

# Computer Networks Laboratory

## UE20CS255

Name: Naman Choudhary

SRN: PES2UG20CS209

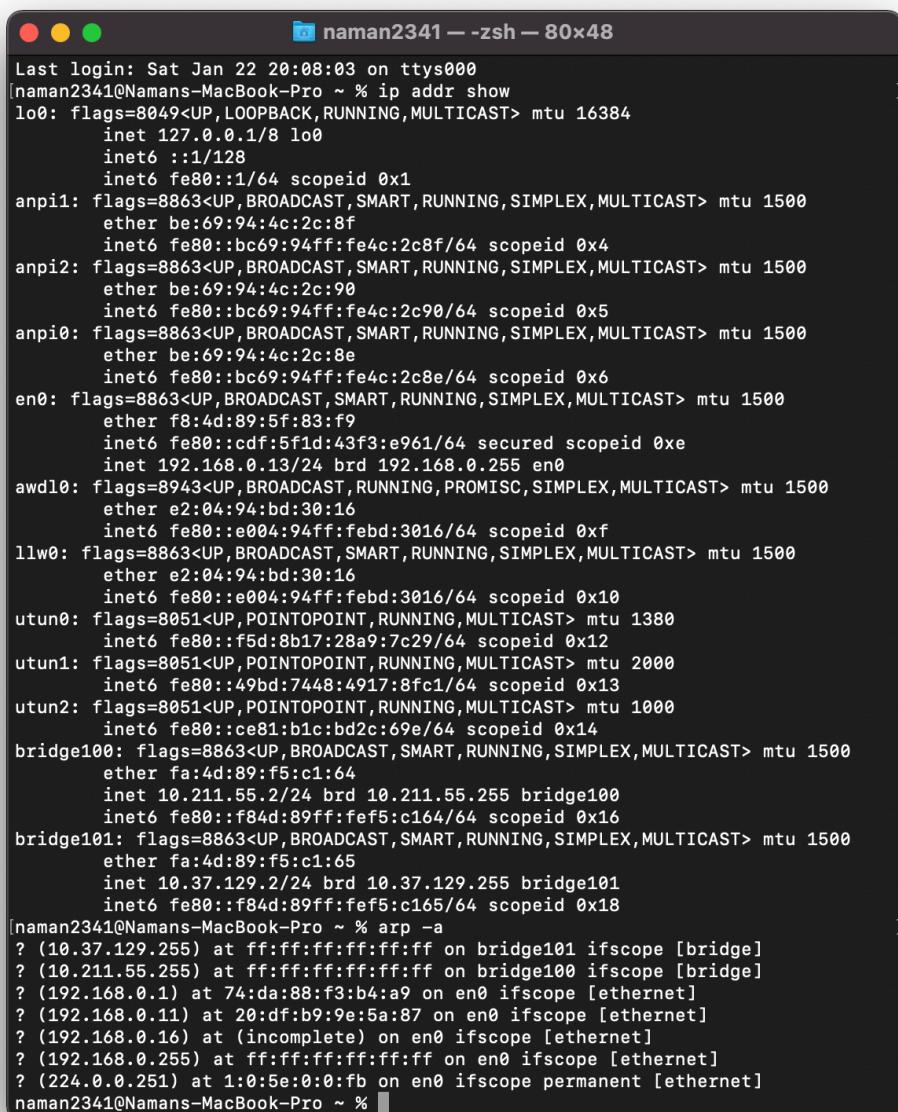
Section: D

### Week 1

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

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

STEP 1: TO DISPLAY STATUS OF ALL ACTIVE NETWORK INTERFACES.



```

naman2341 — zsh — 80x48
Last login: Sat Jan 22 20:08:03 on ttys000
[naman2341@Namans-MacBook-Pro ~ % ip addr show
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet 127.0.0.1/8 brd 127.0.0.1 scopeid 0x1
        inet6 fe80::1/128
            inet6 fe80::1/64 scopeid 0x1
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether be:69:94:4c:2c:8f
    inet6 fe80::bc69:94ff:fe4c:2c8f/64 scopeid 0x4
anpi2: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether be:69:94:4c:2c:90
    inet6 fe80::bc69:94ff:fe4c:2c90/64 scopeid 0x5
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether be:69:94:4c:2c:8e
    inet6 fe80::bc69:94ff:fe4c:2c8e/64 scopeid 0x6
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether f8:4d:89:5f:83:f9
    inet6 fe80::cdf:5f1d:43f3:e961/64 secured scopeid 0xe
    inet 192.168.0.13/24 brd 192.168.0.255 en0
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    ether e2:04:94:bd:30:16
    inet6 fe80::e004:94ff:feb0:3016/64 scopeid 0xf
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether e2:04:94:bd:30:16
    inet6 fe80::e004:94ff:feb0:3016/64 scopeid 0x10
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::f5d:8b17:28a9:7c29/64 scopeid 0x12
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::49bd:7448:4917:8fc1/64 scopeid 0x13
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
    inet6 fe80::ce81:b1c:bd2c:69e/64 scopeid 0x14
bridge100: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether fa:4d:89:f5:c1:64
    inet 10.211.55.2/24 brd 10.211.55.255 bridge100
    inet6 fe80::f84d:89ff:fef5:c164/64 scopeid 0x16
bridge101: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether fa:4d:89:f5:c1:65
    inet 10.37.129.2/24 brd 10.37.129.255 bridge101
    inet6 fe80::f84d:89ff:fef5:c165/64 scopeid 0x18
[naman2341@Namans-MacBook-Pro ~ % arp -a
? (10.37.129.255) at ff:ff:ff:ff:ff:ff on bridge101 ifscope [bridge]
? (10.211.55.255) at ff:ff:ff:ff:ff:ff on bridge100 ifscope [bridge]
? (192.168.0.1) at 74:da:88:f3:b4:a9 on en0 ifscope [ethernet]
? (192.168.0.11) at 20:df:b9:9e:5a:87 on en0 ifscope [ethernet]
? (192.168.0.16) at (incomplete) on en0 ifscope [ethernet]
? (192.168.0.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
[naman2341@Namans-MacBook-Pro ~ % ]

```

Interface Name	IP address	MAC address	Scope
en0	192.168.0.11	20:df:b9:9e:5a:87	ethernet
en0	192.168.0.1	74:da:88:f3:b4:a9	ethernet
bridge100	10.211.55.255	ff:ff:ff:ff:ff:ff	bridge

**STEP 2: TO ASSIGN AN IP ADDRESS TO AN INTERFACE****STEP 3: TO ACTIVATE / DEACTIVATE A NETWORK INTERFACE**

```
[naman2341@Namans-MacBook-Pro ~ % sudo ifconfig en4 10.0.4.12 netmask 225.225.225.0
>Password:
[naman2341@Namans-MacBook-Pro ~ % sudo ifconfig en4 down
[naman2341@Namans-MacBook-Pro ~ % sudo ifconfig en4 up
naman2341@Namans-MacBook-Pro ~ % ]
```

**STEP 4: TO SHOW THE CURRENT NEIGHBOUR TABLE IN KERNEL**

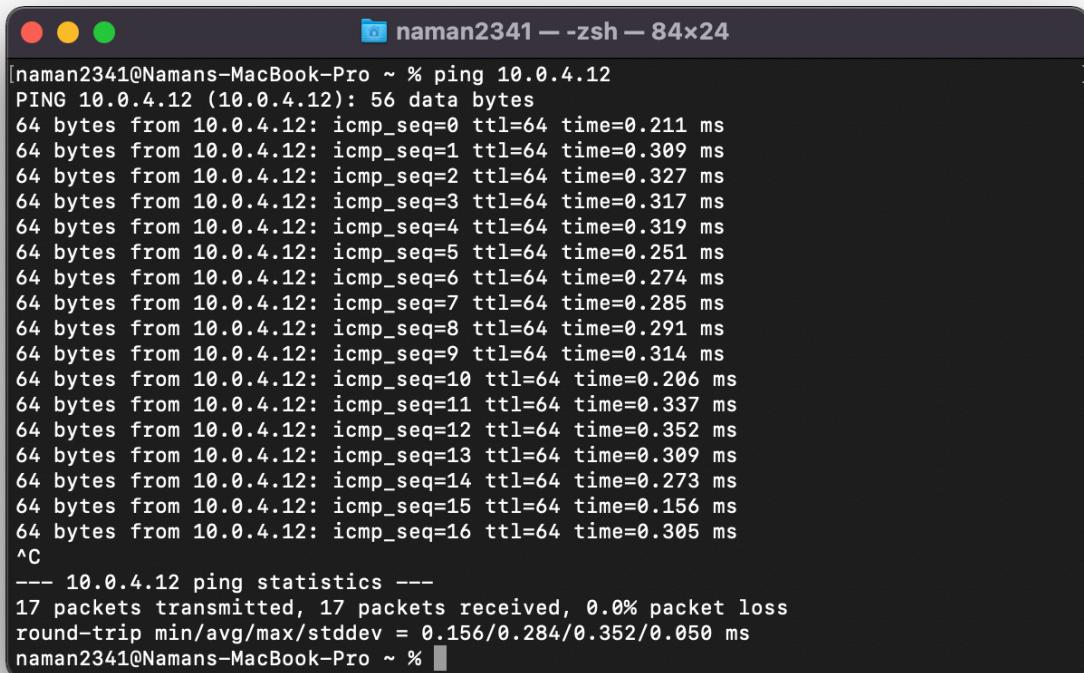
```
[naman2341@Namans-MacBook-Pro ~ % ip neigh
fe80::1 dev lo0 lladdr (incomplete) REACHABLE
fe80::bc69:94ff:fe4c:2c90 dev anpi2 lladdr be:69:94:4c:2c:90 REACHABLE
fe80::bc69:94ff:fe4c:2c8e dev anpi0 lladdr be:69:94:4c:2c:8e REACHABLE
fe80::bc69:94ff:fe4c:2c8f dev anpi1 lladdr be:69:94:4c:2c:8f REACHABLE
fe80::1c67:6947:a06b:eb4a dev en0 lladdr f8:4d:89:5f:83:f9 REACHABLE
fe80::76da:88ff:fef3:b4a9 dev en0 lladdr 74:da:88:f3:b4:a9 STALE
fe80::e027:8fff:fe55:22de dev awd10 lladdr e2:27:8f:55:22:de REACHABLE
fe80::e027:8fff:fe55:22de dev llw0 lladdr e2:27:8f:55:22:de REACHABLE
fe80::8571:f45c:b527:f482 dev utun0 lladdr (incomplete) REACHABLE
fe80::30fd:5473:7768:9d69 dev utun1 lladdr (incomplete) REACHABLE
fe80::ce81:b1c:bd2c:69e dev utun2 lladdr (incomplete) REACHABLE
fe80::f84d:89ff:fef5:c164 dev bridge100 lladdr fa:4d:89:f5:c1:64 REACHABLE
fe80::f84d:89ff:fef5:c165 dev bridge101 lladdr fa:4d:89:f5:c1:65 REACHABLE
10.0.4.12 dev en4 lladdr be:69:94:4c:2c:6e REACHABLE
10.37.129.255 dev bridge10 lladdr ff:ff:ff:ff:ff:ff REACHABLE
10.211.55.255 dev bridge10 lladdr ff:ff:ff:ff:ff:ff REACHABLE
192.168.0.1 dev en0 lladdr 74:da:88:f3:b4:a9 REACHABLE
192.168.0.16 dev en0 lladdr f2:ad:86:b1:98:17 REACHABLE
192.168.0.255 dev en0 lladdr ff:ff:ff:ff:ff:ff REACHABLE
224.0.0.251 dev en0 lladdr 1:0:5e:0:0:fb REACHABLE
239.255.255.250 dev bridge10 lladdr 1:0:5e:7f:ff:fa REACHABLE
239.255.255.250 dev bridge10 lladdr 1:0:5e:7f:ff:fa REACHABLE
naman2341@Namans-MacBook-Pro ~ % ]
```

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

**STEP 1:ASSIGN AN IP ADDRESS TO THE SYSTEM (HOST).**

**STEP 2:LAUNCH WIRESHARK AND SELECT 'ANY' INTERFACE**

**STEP 3:IN TERMINAL, TYPE PING 10.0.YOUR\_SECTION.YOUR\_SNO**



```
[naman2341@Namans-MacBook-Pro ~ % ping 10.0.4.12
PING 10.0.4.12 (10.0.4.12): 56 data bytes
64 bytes from 10.0.4.12: icmp_seq=0 ttl=64 time=0.211 ms
64 bytes from 10.0.4.12: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 10.0.4.12: icmp_seq=2 ttl=64 time=0.327 ms
64 bytes from 10.0.4.12: icmp_seq=3 ttl=64 time=0.317 ms
64 bytes from 10.0.4.12: icmp_seq=4 ttl=64 time=0.319 ms
64 bytes from 10.0.4.12: icmp_seq=5 ttl=64 time=0.251 ms
64 bytes from 10.0.4.12: icmp_seq=6 ttl=64 time=0.274 ms
64 bytes from 10.0.4.12: icmp_seq=7 ttl=64 time=0.285 ms
64 bytes from 10.0.4.12: icmp_seq=8 ttl=64 time=0.291 ms
64 bytes from 10.0.4.12: icmp_seq=9 ttl=64 time=0.314 ms
64 bytes from 10.0.4.12: icmp_seq=10 ttl=64 time=0.206 ms
64 bytes from 10.0.4.12: icmp_seq=11 ttl=64 time=0.337 ms
64 bytes from 10.0.4.12: icmp_seq=12 ttl=64 time=0.352 ms
64 bytes from 10.0.4.12: icmp_seq=13 ttl=64 time=0.309 ms
64 bytes from 10.0.4.12: icmp_seq=14 ttl=64 time=0.273 ms
64 bytes from 10.0.4.12: icmp_seq=15 ttl=64 time=0.156 ms
64 bytes from 10.0.4.12: icmp_seq=16 ttl=64 time=0.305 ms
^C
--- 10.0.4.12 ping statistics ---
17 packets transmitted, 17 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.156/0.284/0.352/0.050 ms
naman2341@Namans-MacBook-Pro ~ % ]
```

### STEP 4:ANALYZE THE FOLLOWING IN TERMINAL

- TTL=64
- Protocol used by ping=icmp
- Time=min/avg/max/stddev = 0.156/0.284/0.352/0.050 ms

### STEP 5:ANALYZE THE FOLLOWING IN WIRESHARK

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP address	10.0.4.12	10.0.4.12
Destination IP address	10.0.4.12	10.0.4.12
ICMP Type Value	8 (Echo (ping) request)	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00

Details	First Echo Request	First Echo Reply
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](http://www.flipkart.com)**

[www.flipkart.com](http://www.flipkart.com) did not send/receive any HTTP packets, so <http://info.cern.ch/> was used instead.

```
> Frame 82: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface en0, id 0
> Ethernet II, Src: Apple_5f:83:f9 (f8:4d:89:5f:83:f9), Dst: Tp-LinkT_f3:b4:a9 (74:da:88:f3:b4:a9)
> Internet Protocol Version 4, Src: 192.168.0.13, Dst: 188.185.82.144
> Transmission Control Protocol, Src Port: 56126, Dst Port: 80, Seq: 1, Ack: 1, Len: 529
> Hypertext Transfer Protocol
```

**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	82	87
Source Port	56126	80
Destination Port	80	56126
Source IP address	192.168.0.13	188.185.82.144
Destination IP address	188.185.82.144	192.168.0.13
Source Ethernet Address	f8:4d:89:5f:83:f9	74:da:88:f3:b4:a9
Destination Ethernet Address	74:da:88:f3:b4:a9	f8:4d:89:5f:83:f9

**STEP 4:ANALYZE THE HTTP REQUEST AND RESPONSE AND COMPLETE THE TABLE BELOW**

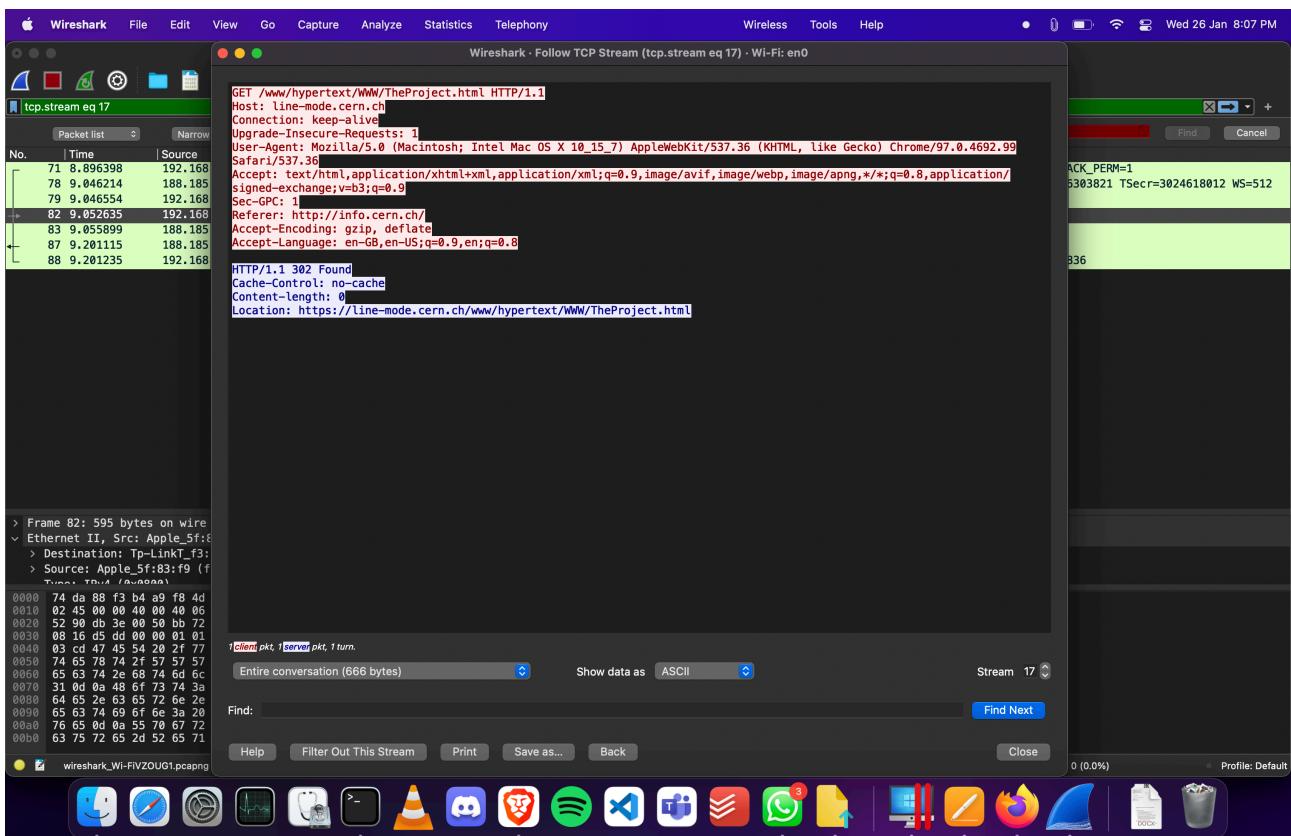
HTTP Request		HTTP Response	
Get	GET /www/hypertext/www/TheProject.html HTTP/1.1\r\n	Server	Apache
Host	line-mode.cern.ch	Content-Type	text/html

HTTP Request		HTTP Response	
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36	Date	Wed, 26 Jan 2022 13:14:33 GMT
Accept-Language	en-GB,en-US;q=0.9,en;q=0.8	Location	<a href="https://line-mode.cern.ch/www/hypertext/www/TheProject.html">https://line-mode.cern.ch/www/hypertext/www/TheProject.html</a>
Accept-Encoding	gzip, deflate	Content-Length	644
Connection	keep-alive	Connection	close

## 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

```
[naman2341@Namans-MacBook-Pro ~ % sudo tcpdump -D
1.en0 [Up, Running]
2.awdl0 [Up, Running]
3.llw0 [Up, Running]
4.utun0 [Up, Running]
5.vmenet0 [Up, Running]
6.ap1 [Up, Running]
7.utun1 [Up, Running]
8.vmenet1 [Up, Running]
9.utun2 [Up, Running]
10.bridge100 [Up, Running]
11.bridge101 [Up, Running]
12.lo0 [Up, Running, Loopback]
13.anpi0 [Up, Running]
14.bridge0 [Up, Running]
15.anpi1 [Up, Running]
16.en1 [Up, Running]
17.anpi2 [Up, Running]
18.en2 [Up, Running]
19.en3 [Up, Running]
20.en4 [Up, Running]
21.en5 [Up, Running]
22.en6 [Up, Running]
23.gif0 [none]
24.stf0 [none]
naman2341@Namans-MacBook-Pro ~ % ]
```

STEP 2: CAPTURE ALL PACKETS IN ANY INTERFACE BY RUNNING THIS COMMAND:  
SUDO TCPDUMP -I ANY

### 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

```
[naman2341@Namans-MacBook-Pro ~ % sudo tcpdump -i any -c5 icmp
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
20:17:27.280811 IP 10.0.4.12 > 10.0.4.12: ICMP echo request, id 42871, seq 0, length 64
20:17:27.280851 IP 10.0.4.12 > 10.0.4.12: ICMP echo request, id 42871, seq 0, length 64
20:17:27.280897 IP 10.0.4.12 > 10.0.4.12: ICMP echo reply, id 42871, seq 0, length 64
20:17:27.280901 IP 10.0.4.12 > 10.0.4.12: ICMP echo reply, id 42871, seq 0, length 64
20:17:28.286068 IP 10.0.4.12 > 10.0.4.12: ICMP echo request, id 42871, seq 1, length 64
5 packets captured
20 packets received by filter
0 packets dropped by kernel
naman2341@Namans-MacBook-Pro ~ % ]
```

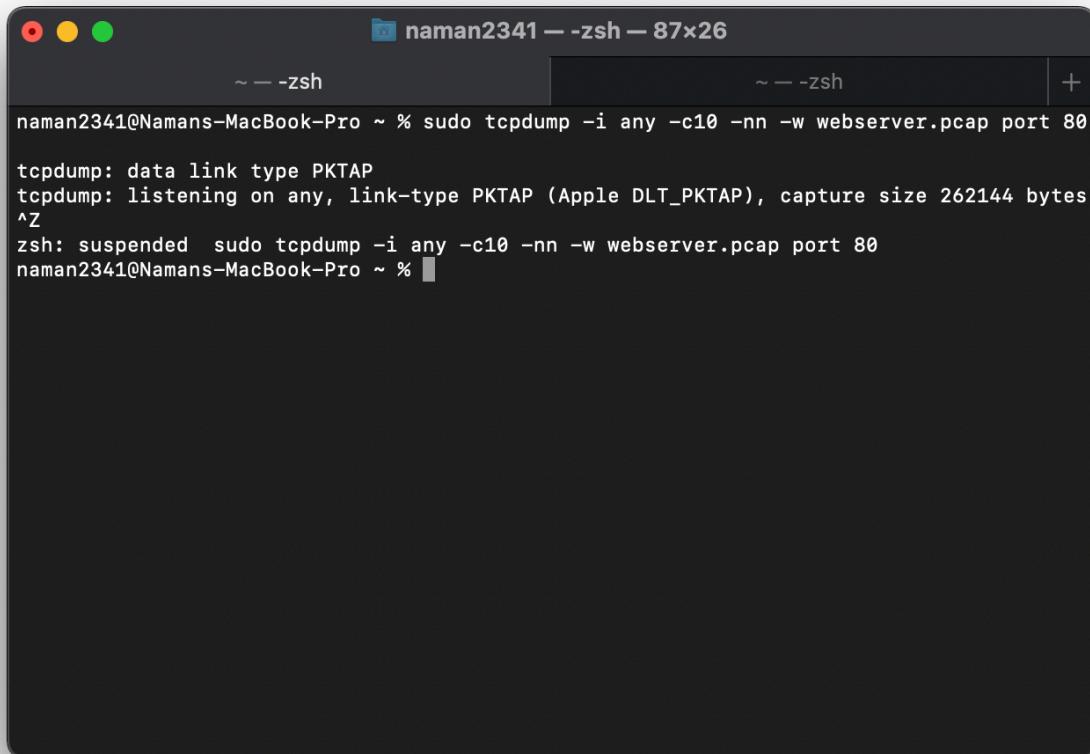
**STEP 5: CHECK THE PACKET CONTENT. FOR EXAMPLE, INSPECT THE HTTP CONTENT OF A WEB REQUEST LIKE THIS:**

**SUDO TCPDUMP -I ANY -C10 -NN -A PORT 80**

```
[naman2341@Namans-MacBook-Pro ~ % sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
20:25:24.895664 IP 77.234.45.88.80 > 192.168.0.13.55125: Flags [.], ack 448449926, win 183, options [nop,nop,TS val 1636644557 ecr 1200025302], length 0
.M._..t.....E..4..@.;.0.M.-X.....P.U..p+.....>.....
a.6.G...
20:25:24.895940 IP 192.168.0.13.55125 > 77.234.45.88.80: Flags [.], ack 1, win 2048, options [nop,nop,TS val 1200045374 ecr 1636634537], length 0
t.....M._....E..4..@.....M.-X.U.P.....p,....."....
G.=>a...
20:25:44.964596 IP 77.234.45.88.80 > 192.168.0.13.55125: Flags [.], ack 1, win 183, options [nop,nop,TS val 1636646564 ecr 1200045374], length 0
.M._..t.....E..4..@.;.0.M.-X.....P.U..p+.....p.....
a.>.G.=>
20:25:44.964887 IP 192.168.0.13.55125 > 77.234.45.88.80: Flags [.], ack 1, win 2048, options [nop,nop,TS val 1200065443 ecr 1636634537], length 0
t.....M._....E..4..@.....M.-X.U.P.....p,.....
G...a...
^C
4 packets captured
554 packets received by filter
0 packets dropped by kernel
naman2341@Namans-MacBook-Pro ~ % ]
```

**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**



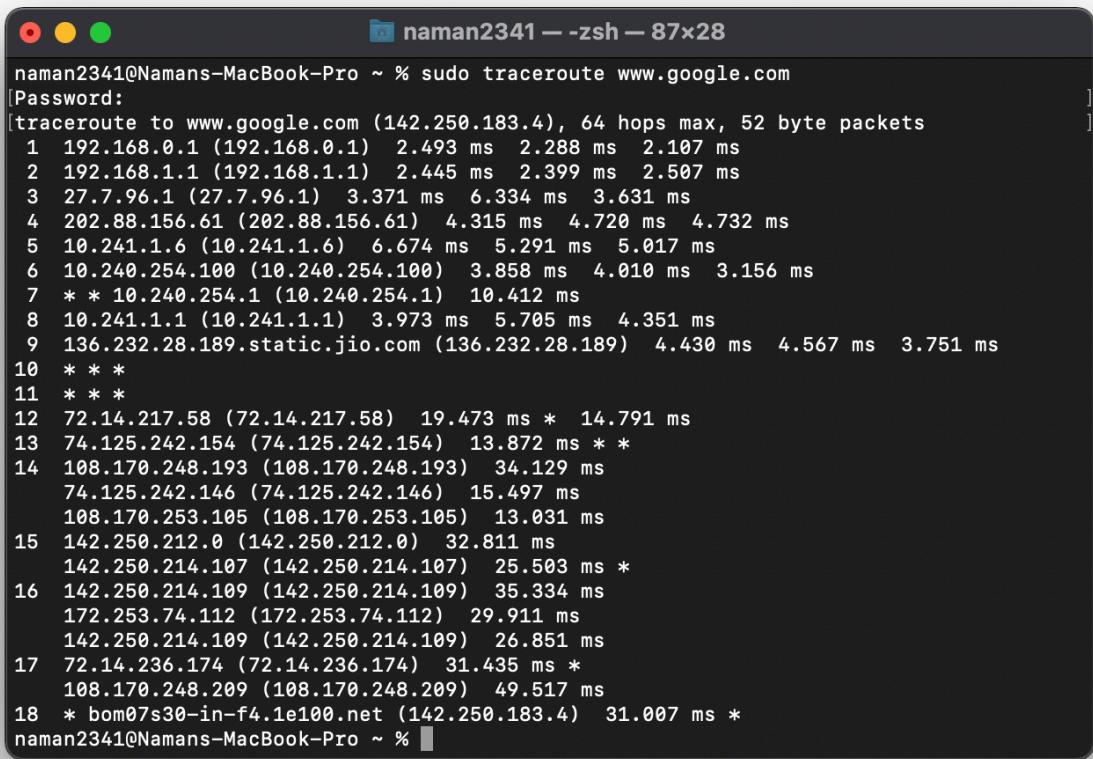
A screenshot of a macOS terminal window titled "naman2341 — zsh — 87x26". The window has two panes. The left pane shows the command being run: "naman2341@Namans-MacBook-Pro ~ % sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80". The right pane shows the output of the command: "tcpdump: data link type PKTAP", "tcpdump: listening on any, link-type PKTAP (Apple DLT\_PKTAP), capture size 262144 bytes ^Z", and "zsh: suspended sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80". The terminal has a dark theme.

---

## **Task 5: Perform Traceroute checks**

**STEP 1: RUN THE TRACEROUTE USING THE FOLLOWING COMMAND.**

**SUDO TRACEROUTE [WWW.GOOGLE.COM](http://WWW.GOOGLE.COM)**



```

naman2341@Namans-MacBook-Pro ~ % sudo traceroute www.google.com
[Password: ]
traceroute to www.google.com (142.250.183.4), 64 hops max, 52 byte packets
 1  192.168.0.1 (192.168.0.1)  2.493 ms  2.288 ms  2.107 ms
 2  192.168.1.1 (192.168.1.1)  2.445 ms  2.399 ms  2.507 ms
 3  27.7.96.1 (27.7.96.1)  3.371 ms  6.334 ms  3.631 ms
 4  202.88.156.61 (202.88.156.61)  4.315 ms  4.720 ms  4.732 ms
 5  10.241.1.6 (10.241.1.6)  6.674 ms  5.291 ms  5.017 ms
 6  10.240.254.100 (10.240.254.100)  3.858 ms  4.010 ms  3.156 ms
 7  * * 10.240.254.1 (10.240.254.1)  10.412 ms
 8  10.241.1.1 (10.241.1.1)  3.973 ms  5.705 ms  4.351 ms
 9  136.232.28.189.static.jio.com (136.232.28.189)  4.430 ms  4.567 ms  3.751 ms
10  * * *
11  * * *
12  72.14.217.58 (72.14.217.58)  19.473 ms *  14.791 ms
13  74.125.242.154 (74.125.242.154)  13.872 ms * *
14  108.170.248.193 (108.170.248.193)  34.129 ms
 74.125.242.146 (74.125.242.146)  15.497 ms
108.170.253.105 (108.170.253.105)  13.031 ms
15  142.250.212.0 (142.250.212.0)  32.811 ms
142.250.214.107 (142.250.214.107)  25.503 ms *
16  142.250.214.109 (142.250.214.109)  35.334 ms
 172.253.74.112 (172.253.74.112)  29.911 ms
142.250.214.109 (142.250.214.109)  26.851 ms
17  72.14.236.174 (72.14.236.174)  31.435 ms *
108.170.248.209 (108.170.248.209)  49.517 ms
18  * bom07s30-in-f4.1e100.net (142.250.183.4)  31.007 ms *
naman2341@Namans-MacBook-Pro ~ %

```

## STEP 2: ANALYZE DESTINATION ADDRESS OF GOOGLE.COM AND NO. OF HOPS

Destination address : 142.250.183.4

Number of hops : 18

## 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](#)

```
[naman2341@Namans-MacBook-Pro ~ % sudo traceroute -n www.google.com
[Password:
traceroute to www.google.com (142.250.183.4), 64 hops max, 52 byte packets
 1  192.168.0.1  3.713 ms  5.912 ms  4.156 ms
 2  192.168.1.1  5.957 ms  5.052 ms  2.951 ms
 3  27.7.96.1  4.402 ms  3.614 ms  3.904 ms
 4  202.88.156.61  6.062 ms  3.725 ms  4.532 ms
 5  10.241.1.6  4.631 ms *  10.035 ms
 6  10.240.254.100  3.667 ms  3.860 ms  4.094 ms
 7  10.240.254.1  4.969 ms  4.784 ms  5.260 ms
 8  10.241.1.1  7.740 ms  3.313 ms  4.110 ms
 9  136.232.28.189  9.568 ms  10.839 ms  7.057 ms
10  * * *
11  * * *
12  72.14.217.58  17.201 ms
    74.125.51.4  12.500 ms  13.311 ms
13  108.170.253.104  13.012 ms
    172.253.72.136  11.858 ms *
14  108.170.253.121  16.420 ms
    216.239.43.172  11.611 ms
    108.170.253.105  14.985 ms
15  142.250.214.107  25.284 ms
    108.170.248.193  29.649 ms
    74.125.242.155  12.467 ms
16  142.250.214.107  28.038 ms
    108.170.248.209  30.001 ms  27.240 ms
17  * 108.170.248.193  28.996 ms
    108.170.248.209  26.135 ms
18  142.250.183.4  43.897 ms
    142.250.214.109  31.252 ms *
naman2341@Namans-MacBook-Pro ~ % ]
```

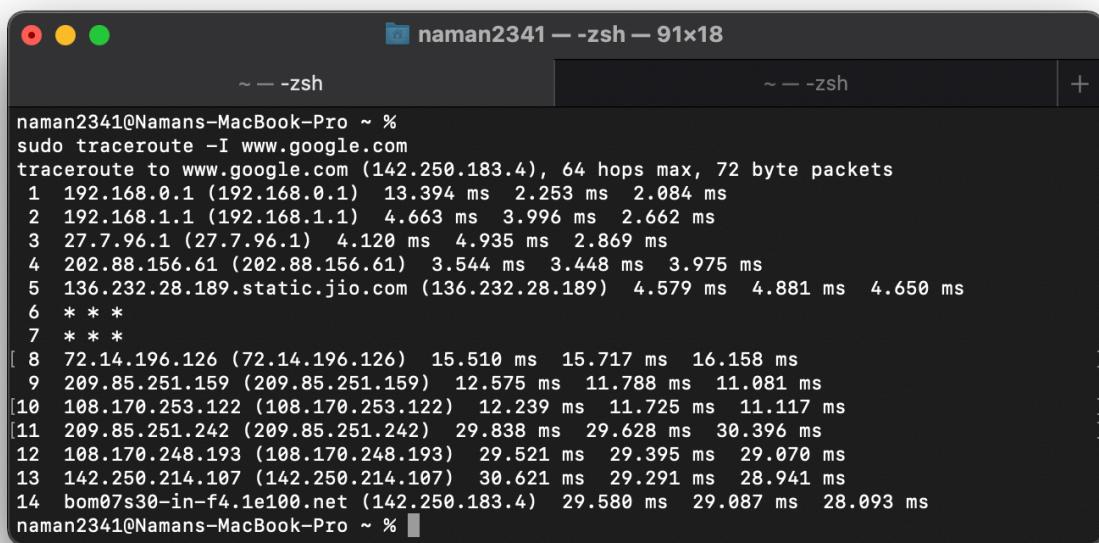
#### STEP 4: THE -I OPTION IS NECESSARY SO THAT THE TRACEROUTE USES ICMP.

#### SUDO TRACEROUTE -I [WWW.GOOGLE.COM](http://www.google.com)

```
[naman2341@Namans-MacBook-Pro ~ %
sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.183.4), 64 hops max, 72 byte packets
 1  192.168.0.1 (192.168.0.1)  13.394 ms  2.253 ms  2.084 ms
 2  192.168.1.1 (192.168.1.1)  4.663 ms  3.996 ms  2.662 ms
 3  27.7.96.1 (27.7.96.1)  4.120 ms  4.935 ms  2.869 ms
 4  202.88.156.61 (202.88.156.61)  3.544 ms  3.448 ms  3.975 ms
 5  136.232.28.189.static.jio.com (136.232.28.189)  4.579 ms  4.881 ms  4.650 ms
 6  * * *
 7  * * *
[ 8  72.14.196.126 (72.14.196.126)  15.510 ms  15.717 ms  16.158 ms
 9  209.85.251.159 (209.85.251.159)  12.575 ms  11.788 ms  11.081 ms
[10  108.170.253.122 (108.170.253.122)  12.239 ms  11.725 ms  11.117 ms
[11  209.85.251.242 (209.85.251.242)  29.838 ms  29.628 ms  30.396 ms
12  108.170.248.193 (108.170.248.193)  29.521 ms  29.395 ms  29.070 ms
13  142.250.214.107 (142.250.214.107)  30.621 ms  29.291 ms  28.941 ms
14  bom07s30-in-f4.1e100.net (142.250.183.4)  29.580 ms  29.087 ms  28.093 ms
naman2341@Namans-MacBook-Pro ~ % ]
```

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)



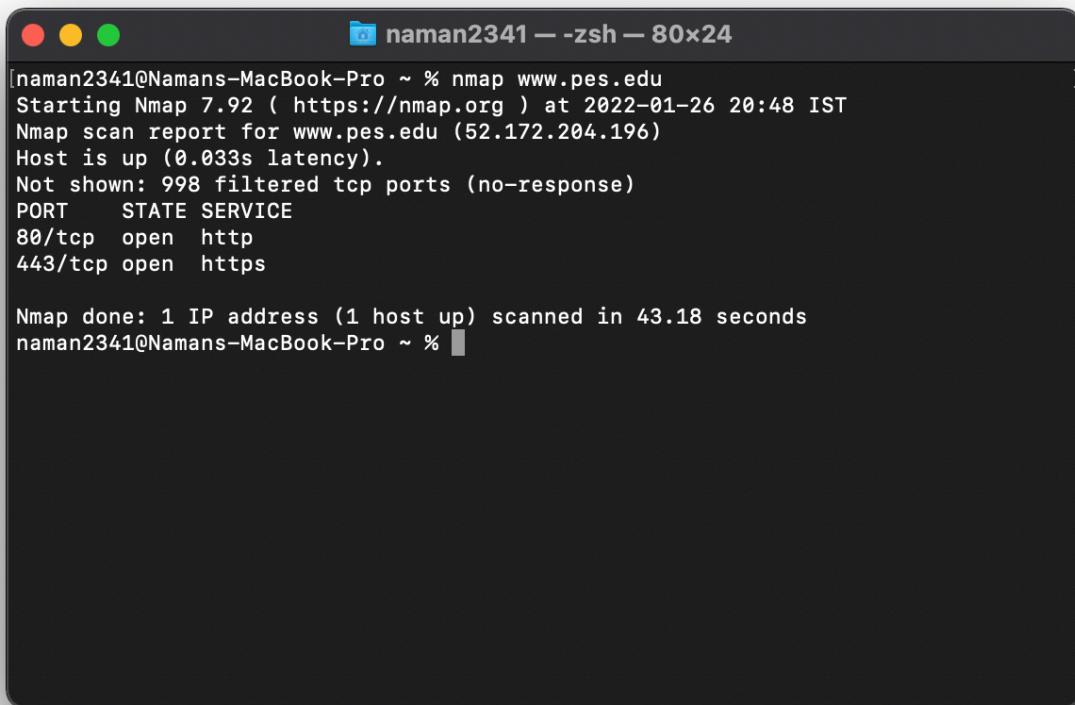
```
naman2341@Namans-MacBook-Pro ~ %
sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.183.4), 64 hops max, 72 byte packets
 1  192.168.0.1 (192.168.0.1)  13.394 ms  2.253 ms  2.084 ms
 2  192.168.1.1 (192.168.1.1)  4.663 ms  3.996 ms  2.662 ms
 3  27.7.96.1 (27.7.96.1)  4.120 ms  4.935 ms  2.869 ms
 4  202.88.156.61 (202.88.156.61)  3.544 ms  3.448 ms  3.975 ms
 5  136.232.28.189.static.jio.com (136.232.28.189)  4.579 ms  4.881 ms  4.650 ms
 6  * * *
 7  * * *
[ 8  72.14.196.126 (72.14.196.126)  15.510 ms  15.717 ms  16.158 ms
 9  209.85.251.159 (209.85.251.159)  12.575 ms  11.788 ms  11.081 ms
[10  108.170.253.122 (108.170.253.122)  12.239 ms  11.725 ms  11.117 ms
[11  209.85.251.242 (209.85.251.242)  29.838 ms  29.628 ms  30.396 ms
12  108.170.248.193 (108.170.248.193)  29.521 ms  29.395 ms  29.070 ms
13  142.250.214.107 (142.250.214.107)  30.621 ms  29.291 ms  28.941 ms
14  bom07s30-in-f4.1e100.net (142.250.183.4)  29.580 ms  29.087 ms  28.093 ms
naman2341@Namans-MacBook-Pro ~ %
```

---

## 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

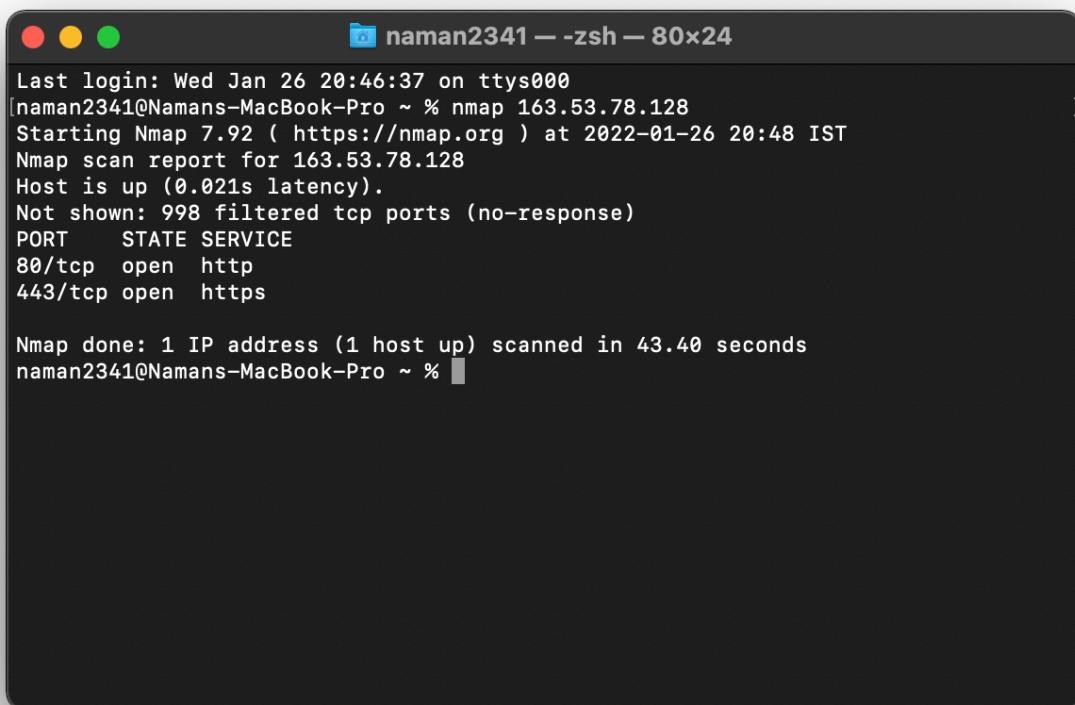


```
naman2341 — -zsh — 80x24
[naman2341@Namans-MacBook-Pro ~ % nmap www.pes.edu
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 20:48 IST
Nmap scan report for www.pes.edu (52.172.204.196)
Host is up (0.033s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 43.18 seconds
naman2341@Namans-MacBook-Pro ~ %
```

STEP 2: ALTERNATIVELY, USE AN IP ADDRESS TO SCAN.

### NMAP 163.53.78.128



```
naman2341 — -zsh — 80x24
Last login: Wed Jan 26 20:46:37 on ttys000
[naman2341@Namans-MacBook-Pro ~ % nmap 163.53.78.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 20:48 IST
Nmap scan report for 163.53.78.128
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 43.40 seconds
naman2341@Namans-MacBook-Pro ~ %
```

### STEP 3: SCAN MULTIPLE IP ADDRESS OR SUBNET (IPV4)

NMAP 192.168.1.1 192.168.1.2 192.168.1.3

```
[naman2341@Namans-MacBook-Pro ~ % nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 20:49 IST
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    filtered telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https

Nmap scan report for 192.168.1.2
Host is up (0.0092s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open     http
554/tcp   open     rtsp
5000/tcp  open     upnp

Nmap scan report for 192.168.1.3
Host is up (0.0036s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open     http
554/tcp   open     rtsp
5000/tcp  open     upnp
49152/tcp open     unknown

Nmap done: 3 IP addresses (3 hosts up) scanned in 4.18 seconds
```

---

### Questions on above observations:

- 1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?  
**HTTP 1.1**
- 2) When was the HTML file that you are retrieving last modified at the server?  
**Wed, 26 Jan 2022 13:12:11 GMT**
- 3) How to tell ping to exit after a specified number of ECHO\_REQUEST packets?  
**Ping website -c number\_of\_ECHO\_REQUESTS**
- 4) How will you identify remote host apps and OS?  
**sudo nmap -O -v ip\_addr**