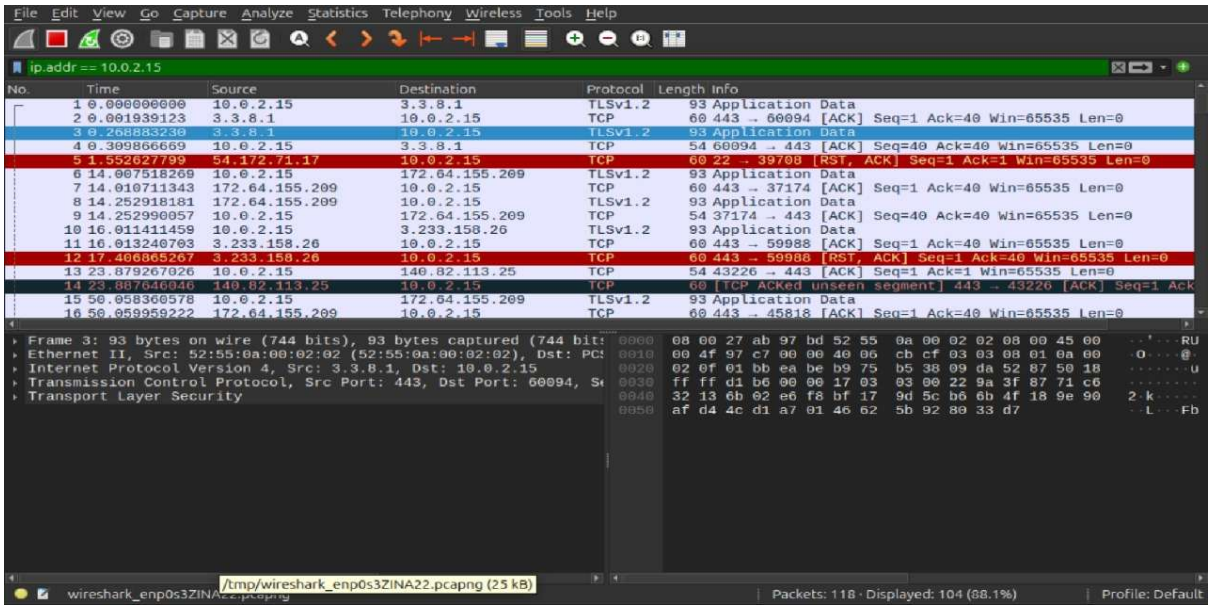
LINUX NETWORKING MODULE 1 AND 2 ASSESSMENT SOLUTIONS

-BY SAKTHI KUMAR S

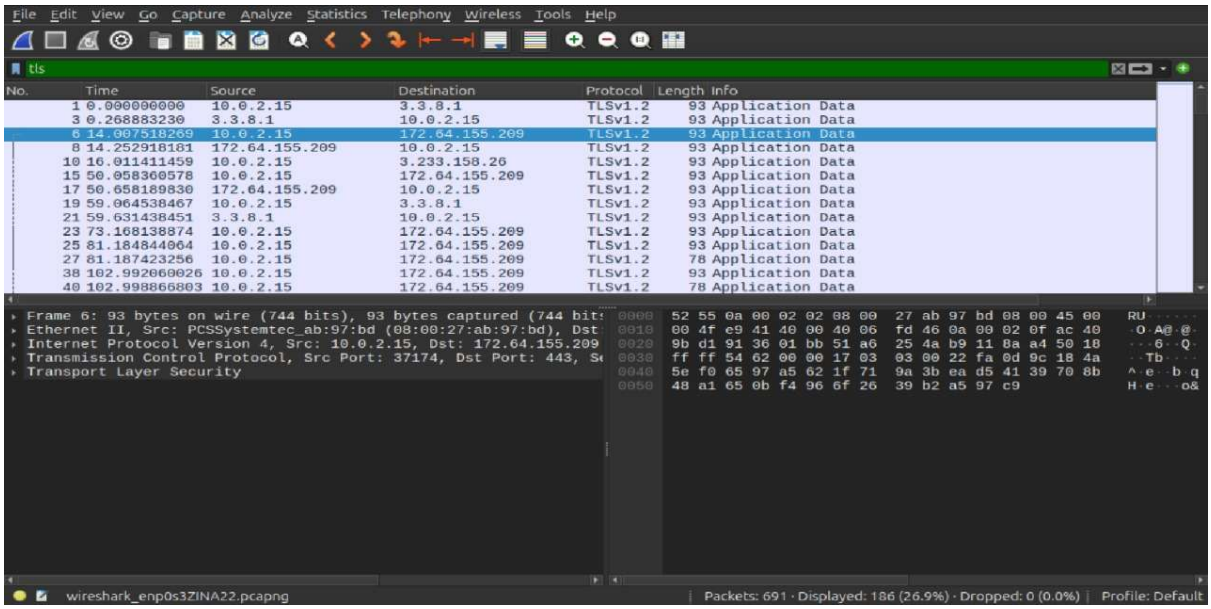
3. Explore with Wireshark/TCP-dump/cisco packet tracer tools and learn about packets filters.

WIRESHARK:

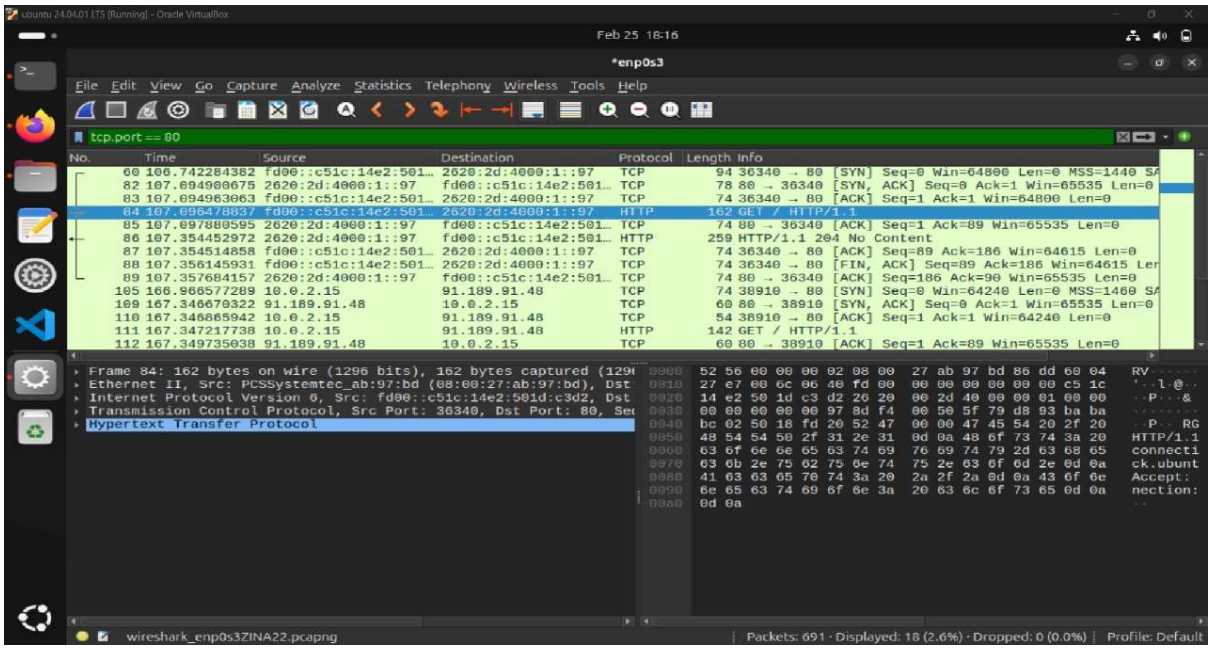
1) Packet tracing with IP address



2) Packet Tracing with protocol names

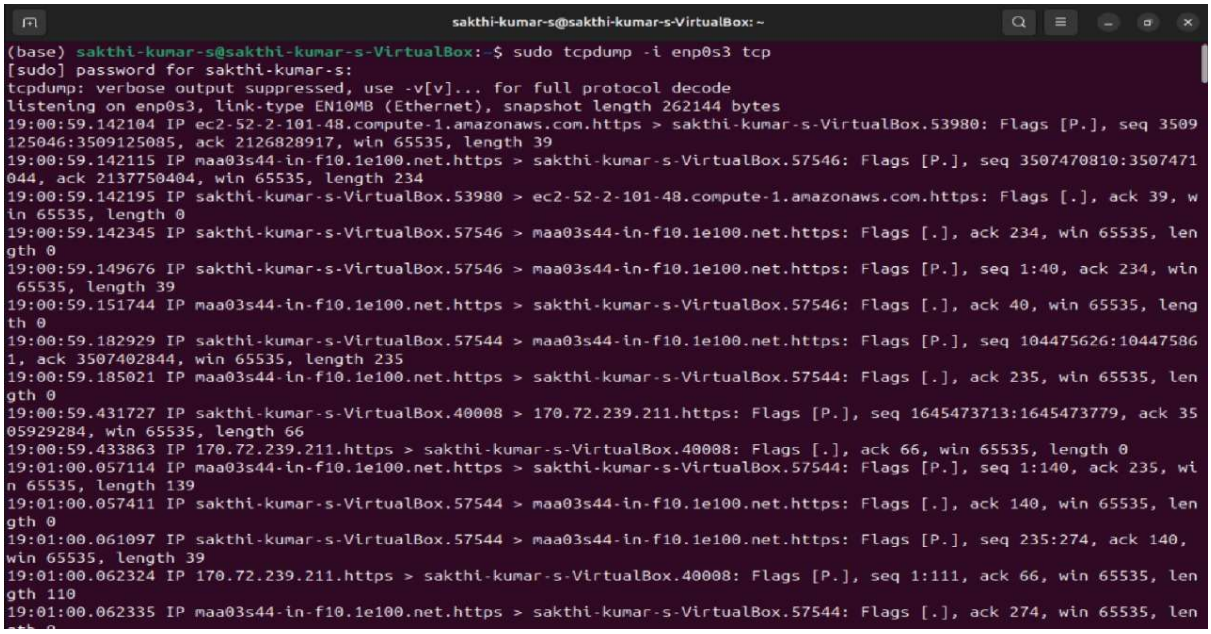


3) Packet Tracing with Port Numbers



TCPDUMP:

1) Capture Packets on a Specific Interface



2) Capture Packets with IP address

```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 host 10.0.2.15
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:05:36.840895 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [P.], seq 3543368917:3543368954, ack 38
73862941, win 65535, length 37
19:05:36.841690 IP sakthi-kumar-s-VirtualBox.47058 > 170.72.239.211.https: Flags [P.], seq 1:42, ack 37, win 65535, leng
th 41
19:05:36.847353 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [.], ack 42, win 65535, length 0
19:05:36.898711 IP sakthi-kumar-s-VirtualBox.33751 > 10.0.2.3.domain: 22896+ PTR? 15.2.0.10.in-addr.arpa. (40)
19:05:36.919196 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.33751: 22896 NXDomain 0/0/0 (40)
19:05:36.921312 IP sakthi-kumar-s-VirtualBox.41659 > 10.0.2.3.domain: 40582+ PTR? 211.239.72.170.in-addr.arpa. (45)
19:05:36.968893 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [P.], seq 3542402279:3542402316, ack 41
6843228, win 65535, length 37
19:05:36.969692 IP sakthi-kumar-s-VirtualBox.47006 > 170.72.239.211.https: Flags [P.], seq 1:42, ack 37, win 64022, leng
th 41
19:05:36.974127 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [.], ack 42, win 65535, length 0
19:05:37.064409 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.41659: 40582 NXDomain 0/1/0 (116)
19:05:37.068592 IP sakthi-kumar-s-VirtualBox.54377 > 10.0.2.3.domain: 11900+ PTR? 3.2.0.10.in-addr.arpa. (39)
19:05:37.077566 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.54377: 11900 NXDomain 0/0/0 (39)
19:05:37.128671 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [P.], seq 37:111, ack 42, win 65535, le
ngth 74
19:05:37.134808 IP sakthi-kumar-s-VirtualBox.47058 > 170.72.239.211.https: Flags [P.], seq 42:79, ack 111, win 65535, le
ngth 37
19:05:37.140043 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [.], ack 79, win 65535, length 0
19:05:37.252190 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [P.], seq 37:112, ack 42, win 65535, le
```

3) using port number

```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 port 80
[sudo] password for sakthi-kumar-s:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:29:07.817552 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [S], seq 1658665569, win 64240, options [
mss 1460,sackOK,TS val 990939449 ecr 0,nop,wscale 7], length 0
03:29:07.861685 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [S.], seq 57856001, ack 1658665570, win 6
5535, options [mss 1460], length 0
03:29:07.861875 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [.], ack 1, win 64240, length 0
03:29:07.863904 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [P.], seq 1:440, ack 1, win 64240, length
 439: HTTP: POST / HTTP/1.1
03:29:07.864510 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [.], ack 440, win 65535, length 0
03:29:07.912779 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [P.], seq 1:891, ack 440, win 65535, leng
th 890: HTTP: HTTP/1.1 200 OK
03:29:07.912935 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [.], ack 891, win 63350, length 0
03:29:08.347278 IP sakthi-kumar-s-VirtualBox.48270 > 82.221.107.34.bc.googleusercontent.com.http: Flags [S], seq 2904251
772, win 64240, options [mss 1460,sackOK,TS val 427881819 ecr 0,nop,wscale 7], length 0
```

```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 ip
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:06:51.492022 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [P.], seq 2656968221:2656968260, ack 35
43480669, win 65535, length 39
19:06:51.492930 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [P.], seq 882180903:882180942, ack 3543
559949, win 65535, length 39
19:06:51.493570 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 39, win 65535, length 0
19:06:51.495844 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 39, win 65535, length 0
19:06:51.499513 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [P.], seq 39:63, ack 1, win 65535, leng
th 24
19:06:51.500357 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 63, win 65535, length 0
19:06:51.501110 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [F.], seq 63, ack 1, win 65535, length
0
19:06:51.502901 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 64, win 65535, length 0
19:06:51.505299 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [P.], seq 39:63, ack 1, win 65535, leng
th 24
19:06:51.505938 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [F.], seq 63, ack 1, win 65535, length
0
19:06:51.507928 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 63, win 65535, length 0
19:06:51.507945 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 64, win 65535, length 0
19:06:51.539815 IP sakthi-kumar-s-VirtualBox.55694 > 10.0.2.3.domain: 45465+ PTR? 213.239.72.170.in-addr.arpa. (45)
19:06:51.991630 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.55694: 45465 NXDomain 0/1/0 (116)
```

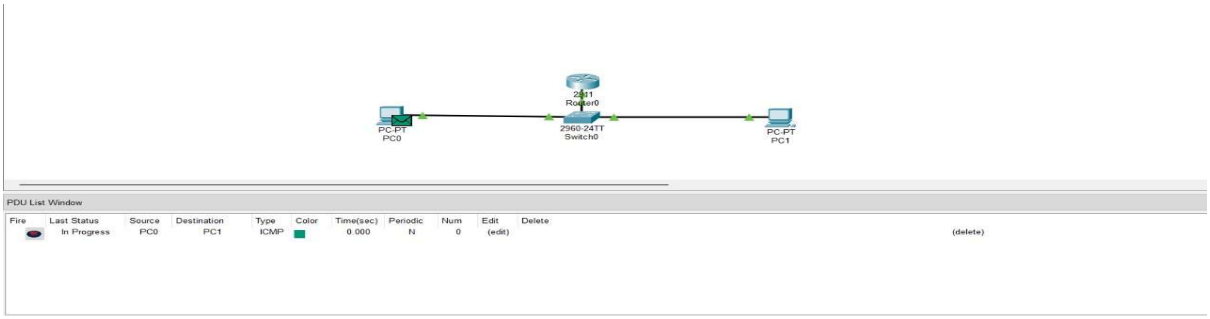
Cisco Packet Tracer:

1) Basic network topology Setup in Cisco Packet Tracer

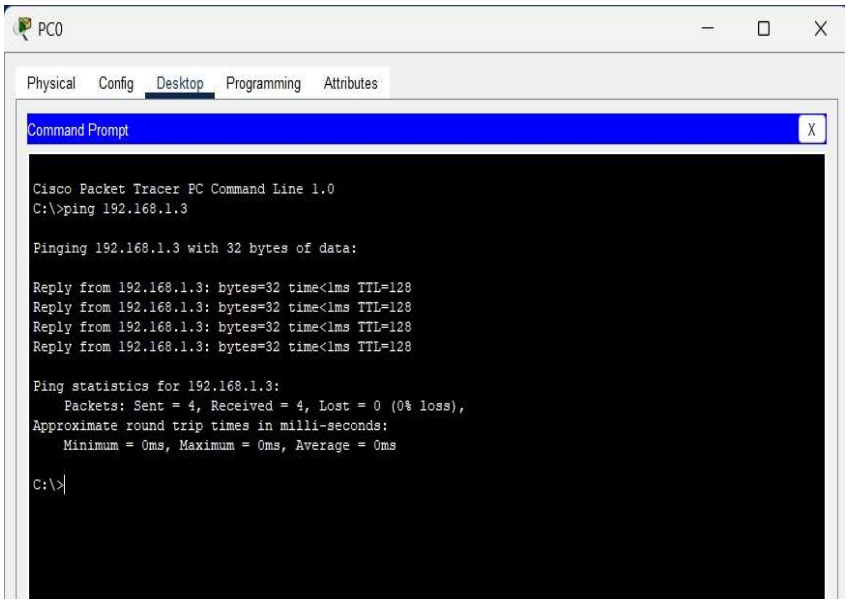
Devices Used

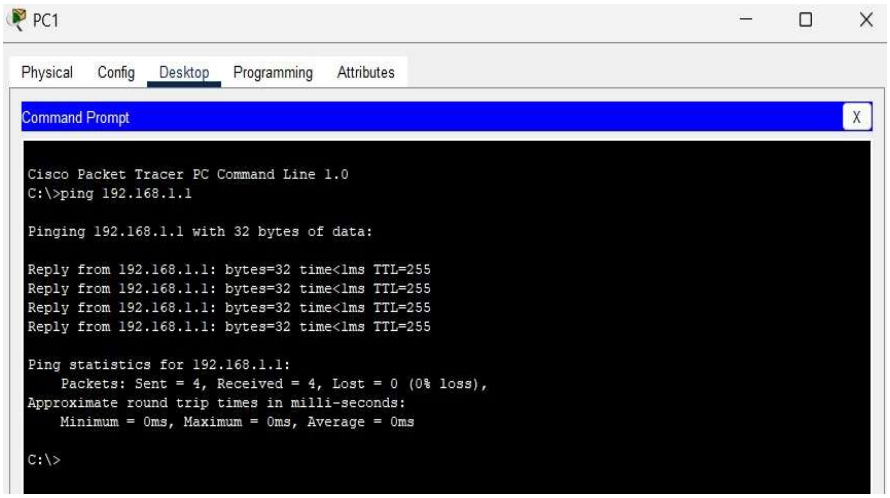
- 2 PCs (PC0 and PC1) (IP addresses: 192.168.1.2 and 192.168.1.3) (Gateway: 192.168.1.1)
- 1 Router (Router0) (192.168.1.1)
- 1 Switch (Switch0)
- Copper Straight-Through Cables

2) Simple PC0 and PC1 Connection:



3)Ping Test on PC0 and PC1





4)PDU Packet Transfer Information