0 | 1956B 812B|   0   0 | 323 1319
 2  1 98  0  0 |     0   0 | 272k   0 |   0   0 |   0   0 | 307 1399 ^C
```

10.ifstat

ifstat neatly prints out network interface statistics. The utility keeps records of the previous data displayed in history files and by default only shows difference between the last and the current call.

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ifstat
      eno2          wlo1
KB/s in KB/s out KB/s in KB/s out
  0.00    0.00    0.00    0.00
  0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    0.12    0.09
  0.00    0.00    0.00    0.00
  0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    0.08    0.07
  0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    69.38   6.97
  0.00    0.00    0.06    0.18
  0.00    0.00    7.37    0.90
  0.00    0.00    0.00    0.00
  0.00    0.00    0.35    0.27
  0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00
  0.00    0.04    0.00    0.00
```

10.1 ignoring history file

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ifstat -a
      lo          eno2          wlo1
KB/s in KB/s out KB/s in KB/s out KB/s in KB/s out
  0.00    0.00    0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00    0.00    0.00
  0.00    0.00    0.00    0.00    0.04    0.00
  0.00    0.00    0.00    0.00    0.18    0.28
  0.00    0.00    0.00    0.00    0.13    0.09
```

10.2 Report average over the last seconds

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ifstat -t
Time          eno2          wlo1
HH:MM:SS  KB/s in KB/s out KB/s in KB/s out
11:29:08    0.00    0.00    0.06    0.18
11:29:09    0.00    0.00    0.17    0.09
11:29:10    0.00    0.00    0.06    0.09
11:29:11    0.00    0.00    0.13    0.18
11:29:12    0.00    0.00    0.11    0.09
11:29:13    0.00    0.00    0.39    0.63
11:29:14    0.00    0.00    0.05    0.00
11:29:15    0.00    0.00    0.00    0.00
11:29:16    0.00    0.00    0.14    0.22
11:29:17    0.00    0.00    0.10    0.22
11:29:18    0.00    0.00    0.06    0.09
11:29:19    0.00    0.00    0.27    0.40
11:29:20    0.00    0.00    0.00    0.00
11:29:21    0.00    0.00    0.19    0.28
11:29:22    0.00    0.00    0.15    0.16
11:29:23    0.00    0.00    0.13    0.18
11:29:24    0.00    0.00    0.12    0.26
```

10.3 Show entries with zero activity

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ifstat -z
      wlo1
KB/s in  KB/s out
  0.34    0.21
  0.04    0.32
  0.00    0.10
  0.20    0.41
  6.52    6.52
  1.59    0.62
  0.05    0.28
  3.40   13.05
  1.98    4.97
  0.00    0.00
  4.22   15.38
  0.52    0.51
  0.00    0.10
  3.29   17.69
  0.11    0.00
  0.30    0.47
  2.37   63.86
  3.53    0.72
```

10.4 show ifstat for a particular interface only

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ ifstat -i wlo1
      wlo1
KB/s in  KB/s out
  0.00    0.00
  2.31    3.98
  2.45    5.45
  2.12   18.69
  1.15    0.60
  0.04    0.09
  0.18    0.09
  0.06    0.13
  0.04    0.00
  0.00    0.10
  1.16   15.00
  2.81    2.09
  7.48   11.00
  4.07    3.74
 13.66   31.10
 10.61    9.90
  6.05    3.96
  2.90   41.29
  4.31    3.76
  8.02    8.67
 11.64   54.37
 16.53   12.90
 11.78   12.01
 10.75   84.58
 10.26   19.33
  8.30    6.37
  3.65   37.44
  1.26    0.50
  0.00    0.21
 13.89   35.26
  2.12    0.51
  0.04    0.00
```

11.wget

Wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.

11.1 Downloading a file

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~/Desktop$ wget https://github.com/mohammedismailb18/Hostel-Management-System/blob/main/Documentation/DDD.pdf
--2021-01-23 16:28:48--  https://github.com/mohammedismailb18/Hostel-Management-System/blob/main/Documentation/DDD.pdf
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... failed: Connection timed out.
Retrying.

--2021-01-23 16:30:59-- (try: 2)  https://github.com/mohammedismailb18/Hostel-Management-System/blob/main/Documentation/DDD.pdf
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'DDD.pdf'

DDD.pdf                                [ =>                               ]  93.40K   447KB/s    in 0.2s

2021-01-23 16:30:59 (447 KB/s) - 'DDD.pdf' saved [95638]

ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~/Desktop$
```

I have downloaded a document from my github page as shown above using wget command.

11.2 turn off output

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ wget -q http://www.bbc.co.uk
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

11.3 turn off verbose output

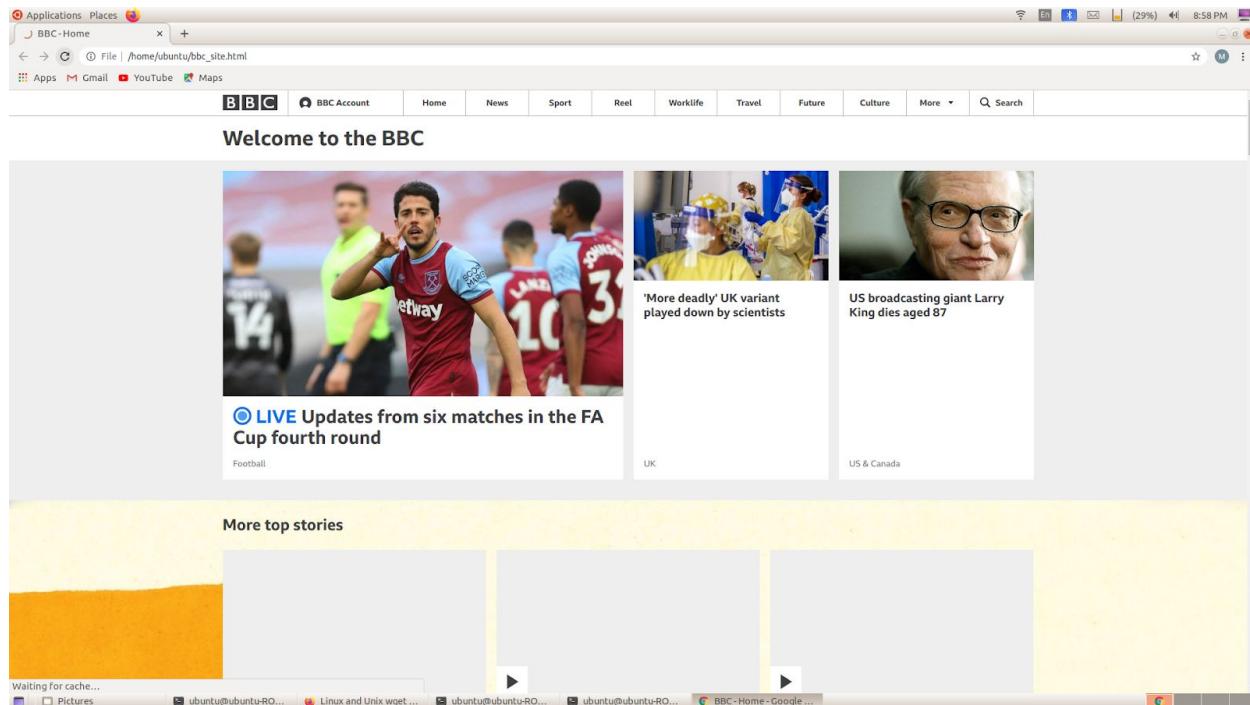
```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ wget -nv http://www.bbc.co.uk
failed: Connection timed out.
2021-01-23 20:48:51 URL:https://www.bbc.co.uk/ [342003/342003] -> "index.html" [1]
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$
```

11.4 download a file with different file name

```
ubuntu@ubuntu-ROG-Strix-G531GD-G531GD:~$ wget http://www.bbc.co.uk -O bbc_site
--2021-01-23 20:46:16--  http://www.bbc.co.uk/
Resolving www.bbc.co.uk (www.bbc.co.uk)... 212.58.237.254, 212.58.233.254
Connecting to www.bbc.co.uk (www.bbc.co.uk)|212.58.237.254|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.bbc.co.uk/ [following]
--2021-01-23 20:46:24--  https://www.bbc.co.uk/
Connecting to www.bbc.co.uk (www.bbc.co.uk)|212.58.237.254|:443... failed: Connection timed out.
Connecting to www.bbc.co.uk (www.bbc.co.uk)|212.58.233.254|:443... failed: Connection timed out.
Resolving www.bbc.co.uk (www.bbc.co.uk)... 212.58.237.253, 212.58.233.253
Connecting to www.bbc.co.uk (www.bbc.co.uk)|212.58.237.253|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 342003 (334K) [text/html]
Saving to: 'bbc_site'

bbc_site          100%[=====] 333.99K 73.8KB/s   in 4.5s

2021-01-23 20:50:52 (73.8 KB/s) - 'bbc_site' saved [342003/342003]
```



This is the downloaded `bbc_site.html` file.

11.5 download multiple file

```
ismail@ismail-VirtualBox:~$ wget http://ftp.gnu.org/gnu/wget/wget-1.5.3.tar.gz ftp://ftp.gnu.org/gnu/wget/wget-1.10.1.tar.gz.sig
--2021-01-23 21:44:25-- http://ftp.gnu.org/gnu/wget/wget-1.5.3.tar.gz
Resolving ftp.gnu.org (ftp.gnu.org)... 209.51.188.20, 2001:470:142:3::b
Connecting to ftp.gnu.org (ftp.gnu.org)|209.51.188.20|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 446966 (436K) [application/x-gzip]
Saving to: 'wget-1.5.3.tar.gz'

wget-1.5.3.tar.gz    100%[=====] 436.49K 37.1KB/s   in 10s

2021-01-23 21:44:41 (41.7 KB/s) - 'wget-1.5.3.tar.gz' saved [446966/446966]

--2021-01-23 21:44:41-- ftp://ftp.gnu.org/gnu/wget/wget-1.10.1.tar.gz.sig
      => 'wget-1.10.1.tar.gz.sig'
Connecting to ftp.gnu.org (ftp.gnu.org)|209.51.188.20|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done. ==> PWD ... done.
==> TYPE I ... done. ==> CWD (1) /gnu/wget ... done.
==> SIZE wget-1.10.1.tar.gz.sig ... 65
==> PASV ... done. ==> RETR wget-1.10.1.tar.gz.sig ... done.
Length: 65 (unauthoritative)

wget-1.10.1.tar.gz. 100%[=====]       65  ---KB/s   in 0s

2021-01-23 21:47:02 (13.4 MB/s) - 'wget-1.10.1.tar.gz.sig' saved [65]

FINISHED --2021-01-23 21:47:02--
Total wall clock time: 2m 37s
Downloaded: 2 files, 437K in 10s (41.7 KB/s)
ismail@ismail-VirtualBox:~$
```

11.6 Read url from a file and download multiple files

Here I have given two links in url_file.txt. i.e.,

<https://en.wikipedia.org/wiki/Wikipedia> and <http://www.google.com>.

```
ismail@ismail-VirtualBox:~$ wget -i url_file.txt
--2021-01-23 21:54:51-- https://en.wikipedia.org/wiki/Wikipedia
Resolving en.wikipedia.org (en.wikipedia.org)... 103.102.166.224, 2001:df2:e500:ed1a::1
Connecting to en.wikipedia.org (en.wikipedia.org)|103.102.166.224|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 941998 (920K) [text/html]
Saving to: 'Wikipedia'

Wikipedia          100%[=====] 919.92K 56.4KB/s   in 16s

2021-01-23 21:56:12 (57.7 KB/s) - 'Wikipedia' saved [941998/941998]

--2021-01-23 21:56:12-- http://www.google.com/
Resolving www.google.com (www.google.com)... 216.58.199.164, 2404:6800:4009:807::2004
Connecting to www.google.com (www.google.com)|216.58.199.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.2'

index.html.2          [ <=> ] 14.83K  ---KB/s   in 0.07s

2021-01-23 21:56:44 (202 KB/s) - 'index.html.2' saved [15186]

FINISHED --2021-01-23 21:56:44--
Total wall clock time: 1m 53s
Downloaded: 2 files, 935K in 16s (58.3 KB/s)
```

11.7 Downloading file in background

```
ismail@ismail-VirtualBox:~$ wget -b www.google.com
Continuing in background, pid 5277.
Output will be written to 'wget-log'.
ismail@ismail-VirtualBox:~$
```