PES UNIVERSITY

EC CAMPUS, BANGALORE

NAME RICHA ANGADI

SRN PES2201800111

WEEK 1

SUBJECT COMPUTER NETWORK LABORATORY

OBJECTIVE STUDY AND UNDERSTAND THE BASIC NETWORKING TOOLS - WIRESHARK, TCPDUMP, PING, TRACEROUTE AND NETCAT.

TASK 1: LINUX INTERFACE CONFIGURATION (IFCONFIG / IP COMMAND)

Step 1: To display status of all active network interfaces

```
richa@richa-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 08:00:27:73:c4:03 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 69499sec preferred_lft 69499sec
    inet6 fe80::384e:49ff:3e6e:4088/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

INTERFACE NAME	IP ADDRESS (IPV4/IPV6)	MAC ADDRESS
lo	IPV4: 127.0.0.1/8 IPV6: 1/128	00:00:00:00:00:00
enp0s3	IPV4:10.0.2.15/24 IPV6: fe80::384e:49ff:3e6e:4088/64	08:00:27:73:c4:03

Step 2: To assign an IP address to an interface

```
richa@richa-VirtualBox:~$ sudo ifconfig enp0s3 10.0.4.17 netmask 255.255.255.0
[sudo] password for richa:
```

Step 3: To activate / deactivate a network interface

```
richa@richa-VirtualBox:~$ sudo ifconfig enp0s3 up
[sudo] password for richa:
richa@richa-VirtualBox:~$ sudo ifconfig lo up
```

Step 4: To show the current neighbor table in kernel

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

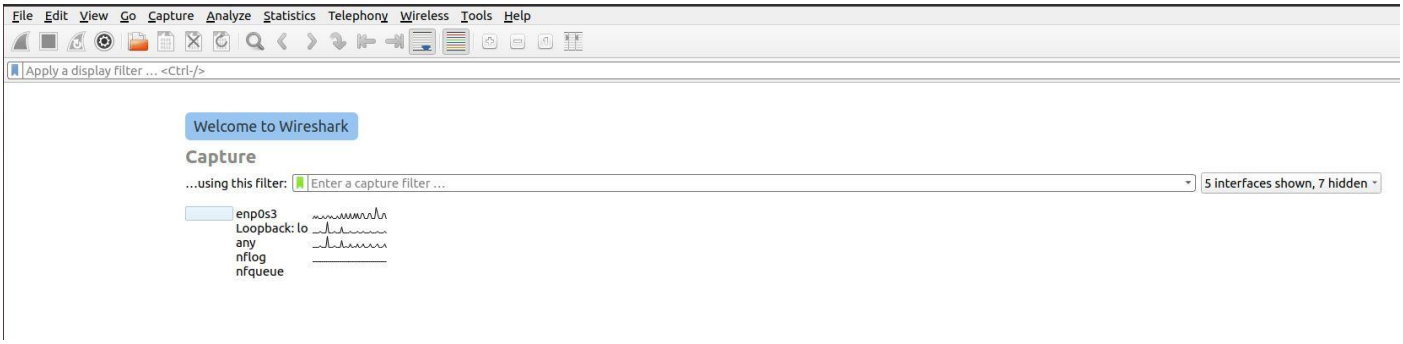
Shows neighbour objects as REACHABLE

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.

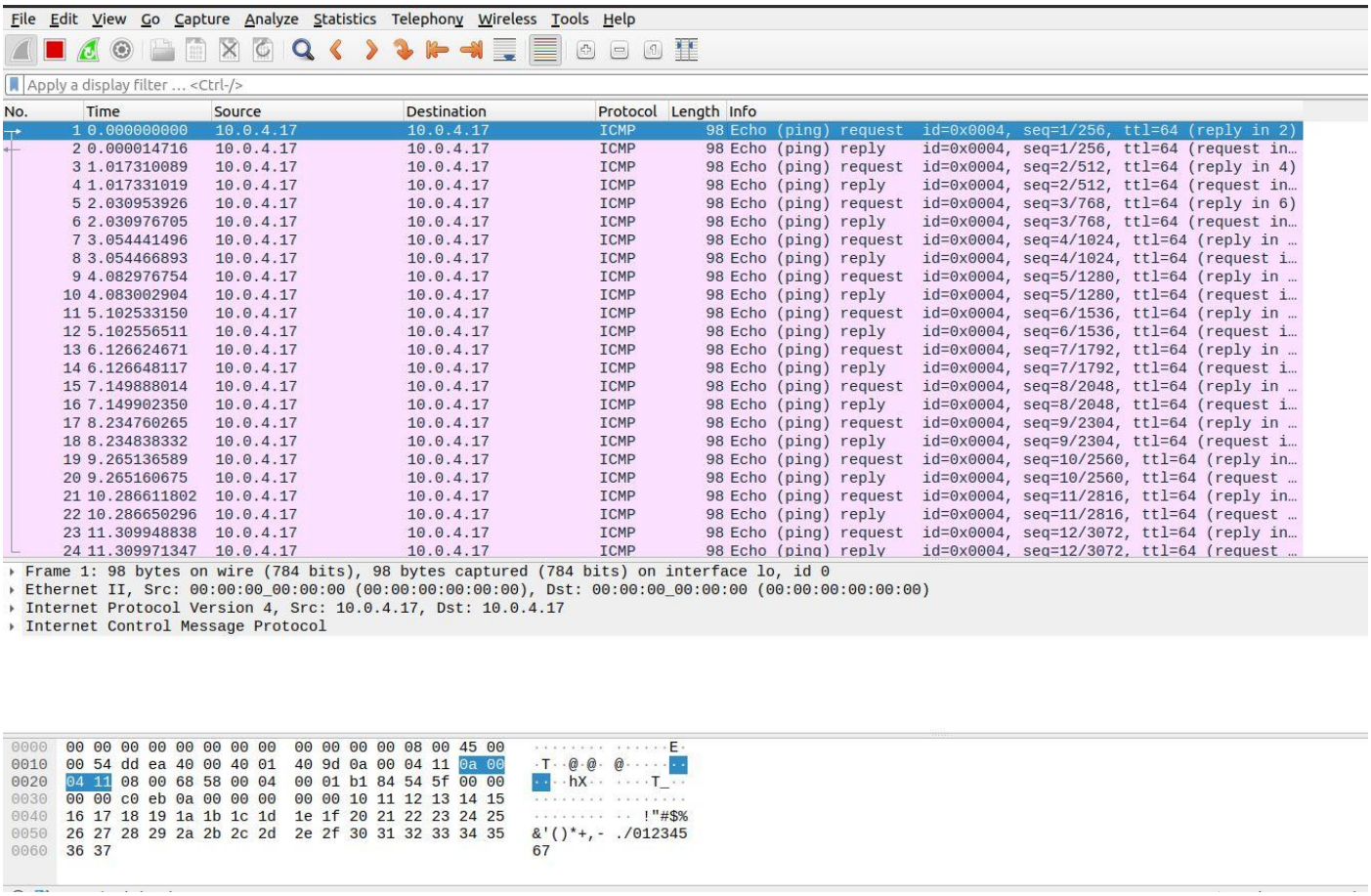
Step 2: Launch Wireshark and select ‘any’ interface



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

```
richa@richa-VirtualBox:~$ ping 10.0.4.17
PING 10.0.4.17 (10.0.4.17) 56(84) bytes of data.
64 bytes from 10.0.4.17: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 10.0.4.17: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 10.0.4.17: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 10.0.4.17: icmp_seq=4 ttl=64 time=0.045 ms
64 bytes from 10.0.4.17: icmp_seq=5 ttl=64 time=0.047 ms
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 0.030/0.048/0.062/0.011 ms
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 2)
2	0.000014716	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=1/256, ttl=64 (request in…
3	1.017310089	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 4)
4	1.017331019	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=2/512, ttl=64 (request in…
5	2.030953926	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 6)
6	2.030976705	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=3/768, ttl=64 (request in…
7	3.054441496	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (reply in …
8	3.054466893	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=4/1024, ttl=64 (request i…
9	4.082976754	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=64 (reply in …
10	4.083002904	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=5/1280, ttl=64 (request i…
11	5.102533150	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=64 (reply in …
12	5.102556511	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=6/1536, ttl=64 (request i…
13	6.126624671	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792, ttl=64 (reply in …
14	6.126648117	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=7/1792, ttl=64 (request i…
15	7.149888014	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048, ttl=64 (reply in …
16	7.149902350	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=8/2048, ttl=64 (request i…
17	8.234760265	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=9/2304, ttl=64 (reply in …
18	8.234838332	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=9/2304, ttl=64 (request i…
19	9.265136589	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=10/2560, ttl=64 (reply in…
20	9.265160675	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=10/2560, ttl=64 (request …
21	10.286611802	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=11/2816, ttl=64 (reply in…
22	10.286650296	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=11/2816, ttl=64 (request …
23	11.309948838	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) request id=0x0004, seq=12/3072, ttl=64 (reply in…
24	11.309971347	10.0.4.17	10.0.4.17	ICMP	98	Echo (ping) reply id=0x0004, seq=12/3072, ttl=64 (request …

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 10.0.4.17, Dst: 10.0.4.17
▸ Internet Control Message Protocol
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  00 54 dd ea 40 00 40 01  40 9d 0a 00 04 11 0a 00   ·T··@·@· @·······
0020  04 11 08 00 68 58 00 04  00 01 b1 84 54 5f 00 00   ····hX·· ····T_··
0030  00 00 c0 eb 0a 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

OBSERVATIONS TO BE MADE

Step 4: Analyse the following in Terminal

• **TTL** - 64

• **PROTOCOL USED BY PING** - ICMP

• **TIME** - 4081ms

Step 5: Analyse the following in Wireshark

Details	**First Echo Request**	**First Echo Reply**
Frame Number	1	2
Source IP address	10.0.4.17	10.0.4.17
Destination IP address	10.0.4.17	10.0.4.17
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

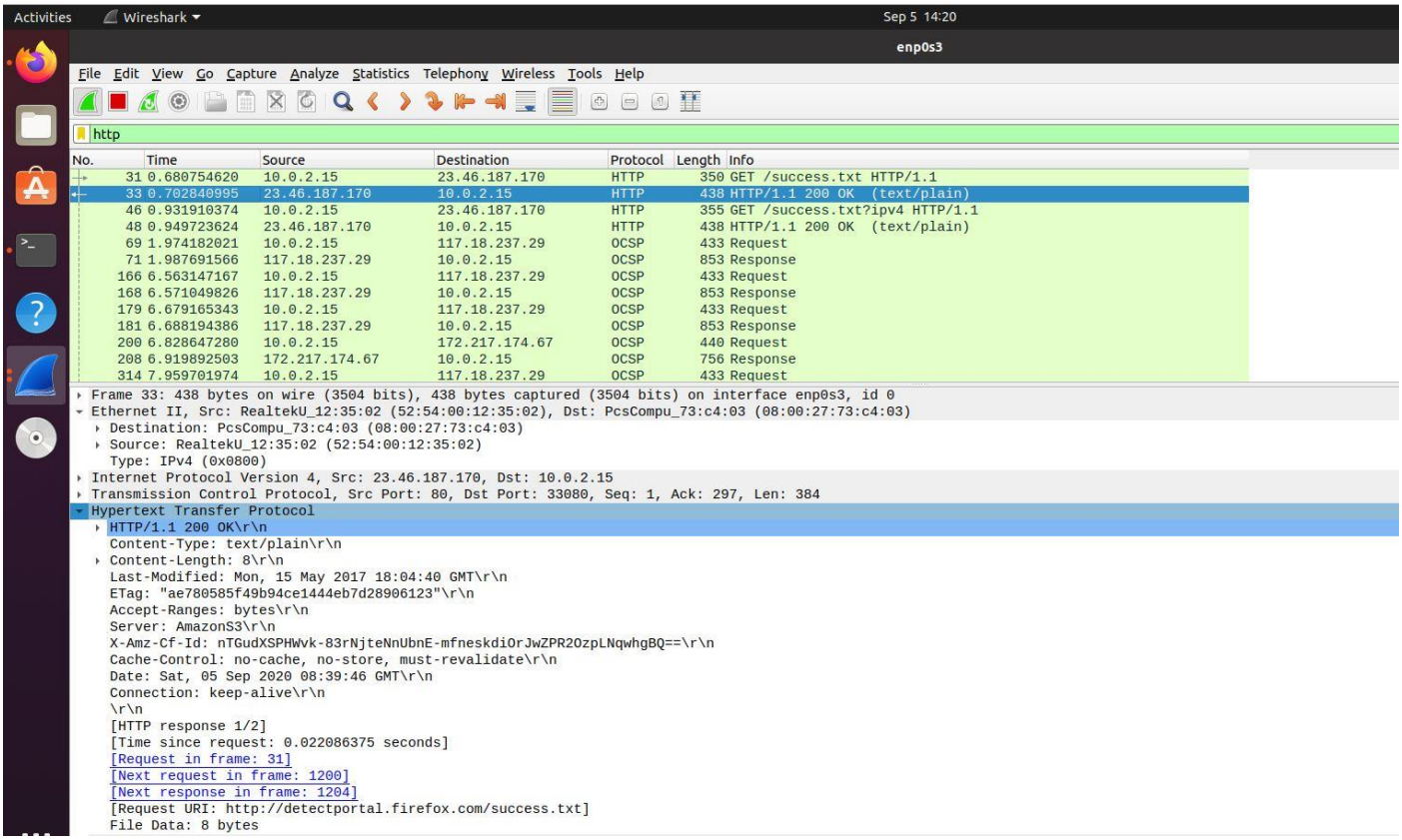
Step 1: Launch Wireshark and select 'any' interface. On the Filter toolbar, type-in 'http' and press enter

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	31	33
Source IP address	10.0.2.15	23.46.187.17
Destination IP address	23.46.187.17	10.0.2.15
ICMP Type Value	IPv4	IPv4
ICMP Code Value	0x800	0x800
Source Ethernet Address	PcsCompu_73:c4:03 (08:00:27:c4:03)	RealtekU_12:35:02 (52:54:00:12:35:02)
Destination Ethernet Address	RealtekU_12:35:02 (52:54:00:12:35:02)	PcsCompu_73:c4:03 (08:00:27:c4:03)
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64



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

HTTP Request		**HTTP Response**	
Get	GET / HTTP / 1.1	**Server**	Apache (ubuntu)
Host	connectivity-check.ubuntu.com	**Content-Type**	text/plain
User-Agent	Mozilla (Ubuntu)	**Date**	Sat, 05 Sept 2020
Accept-Language	/*	**Location**	
Accept-Encoding	*	**Content-Length**	8\r\n
Connection	close	**Connection**	keep-alive\r\n

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.

TASK 4: CAPTURING PACKETS WITH TCPDUMP

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

sudo tcpdump -D

```
richa@richa-VirtualBox:~$ sudo tcpdump -D
[sudo] password for richa:
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]
richa@richa-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.

OBSERVATION

Step 3: Understand the output format.

Capture all packets in any interface by running this command:

```
richa@richa-VirtualBox:~$ ping -c 6 google.com & sudo tcpdump -i any
[1] 2690
PING google.com (216.58.203.174) 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 bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=1 ttl=119 time=102 ms
14:27:34.052891 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 1, length 64
14:27:34.053556 IP localhost.55829 > localhost.domain: 7060+ [1au] PTR? 174.203.58.216.in-addr.arpa. (56)
14:27:34.054217 IP richa-VirtualBox.40297 > 192.168.0.1.domain: 28369+ [1au] PTR? 174.203.58.216.in-addr.arpa. (56)
14:27:34.056627 IP localhost.37439 > localhost.domain: 58129+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
14:27:34.057112 IP richa-VirtualBox.53904 > 192.168.0.1.domain: 679+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
14:27:34.061324 IP 192.168.0.1.domain > richa-VirtualBox.40297: 28369 1/0/1 PTR bom07s11-in-f14.1e100.net. (95)
14:27:34.070420 IP localhost.36863 > localhost.domain: 25840+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
14:27:34.957273 IP richa-VirtualBox > bom07s11-in-f14.1e100.net: ICMP echo request, id 1, seq 2, length 64
64 bytes from bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=2 ttl=119 time=27.1 ms
14:27:34.984288 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 2, length 64
14:27:35.958844 IP richa-VirtualBox > bom07s11-in-f14.1e100.net: ICMP echo request, id 1, seq 3, length 64
14:27:35.987995 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 3, length 64
64 bytes from bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=3 ttl=119 time=29.2 ms
14:27:36.976275 IP richa-VirtualBox > bom07s11-in-f14.1e100.net: ICMP echo request, id 1, seq 4, length 64
64 bytes from bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=4 ttl=119 time=24.9 ms
14:27:37.001143 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 4, length 64
14:27:37.975702 IP richa-VirtualBox > bom07s11-in-f14.1e100.net: ICMP echo request, id 1, seq 5, length 64
14:27:38.000851 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 5, length 64
64 bytes from bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=5 ttl=119 time=25.2 ms
14:27:39.000227 IP richa-VirtualBox > bom07s11-in-f14.1e100.net: ICMP echo request, id 1, seq 6, length 64
14:27:39.025378 IP bom07s11-in-f14.1e100.net > richa-VirtualBox: ICMP echo reply, id 1, seq 6, length 64
64 bytes from bom07s11-in-f14.1e100.net (216.58.203.174): icmp_seq=6 ttl=119 time=25.3 ms

--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5049ms
rtt min/avg/max/mdev = 24.911/38.974/102.196/28.312 ms
14:27:39.087908 ARP, Request who-has _gateway tell richa-VirtualBox, length 28
14:27:39.088292 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
14:27:39.088600 IP localhost.49496 > localhost.domain: 7948+ [1au] PTR? 2.2.0.10.in-addr.arpa. (50)
14:27:39.089101 IP richa-VirtualBox.36286 > 192.168.0.1.domain: 24028+ [1au] PTR? 2.2.0.10.in-addr.arpa. (50)
14:27:39.094396 IP 192.168.0.1.domain > richa-VirtualBox.36286: 24028 NXDomain 0/1/1 (99)
14:27:39.094889 IP richa-VirtualBox.36286 > 192.168.0.1.domain: 24028+ PTR? 2.2.0.10.in-addr.arpa. (39)
14:27:39.100237 IP 192.168.0.1.domain > richa-VirtualBox.36286: 24028 NXDomain 0/1/0 (88)
```

Listen, report the list of link-layer types, report the list of time stamp types, or report the results of compiling a filter expression on interface.

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

```
richa@richa-VirtualBox:~$ sudo tcpdump -i any -c5 icmp -v
tcpdump: 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

```
373 packets captured
538 packets received by filter
93 packets dropped by kernel
richa@richa-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
14:33:27.664193 IP richa-VirtualBox > 10.0.4.17: ICMP echo request, id 2, seq 65, length 64
14:33:28.700987 IP richa-VirtualBox > 10.0.4.17: ICMP echo request, id 2, seq 66, length 64
14:33:29.712116 IP richa-VirtualBox > 10.0.4.17: ICMP echo request, id 2, seq 67, length 64
14:33:30.736583 IP richa-VirtualBox > 10.0.4.17: ICMP echo request, id 2, seq 68, length 64
14:33:31.760002 IP richa-VirtualBox > 10.0.4.17: ICMP echo request, id 2, seq 69, length 64
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

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

```
richa@richa-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
14:34:53.729495 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [S], seq 3427877449, win 64240, options [mss 1460,sackOK,TS val 2582518016 ecr 0,nop,wscale 7], length 0
E..<..@.@..2
...#.c....P.QBI..................
............
14:34:54.028898 IP 35.224.99.156.80 > 10.0.2.15.41244: Flags [S.], seq 196416001, ack 3427877450, win 65535, options [mss 1460], length 0
E..,....@..`#.c.
....P.......QBJ`...6.........
14:34:54.029071 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [.], ack 1, win 64240, length 0
E..(..@.@..E
...#.c....P.QBJ....P.......
14:34:54.029564 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1.1
E.....@.@...
...#.c....P.QBJ....P.......GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
Connection: close


14:34:54.030535 IP 35.224.99.156.80 > 10.0.2.15.41244: Flags [.], ack 88, win 65535, length 0
E..(....@..c#.c.
....P.......QB.P...N3........
14:34:54.321273 IP 35.224.99.156.80 > 10.0.2.15.41244: Flags [P.], seq 1:149, ack 88, win 65535, length 148: HTTP: HTTP/1.1 204 No Content
E.......@...#.c.
....P.......QB.P....e..HTTP/1.1 204 No Content
Date: Sat, 05 Sep 2020 09:04:54 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close


14:34:54.321344 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [.], ack 149, win 64092, length 0
E..(..@.@..C
...#.c....P.QB.....P..\....
14:34:54.321688 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [F.], seq 88, ack 149, win 64092, length 0
E..(..@.@..B
...#.c....P.QB.....P..\....
14:34:54.321710 IP 35.224.99.156.80 > 10.0.2.15.41244: Flags [F.], seq 149, ack 88, win 65535, length 0
E..(....@.._#.c.
....P.......QB.P...M.........
14:34:54.321755 IP 10.0.2.15.41244 > 35.224.99.156.80: Flags [.], ack 150, win 64091, length 0
E..(..@.@..A
...#.c....P.QB.....P..[....
10 packets captured
10 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

```
richa@richa-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (216.58.203.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.779 ms  0.589 ms  0.520 ms
 2  _gateway (10.0.2.2)  17.270 ms  19.130 ms  22.602 ms
```

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

The destination address is 216.58.203.36 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

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

sudo traceroute -I www.google.com

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

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
richa@richa-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (216.58.203.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.779 ms  0.589 ms  0.520 ms
 2  _gateway (10.0.2.2)  17.270 ms  19.130 ms  22.602 ms
richa@richa-VirtualBox:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (216.58.203.36), 30 hops max, 60 byte packets
 1  10.0.2.2  0.385 ms  0.334 ms  0.301 ms
 2  10.0.2.2  8.071 ms  9.665 ms  9.618 ms
richa@richa-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (216.58.203.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.772 ms  0.749 ms  0.731 ms
 2  192.168.0.1 (192.168.0.1)  4.815 ms  7.408 ms  7.417 ms
 3  10.46.0.1 (10.46.0.1)  11.635 ms  12.228 ms  12.117 ms
 4  103.126.228.37 (103.126.228.37)  7.665 ms  7.621 ms  7.595 ms
 5  103.27.170.10 (103.27.170.10)  28.207 ms  28.679 ms  28.499 ms
 6  108.170.248.177 (108.170.248.177)  29.897 ms  30.577 ms  30.466 ms
 7  216.239.54.147 (216.239.54.147)  30.431 ms  28.527 ms  29.018 ms
 8  hkg12s10-in-f36.1e100.net (216.58.203.36)  27.709 ms  26.720 ms  27.683 ms
richa@richa-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (216.58.203.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.578 ms  0.478 ms  0.445 ms
 2  bom12s05-in-f4.1e100.net (216.58.203.36)  43.180 ms  43.027 ms  45.976 ms
richa@richa-VirtualBox:~$
```

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

```
richa@richa-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 14:45 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.070s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
```

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

nmap 163.53.78.128

```
richa@richa-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 15:18 IST
Nmap scan report for 163.53.78.128
Host is up (0.045s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.97 seconds
richa@richa-VirtualBox:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 15:20 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.14 seconds
```

Step 3: Scan multiple IP address or subnet (IPv4)

nmap 192.168.1.1 192.168.1.2 192.168.1.3

TASK 7 A): NETCAT AS CHAT TOOL

a) Intra system communication (Using 2 terminals in the same system)

Step 1: Open a terminal (Ctrl+Alt+T). This will act as a Server.

Step 2: Type nc -l any_portnum (For eg., nc -l 1234)

Note: It will goto listening mode

Step 3: Open another terminal and this will act as a client.

Step 4: Type nc <your-system-ip-address> portnum

Note: portnum should be common in both the terminals (for eg., nc 10.0.2.8 1234)

Step 5: Type anything in client will appear in server

```
richa@richa-VirtualBox:~$ nc -l 9000
1233
```

```
richa@richa-VirtualBox:~$ nc 10.0.2.15 9000
1233
```

TASK 7 B): USE NETCAT TO TRANSFER FILES

The netcat utility can also be used to transfer files.

Step 1: At the server side, create an empty file named 'test.txt'

sudo nc -l 555 > test.txt

Step 2: At the client side, we have a file 'testfile.txt'. Add some contents to it.

Step 3: Run the client as:

sudo nc 10.0.2.8 555 < testfile.txt

here, 10.0.2.8 is the IP address of server and 555 is the port number.

Step 4: At server side, verify the file transfer using the command

cat test.txt

```
richa@richa-VirtualBox:~$ cat >hell.txt
richa@richa-VirtualBox:~$ sudo nc
[sudo] password for richa:
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
richa@richa-VirtualBox:~$ sudo nc -l 10.0.2.15 9000 <hello.txt
```

```
richa@richa-VirtualBox:~$ cat hell.txt
```

Since the file does not contain anything, nothing is displayed on the output.

TASK 7 C): OTHER COMMANDS

1) To test if a particular TCP port of a remote host is open.

nc -vn 10.0.2.8 555

2) Run a web server with a static web page.

Step 1: Run the command below on local host (e.g. 10.0.2.8) to start a web server that serves test.html on port 80.

while true; do sudo nc -lp 80 < test.html; done

Step 2: Now open http://10.0.2.8/test.html from another host to access it.

Step 3: Observe the details on the terminal

```
richa@richa-VirtualBox:~$ nc -vn 10.0.2.15 9000
Connection to 10.0.2.15 9000 port [tcp/*] succeeded!
<html>
<head><title>hw</title></head>
<body>
<h4> Hello World!</h4>
</body>
</html>
```

```
richa@richa-VirtualBox:~$ cat hw.html
<html>
<head><title>hw</title></head>
<body>
<h4> Hello World!</h4>
</body>
</html>
richa@richa-VirtualBox:~$ while true; do sudo nc -lp 9000 < hw.html; d
one

nc: connect to 10.0.2.15 port 9000 (tcp) failed: Connection refused
richa@richa-VirtualBox:~$ nc -vn 10.0.2.15 9000
Connection to 10.0.2.15 9000 port [tcp/*] succeeded!
<html>
<head><title>hw</title></head>
<body>
<h4> Hello World!</h4>
</body>
</html>
```

QUESTIONS ON ABOVE OBSERVATIONS:

1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

Both the server and browser are running on 1.1

2) When was the HTML file that you are retrieving last modified at the server?

```
richa@richa-VirtualBox:~$ ls -all| grep .html
-rw-rw-r--  1 richa   richa          84 Sep  5 16:24 hw.html
```

Sept 5, 4:24 pm

3) How to tell ping to exit after a specified number of ECHO_REQUEST packets?

Use Ctrl+C to exit

4) How will you identify remote host apps and OS?
Use ip neigh

EXERCISES:

1) Capture and Analyze IPv4 / IPv6 packets

IPv4 / IPv6 packet header

GET	GET / HTTP / 1.1
HOST	connectivity-check.ubuntu.com
USER-AGENT	Mozilla (Ubuntu)
ACCEPT-LANGUAGE	*
CACHE-CONTROL	no cache, no store
PRAGMA	
CONNECTION	close

2) Explore various other network configuration, troubleshooting and debugging tools such as Route, Netstat, etc.

```
richa@richa-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

```
richa@richa-VirtualBox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 richa-VirtualBox:bootpc _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    14524    /run/systemd/journal/syslog
unix  2      [ ]         DGRAM                    29882    /run/user/1000/systemd/notify
unix  17     [ ]         DGRAM                    14534    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    14538    /run/systemd/journal/socket
unix  3      [ ]         DGRAM                    14510    /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     32622    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     30861
unix  3      [ ]         STREAM     CONNECTED     30080    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     33659
unix  3      [ ]         STREAM     CONNECTED     33522
unix  3      [ ]         STREAM     CONNECTED     31512
unix  3      [ ]         STREAM     CONNECTED     20486
unix  3      [ ]         STREAM     CONNECTED     32990    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     31849    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     30737
unix  3      [ ]         STREAM     CONNECTED     19578    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     36469    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     34312
unix  3      [ ]         STREAM     CONNECTED     31991    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31878    /run/user/1000/bus
unix  3      [ ]         DGRAM                    29884
unix  3      [ ]         STREAM     CONNECTED     35932    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     35856    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     31511
unix  3      [ ]         STREAM     CONNECTED     19576    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     30429    /run/user/1000/bus
unix  2      [ ]         DGRAM                    28587
unix  3      [ ]         STREAM     CONNECTED     29353
unix  3      [ ]         STREAM     CONNECTED     28138
unix  2      [ ]         STREAM     CONNECTED     21585
unix  3      [ ]         STREAM     CONNECTED     33338    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     30570
```