# Atul Anurag

# PES2UG19CS075

# COMPUTER NETWORKS LAB

# Week #1

**Study and understand the basic networking tools - Wireshark, Tcpdump, Ping, Traceroute and Netcat.**

**Learn and Understand Network Tools**

**1. Wireshark**

- Perform and analyze Ping PDU capture
- Examine HTTP packet capture
- Analyze HTTP packet capture using filter

**2. Netcat**

- Establish communication between client and server
- Transfer files

**3. Tcpdump**

- Capture packets

**4. Ping**

- Test the connectivity between 2 systems

**5. Traceroute**

- Perform traceroute checks

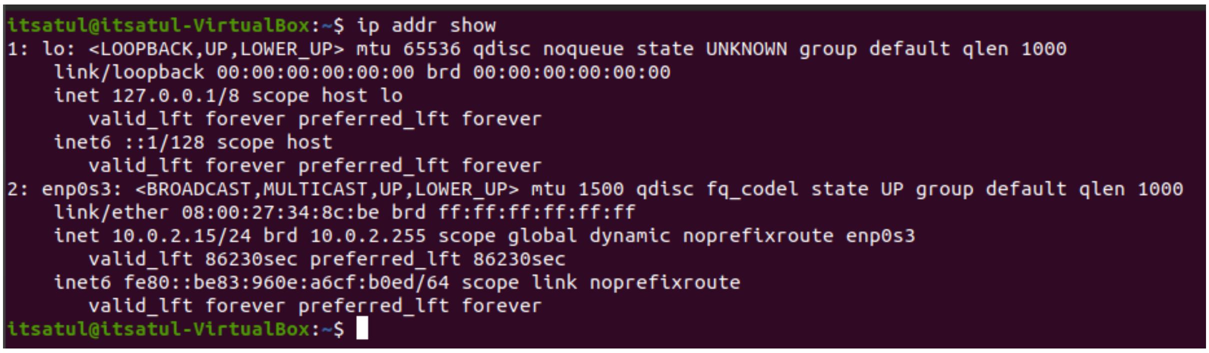
**6. Nmap**

- Explore an entire network

## Task 1: Linux Interface Configuration (ifconfig / IP command)

**Step 1:** To display status of all active network interfaces.

**ifconfig** (or) **ip addr show**



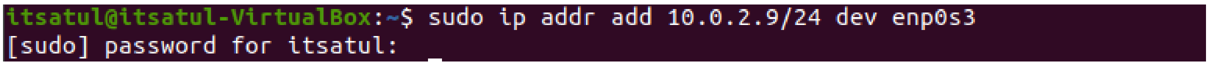
```
itsatul@itsatul-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:34:8c:be brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86230sec preferred_lft 86230sec
    inet6 fe80::be83:960e:a6cf:b0ed/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
itsatul@itsatul-VirtualBox:~$ 
```

Analyze and fill the following table:

**ip address table:**

| Interface name | IP address (IPv4 / IPv6) | MAC address |
|---|---|---|
| lo | IPV4: 127.0.0.1/8<br>IPV6: 1/128 | 00:00:00:00:00:00 |
| enp0s3 | IPV4: 10.0.2.15/24<br>IPV6: fe80::be83:960e:a6cf:b0ed/64 | 08:00:27:34:8c:be |

**Step 2:** To assign an IP address to an interface, use the following command. **sudo ifconfig interface_name 10.0.your_section.your_sno netmask 255.255.255.0** (or) **sudo ip addr add 10.0.your_section.your_sno /24 dev interface_name**

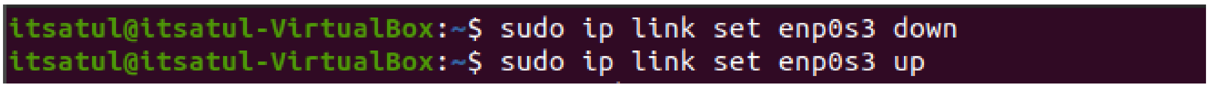


```
itsatul@itsatul-VirtualBox:~$ sudo ip addr add 10.0.2.9/24 dev enp0s3
[sudo] password for itsatul: _
```

**Step 3:** To activate / deactivate a network interface,

type. **sudo ifconfig interface_name down**

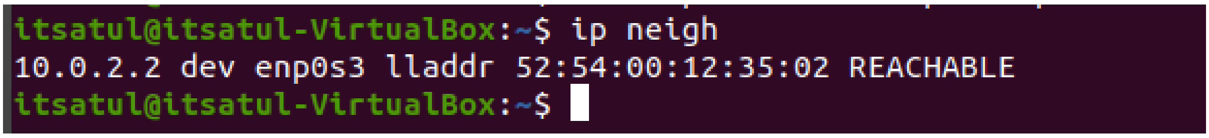
**sudo ifconfig interface_name up**



```
itsatul@itsatul-VirtualBox:~$ sudo ip link set enp0s3 down
itsatul@itsatul-VirtualBox:~$ sudo ip link set enp0s3 up
```

**Step 4:** To show the current neighbor table in kernel, type

**ip neigh**



```
itsatul@itsatul-VirtualBox:~$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
itsatul@itsatul-VirtualBox:~$ 
```

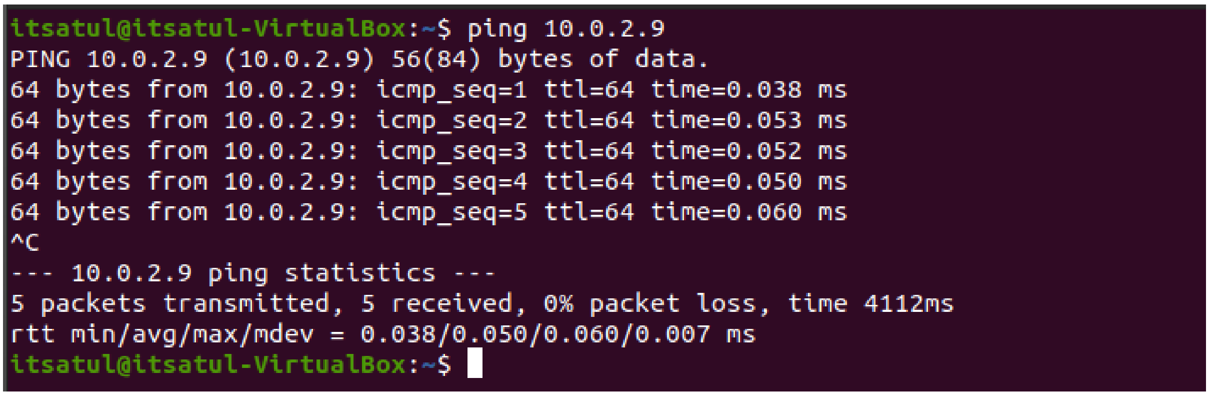
## Task 2: Ping PDU (Packet Data Units or Packets) Capture

**Step 1:** Assign an IP address to the system (Host).

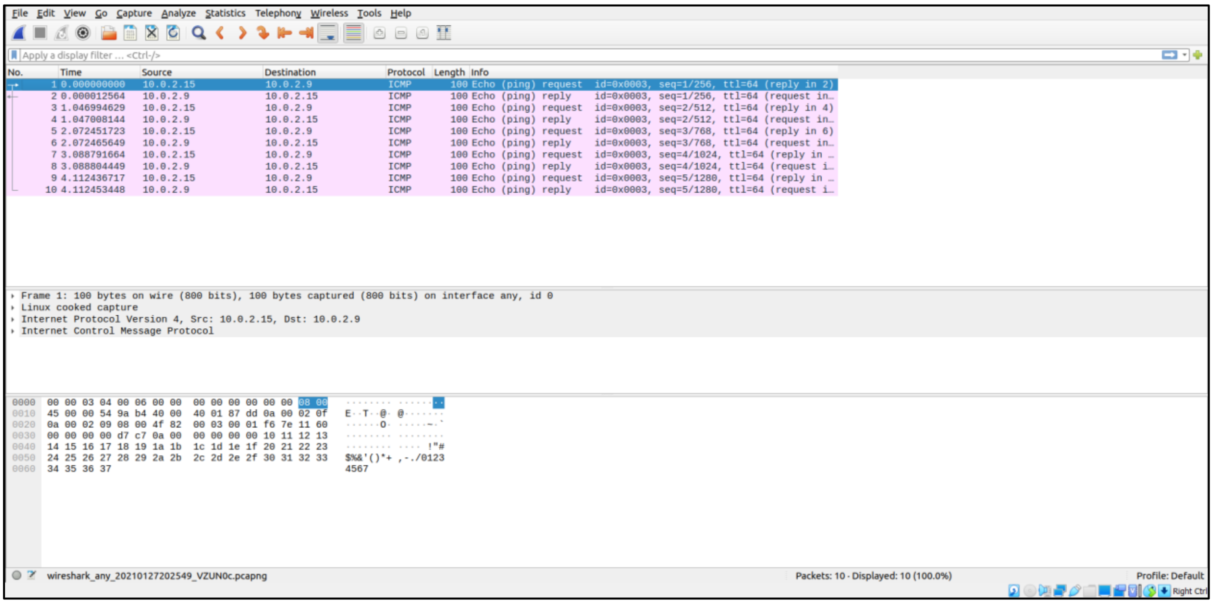
Note: IP address of your system should be 10.0.your_section.your_sno.

**Step 2:** Launch Wireshark and select ‘any’ interface

**Step 3:** In terminal, type **ping 10.0.your_section.your_sno**



```
itsatul@itsatul-VirtualBox:~$ ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 10.0.2.9: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 10.0.2.9: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 10.0.2.9: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from 10.0.2.9: icmp_seq=5 ttl=64 time=0.060 ms
^C
--- 10.0.2.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4112ms
rtt min/avg/max/mdev = 0.038/0.050/0.060/0.007 ms
itsatul@itsatul-VirtualBox:~$
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source      Destination  Protocol  Length  Info
    1 0.000000000   10.0.2.15   10.0.2.9     ICMP      100 Echo (ping) request  id=0x0003, seq=1/256, ttl=64 (reply in 2)
    2 0.000012564   10.0.2.9    10.0.2.15    ICMP      100 Echo (ping) reply    id=0x0003, seq=1/256, ttl=64 (request in…
    3 1.046994629   10.0.2.15   10.0.2.9     ICMP      100 Echo (ping) request  id=0x0003, seq=2/512, ttl=64 (reply in 4)
    4 1.047008144   10.0.2.9    10.0.2.15    ICMP      100 Echo (ping) reply    id=0x0003, seq=2/512, ttl=64 (request in…
    5 2.072451723   10.0.2.15   10.0.2.9     ICMP      100 Echo (ping) request  id=0x0003, seq=3/768, ttl=64 (reply in 6)
    6 2.072465649   10.0.2.9    10.0.2.15    ICMP      100 Echo (ping) reply    id=0x0003, seq=3/768, ttl=64 (request in…
    7 3.088791664   10.0.2.15   10.0.2.9     ICMP      100 Echo (ping) request  id=0x0003, seq=4/1024, ttl=64 (reply in …
    8 3.088804449   10.0.2.9    10.0.2.15    ICMP      100 Echo (ping) reply    id=0x0003, seq=4/1024, ttl=64 (request i…
    9 4.112436717   10.0.2.15   10.0.2.9     ICMP      100 Echo (ping) request  id=0x0003, seq=5/1280, ttl=64 (reply in …
   10 4.112453448   10.0.2.9    10.0.2.15    ICMP      100 Echo (ping) reply    id=0x0003, seq=5/1280, ttl=64 (request i…
```

```
› Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.9
› Internet Control Message Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 54 9a b4 40 00  40 01 87 dd 0a 00 02 0f   E··T··@· @·······
0020  0a 00 02 09 08 00 4f 82  00 03 00 01 f6 7e 11 60   ······O· ·····~·`
0030  00 00 00 00 d7 c7 0a 00  00 00 00 00 10 11 12 13   ········ ········
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ········ ···· !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567
```

```
wireshark_any_20210127202549_VZUN0c.pcapng          Packets: 10 · Displayed: 10 (100.0%)          Profile: Default
```

### Observations to be made

**Step 4:** Analyze the following in Terminal

- TTL - 64
- Protocol used by ping - ICMP
- Time – 4112 ms

**Step 5:** Analyze the following in Wireshark

On Packet List Pane, select the first echo packet on the list. On Packet Details Pane, click on each of the four “+” to expand the information. Analyze the frames with the first echo request and echo reply and complete the table below.

| Details | First Echo Request | First Echo Reply |
|---|---|---|
| Frame Number | 1 | 2 |
| Source IP address | 10.0.2.15 | 10.0.2.9 |
| Destination IP address | 10.0.2.9 | 10.0.2.15 |
| ICMP Type Value | 8 | 0 |
| ICMP Code Value | 0 | 0 |
| Source Ethernet Address | 00:00:00:00:00:00 | 00:00:00:00:00:00 |
| Destination Ethernet Address | 00:00:00:00:00:00 | 00:00:00:00:00:00 |
| Internet Protocol Version | 4 | 4 |
| Time To Live (TTL) Value | 64 | 64 |

## Task 3: HTTP PDU Capture

### Using Wireshark’s Filter feature

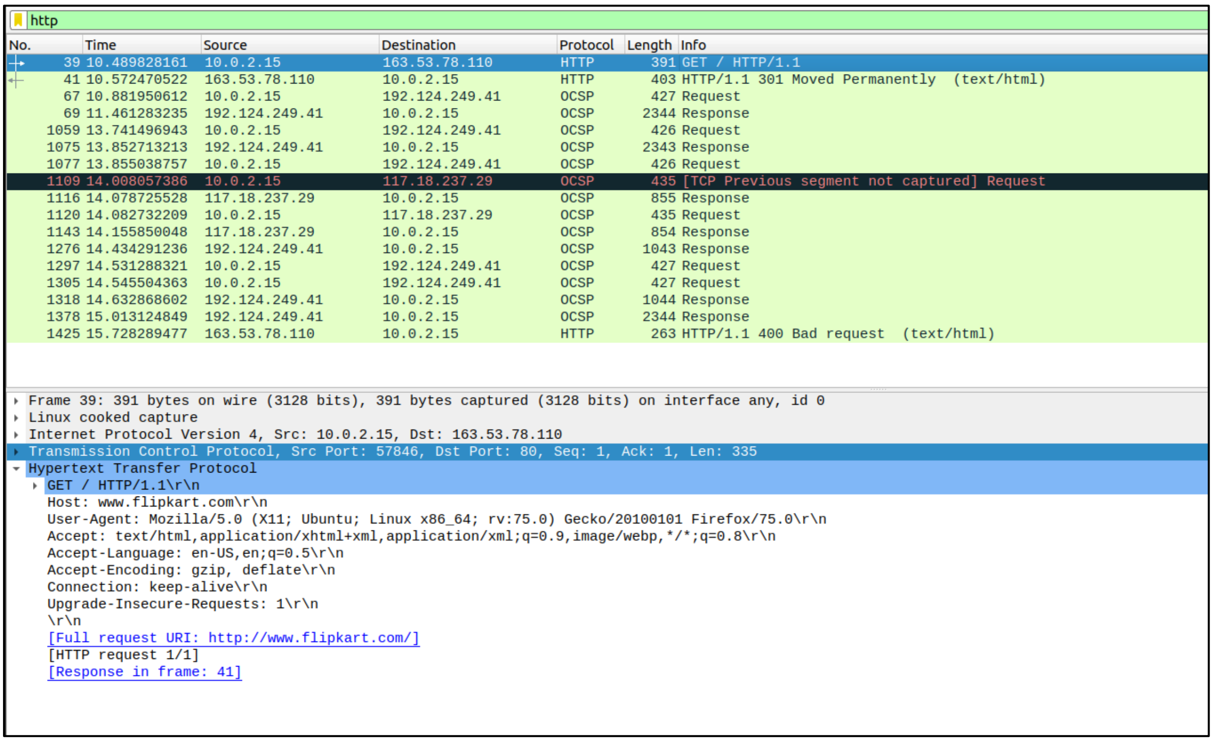
**Step 1:** Launch Wireshark and select ‘any’ interface. On the Filter toolbar, type-in ‘http’ and press enter

**Step 2:** Open Firefox browser, and browse www.flipkart.com

### Observations to be made

**Step 3:** Analyze the first (interaction of host to the web server) and second frame (response of server to the client). By analyzing the filtered frames, complete the table below:

| Details | First Echo Request | First Echo Reply |
|---|---|---|
| Frame Number | 39 | 41 |
| Source Port | 57846 | 80 |
| Destination Port | 80 | 57846 |
| Source IP address | 10.0.2.15 | 163.53.78.110 |
| Destination IP address | 163.53.78.110 | 10.0.2.15 |
| Source Ethernet Address | PesCompu_34:8c:be<br>(08:00:27:34:8c:be) | RealtekU_12:35:02<br>(52:54:00:12:35:02) |
| Destination Ethernet Address | RealtekU_12:35:02<br>(52:54:00:12:35:02) | PesCompu_34:8c:be<br>(08:00:27:34:8c:be) |



```
http
No.     Time         Source          Destination     Protocol Length Info
     39 10.489828161 10.0.2.15       163.53.78.110   HTTP      391 GET / HTTP/1.1
     41 10.572470522 163.53.78.110   10.0.2.15       HTTP      403 HTTP/1.1 301 Moved Permanently  (text/html)
     67 10.881950612 10.0.2.15       192.124.249.41  OCSP      427 Request
     69 11.461283235 192.124.249.41  10.0.2.15       OCSP     2344 Response
   1059 13.741496943 10.0.2.15       192.124.249.41  OCSP      426 Request
   1075 13.852713213 192.124.249.41  10.0.2.15       OCSP     2343 Response
   1077 13.855038757 10.0.2.15       192.124.249.41  OCSP      426 Request
   1109 14.008057386 10.0.2.15       117.18.237.29   OCSP      435 [TCP Previous segment not captured] Request
   1116 14.078725528 117.18.237.29   10.0.2.15       OCSP      855 Response
   1120 14.082732209 10.0.2.15       117.18.237.29   OCSP      435 Request
   1143 14.155850048 117.18.237.29   10.0.2.15       OCSP      854 Response
   1276 14.434291236 192.124.249.41  10.0.2.15       OCSP     1043 Response
   1297 14.531288321 10.0.2.15       192.124.249.41  OCSP      427 Request
   1305 14.545504363 10.0.2.15       192.124.249.41  OCSP      427 Request
   1318 14.632868602 192.124.249.41  10.0.2.15       OCSP     1044 Response
   1378 15.013124849 192.124.249.41  10.0.2.15       OCSP     2344 Response
   1425 15.728289477 163.53.78.110   10.0.2.15       HTTP      263 HTTP/1.1 400 Bad request  (text/html)

▸ Frame 39: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 163.53.78.110
▸ Transmission Control Protocol, Src Port: 57846, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.flipkart.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.flipkart.com/]
    [HTTP request 1/1]
    [Response in frame: 41]
```

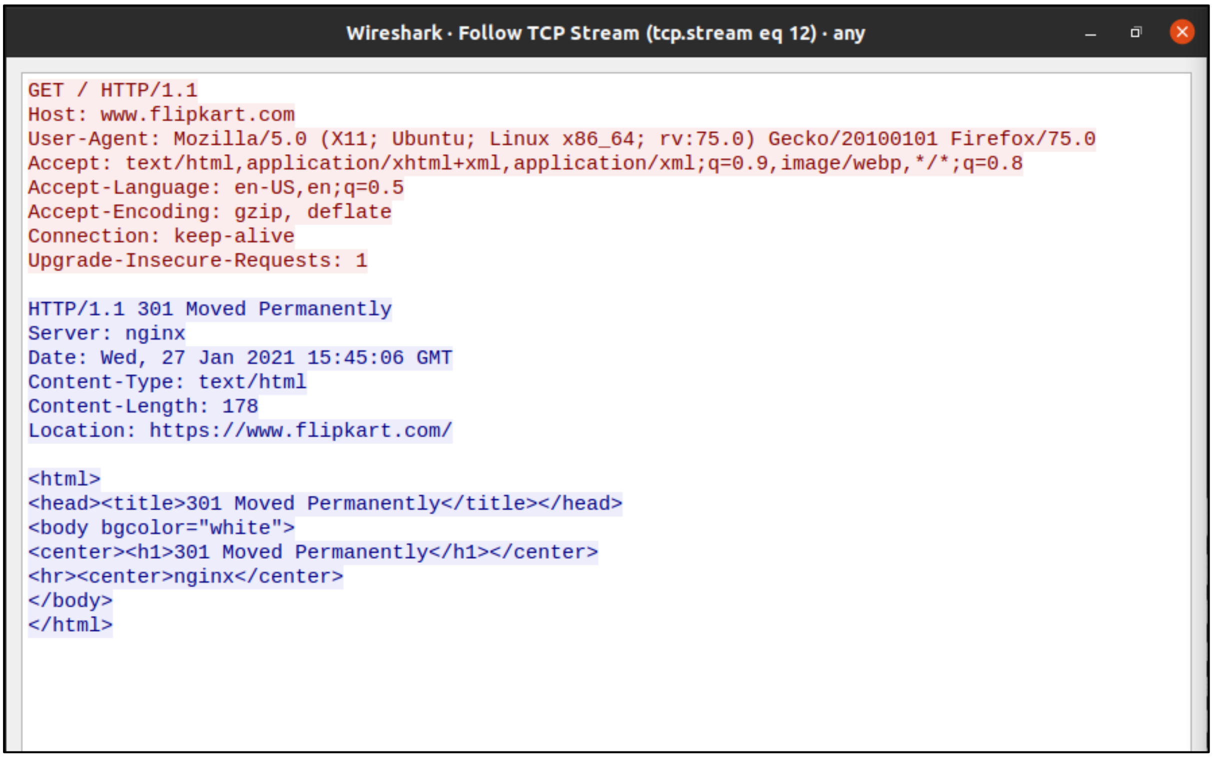
**Step 4:** Analyze the HTTP request and response and complete the table below.

| HTTP Request | | HTTP Response | |
|---|---|---|---|
| Get | GET/HTTP/1.1 | Server | nginx |
| Host | www.flipkart.com | Content-Type | text/html |
| User-Agent | Mozilla/5.0 | Date | Wed, 27 Jan 2021 |
| Accept-Language | en-US | Location | https://www.flipkart.com/ |
| Accept-Encoding | gzip | Content-Length | 178 |
| Connection | keep-alive | Connection | |

## Using Wireshark's Follow TCP Stream

**Step 1:** Make sure the filter is blank. Right-click any packet inside the Packet List Pane, then select 'Follow TCP Stream'. For demo purpose, a packet containing the HTTP GET request "GET / HTTP / 1.1" can be selected.

Step 2: Upon following a TCP stream, screenshot the whole window.

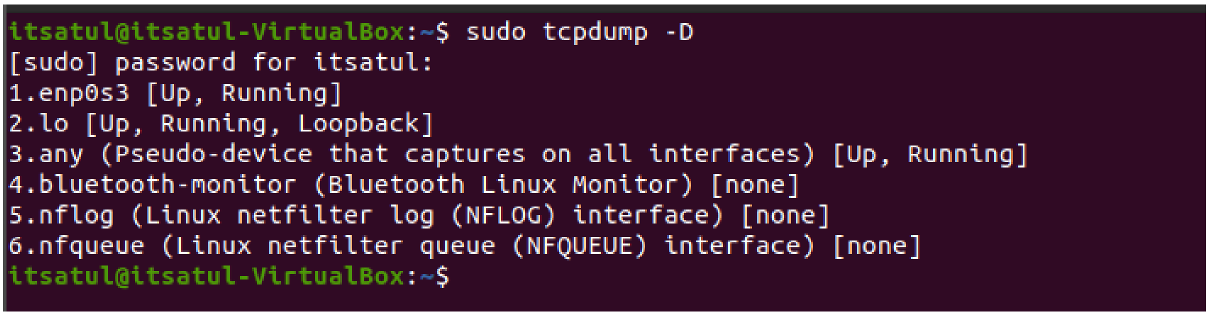


```
GET / HTTP/1.1
Host: www.flipkart.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 27 Jan 2021 15:45:06 GMT
Content-Type: text/html
Content-Length: 178
Location: https://www.flipkart.com/

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

## Task 4: Capturing packets with tcpdump

**Step 1:** Use the command **tcpdump -D** to see which interfaces are available for capture.

**sudo tcpdump -D**

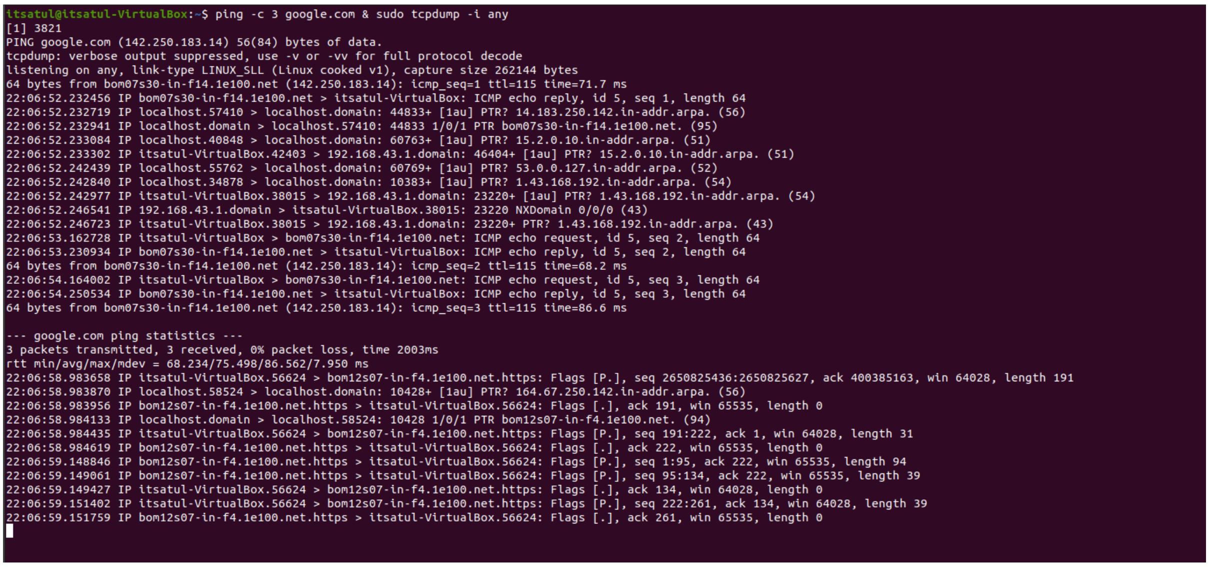


```
itsatul@itsatul-VirtualBox:~$ sudo tcpdump -D
[sudo] password for itsatul:
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
itsatul@itsatul-VirtualBox:~$
```

**Step 2:** Capture all packets in any interface by running this command:

**sudo tcpdump -i any**

Note: Perform some pinging operation while giving above command. Also type www.google.com in browser.



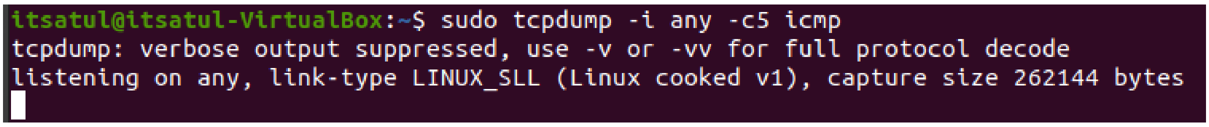
```
itsatul@itsatul-VirtualBox:~$ ping -c 3 google.com & sudo tcpdump -i any
[1] 3821
PING google.com (142.250.183.14) 56(84) bytes of data.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
64 bytes from bom07s30-in-f14.1e100.net (142.250.183.14): icmp_seq=1 ttl=115 time=71.7 ms
22:06:52.232456 IP bom07s30-in-f14.1e100.net > itsatul-VirtualBox: ICMP echo reply, id 5, seq 1, length 64
22:06:52.232719 IP localhost.57410 > localhost.domain: 44833+ [1au] PTR? 14.183.250.142.in-addr.arpa. (56)
22:06:52.232941 IP localhost.domain > localhost.57410: 44833 1/0/1 PTR bom07s30-in-f14.1e100.net. (95)
22:06:52.233084 IP localhost.40848 > localhost.domain: 60763+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
22:06:52.233302 IP itsatul-VirtualBox.42403 > 192.168.43.1.domain: 46404+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
22:06:52.242439 IP localhost.55762 > localhost.domain: 60769+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
22:06:52.242840 IP localhost.34878 > localhost.domain: 10383+ [1au] PTR? 1.43.168.192.in-addr.arpa. (54)
22:06:52.242977 IP itsatul-VirtualBox.38015 > 192.168.43.1.domain: 23220+ [1au] PTR? 1.43.168.192.in-addr.arpa. (54)
22:06:52.246541 IP 192.168.43.1.domain > itsatul-VirtualBox.38015: 23220 NXDomain 0/0/0 (43)
22:06:52.246723 IP itsatul-VirtualBox.38015 > 192.168.43.1.domain: 23220+ PTR? 1.43.168.192.in-addr.arpa. (43)
22:06:53.162728 IP itsatul-VirtualBox > bom07s30-in-f14.1e100.net: ICMP echo request, id 5, seq 2, length 64
22:06:53.230934 IP bom07s30-in-f14.1e100.net > itsatul-VirtualBox: ICMP echo reply, id 5, seq 2, length 64
64 bytes from bom07s30-in-f14.1e100.net (142.250.183.14): icmp_seq=2 ttl=115 time=68.2 ms
22:06:54.164002 IP itsatul-VirtualBox > bom07s30-in-f14.1e100.net: ICMP echo request, id 5, seq 3, length 64
22:06:54.250534 IP bom07s30-in-f14.1e100.net > itsatul-VirtualBox: ICMP echo reply, id 5, seq 3, length 64
64 bytes from bom07s30-in-f14.1e100.net (142.250.183.14): icmp_seq=3 ttl=115 time=86.6 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 68.234/75.498/86.562/7.950 ms
22:06:58.983658 IP itsatul-VirtualBox.56624 > bom12s07-in-f4.1e100.net.https: Flags [P.], seq 2650825436:2650825627, ack 400385163, win 64028, length 191
22:06:58.983870 IP localhost.58524 > localhost.domain: 10428+ [1au] PTR? 164.67.250.142.in-addr.arpa. (56)
22:06:58.983956 IP bom12s07-in-f4.1e100.net.https > itsatul-VirtualBox.56624: Flags [.], ack 191, win 65535, length 0
22:06:58.984133 IP localhost.domain > localhost.58524: 10428 1/0/1 PTR bom12s07-in-f4.1e100.net. (94)
22:06:58.984435 IP itsatul-VirtualBox.56624 > bom12s07-in-f4.1e100.net.https: Flags [P.], seq 191:222, ack 1, win 64028, length 31
22:06:58.984619 IP bom12s07-in-f4.1e100.net.https > itsatul-VirtualBox.56624: Flags [.], ack 222, win 65535, length 0
22:06:59.148846 IP bom12s07-in-f4.1e100.net.https > itsatul-VirtualBox.56624: Flags [P.], seq 1:95, ack 222, win 65535, length 94
22:06:59.149061 IP bom12s07-in-f4.1e100.net.https > itsatul-VirtualBox.56624: Flags [P.], seq 95:134, ack 222, win 65535, length 39
22:06:59.149427 IP itsatul-VirtualBox.56624 > bom12s07-in-f4.1e100.net.https: Flags [.], ack 134, win 64028, length 0
22:06:59.151402 IP itsatul-VirtualBox.56624 > bom12s07-in-f4.1e100.net.https: Flags [P.], seq 222:261, ack 134, win 64028, length 39
22:06:59.151759 IP bom12s07-in-f4.1e100.net.https > itsatul-VirtualBox.56624: Flags [.], ack 261, win 65535, length 0
```

### Observation

**Step 3:** Understand the output format.

**Step 4:** To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets only by using this command:

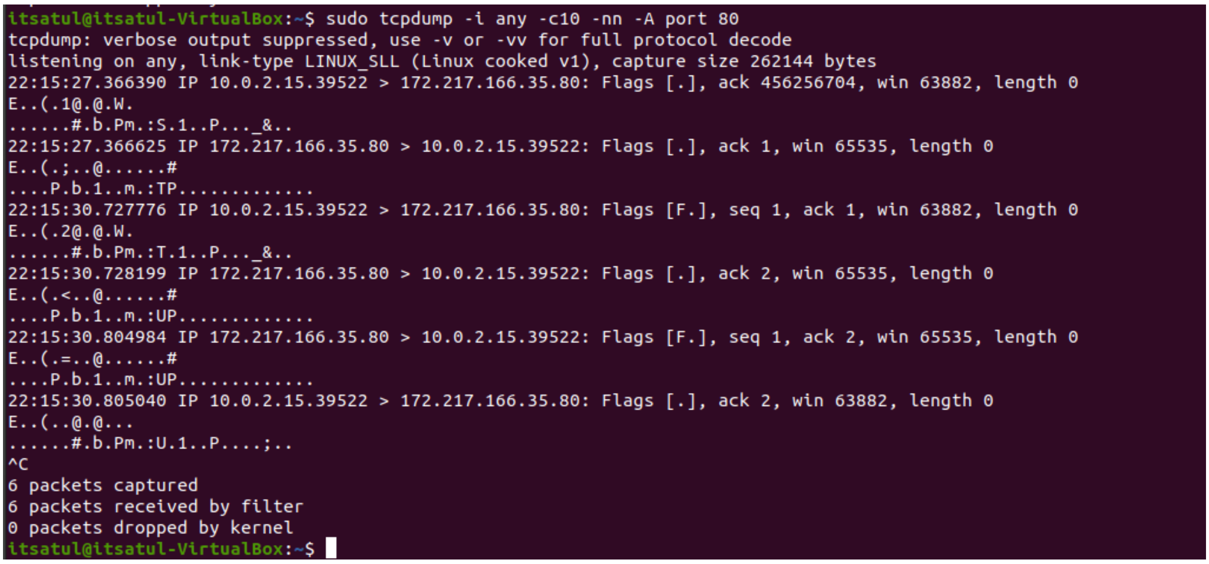
**sudo tcpdump -i any -c5 icmp**



```
itsatul@itsatul-VirtualBox:~$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
```

**Step 5:** Check the packet content. For example, inspect the HTTP content of a web request like this:

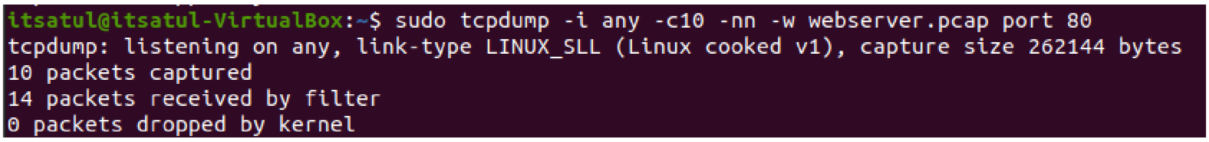
**sudo tcpdump -i any -c10 -nn -A port 80**



```
itsatul@itsatul-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
22:15:27.366390 IP 10.0.2.15.39522 > 172.217.166.35.80: Flags [.], ack 456256704, win 63882, length 0
E..(.1@.@.W.
......#.b.Pm.:S.1..P..._&..
22:15:27.366625 IP 172.217.166.35.80 > 10.0.2.15.39522: Flags [.], ack 1, win 65535, length 0
E..(.;..@......#
....P.b.1..m.:TP.............
22:15:30.727776 IP 10.0.2.15.39522 > 172.217.166.35.80: Flags [F.], seq 1, ack 1, win 63882, length 0
E..(.2@.@.W.
......#.b.Pm.:T.1..P..._&..
22:15:30.728199 IP 172.217.166.35.80 > 10.0.2.15.39522: Flags [.], ack 2, win 65535, length 0
E..(.<..@......#
....P.b.1..m.:UP.............
22:15:30.804984 IP 172.217.166.35.80 > 10.0.2.15.39522: Flags [F.], seq 1, ack 2, win 65535, length 0
E..(.=..@......#
....P.b.1..m.:UP.............
22:15:30.805040 IP 10.0.2.15.39522 > 172.217.166.35.80: Flags [.], ack 2, win 63882, length 0
E..(..@.@...
......#.b.Pm.:U.1..P....;..
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
itsatul@itsatul-VirtualBox:~$
```

**Step 6:** To save packets to a file instead of displaying them on screen, use the option -w:

**sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80**

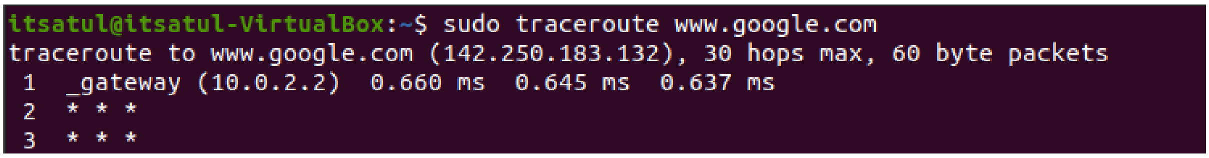


```
itsatul@itsatul-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
14 packets received by filter
0 packets dropped by kernel
```

## Task 5: Perform Traceroute checks

**Step 1:** Run the traceroute using the following command.

**sudo traceroute [www.google.com](http://www.google.com)**



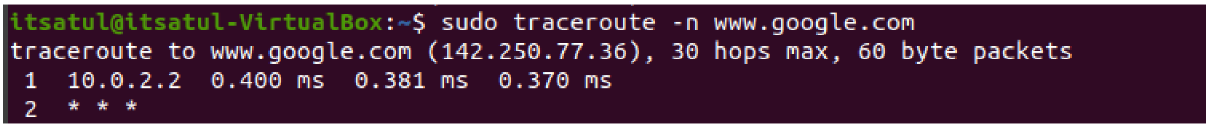
```
itsatul@itsatul-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.183.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.660 ms  0.645 ms  0.637 ms
 2  * * *
 3  * * *
```

**Step 2:** Analyze destination address of google.com and no. of hops

The destination address is **142.250.183.132** and there were **30 hops**.

**Step 3:** To speed up the process, you can disable the mapping of IP addresses with hostnames by using the -*n* option

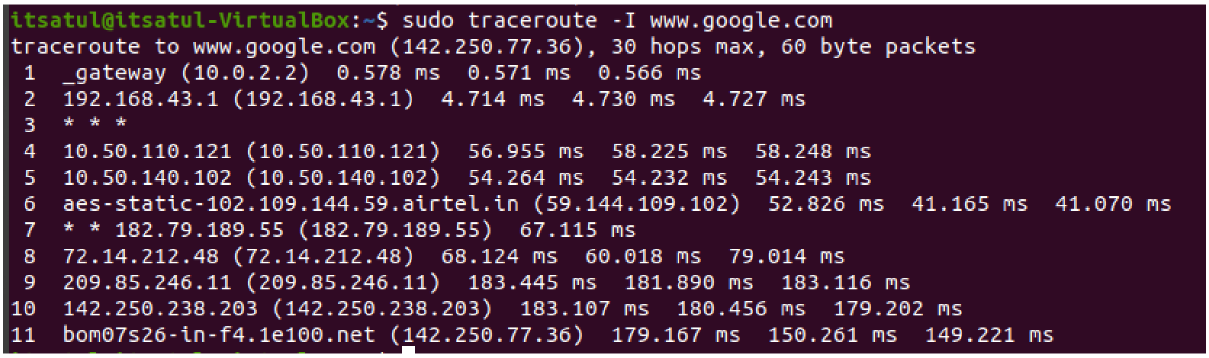
**sudo traceroute -n [www.google.com](http://www.google.com)**



```
itsatul@itsatul-VirtualBox:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.77.36), 30 hops max, 60 byte packets
 1  10.0.2.2  0.400 ms  0.381 ms  0.370 ms
 2  * * *
```

**Step 4:** The -I option is necessary so that the traceroute uses ICMP.

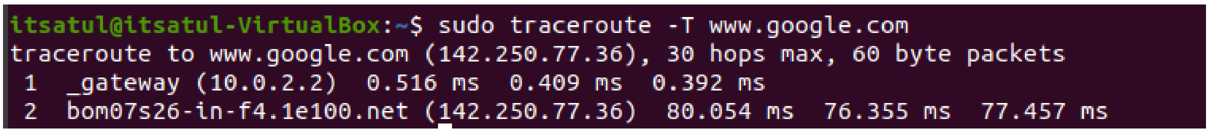
**sudo traceroute -I [www.google.com](http://www.google.com)**



```
itsatul@itsatul-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.77.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.578 ms  0.571 ms  0.566 ms
 2  192.168.43.1 (192.168.43.1)  4.714 ms  4.730 ms  4.727 ms
 3  * * *
 4  10.50.110.121 (10.50.110.121)  56.955 ms  58.225 ms  58.248 ms
 5  10.50.140.102 (10.50.140.102)  54.264 ms  54.232 ms  54.243 ms
 6  aes-static-102.109.144.59.airtel.in (59.144.109.102)  52.826 ms  41.165 ms  41.070 ms
 7  * * 182.79.189.55 (182.79.189.55)  67.115 ms
 8  72.14.212.48 (72.14.212.48)  68.124 ms  60.018 ms  79.014 ms
 9  209.85.246.11 (209.85.246.11)  183.445 ms  181.890 ms  183.116 ms
10  142.250.238.203 (142.250.238.203)  183.107 ms  180.456 ms  179.202 ms
11  bom07s26-in-f4.1e100.net (142.250.77.36)  179.167 ms  150.261 ms  149.221 ms
```

**Step 5:** By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag.

**sudo traceroute -T [www.google.com](http://www.google.com)**

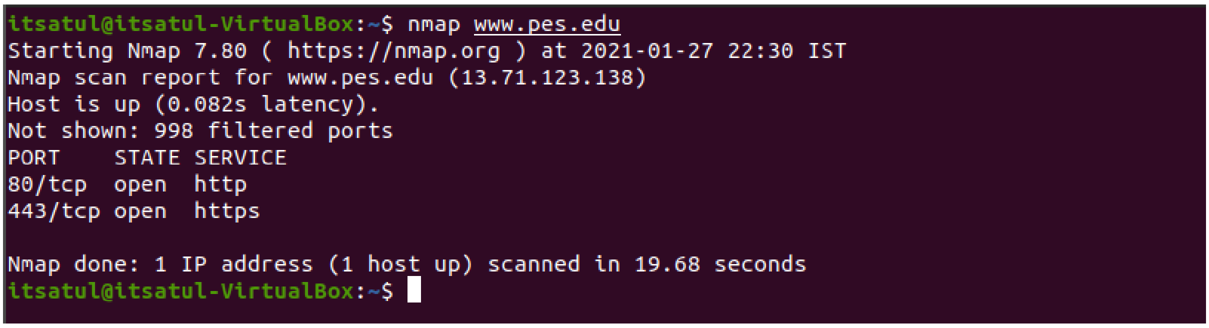


```
itsatul@itsatul-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.77.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.516 ms  0.409 ms  0.392 ms
 2  bom07s26-in-f4.1e100.net (142.250.77.36)  80.054 ms  76.355 ms  77.457 ms
```

## Task 6: Explore an entire network for information (Nmap)

**Step 1:** You can scan a host using its host name or IP address, for instance.

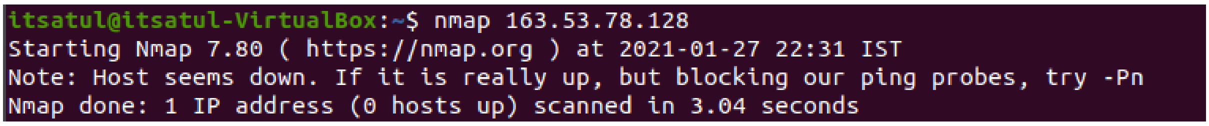
**nmap [www.pes.edu](http://www.pes.edu)**



```
itsatul@itsatul-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-27 22:30 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.082s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 19.68 seconds
itsatul@itsatul-VirtualBox:~$ 
```

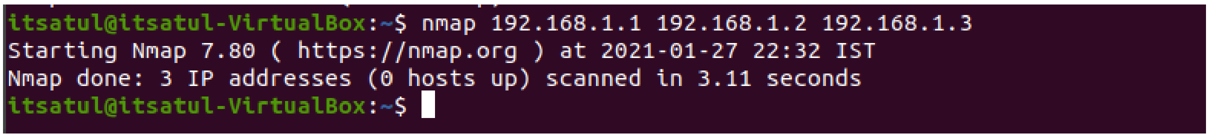
**Step 2:** Alternatively, use an IP address to scan.

**nmap 163.53.78.128**



```
itsatul@itsatul-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-27 22:31 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
```

**Step 3:** Scan multiple IP address or subnet (IPv4) **nmap 192.168.1.1 192.168.1.2 192.168.1.3**



```
itsatul@itsatul-VirtualBox:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-27 22:32 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.11 seconds
itsatul@itsatul-VirtualBox:~$ 
```