Computer Networks Laboratory

UE20CS255

Name: Naman Choudhary	SRN: PES2UG20CS209	Section: D

Week 1

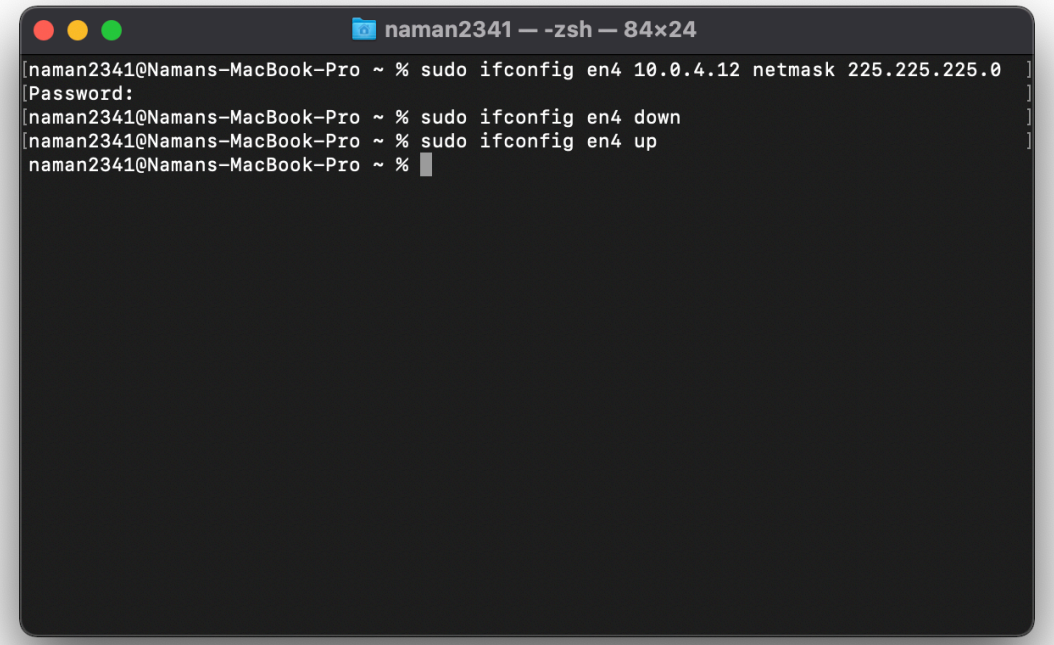
Study and understand the basic networking tools - Wireshark, Tcpdump, Ping, Traceroute.

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

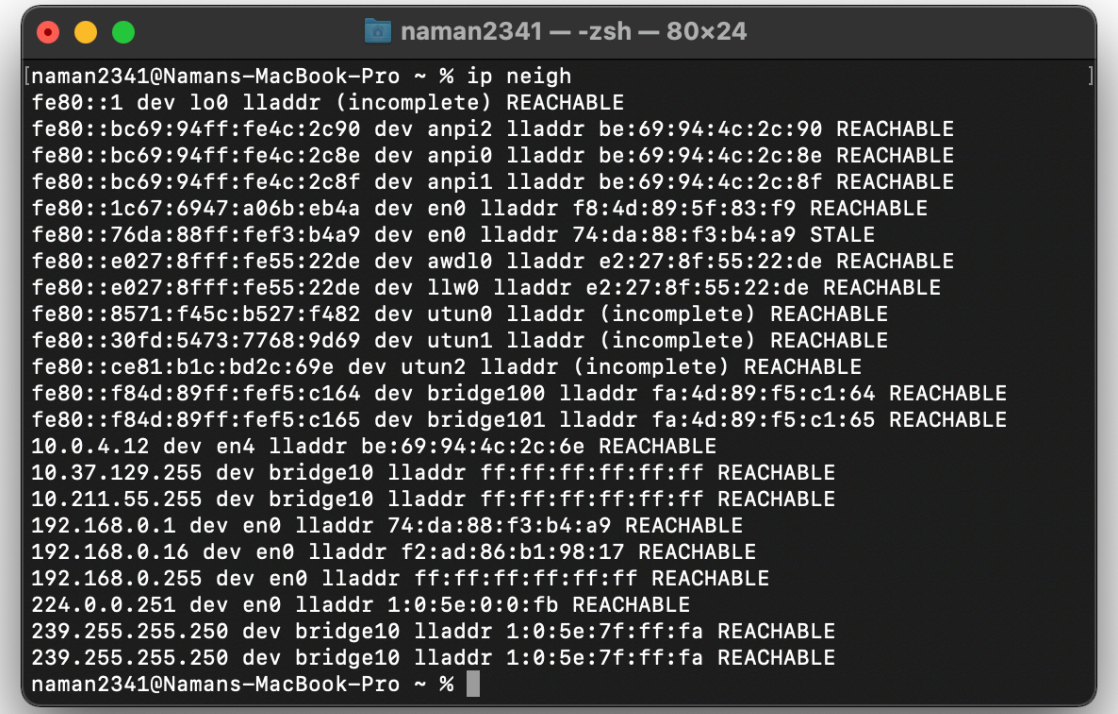
STEP 1:TO DISPLAY STATUS OF ALL ACTIVE NETWORK INTERFACES.

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

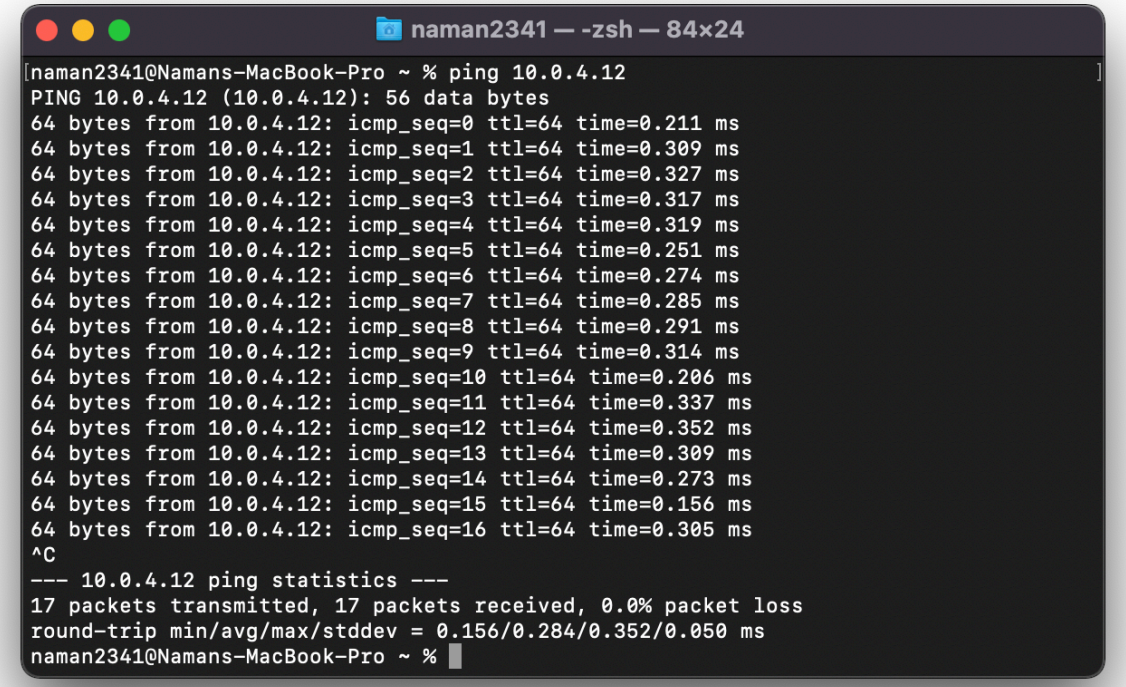


STEP 4:TO SHOW THE CURRENT NEIGHBOUR TABLE IN KERNEL



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



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

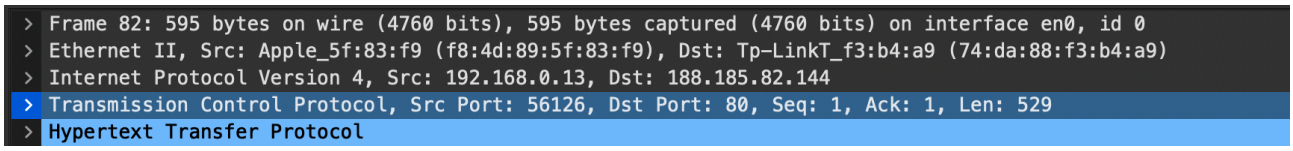
Details	First Echo Request	First Echo Reply
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

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

www.flipkart.com did not send/receive any HTTP packets, so http://info.cern.ch/ was used instead.



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

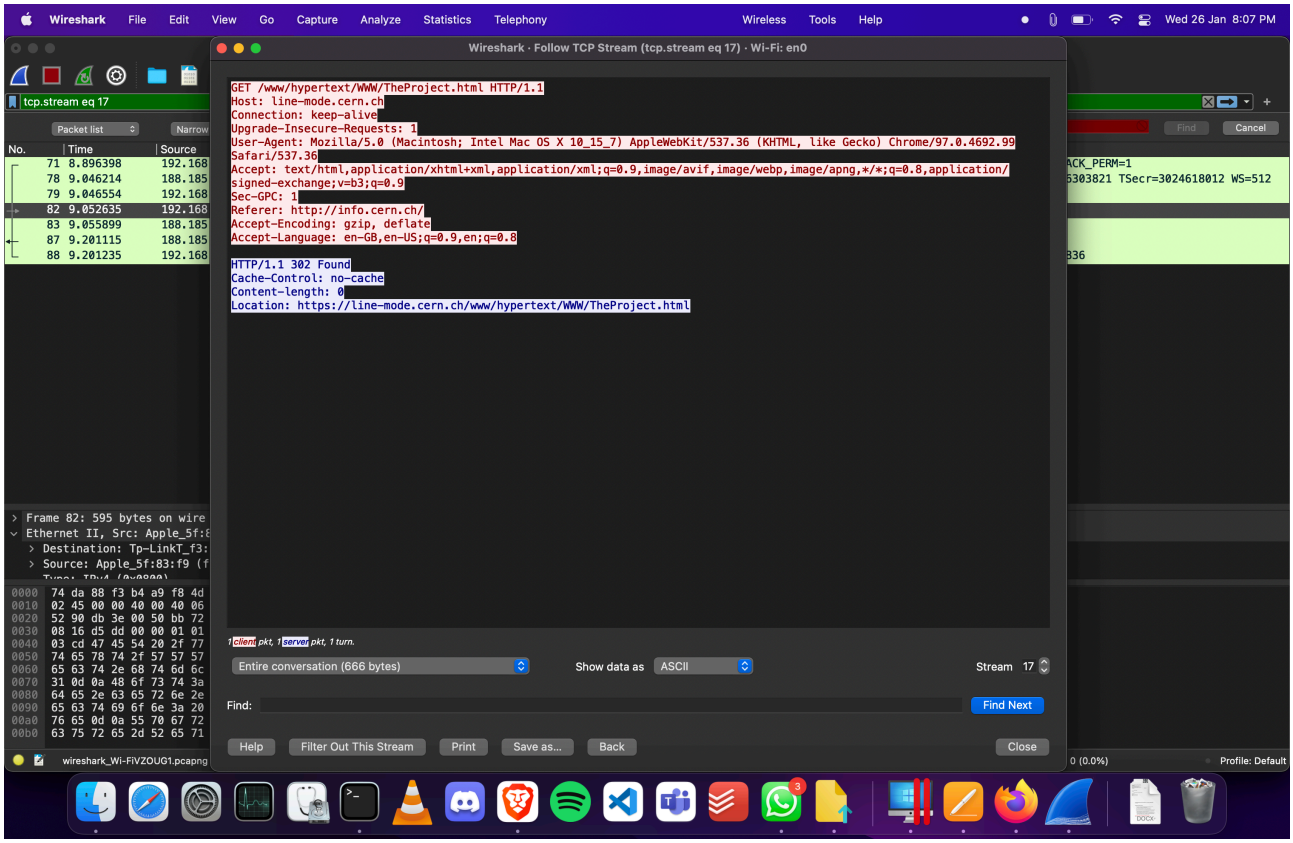
HTTP Request		HTTP Response	
Get	GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n	Server	Apache
Host	line-mode.cern.ch	Content-Type	text/html

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	https://line-mode.cern.ch/www/hypertext/WWW/TheProject.html
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.

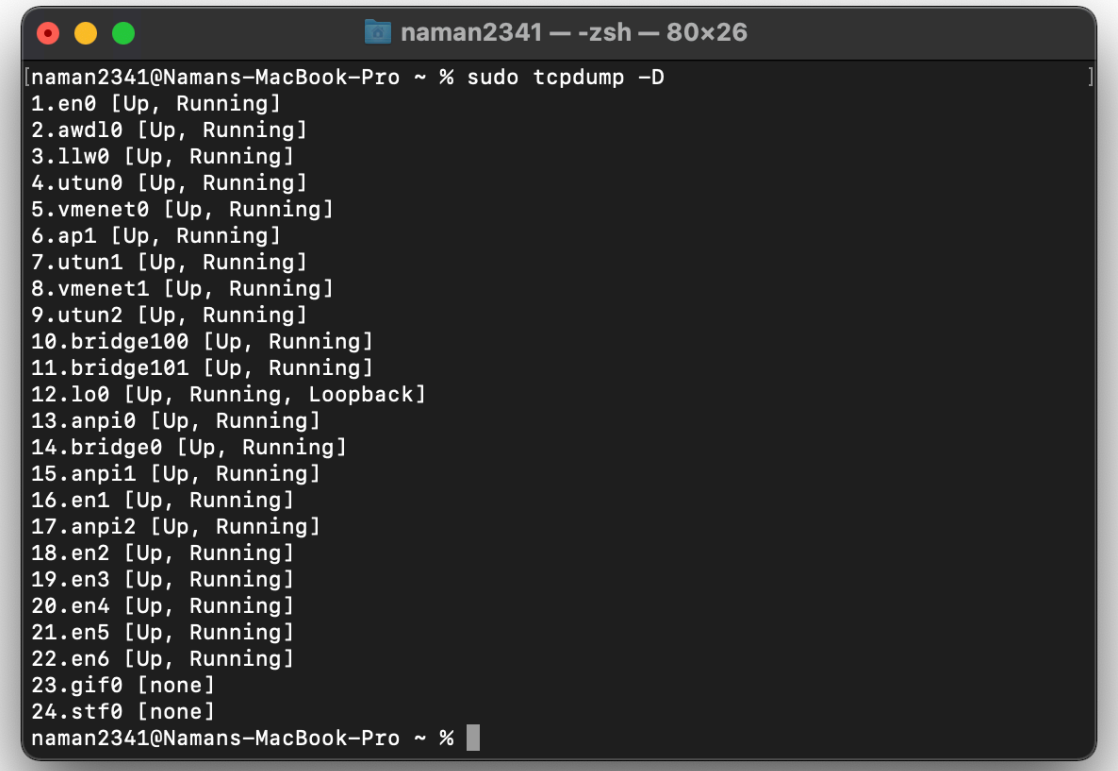
STEP 2: UPON FOLLOWING A TCP STREAM, SCREENSHOT THE WHOLE WINDOW



Task 4: Capturing packets with tcpdump

STEP 1: USE THE COMMAND TCPDUMP -D TO SEE WHICH INTERFACES ARE AVAILABLE FOR CAPTURE.

SUDO TCPDUMP -D

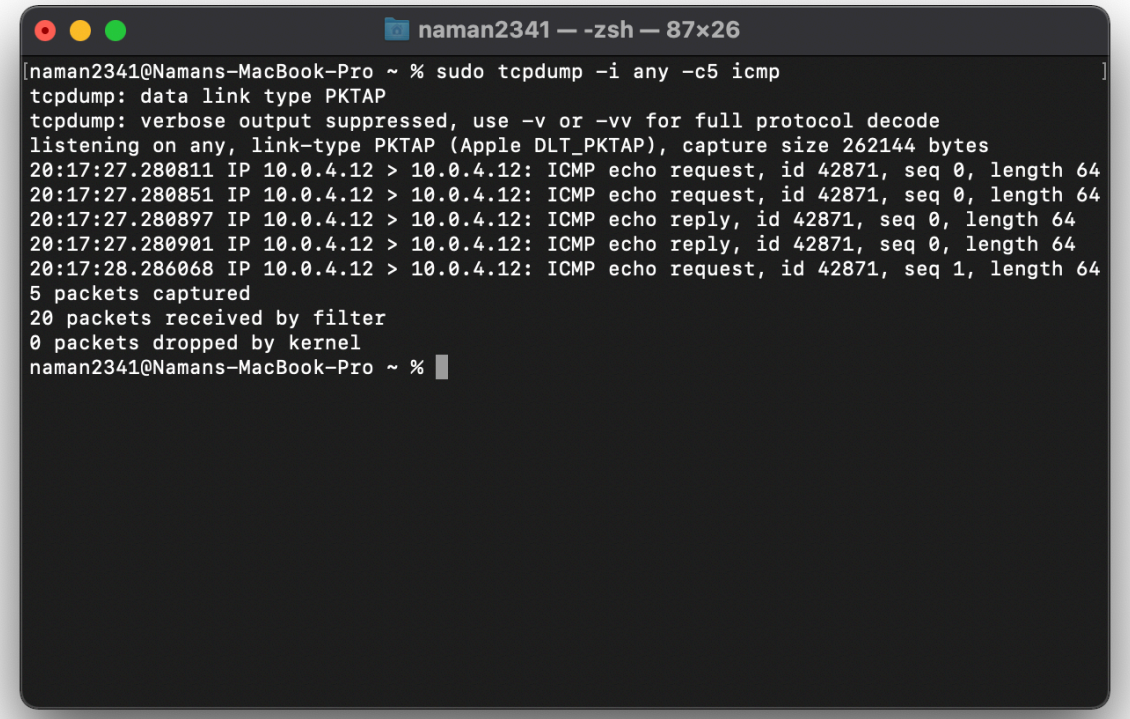


STEP 2: CAPTURE ALL PACKETS IN ANY INTERFACE BY RUNNING THIS COMMAND:
SUDO TCPDUMP -I ANY

Observation

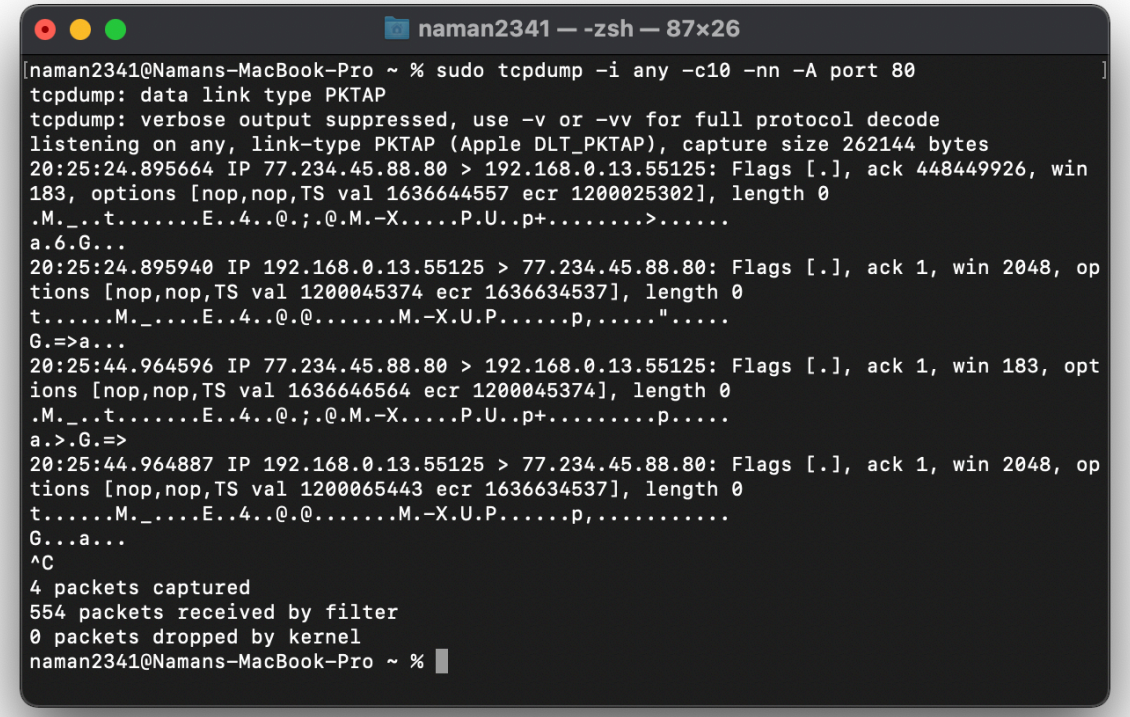
STEP 3: UNDERSTAND THE OUTPUT FORMAT.
STEP 4: TO FILTER PACKETS BASED ON PROTOCOL, SPECIFYING THE PROTOCOL IN THE COMMAND LINE. FOR EXAMPLE, CAPTURE ICMP PACKETS ONLY BY USING THIS COMMAND:

SUDO TCPDUMP -I ANY -C5 ICMP



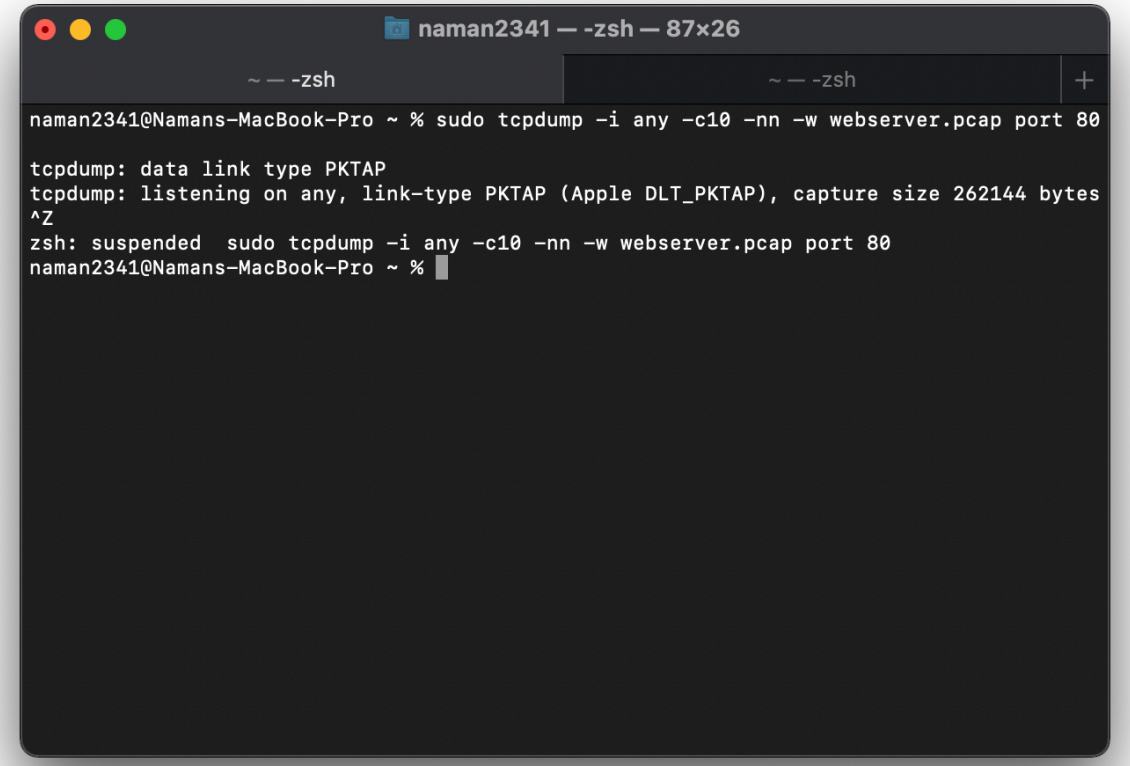
STEP 5: CHECK THE PACKET CONTENT. FOR EXAMPLE, INSPECT THE HTTP CONTENT OF A WEB REQUEST LIKE THIS:

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



STEP 6: TO SAVE PACKETS TO A FILE INSTEAD OF DISPLAYING THEM ON SCREEN, USE THE OPTION -W:

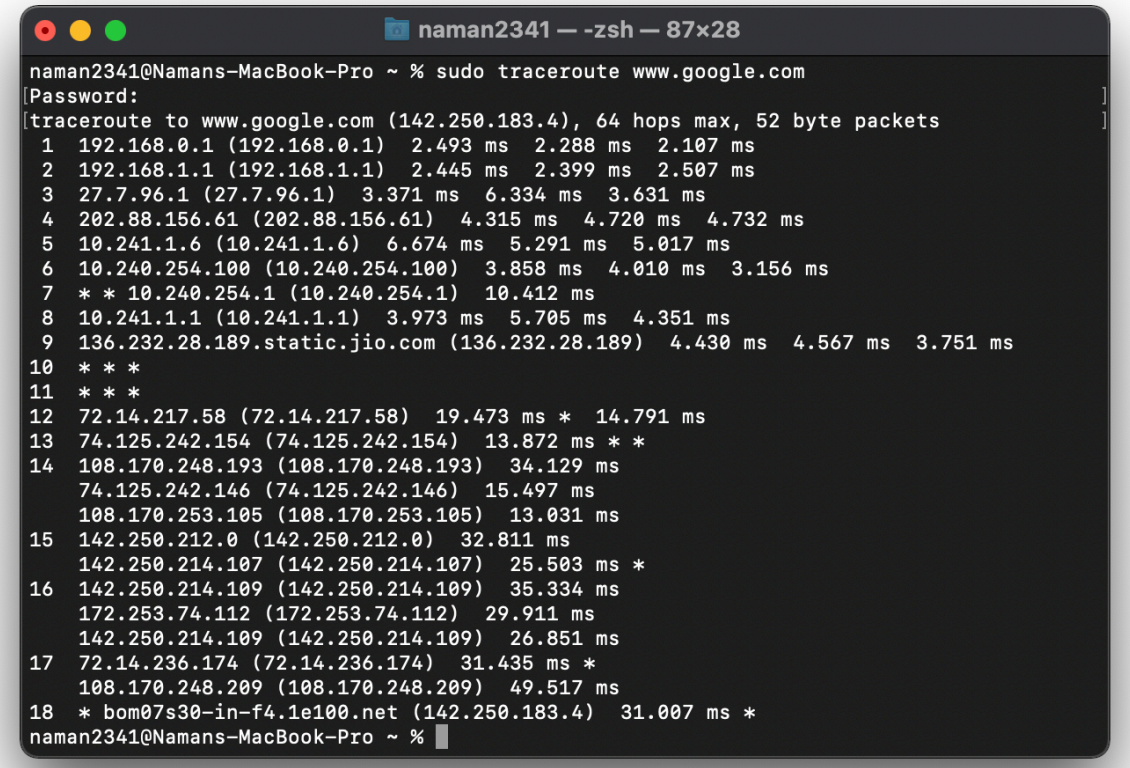
SUDO TCPDUMP -I ANY -C10 -NN -W WEBSERVER.PCAP PORT 80



Task 5: Perform Traceroute checks

STEP 1: RUN THE TRACEROUTE USING THE FOLLOWING COMMAND.

SUDO TRACEROUTE WWW.GOOGLE.COM

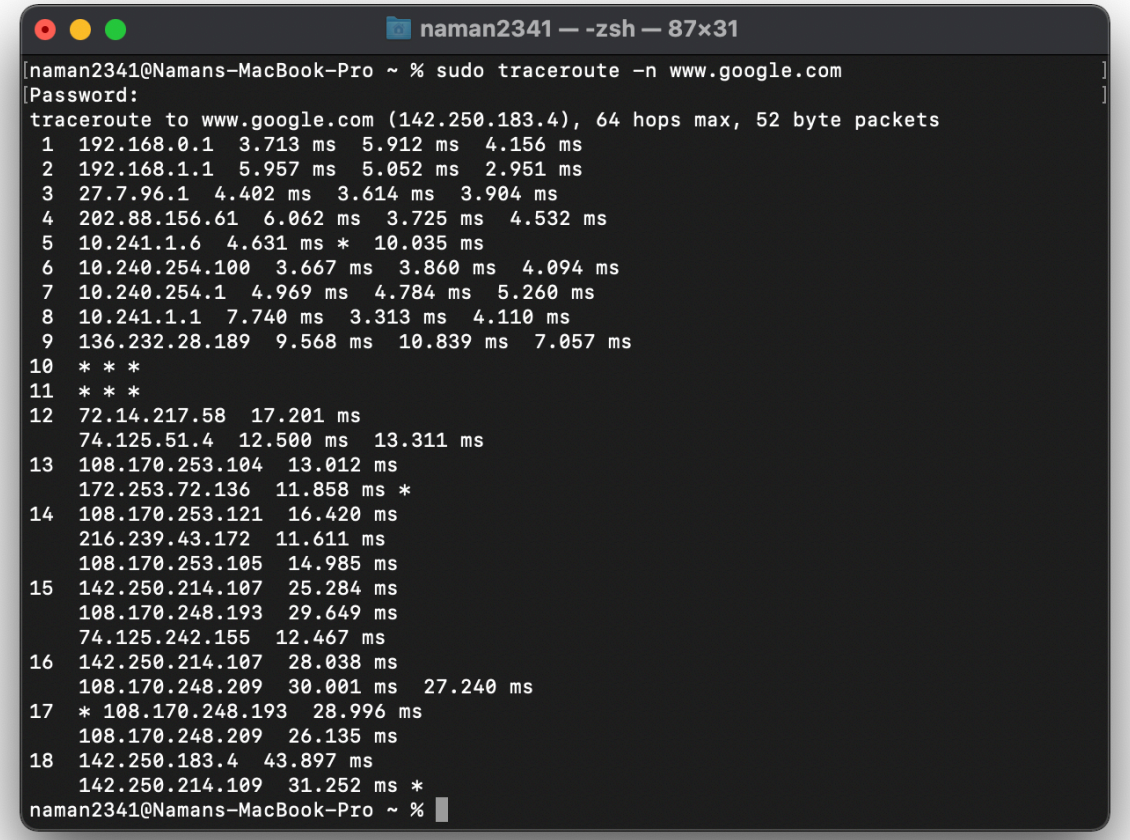


STEP 2: ANALYZE DESTINATION ADDRESS OF GOOGLE.COM AND NO. OF HOPS

Destination address : 142.250.183.4
Number of hops : 18

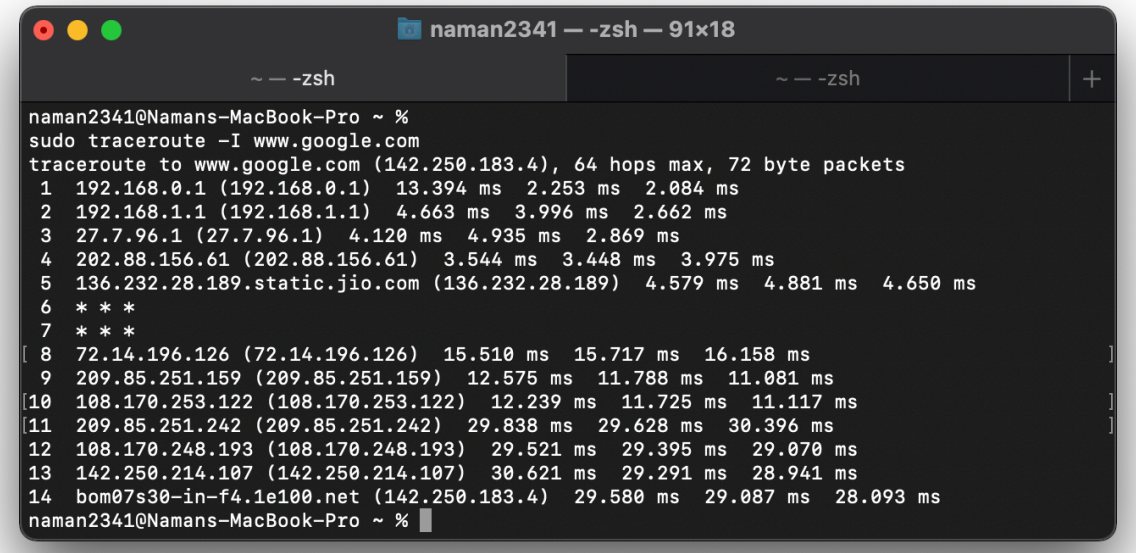
STEP 3: TO SPEED UP THE PROCESS, YOU CAN DISABLE THE MAPPING OF IP ADDRESSES WITH HOSTNAMES BY USING THE -N OPTION

SUDO TRACEROUTE -N WWW.GOOGLE.COM



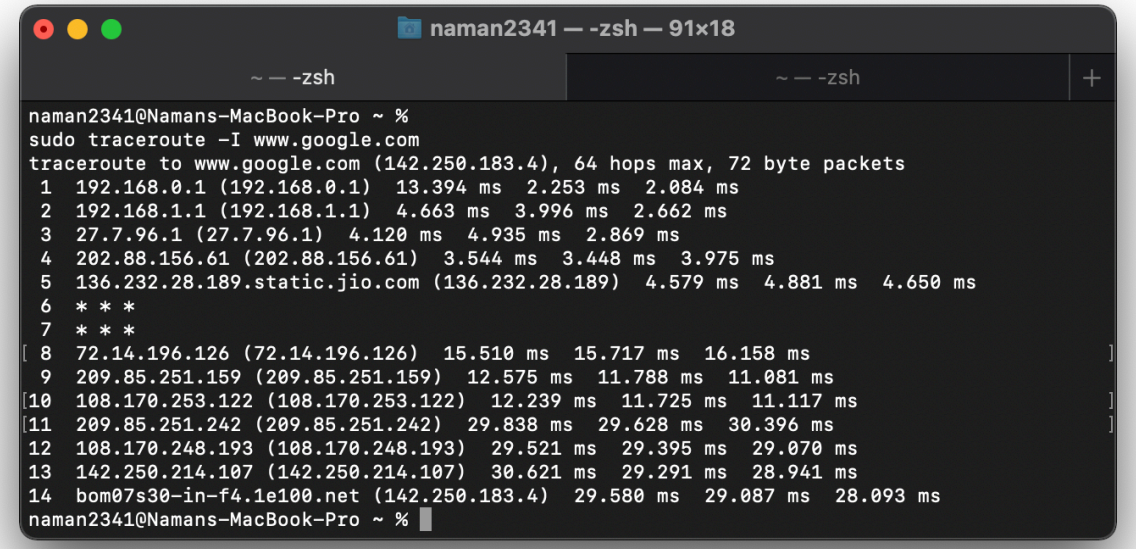
STEP 4: THE -I OPTION IS NECESSARY SO THAT THE TRACEROUTE USES ICMP.

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.

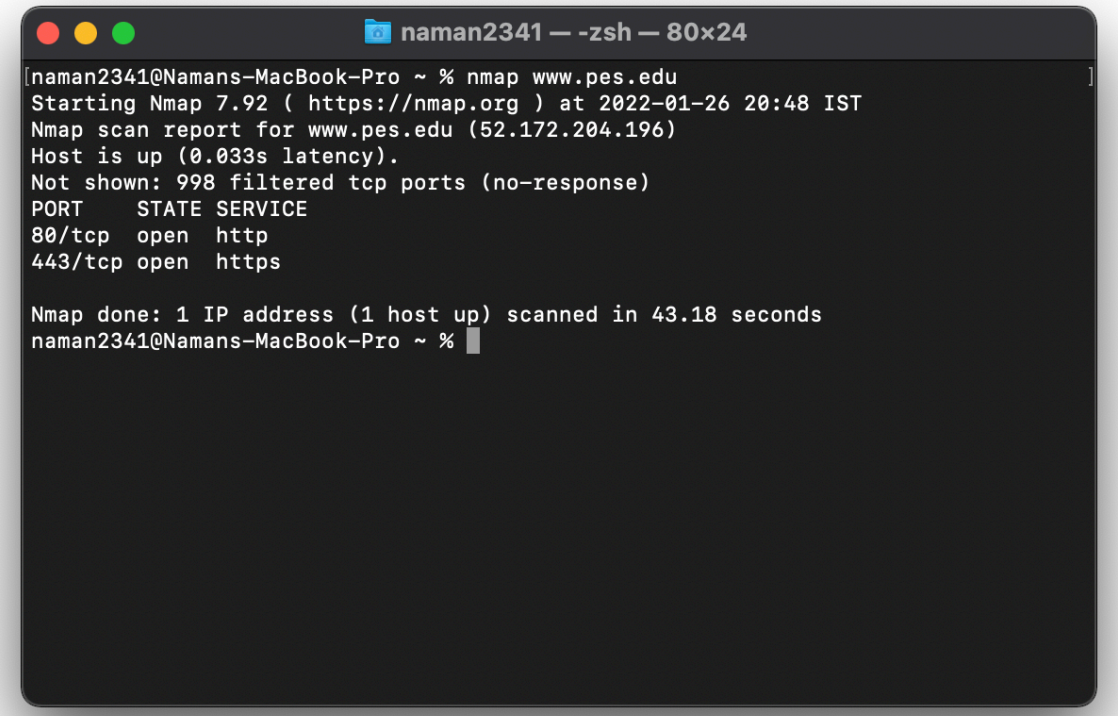
SUDO TRACEROUTE -T WWW.GOOGLE.COM



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

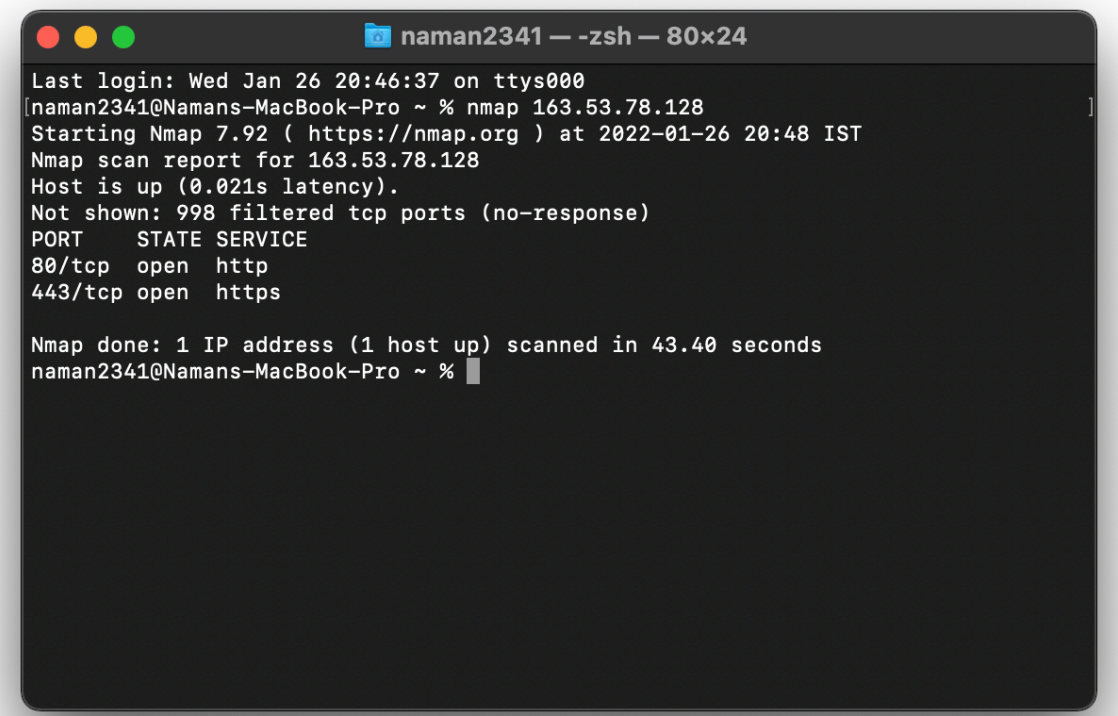
STEP 1: YOU CAN SCAN A HOST USING ITS HOST NAME OR IP ADDRESS, FOR INSTANCE.

NMAP WWW.PES.EDU



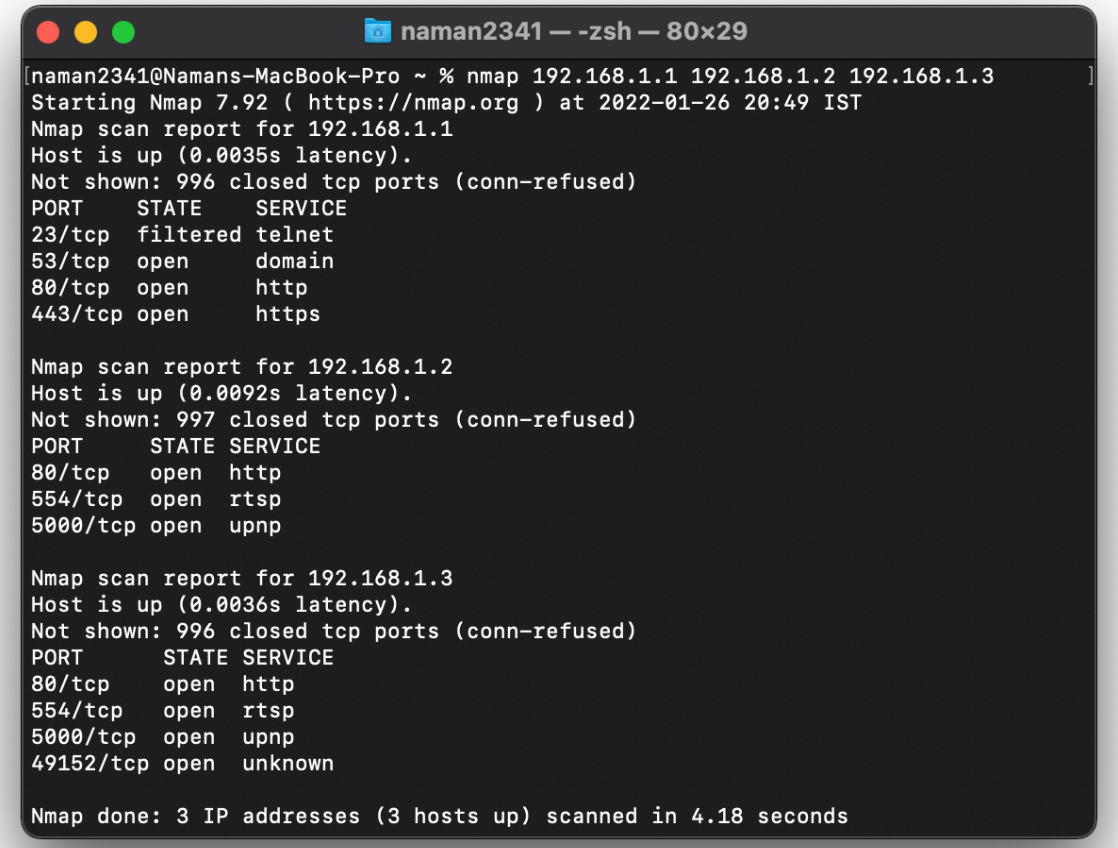
STEP 2: ALTERNATIVELY, USE AN IP ADDRESS TO SCAN.

NMAP 163.53.78.128



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

NMAP 192.168.1.1 192.168.1.2 192.168.1.3



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