Tanvir Ahmed

IT-18043

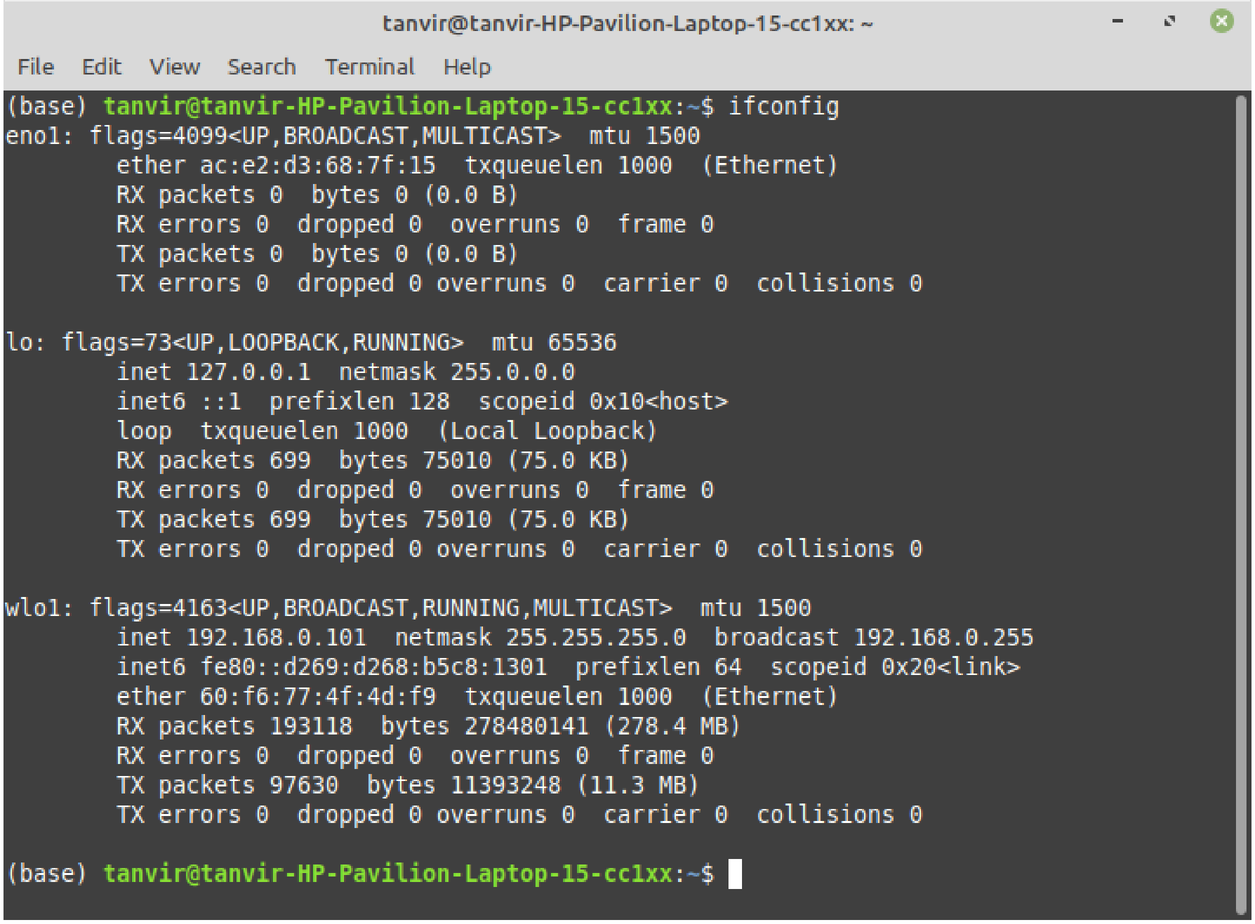
Linux Network Tools

There are some common linux networking tools given bellow :

ifconfig

The command ifconfig stands for interface configurator. This command enables us to initialize an interface, assign IP address, enable or disable an interface. It display route and network interface.

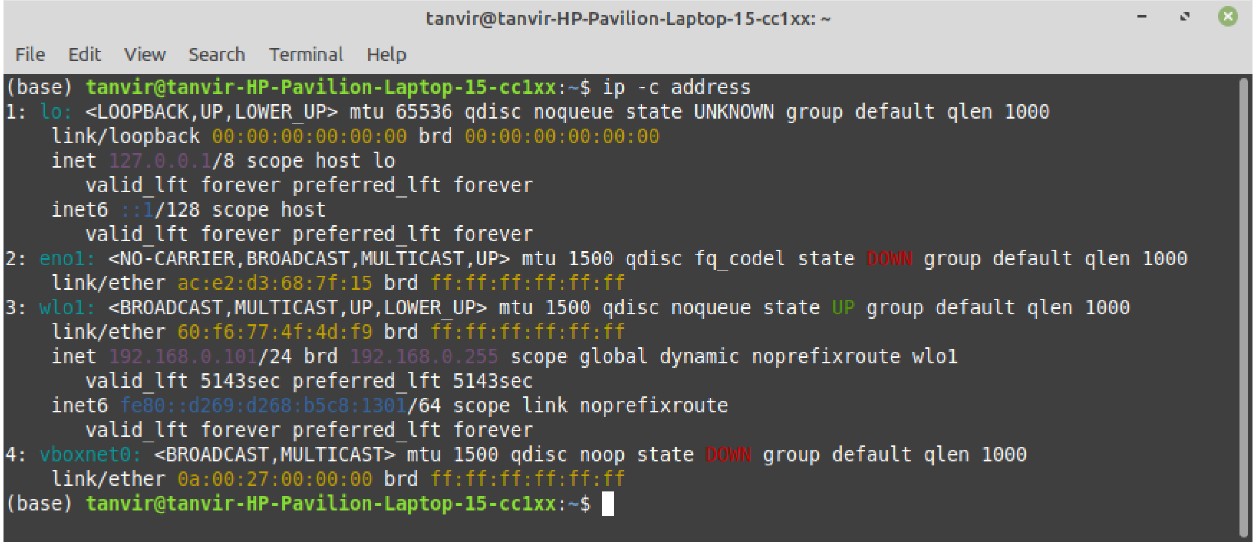
A newer version of ifconfig is ip command. ifconfig command works for all the versions.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:e2:d3:68:7f:15  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 699  bytes 75010 (75.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 699  bytes 75010 (75.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.101  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::d269:d268:b5c8:1301  prefixlen 64  scopeid 0x20<link>
        ether 60:f6:77:4f:4d:f9  txqueuelen 1000  (Ethernet)
        RX packets 193118  bytes 278480141 (278.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 97630  bytes 11393248 (11.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

IP

Linux IP command is the newer version of the ifconfig command. It is a handy tool for configuring the network interfaces for Linux administrators. It can be used to assign and remove addresses, take the interfaces up or down, and much more useful tasks.



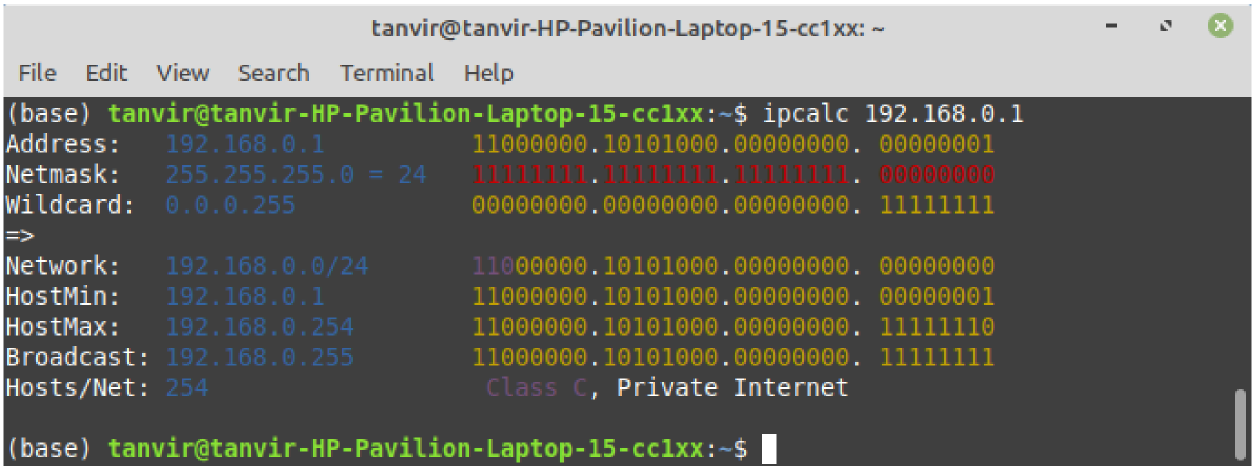
tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ ip -c address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether ac:e2:d3:68:7f:15 brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 60:f6:77:4f:4d:f9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.101/24 brd 192.168.0.255 scope global dynamic noprefixroute wlo1
       valid_lft 5143sec preferred_lft 5143sec
    inet6 fe80::d269:d268:b5c8:1301/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: vboxnet0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

ipcalc

Ipcalc actually does a lot more – it takes an IP address and netmask and provides the resulting broadcast, network, Cisco wildcard mask, and host range. You can also use it as a teaching tool to present subnetting results in an easy to understand binary values. Some of the uses of **ipcalc** are:

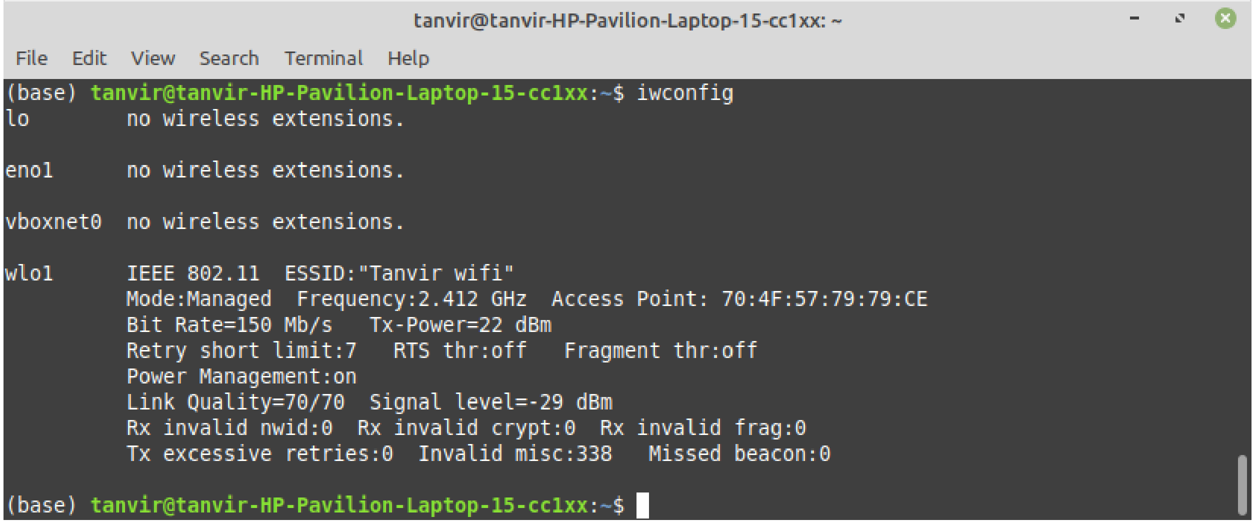
- Validate IP address
- Show calculated broadcast address
- Display hostname determined via DNS
- Display network address or prefix


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ ipcalc 192.168.0.1
Address:   192.168.0.1          11000000.10101000.00000000. 00000001
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.0.0/24       11000000.10101000.00000000. 00000000
HostMin:   192.168.0.1          11000000.10101000.00000000. 00000001
HostMax:   192.168.0.254        11000000.10101000.00000000. 11111110
Broadcast: 192.168.0.255        11000000.10101000.00000000. 11111111
Hosts/Net: 254                   Class C, Private Internet

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

iwconfig

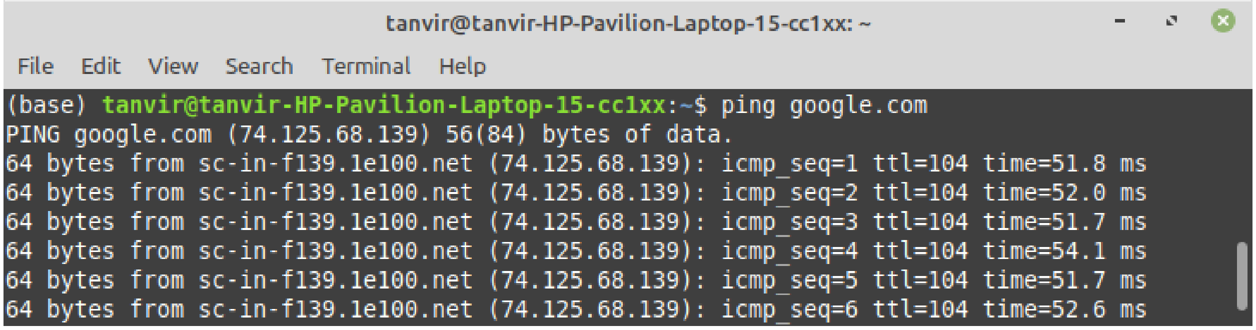
iwconfig command in Linux is like ifconfig command, in the sense it works with kernel-resident network interface but it is dedicated to wireless networking interfaces only. It is used to set the parameters of the network interface that are particular to the wireless operation like SSID, frequency etc. *iwconfig* may also be used to display the parameters, and the wireless statistics which are extracted from */proc/net/wireless*.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ iwconfig
lo        no wireless extensions.

eno1      no wireless extensions.

vboxnet0  no wireless extensions.

wlo1      IEEE 802.11  ESSID:"Tanvir wifi"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 70:4F:57:79:79:CE
          Bit Rate=150 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70  Signal level=-29 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:338   Missed beacon:0

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

Ping

Ping command stands for (Packet Internet Groper). It checks connectivity between two nodes to see if a server is available. It sends ICMP ECHO_REQUEST packets to network hosts and displays the data on the remote server's response. It checks if a remote host is up, or that network interfaces can be reached. Further, it is used to check if a network connection is available between two devices. It is also handy tool for checking your network connection and verifying network issues.

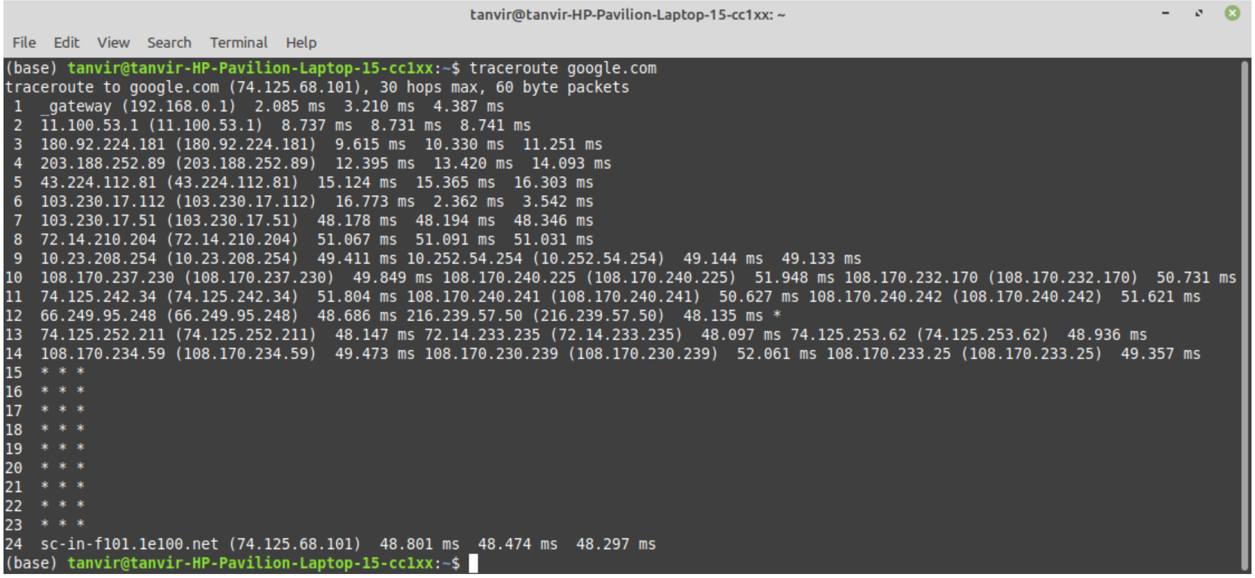


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ ping google.com
PING google.com (74.125.68.139) 56(84) bytes of data.
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=1 ttl=104 time=51.8 ms
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=2 ttl=104 time=52.0 ms
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=3 ttl=104 time=51.7 ms
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=4 ttl=104 time=54.1 ms
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=5 ttl=104 time=51.7 ms
64 bytes from sc-in-f139.1e100.net (74.125.68.139): icmp_seq=6 ttl=104 time=52.6 ms
```

Traceroute

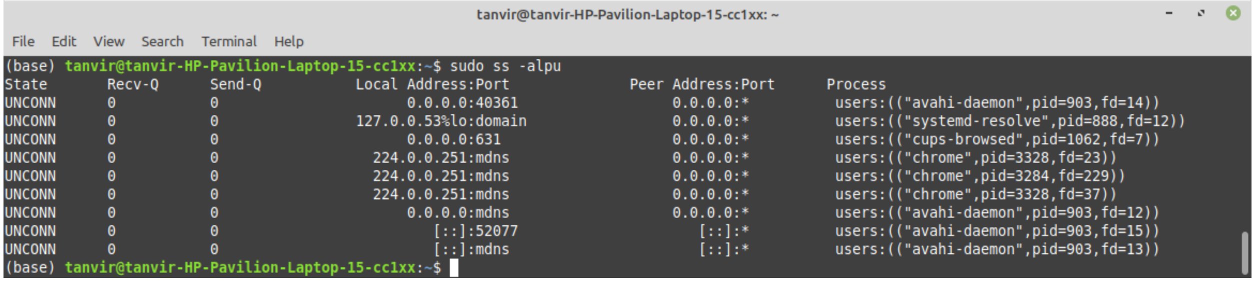
Traceroute command is a network troubleshooting utility that helps us determine the number of hops and packets traveling path required to reach a destination. It is used to display how the data transmitted from a local machine to a remote machine. Loading a web page is one of the common examples of the traceroute. A web page loading transfers data through a network and routers. The traceroute can display the routes, IP addresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ traceroute google.com
traceroute to google.com (74.125.68.101), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  2.085 ms  3.210 ms  4.387 ms
 2  11.100.53.1 (11.100.53.1)  8.737 ms  8.731 ms  8.741 ms
 3  180.92.224.181 (180.92.224.181)  9.615 ms  10.330 ms  11.251 ms
 4  203.188.252.89 (203.188.252.89)  12.395 ms  13.420 ms  14.093 ms
 5  43.224.112.81 (43.224.112.81)  15.124 ms  15.365 ms  16.303 ms
 6  103.230.17.112 (103.230.17.112)  16.773 ms  2.362 ms  3.542 ms
 7  103.230.17.51 (103.230.17.51)  48.178 ms  48.194 ms  48.346 ms
 8  72.14.210.204 (72.14.210.204)  51.067 ms  51.091 ms  51.031 ms
 9  10.23.208.254 (10.23.208.254)  49.411 ms 10.252.54.254 (10.252.54.254)  49.144 ms  49.133 ms
10  108.170.237.230 (108.170.237.230)  49.849 ms 108.170.240.225 (108.170.240.225)  51.948 ms 108.170.232.170 (108.170.232.170)  50.731 ms
11  74.125.242.34 (74.125.242.34)  51.804 ms 108.170.240.241 (108.170.240.241)  50.627 ms 108.170.240.242 (108.170.240.242)  51.621 ms
12  66.249.95.248 (66.249.95.248)  48.686 ms 216.239.57.50 (216.239.57.50)  48.135 ms *
13  74.125.252.211 (74.125.252.211)  48.147 ms 72.14.233.235 (72.14.233.235)  48.097 ms 74.125.253.62 (74.125.253.62)  48.936 ms
14  108.170.234.59 (108.170.234.59)  49.473 ms 108.170.230.239 (108.170.230.239)  52.061 ms 108.170.233.25 (108.170.233.25)  49.357 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  sc-in-f101.1e100.net (74.125.68.101)  48.801 ms  48.474 ms  48.297 ms
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

Ss

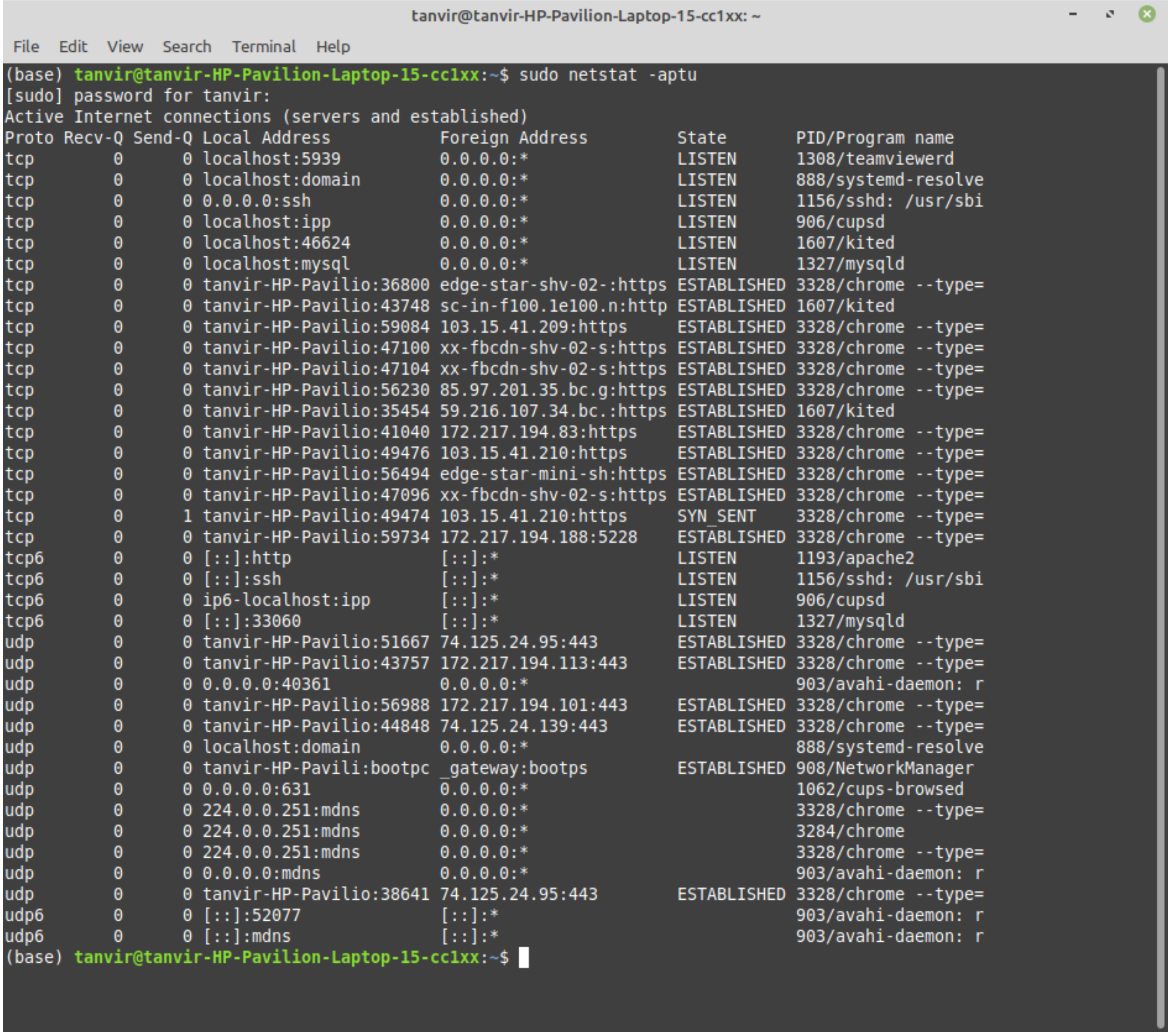
The ss command is a replacement for netstat command. This command gives more information in comparison to the netstat. It is also faster than netstat as it gets all information from kernel userspace.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ sudo ss -alpu
State       Recv-Q      Send-Q          Local Address:Port          Peer Address:Port       Process
UNCONN      0           0                    0.0.0.0:40361               0.0.0.0:*           users:(("avahi-daemon",pid=903,fd=14))
UNCONN      0           0               127.0.0.53%lo:domain             0.0.0.0:*           users:(("systemd-resolve",pid=888,fd=12))
UNCONN      0           0                    0.0.0.0:631                 0.0.0.0:*           users:(("cups-browsed",pid=1062,fd=7))
UNCONN      0           0                224.0.0.251:mdns                0.0.0.0:*           users:(("chrome",pid=3328,fd=23))
UNCONN      0           0                224.0.0.251:mdns                0.0.0.0:*           users:(("chrome",pid=3284,fd=229))
UNCONN      0           0                224.0.0.251:mdns                0.0.0.0:*           users:(("chrome",pid=3328,fd=37))
UNCONN      0           0                    0.0.0.0:mdns                0.0.0.0:*           users:(("avahi-daemon",pid=903,fd=12))
UNCONN      0           0                       [::]:52077                  [::]:*           users:(("avahi-daemon",pid=903,fd=15))
UNCONN      0           0                       [::]:mdns                   [::]:*           users:(("avahi-daemon",pid=903,fd=13))
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

netstat

Netstat command stands for Network statistics. It displays information about different interface statistics, including open sockets, routing tables, and connection information. Further, it can be used to displays all the socket connections (including TCP, UDP). Apart from connected sockets, it also displays the sockets that are pending for connections. It is a handy tool for network and system administrators.



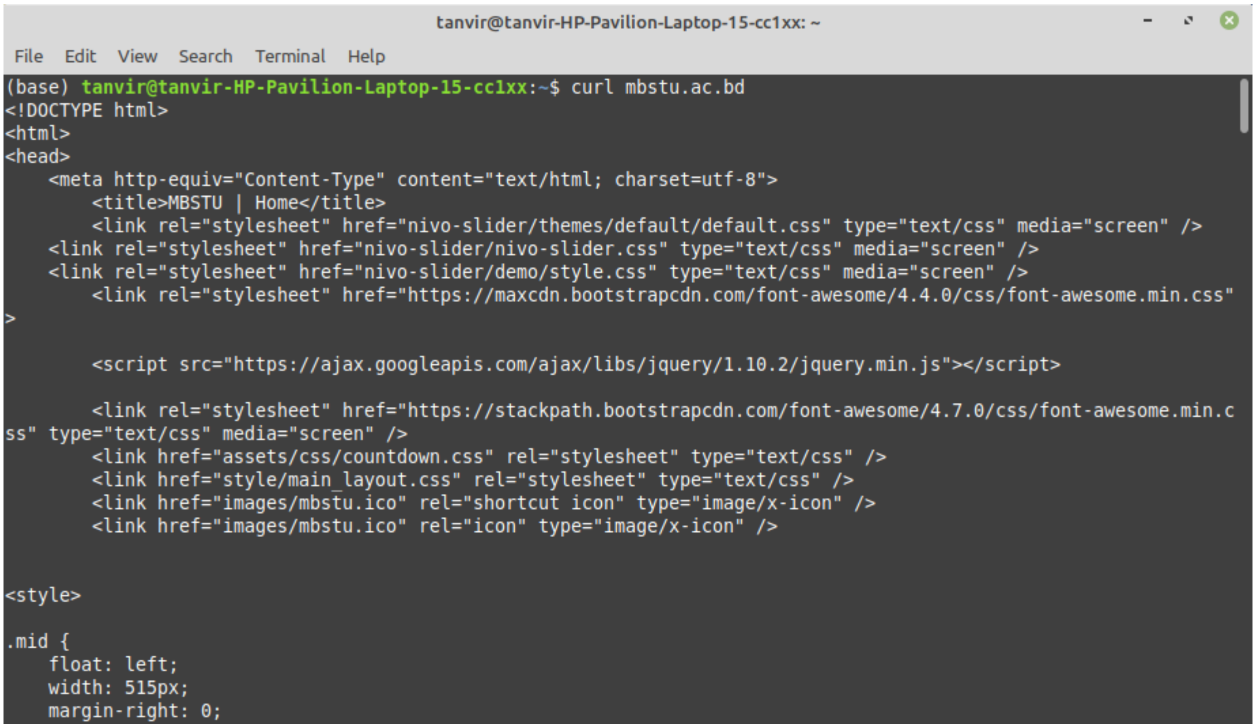
tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ sudo netstat -aptu
[sudo] password for tanvir:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:5939          0.0.0.0:*               LISTEN      1308/teamviewerd
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      888/systemd-resolve
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1156/sshd: /usr/sbi
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      906/cupsd
tcp        0      0 localhost:46624         0.0.0.0:*               LISTEN      1607/kited
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN      1327/mysqld
tcp        0      0 tanvir-HP-Pavilio:36800 edge-star-shv-02-:https ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:43748 sc-in-f100.1e100.n:http ESTABLISHED 1607/kited
tcp        0      0 tanvir-HP-Pavilio:59084 103.15.41.209:https     ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:47100 xx-fbcdn-shv-02-s:https ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:47104 xx-fbcdn-shv-02-s:https ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:56230 85.97.201.35.bc.g:https ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:35454 59.216.107.34.bc.:https ESTABLISHED 1607/kited
tcp        0      0 tanvir-HP-Pavilio:41040 172.217.194.83:https    ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:49476 103.15.41.210:https     ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:56494 edge-star-mini-sh:https ESTABLISHED 3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:47096 xx-fbcdn-shv-02-s:https ESTABLISHED 3328/chrome --type=
tcp        0      1 tanvir-HP-Pavilio:49474 103.15.41.210:https     SYN_SENT    3328/chrome --type=
tcp        0      0 tanvir-HP-Pavilio:59734 172.217.194.188:5228    ESTABLISHED 3328/chrome --type=
tcp6       0      0 [::]:http               [::]:*                  LISTEN      1193/apache2
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      1156/sshd: /usr/sbi
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      906/cupsd
tcp6       0      0 [::]:33060              [::]:*                  LISTEN      1327/mysqld
udp        0      0 tanvir-HP-Pavilio:51667 74.125.24.95:443        ESTABLISHED 3328/chrome --type=
udp        0      0 tanvir-HP-Pavilio:43757 172.217.194.113:443     ESTABLISHED 3328/chrome --type=
udp        0      0 0.0.0.0:40361           0.0.0.0:*                           903/avahi-daemon: r
udp        0      0 tanvir-HP-Pavilio:56988 172.217.194.101:443     ESTABLISHED 3328/chrome --type=
udp        0      0 tanvir-HP-Pavilio:44848 74.125.24.139:443       ESTABLISHED 3328/chrome --type=
udp        0      0 localhost:domain        0.0.0.0:*                           888/systemd-resolve
udp        0      0 tanvir-HP-Pavili:bootpc _gateway:bootps         ESTABLISHED 908/NetworkManager
udp        0      0 0.0.0.0:631             0.0.0.0:*                           1062/cups-browsed
udp        0      0 224.0.0.251:mdns        0.0.0.0:*                           3328/chrome --type=
udp        0      0 224.0.0.251:mdns        0.0.0.0:*                           3284/chrome
udp        0      0 224.0.0.251:mdns        0.0.0.0:*                           3328/chrome --type=
udp        0      0 0.0.0.0:mdns            0.0.0.0:*                           903/avahi-daemon: r
udp        0      0 tanvir-HP-Pavilio:38641 74.125.24.95:443        ESTABLISHED 3328/chrome --type=
udp6       0      0 [::]:52077              [::]:*                              903/avahi-daemon: r
udp6       0      0 [::]:mdns               [::]:*                              903/avahi-daemon: r
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

Curl

Linux curl command is used to download or upload data to a server via supported protocols such as HTTP, FTP, IMAP, SFTP, TFTP, IMAP, POP3, SCP, etc. It is a remote utility, so it works without user interaction.

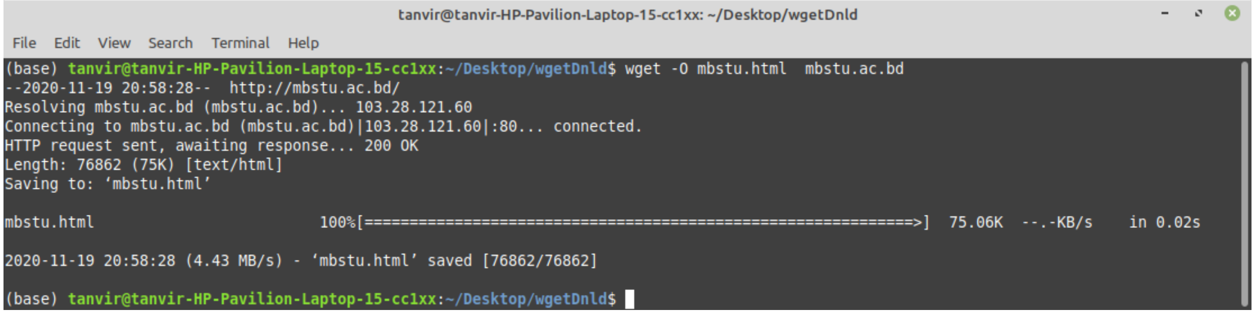
The data transfer from one place to another is one of the vital and most used tasks of a computer system. However, there are many GUI tools available for data transfer. But, when working on the command-line, it becomes a bit complicated. The curl utility allows us to transfer data via the command line.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ curl mbstu.ac.bd
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <title>MBSTU | Home</title>
        <link rel="stylesheet" href="nivo-slider/themes/default/default.css" type="text/css" media="screen" />
    <link rel="stylesheet" href="nivo-slider/nivo-slider.css" type="text/css" media="screen" />
    <link rel="stylesheet" href="nivo-slider/demo/style.css" type="text/css" media="screen" />
        <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-awesome.min.css"
>


        <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script>

        <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.c
ss" type="text/css" media="screen" />
        <link href="assets/css/countdown.css" rel="stylesheet" type="text/css" />
        <link href="style/main_layout.css" rel="stylesheet" type="text/css" />
        <link href="images/mbstu.ico" rel="shortcut icon" type="image/x-icon" />
        <link href="images/mbstu.ico" rel="icon" type="image/x-icon" />


<style>

.mid {
    float: left;
    width: 515px;
    margin-right: 0;
```

Wget

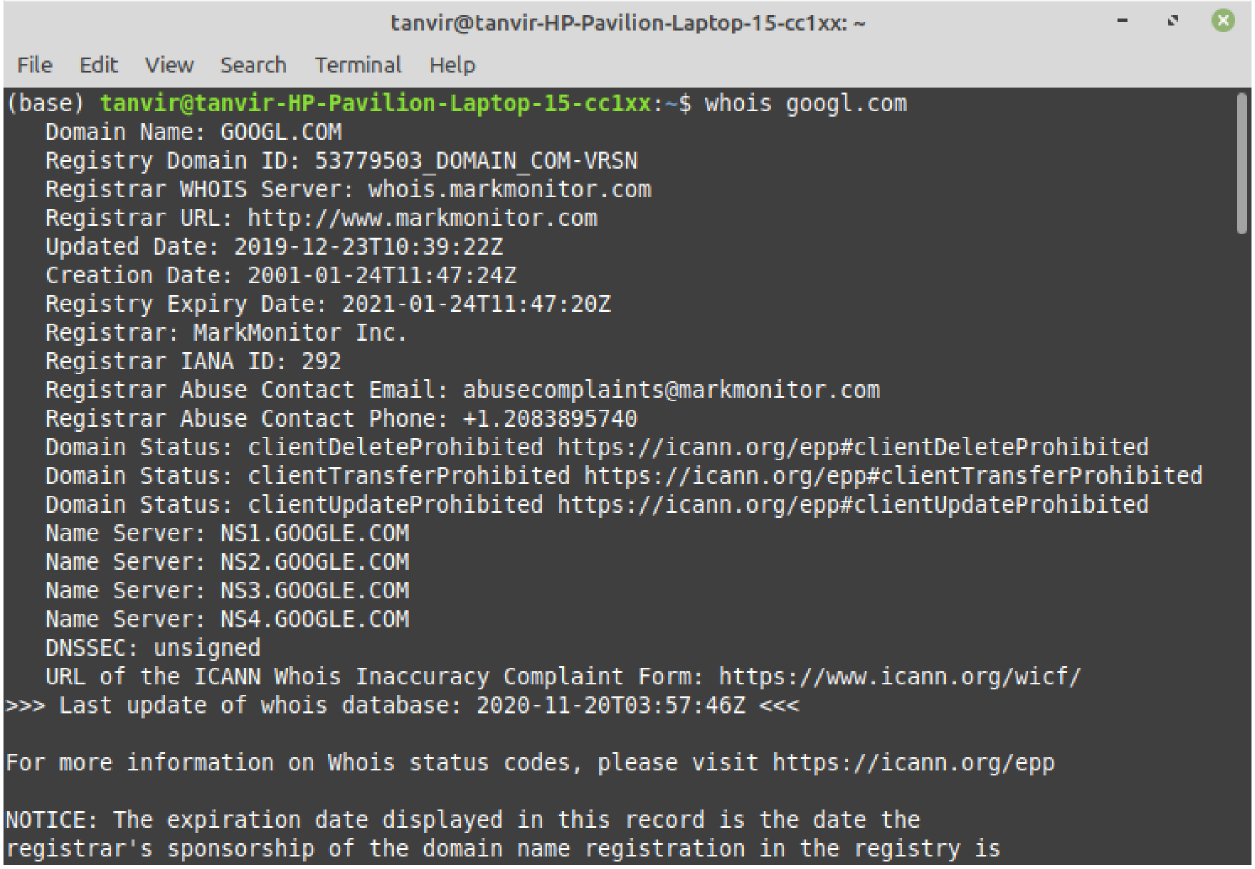
On Unix-like operating systems, the wget command downloads files served with HTTP, HTTPS, or FTP over a network.
wget is a free utility for non-interactive download of files from the web. It supports HTTP, HTTPS, and FTP protocols, as well as retrieval through HTTP proxies.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~/Desktop/wgetDnld
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~/Desktop/wgetDnld$ wget -O mbstu.html  mbstu.ac.bd
--2020-11-19 20:58:28--  http://mbstu.ac.bd/
Resolving mbstu.ac.bd (mbstu.ac.bd)... 103.28.121.60
Connecting to mbstu.ac.bd (mbstu.ac.bd)|103.28.121.60|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 76862 (75K) [text/html]
Saving to: ‘mbstu.html’

mbstu.html                    100%[==============================================================>]  75.06K  --.-KB/s    in 0.02s

2020-11-19 20:58:28 (4.43 MB/s) - ‘mbstu.html’ saved [76862/76862]

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~/Desktop/wgetDnld$ 
```

whois

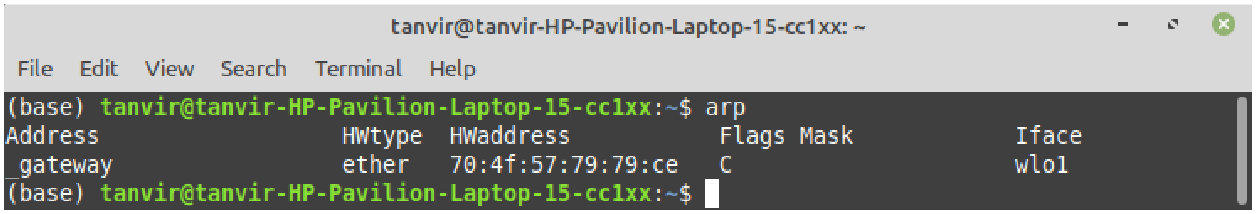
WHOIS (pronounced as the phrase "**who is**") is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ whois googl.com
   Domain Name: GOOGL.COM
   Registry Domain ID: 53779503_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-12-23T10:39:22Z
   Creation Date: 2001-01-24T11:47:24Z
   Registry Expiry Date: 2021-01-24T11:47:20Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-11-20T03:57:46Z <<<

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
```

arp

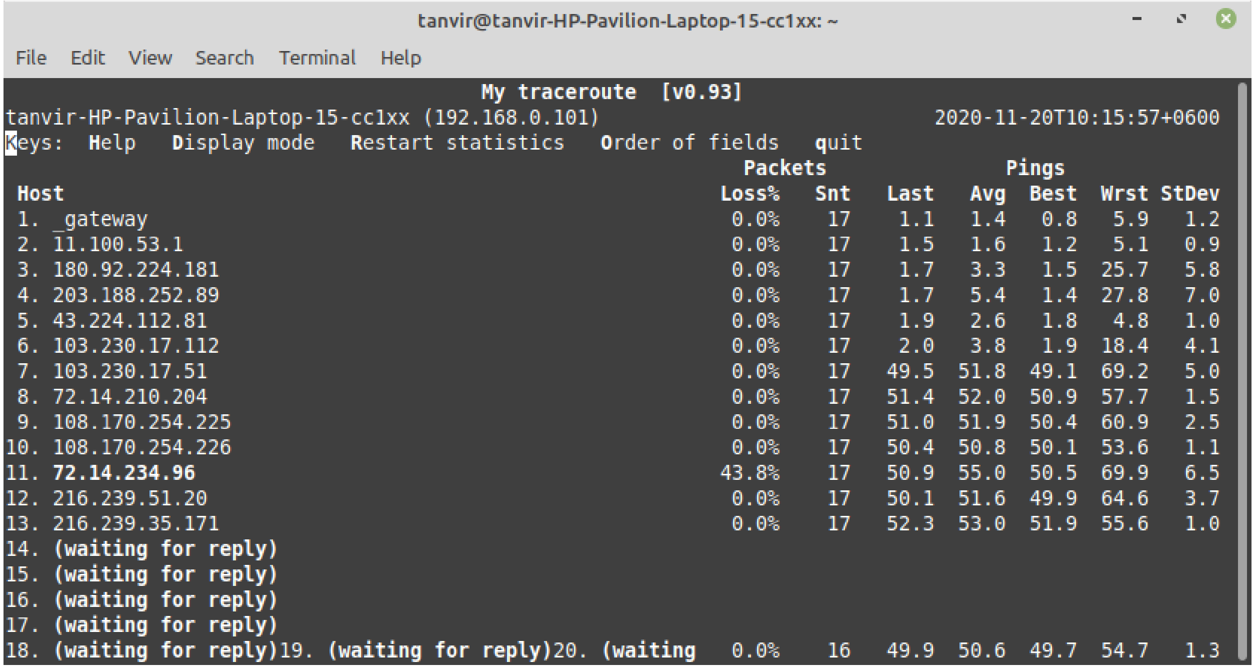
The command arp stands for Address Resoslution Protocol. It allows us to view or add content into kernel's ARP table.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   70:4f:57:79:79:ce   C                     wlo1
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

mtr

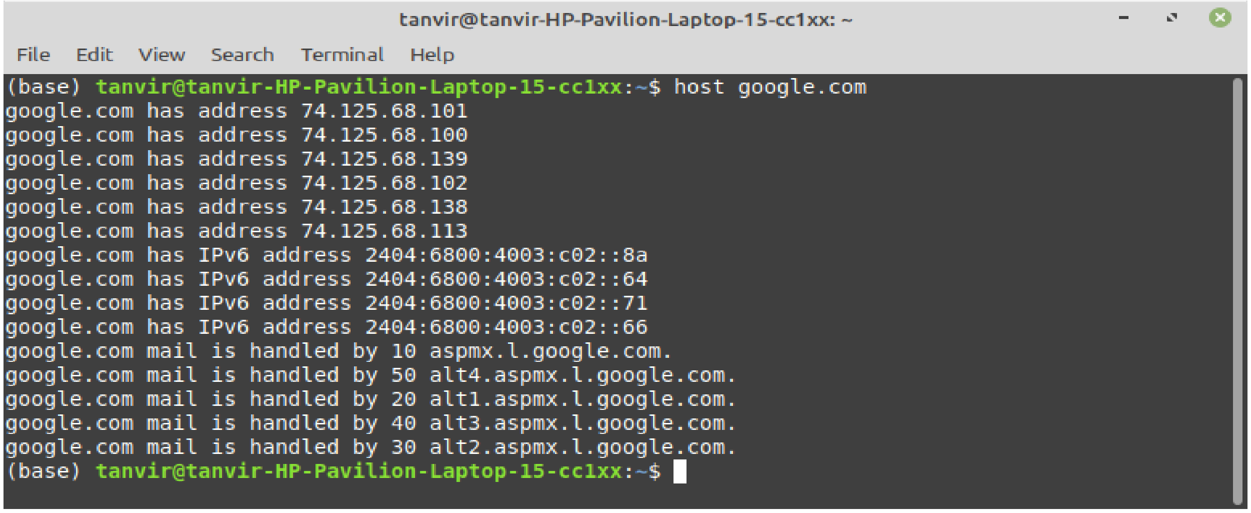
The mtr command is a combination of ping and traceroute commands. It is a network diagnostic tool that continuously sends packets showing ping time for each hop. It also displays network problems of the entire route taken by the network packets.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
                                   My traceroute  [v0.93]
tanvir-HP-Pavilion-Laptop-15-cc1xx (192.168.0.101)                 2020-11-20T10:15:57+0600
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                  Packets               Pings
 Host                                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway                                     0.0%    17    1.1   1.4   0.8   5.9   1.2
 2. 11.100.53.1                                  0.0%    17    1.5   1.6   1.2   5.1   0.9
 3. 180.92.224.181                               0.0%    17    1.7   3.3   1.5  25.7   5.8
 4. 203.188.252.89                               0.0%    17    1.7   5.4   1.4  27.8   7.0
 5. 43.224.112.81                                0.0%    17    1.9   2.6   1.8   4.8   1.0
 6. 103.230.17.112                               0.0%    17    2.0   3.8   1.9  18.4   4.1
 7. 103.230.17.51                                0.0%    17   49.5  51.8  49.1  69.2   5.0
 8. 72.14.210.204                                0.0%    17   51.4  52.0  50.9  57.7   1.5
 9. 108.170.254.225                              0.0%    17   51.0  51.9  50.4  60.9   2.5
10. 108.170.254.226                              0.0%    17   50.4  50.8  50.1  53.6   1.1
11. 72.14.234.96                                43.8%    17   50.9  55.0  50.5  69.9   6.5
12. 216.239.51.20                                0.0%    17   50.1  51.6  49.9  64.6   3.7
13. 216.239.35.171                               0.0%    17   52.3  53.0  51.9  55.6   1.0
14. (waiting for reply)
15. (waiting for reply)
16. (waiting for reply)
17. (waiting for reply)
18. (waiting for reply)19. (waiting for reply)20. (waiting  0.0%    16   49.9  50.6  49.7  54.7   1.3
```

host

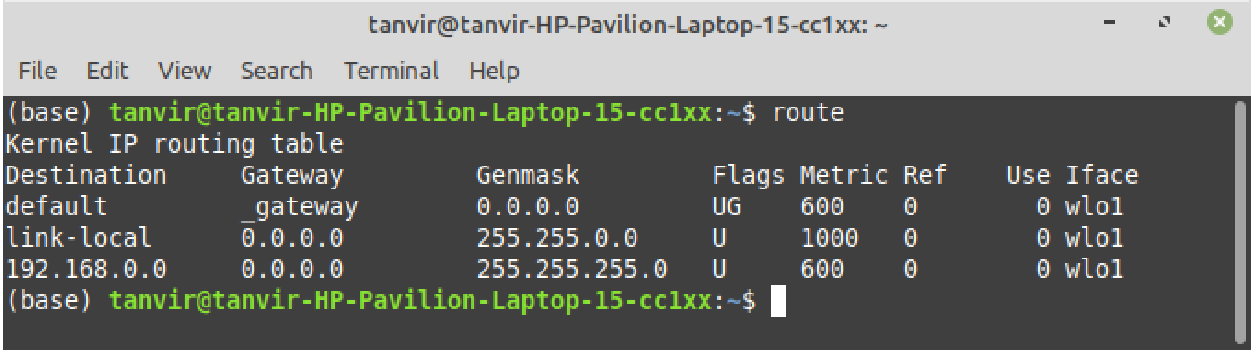
Linux host command displays domain name for given IP address or vice-versa. It also performs DNS lookups related to the DNS query. The host command's default behavior displays a summary of its command-line arguments and supported options.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ host google.com
google.com has address 74.125.68.101
google.com has address 74.125.68.100
google.com has address 74.125.68.139
google.com has address 74.125.68.102
google.com has address 74.125.68.138
google.com has address 74.125.68.113
google.com has IPv6 address 2404:6800:4003:c02::8a
google.com has IPv6 address 2404:6800:4003:c02::64
google.com has IPv6 address 2404:6800:4003:c02::71
google.com has IPv6 address 2404:6800:4003:c02::66
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

route

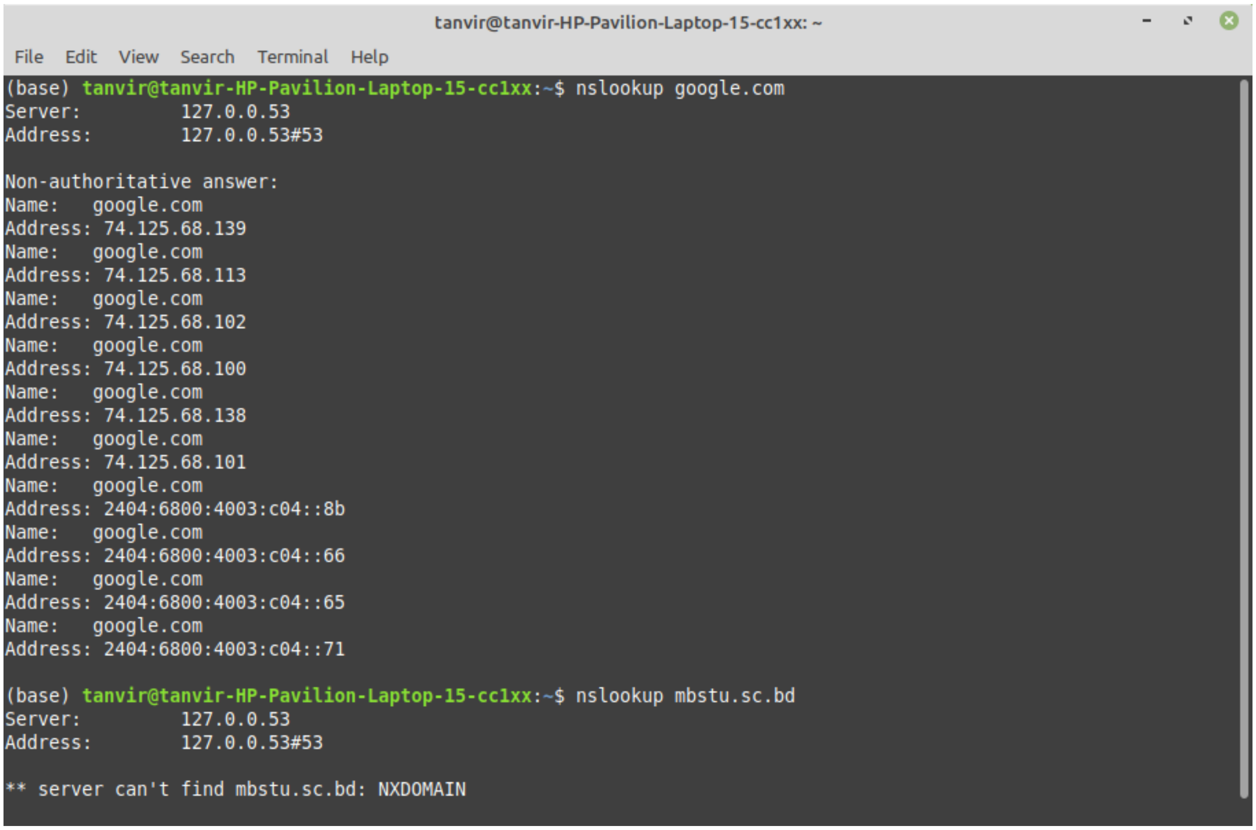
The route command displays and manipulate IP routing table for your system.
A router is a device which is basically used to determine the best way to route packets to a destination.



```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 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
192.168.0.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

nslookup

This command is also used to find DNS related query.

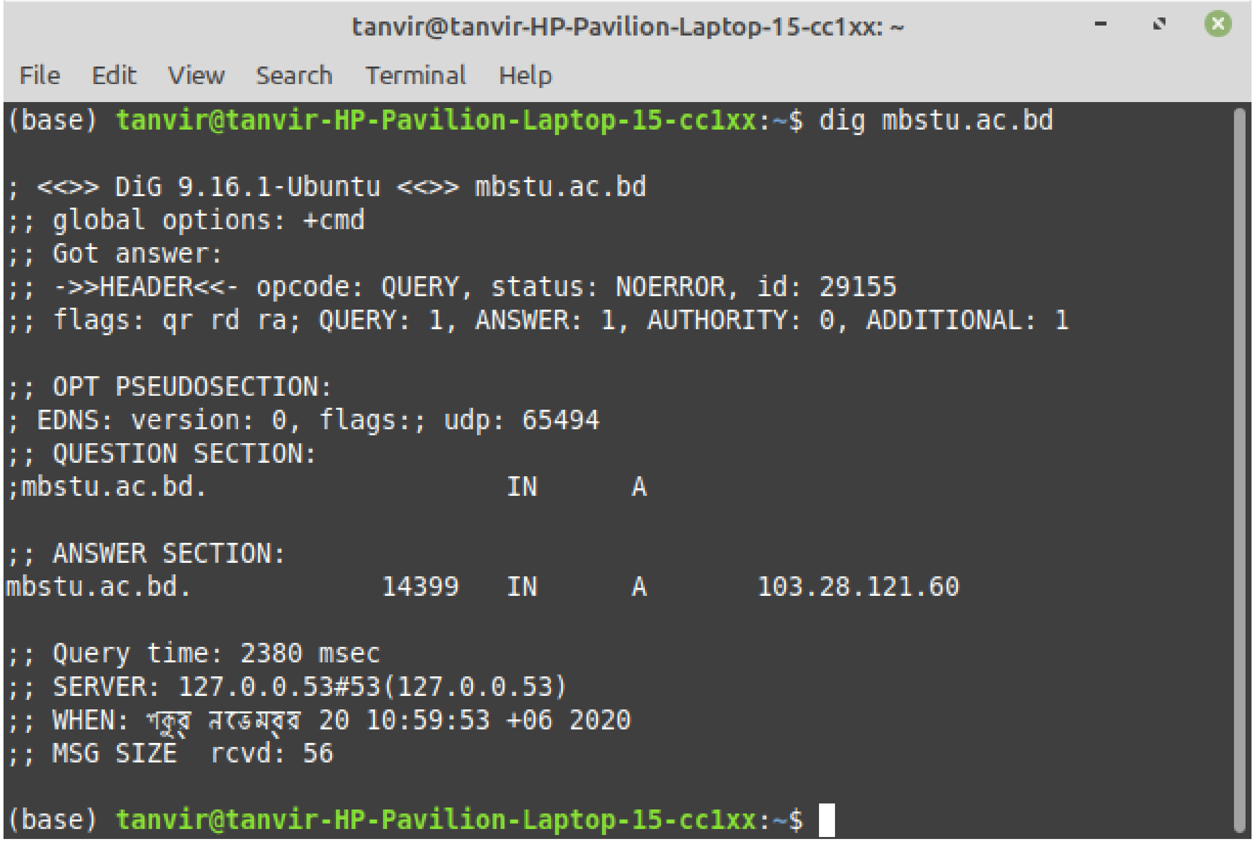


```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 74.125.68.139
Name:   google.com
Address: 74.125.68.113
Name:   google.com
Address: 74.125.68.102
Name:   google.com
Address: 74.125.68.100
Name:   google.com
Address: 74.125.68.138
Name:   google.com
Address: 74.125.68.101
Name:   google.com
Address: 2404:6800:4003:c04::8b
Name:   google.com
Address: 2404:6800:4003:c04::66
Name:   google.com
Address: 2404:6800:4003:c04::65
Name:   google.com
Address: 2404:6800:4003:c04::71

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ nslookup mbstu.sc.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find mbstu.sc.bd: NXDOMAIN
```

dig

Linux dig command stands for Domain Information Groper. This command is used for tasks related to DNS lookup to query DNS name servers. It mainly deals with troubleshooting DNS related problems. It is a flexible utility for examining the DNS (Domain Name Servers). It is used to perform the DNS lookups and returns the queried answers from the name server. Usually, it is used by most DNS administrators to troubleshoot the DNS problems. It is a straightforward tool and provides a clear output. It is more functional than other lookups tools.

The dig command supports plenty of command-line options. Additionally, it facilitates batch mode, which is useful for accessing the lookup requests from a file. If it is not specified to the dig command to query a specific name server, it will access each of the servers from "/etc/resolv.conf." The dig without any command-line options will perform an NS query for "." (the root).

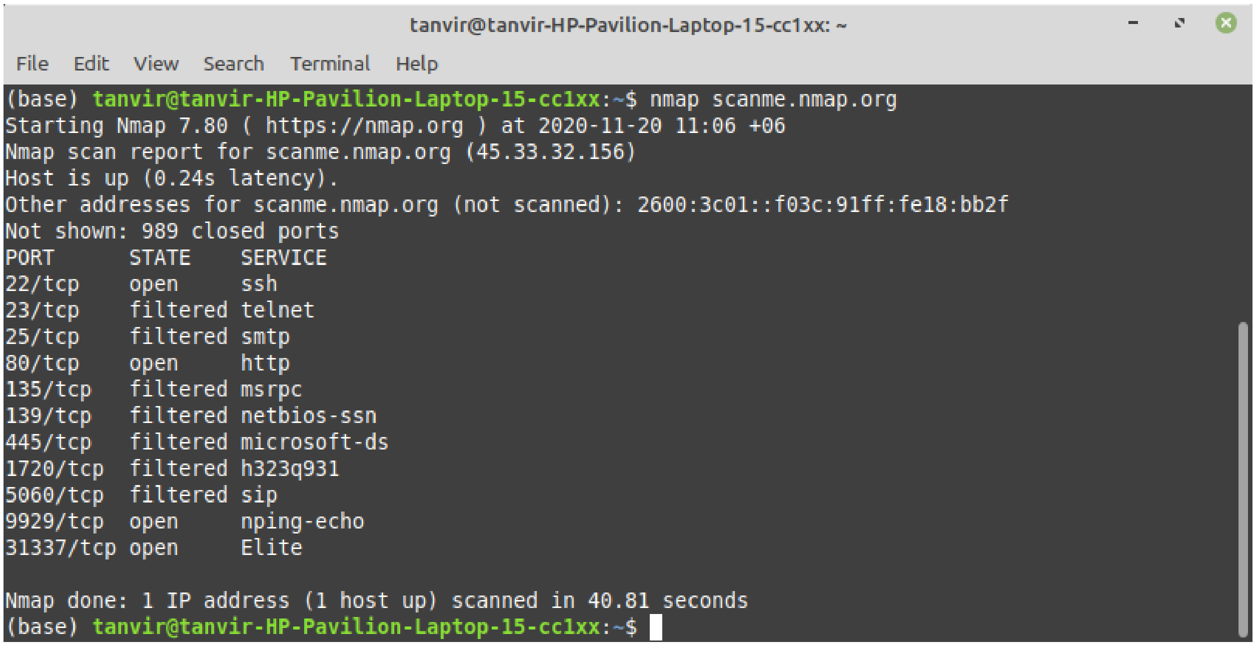


```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ dig mbstu.ac.bd

; <<>> DiG 9.16.1-Ubuntu <<>> mbstu.ac.bd
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29155
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mbstu.ac.bd.                   IN      A

;; ANSWER SECTION:
mbstu.ac.bd.            14399   IN      A       103.28.121.60

;; Query time: 2380 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: শুক্র নভেম্বর 20 10:59:53 +06 2020
;; MSG SIZE  rcvd: 56

(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

Nmap

Nmap, short for Network Mapper, is a network discovery and security auditing tool. It is known for its simple and easy to remember flags that provide powerful scanning options. Nmap is widely used by network administrators to scan for:

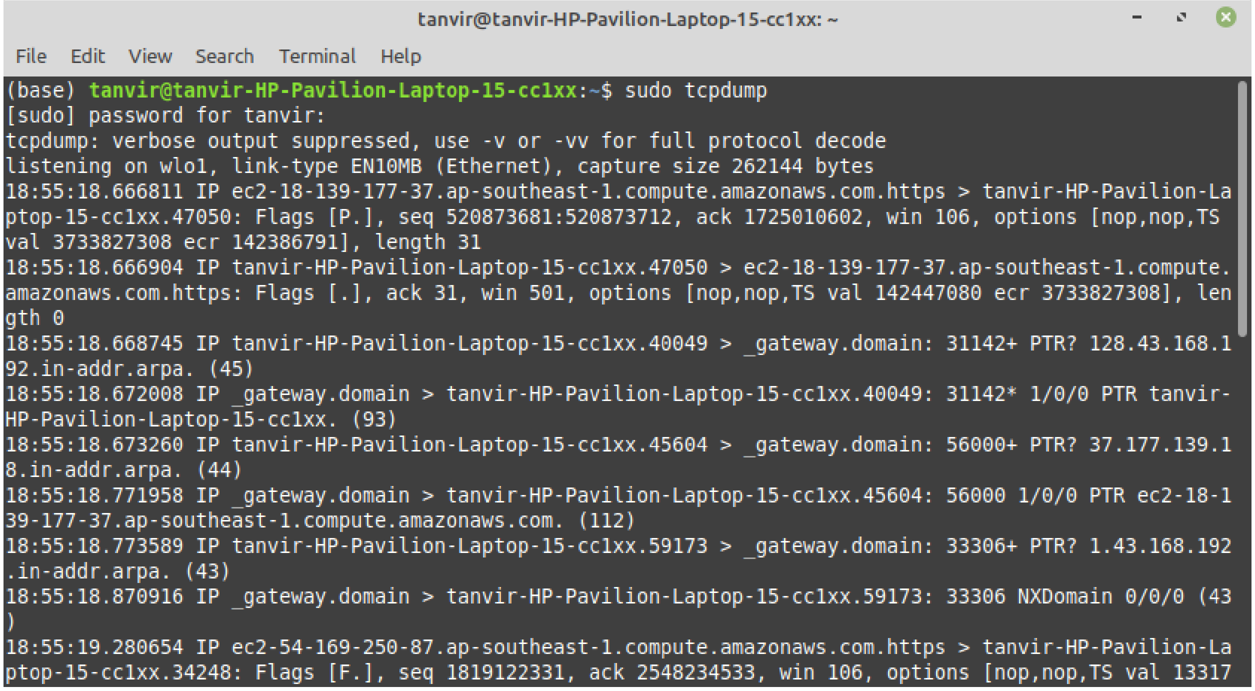
- Open ports and services
- Discover services along with their versions
- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Monitoring hosts



```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-20 11:06 +06
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 989 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1720/tcp  filtered h323q931
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 40.81 seconds
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ 
```

tcpdump

Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.A powerful and versatile tool that includes many options and filters, tcpdump can be used in a variety of cases. Since it's a command line tool, it is ideal to run in remote servers or devices for which a GUI is not available, to collect data that can be analyzed later. It can also be launched in the background or as a scheduled job using tools like cron.

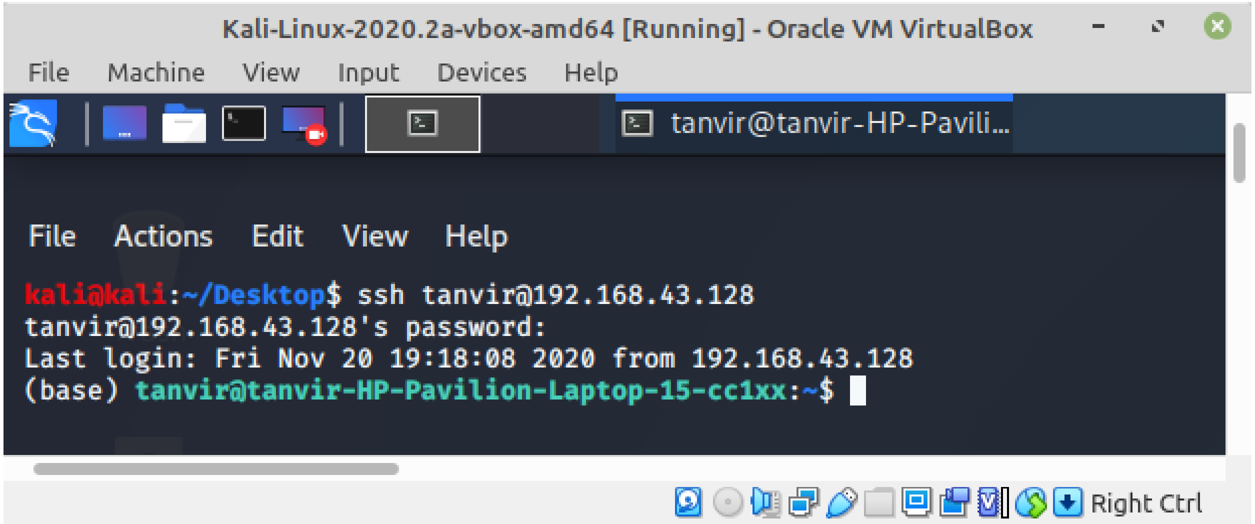


```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$ sudo tcpdump
[sudo] password for tanvir:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:55:18.666811 IP ec2-18-139-177-37.ap-southeast-1.compute.amazonaws.com.https > tanvir-HP-Pavilion-La
ptop-15-cc1xx.47050: Flags [P.], seq 520873681:520873712, ack 1725010602, win 106, options [nop,nop,TS
val 3733827308 ecr 142386791], length 31
18:55:18.666904 IP tanvir-HP-Pavilion-Laptop-15-cc1xx.47050 > ec2-18-139-177-37.ap-southeast-1.compute.
amazonaws.com.https: Flags [.], ack 31, win 501, options [nop,nop,TS val 142447080 ecr 3733827308], len
gth 0
18:55:18.668745 IP tanvir-HP-Pavilion-Laptop-15-cc1xx.40049 > _gateway.domain: 31142+ PTR? 128.43.168.1
92.in-addr.arpa. (45)
18:55:18.672008 IP _gateway.domain > tanvir-HP-Pavilion-Laptop-15-cc1xx.40049: 31142* 1/0/0 PTR tanvir-
HP-Pavilion-Laptop-15-cc1xx. (93)
18:55:18.673260 IP tanvir-HP-Pavilion-Laptop-15-cc1xx.45604 > _gateway.domain: 56000+ PTR? 37.177.139.1
8.in-addr.arpa. (44)
18:55:18.771958 IP _gateway.domain > tanvir-HP-Pavilion-Laptop-15-cc1xx.45604: 56000 1/0/0 PTR ec2-18-1
39-177-37.ap-southeast-1.compute.amazonaws.com. (112)
18:55:18.773589 IP tanvir-HP-Pavilion-Laptop-15-cc1xx.59173 > _gateway.domain: 33306+ PTR? 1.43.168.192
.in-addr.arpa. (43)
18:55:18.870916 IP _gateway.domain > tanvir-HP-Pavilion-Laptop-15-cc1xx.59173: 33306 NXDomain 0/0/0 (43
)
18:55:19.280654 IP ec2-54-169-250-87.ap-southeast-1.compute.amazonaws.com.https > tanvir-HP-Pavilion-La
ptop-15-cc1xx.34248: Flags [F.], seq 1819122331, ack 2548234533, win 106, options [nop,nop,TS val 13317
```

SSH

SSH, or Secure Shell, is a remote administration protocol that allows users to control and modify their remote servers over the Internet. The service was created as a secure replacement for the unencrypted Telnet and uses cryptographic techniques to ensure that all communication to and from the remote server happens in an encrypted manner. It provides a mechanism for authenticating a remote user, transferring inputs from the client to the host, and relaying the output back to the client.

The Figure Below shows a typical SSH Window. Any Linux or macOS user can SSH into their remote server directly from the terminal window. Windows users can take advantage of SSH clients like Putty.

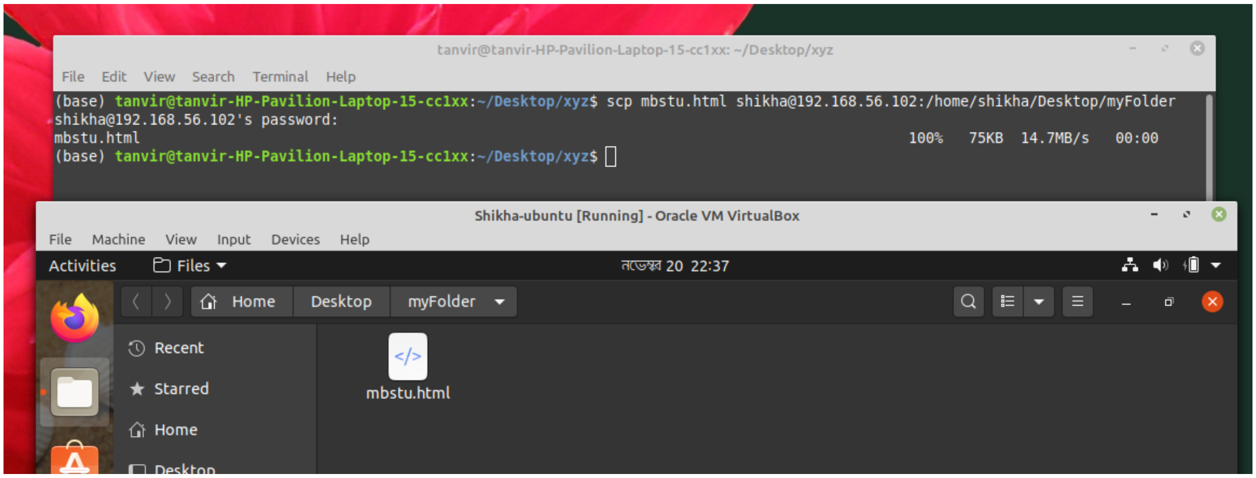


Kali-Linux-2020.2a-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
tanvir@tanvir-HP-Pavili...
File Actions Edit View Help
Right Ctrl

```
kali@kali:~/Desktop$ ssh tanvir@192.168.43.128
tanvir@192.168.43.128's password:
Last login: Fri Nov 20 19:18:08 2020 from 192.168.43.128
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~$
```

SCP

scp is a program for copying files between computers. It uses the SSH protocol. It is included by default in most Linux and Unix distributions. It is also included in the [Tectia SSH}(/products/tectia-ssh/) and OpenSSH packages.



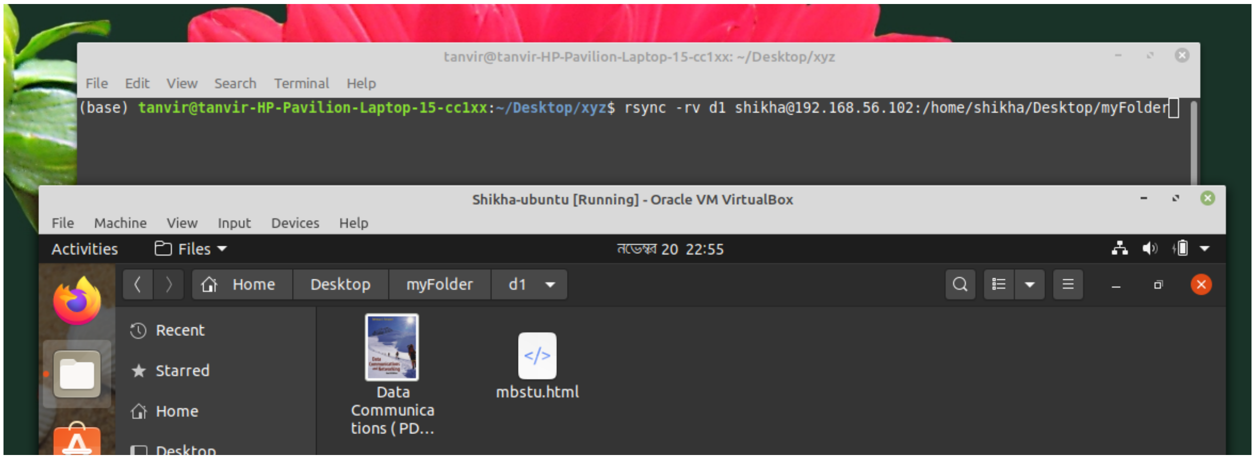
tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~/Desktop/xyz
File Edit View Search Terminal Help

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~/Desktop/xyz$ scp mbstu.html shikha@192.168.56.102:/home/shikha/Desktop/myFolder
shikha@192.168.56.102's password:
mbstu.html                                                                     100%   75KB  14.7MB/s   00:00
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~/Desktop/xyz$
```

Shikha-ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Files
নভেম্বর 20 22:37
Home
Desktop
myFolder
Recent
Starred
Home
Desktop
mbstu.html

Rsync

Rsync (Remote Sync) is a most commonly used command for copying and synchronizing files and directories remotely as well as locally in Linux/Unix systems. With the help of rsync command we can copy and synchronize your data remotely and locally across directories, across disks and networks, perform data backups and mirroring between two Linux machines.


tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx: ~/Desktop/xyz
File Edit View Search Terminal Help
Shikha-ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Files
নভেম্বর 20 22:55
Home Desktop myFolder d1
Recent
Starred
Home
Desktop
Data Communications (PD...
mbstu.html

```
(base) tanvir@tanvir-HP-Pavilion-Laptop-15-cc1xx:~/Desktop/xyz$ rsync -rv d1 shikha@192.168.56.102:/home/shikha/Desktop/myFolder
```

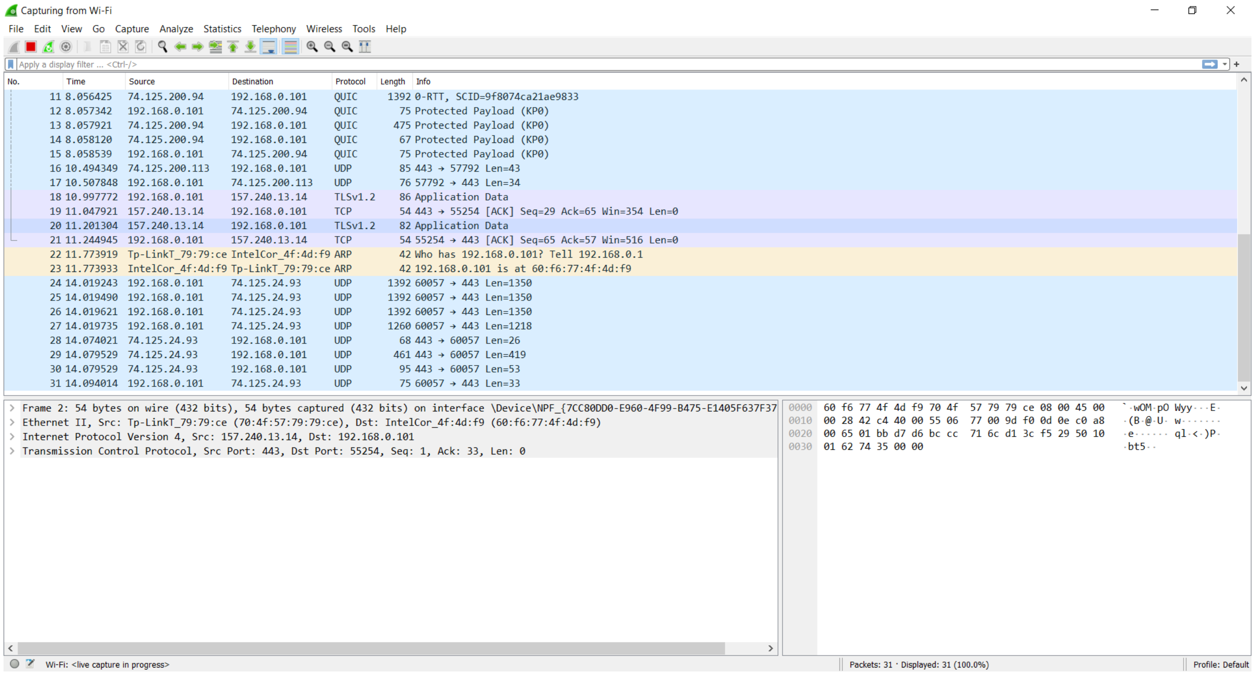
Wireshark

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source            Destination       Protocol Length Info
   11 8.056425  74.125.200.94     192.168.0.101     QUIC     1392 0-RTT, SCID=9f8074ca21ae9833
   12 8.057342  192.168.0.101     74.125.200.94     QUIC       75 Protected Payload (KP0)
   13 8.057921  74.125.200.94     192.168.0.101     QUIC      475 Protected Payload (KP0)
   14 8.058120  74.125.200.94     192.168.0.101     QUIC       67 Protected Payload (KP0)
   15 8.058539  192.168.0.101     74.125.200.94     QUIC       75 Protected Payload (KP0)
   16 10.494349 74.125.200.113    192.168.0.101     UDP        85 443 → 57792 Len=43
   17 10.507848 192.168.0.101     74.125.200.113    UDP        76 57792 → 443 Len=34
   18 10.997772 192.168.0.101     157.240.13.14     TLSv1.2    86 Application Data
   19 11.047921 157.240.13.14     192.168.0.101     TCP        54 443 → 55254 [ACK] Seq=29 Ack=65 Win=354 Len=0
   20 11.201304 157.240.13.14     192.168.0.101     TLSv1.2    82 Application Data
   21 11.244945 192.168.0.101     157.240.13.14     TCP        54 55254 → 443 [ACK] Seq=65 Ack=57 Win=516 Len=0
   22 11.773919 Tp-LinkT_79:79:ce IntelCor_4f:4d:f9 ARP        42 Who has 192.168.0.101? Tell 192.168.0.1
   23 11.773933 IntelCor_4f:4d:f9 Tp-LinkT_79:79:ce ARP        42 192.168.0.101 is at 60:f6:77:4f:4d:f9
   24 14.019243 192.168.0.101     74.125.24.93      UDP      1392 60057 → 443 Len=1350
   25 14.019490 192.168.0.101     74.125.24.93      UDP      1392 60057 → 443 Len=1350
   26 14.019621 192.168.0.101     74.125.24.93      UDP      1392 60057 → 443 Len=1350
   27 14.019735 192.168.0.101     74.125.24.93      UDP      1260 60057 → 443 Len=1218
   28 14.074021 74.125.24.93      192.168.0.101     UDP        68 443 → 60057 Len=26
   29 14.079529 74.125.24.93      192.168.0.101     UDP       461 443 → 60057 Len=419
   30 14.079529 74.125.24.93      192.168.0.101     UDP        95 443 → 60057 Len=53
   31 14.094014 192.168.0.101     74.125.24.93      UDP        75 60057 → 443 Len=33
```

```
> Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{7CC80DD0-E960-4F99-B475-E1405F637F37
> Ethernet II, Src: Tp-LinkT_79:79:ce (70:4f:57:79:79:ce), Dst: IntelCor_4f:4d:f9 (60:f6:77:4f:4d:f9)
> Internet Protocol Version 4, Src: 157.240.13.14, Dst: 192.168.0.101
> Transmission Control Protocol, Src Port: 443, Dst Port: 55254, Seq: 1, Ack: 33, Len: 0
```

```
0000  60 f6 77 4f 4d f9 70 4f  57 79 79 ce 08 00 45 00   `·wOM·pO Wyy···E·
0010  00 28 42 c4 40 00 55 06  77 00 9d f0 0d 0e c0 a8   ·(B·@·U· w·······
0020  00 65 01 bb d7 d6 bc cc  71 6c d1 3c f5 29 50 10   ·e······ ql·<·)P·
0030  01 62 74 35 00 00                                  ·bt5··
```

Wi-Fi: <live capture in progress>   Packets: 31 · Displayed: 31 (100.0%)   Profile: Default