Week #1

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

Learn and Understand Network Tools

1. Wireshark

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

2. Tcpdump

- Capture packets

3. Ping

- Test the connectivity between 2 systems

4. Traceroute

- Perform traceroute checks

5. Nmap

- Explore an entire network

IMPORTANT INSTRUCTIONS:

- This manual is written for Ubuntu Linux OS only. You can also execute these experiments on VirtualBox or VMWare platform.
- For few tasks, you may need to create 2 VMs for experimental setup.
- Perform **sudo apt-get update** before installing any tool or utility.
- Install any tool or utility using the command **sudo apt-get install name_of_the_tool**
- Take screenshots wherever necessary and upload it to Edmodo as a single PDF file. (Refer general guidelines for submission requirements).
- To define an IP address for your machine (e.g., Section – ‘a’ & Serial number is 1, then your IP address should be 10.0.1.1. Section – ‘h’ & & Serial number is 23, then your IP address should be 10.0.8.23) – applicable only for relevant tasks (which doesn’t requires internet connectivity to execute the tasks).

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

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

ifconfig (or) **ip addr show**

Analyze and fill the following table:

ip address table:

Interface name	IP address (IPv4 / IPv6)	MAC address	
Enp0s3	10.0.2.15	08:00:27:0c:3c:65	
lo	127.0.0.1		

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

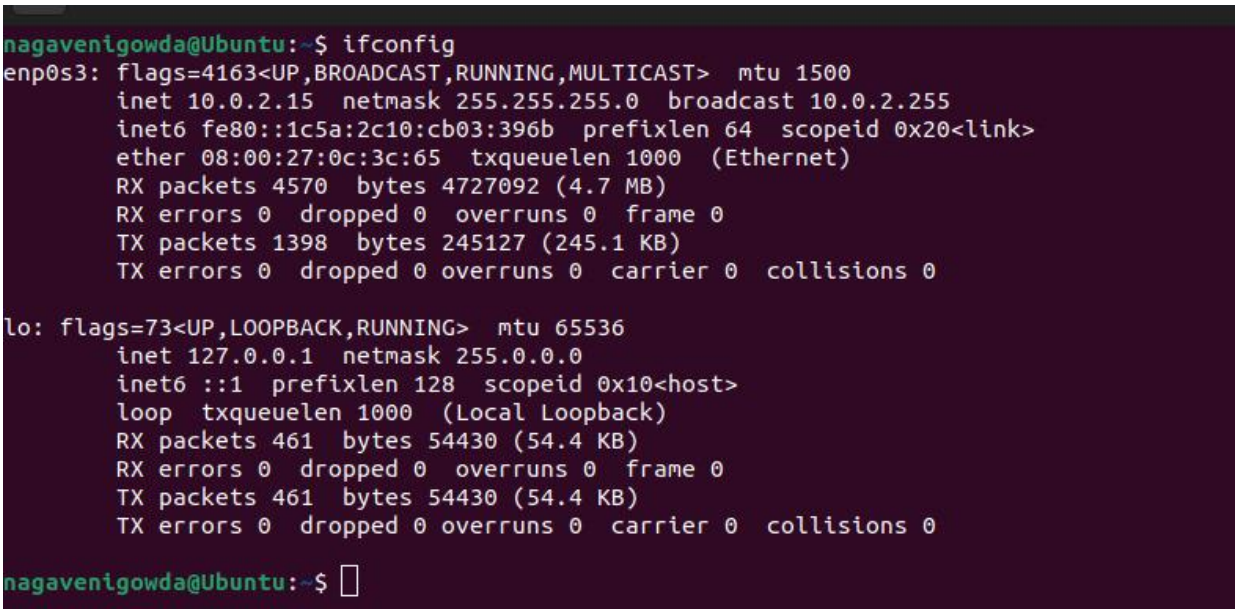
Step 3: To activate / deactivate a network interface, type.

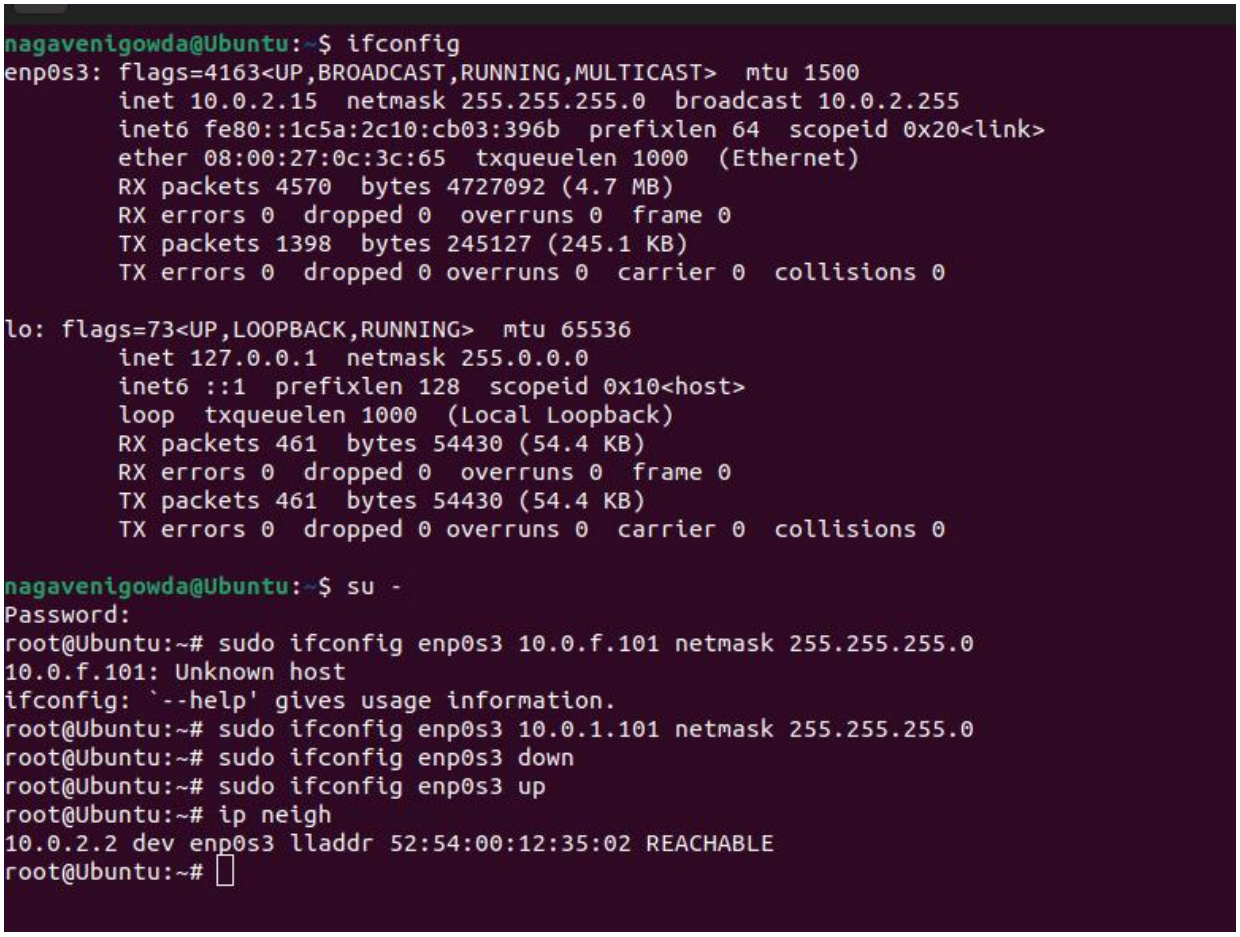
sudo ifconfig interface_name down

sudo ifconfig interface_name up

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

ip neigh





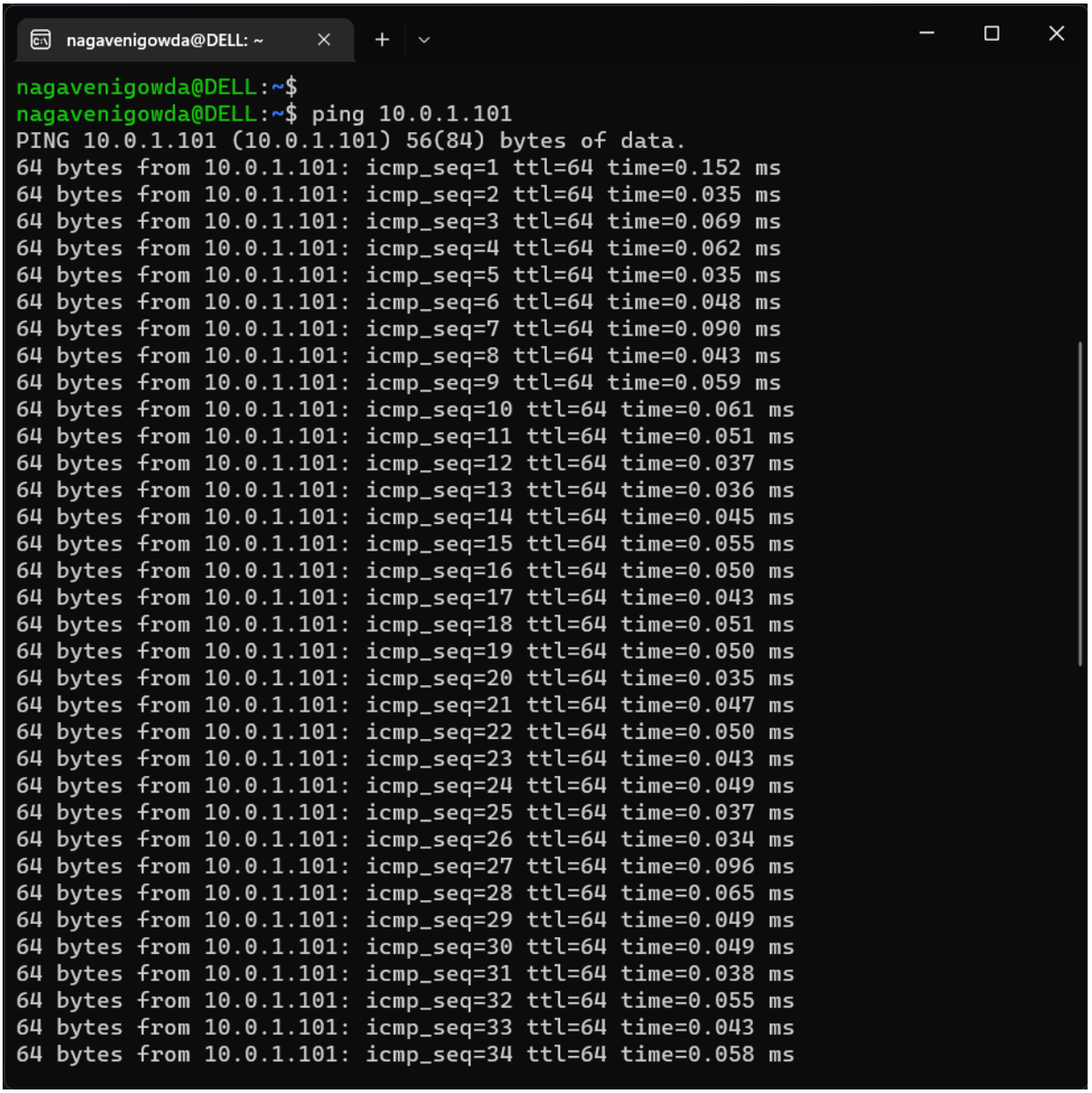
Task 2: Ping PDU (Packet Data Units or Packets) Capture

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**

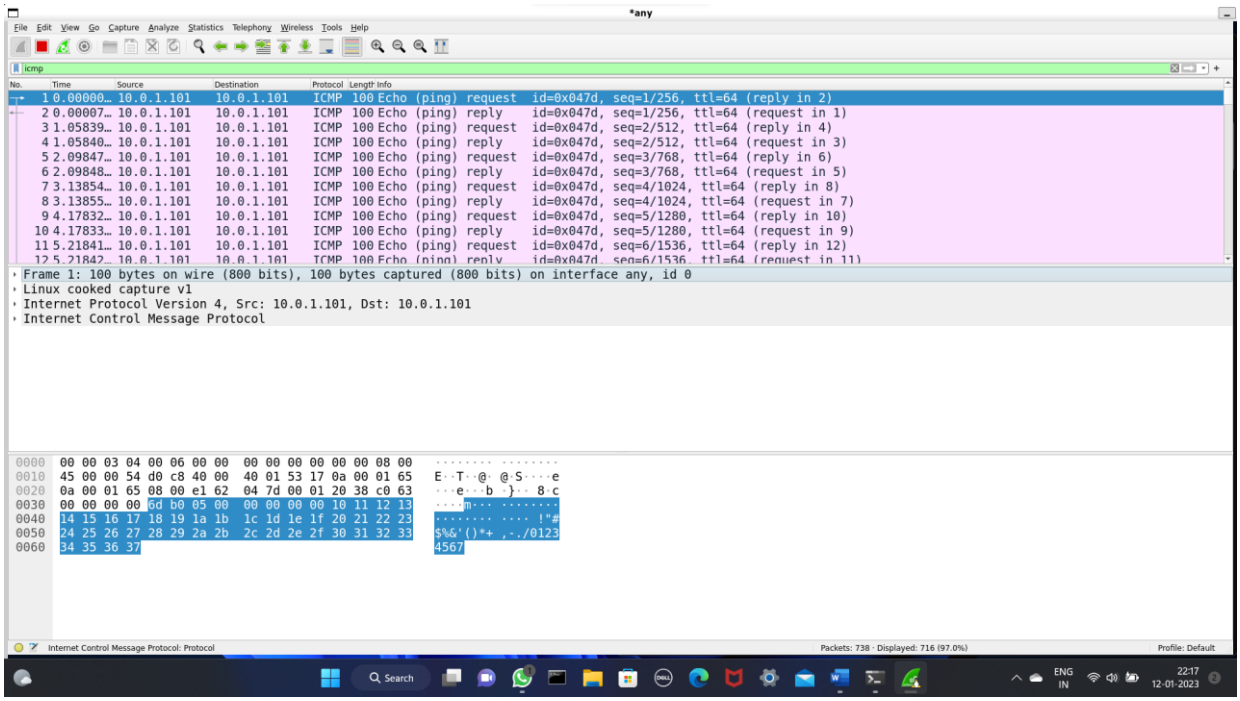


Observations to be made

Step 4: Analyze the following in Terminal

- TTL
- Protocol used by ping
- Time

Step 5: Analyze the following in Wireshark



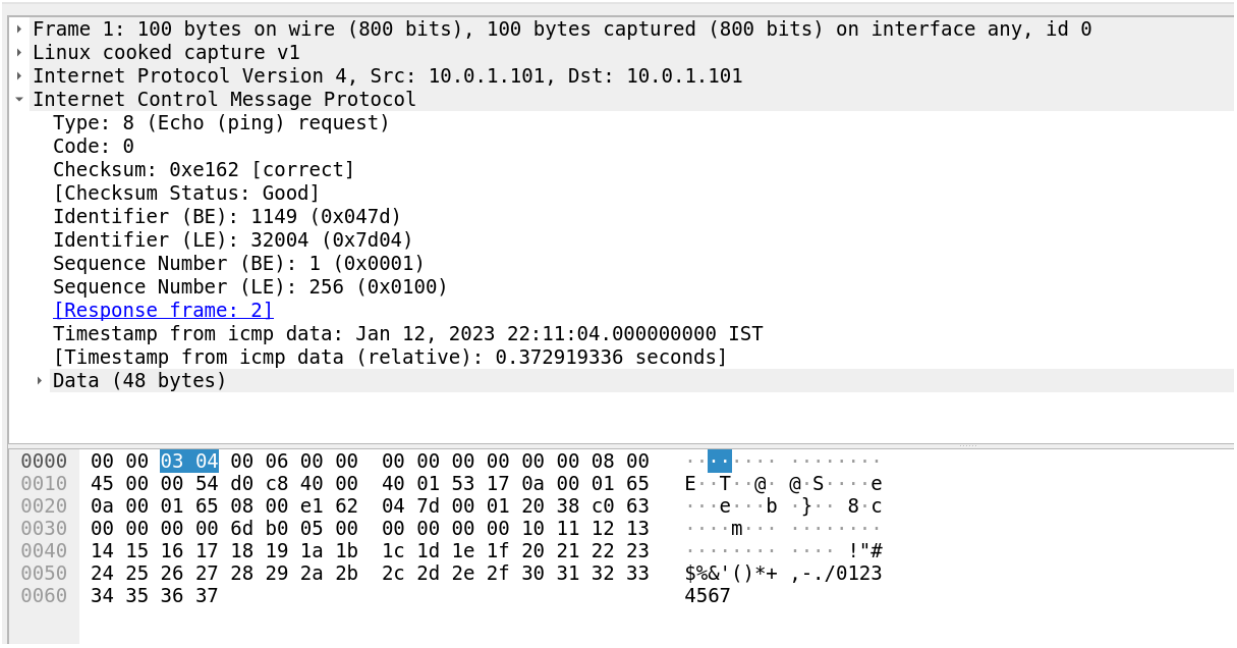
icmp

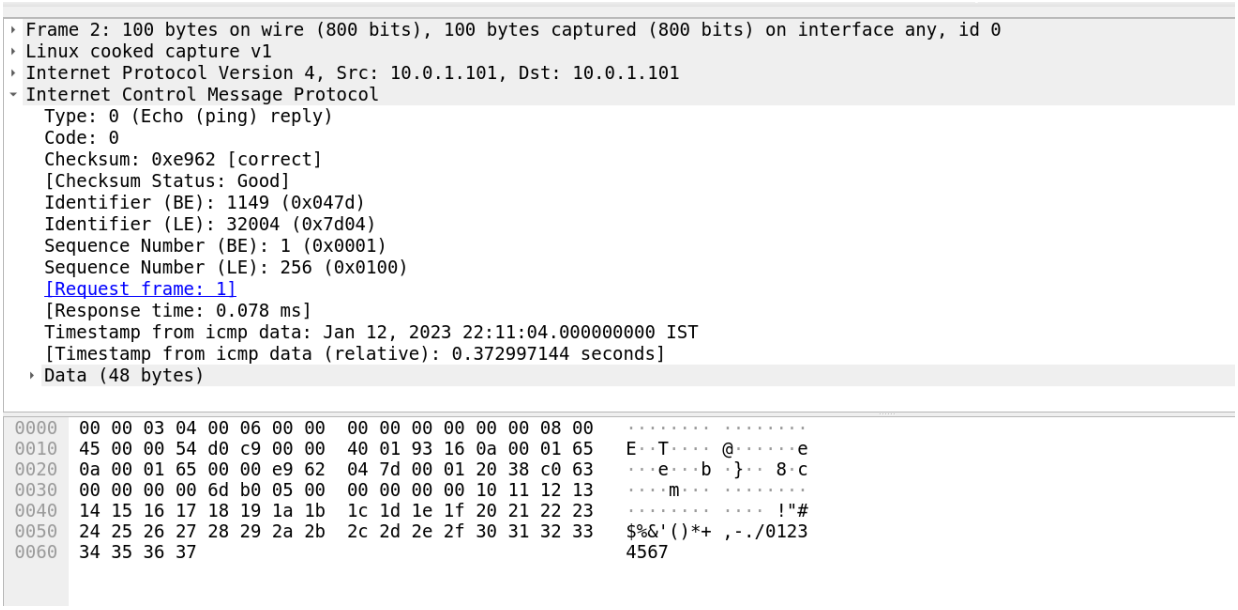
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=1/256, ttl=64 (reply in 2)
2	0.000077808	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=1/256, ttl=64 (request in 1)
3	1.058397455	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=2/512, ttl=64 (reply in 4)
4	1.058406585	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=2/512, ttl=64 (request in 3)
5	2.098473285	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=3/768, ttl=64 (reply in 6)
6	2.098485267	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=3/768, ttl=64 (request in 5)
7	3.138542499	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=4/1024, ttl=64 (reply in 8)
8	3.138556639	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=4/1024, ttl=64 (request in 7)
9	4.178324129	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=5/1280, ttl=64 (reply in 10)
10	4.178332702	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=5/1280, ttl=64 (request in 9)
11	5.218417033	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=6/1536, ttl=64 (reply in 12)
12	5.218429249	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=6/1536, ttl=64 (request in 11)
13	6.258401724	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=7/1792, ttl=64 (reply in 14)
14	6.258422618	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=7/1792, ttl=64 (request in 13)
15	7.298455819	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=8/2048, ttl=64 (reply in 16)
16	7.298467225	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=8/2048, ttl=64 (request in 15)
17	8.338457748	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) request id=0x047d, seq=9/2304, ttl=64 (reply in 18)
18	8.338473416	10.0.1.101	10.0.1.101	ICMP	100	Echo (ping) reply id=0x047d, seq=9/2304, ttl=64 (request in 17)

```
Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.1.101, Dst: 10.0.1.101
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 d0 c8 40 00  40 01 53 17 0a 00 01 65   E··T··@· @·S····e
0020  0a 00 01 65 08 00 e1 62  04 7d 00 01 20 38 c0 63   ···e···b ·}·· 8·c
0030  00 00 00 00 6d b0 05 00  00 00 00 00 10 11 12 13   ····m··· ........
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
```

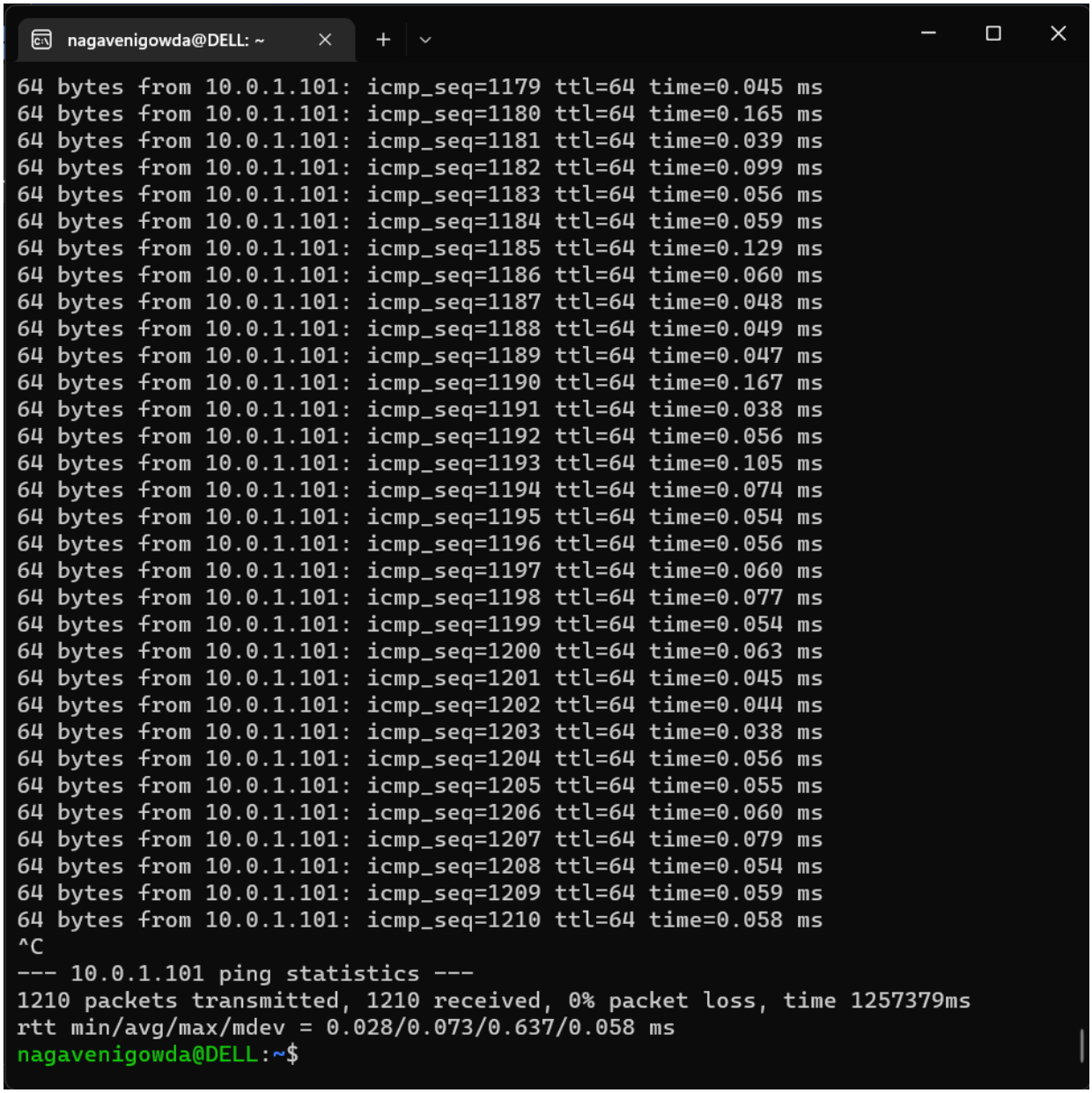
On Packet List Pane, select the first echo packet on the list. On Packet Details Pane, click on each of the four "+" to expand the information. Analyze the frames with the first echo request and echo reply and complete the table below.





Details	First Echo Request	First Echo Reply
Frame Number	Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0	Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Source IP address	Src: 10.0.1.101	Src: 10.0.1.101
Destination IP address	Dst: 10.0.1.101	Dst: 10.0.1.101
ICMP Type Value	Type: 8 (Echo (ping) request)	Type: 0 (Echo (ping) reply)
ICMP Code Value	Code: 0	Code: 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	Version 4	Version 4
Time To Live (TTL) Value	Timestamp from icmp data: Jan 12, 2023 22:11:04.000000000 IST [Timestamp from icmp data (relative): 0.372919336 seconds]	Timestamp from icmp data: Jan 12, 2023 22:11:04.000000000 IST [Timestamp from icmp data (relative): 0.372997144 seconds]

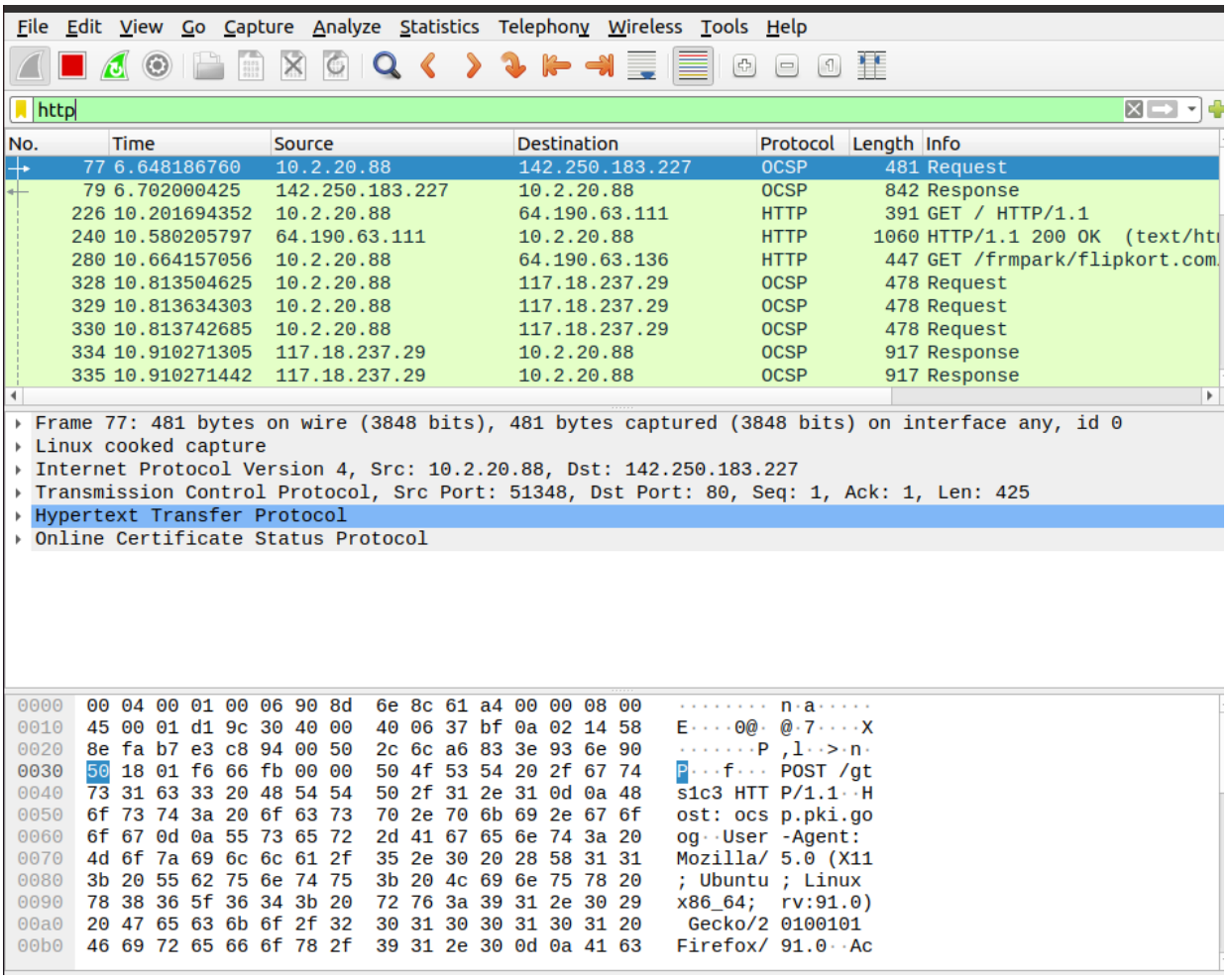


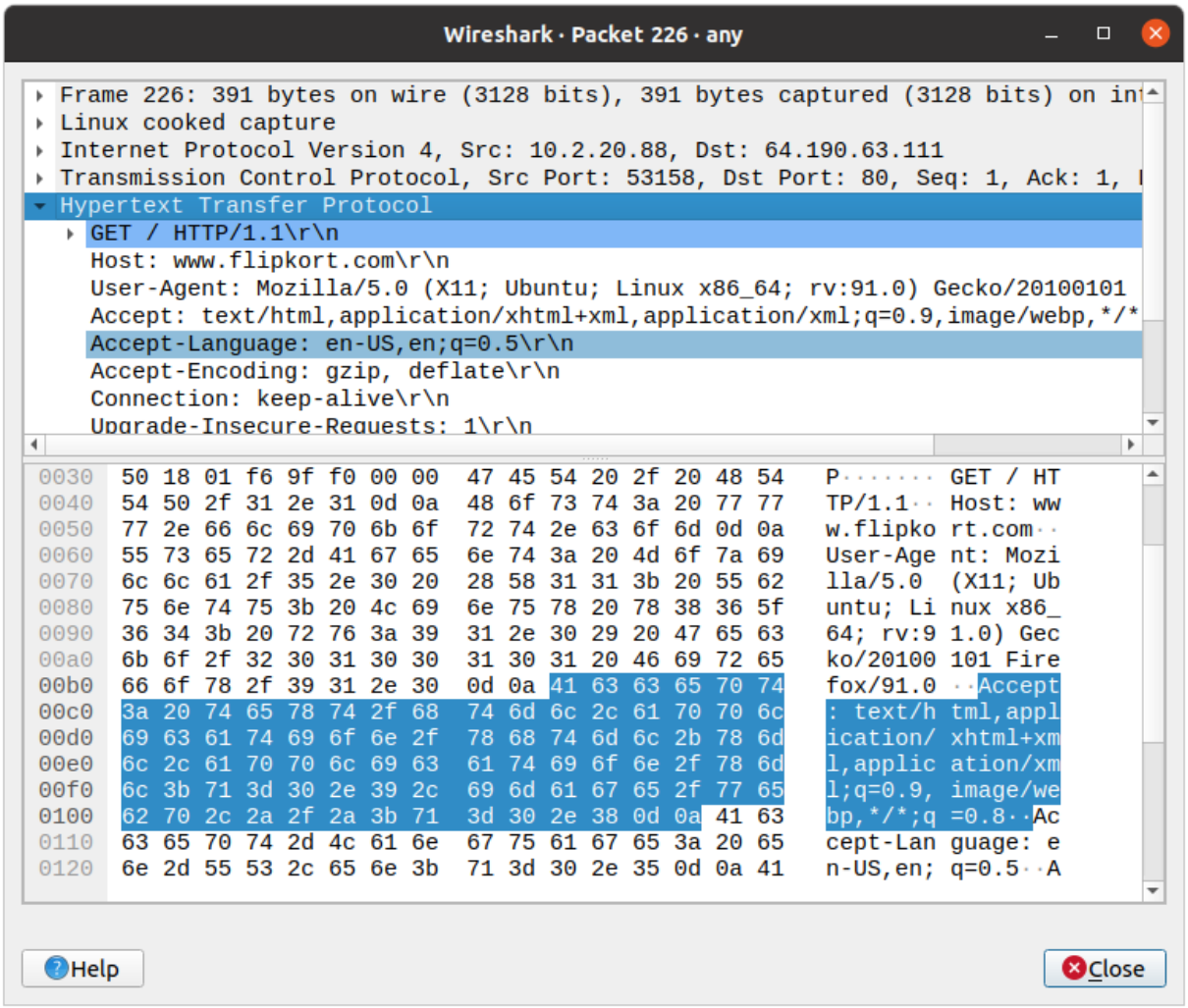
Task 3: HTTP PDU Capture

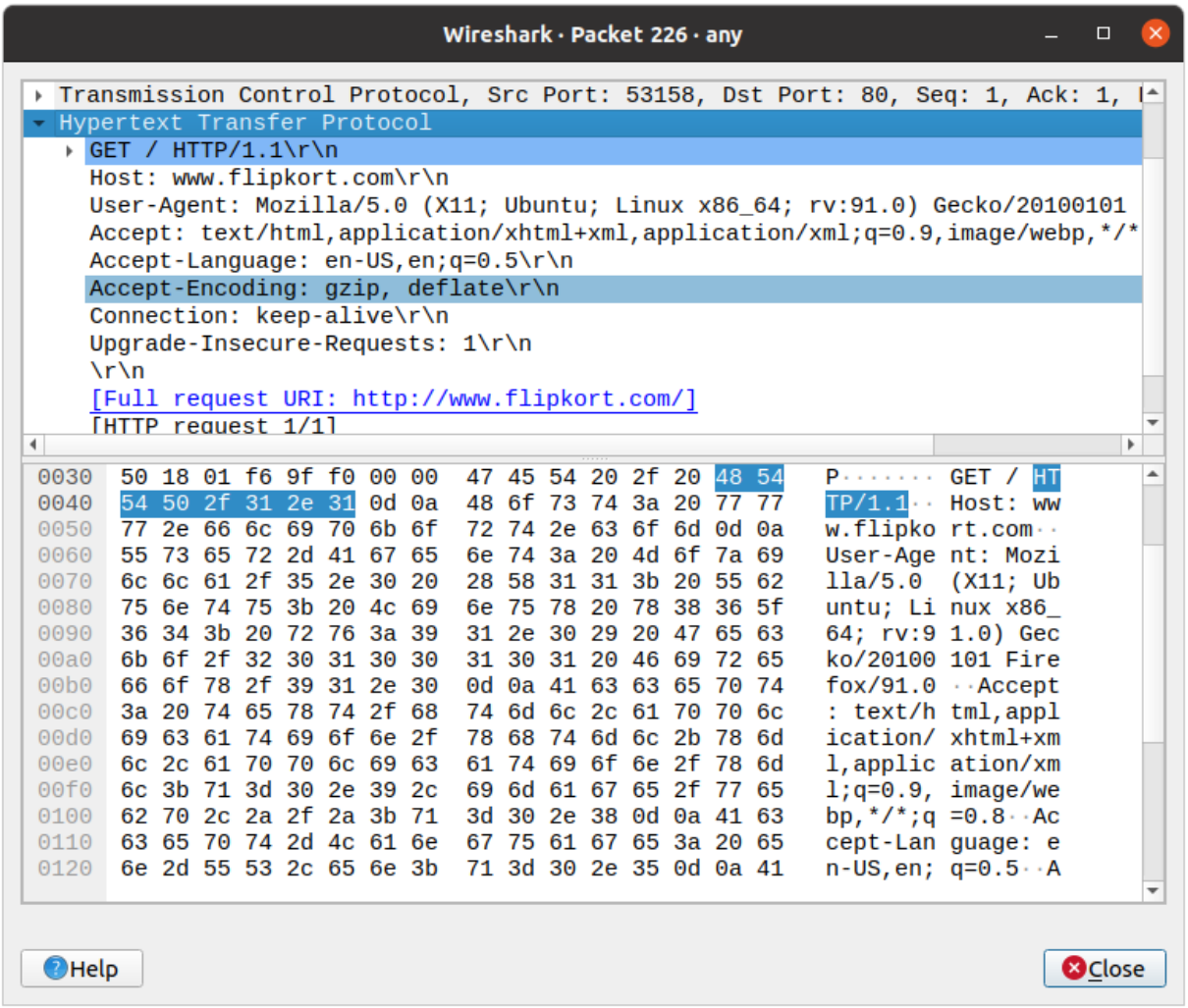
Using Wireshark's Filter feature

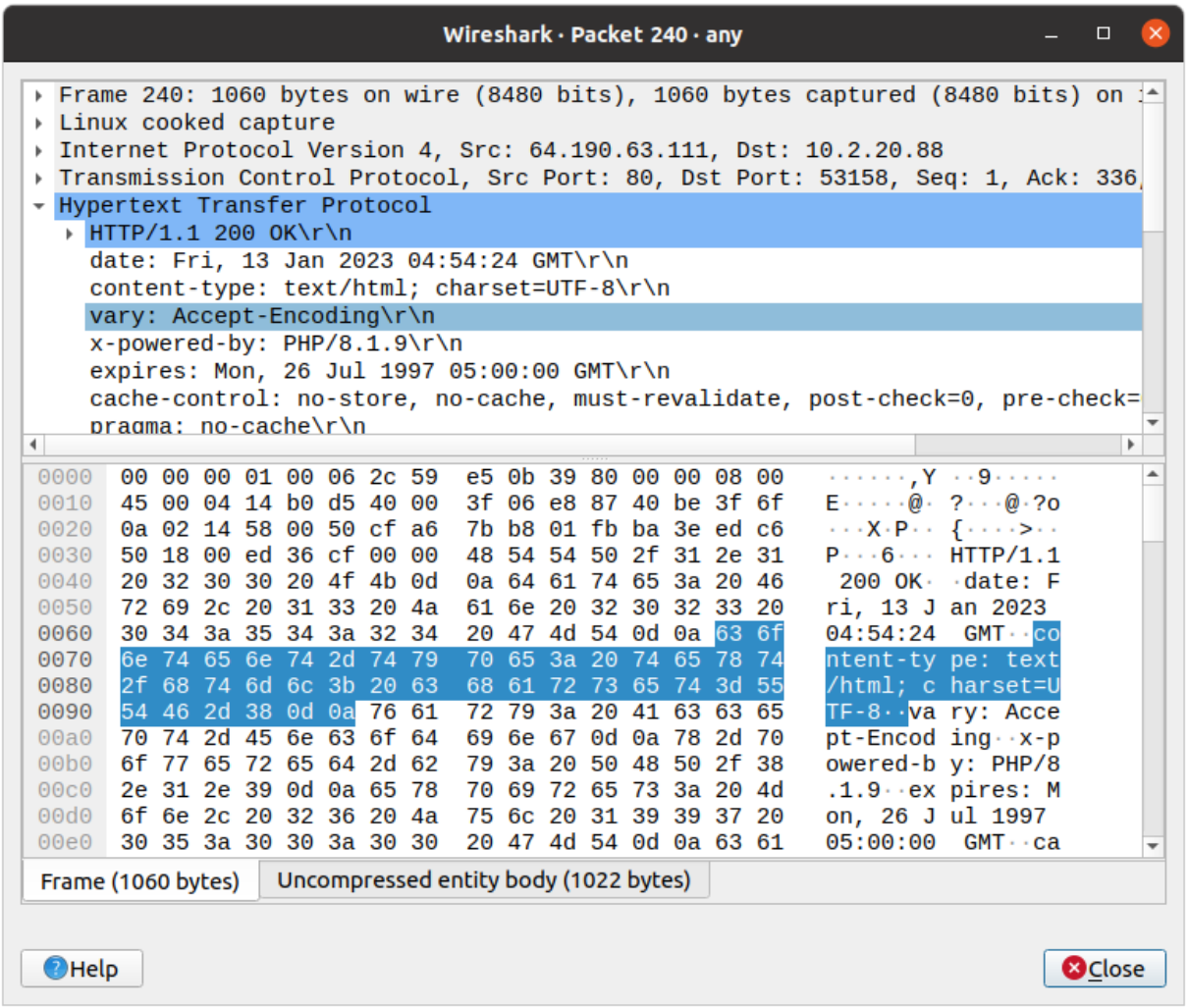
Step 1: Launch Wireshark and select 'any' interface. On the Filter toolbar, type-in 'http' and press enter

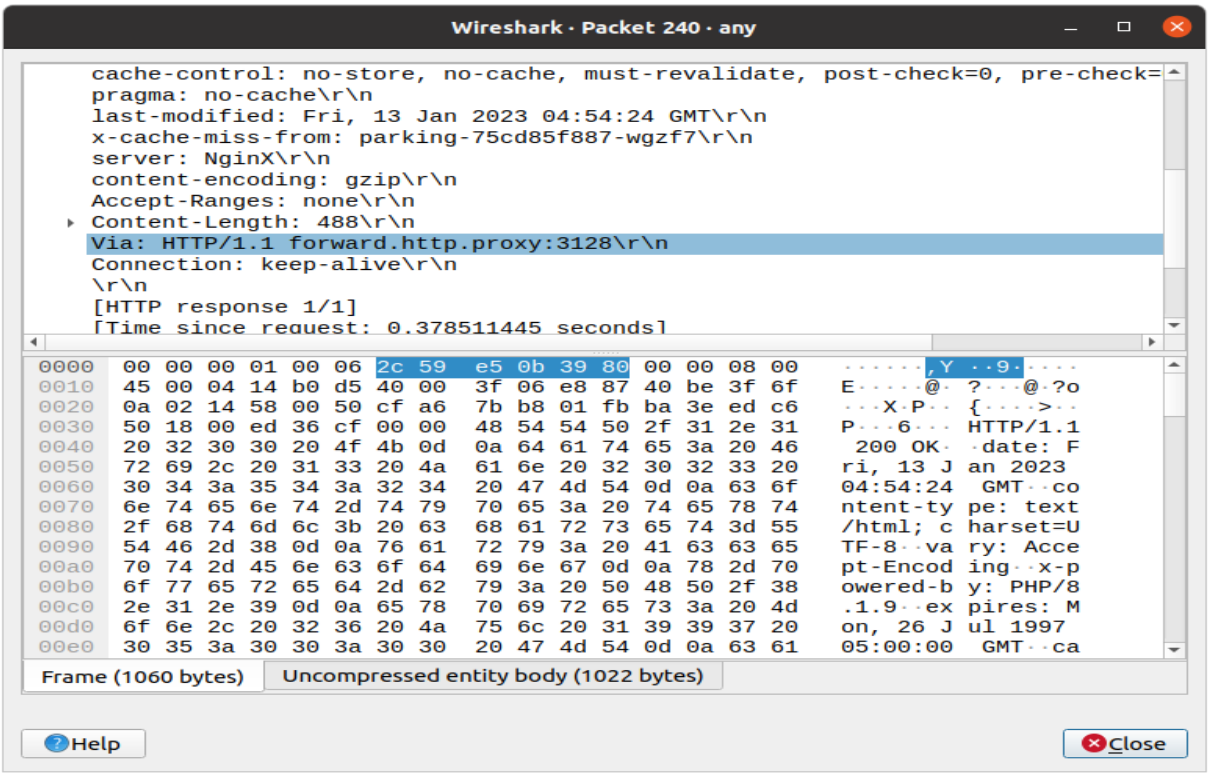
Step 2: Open Firefox browser, and browse www.flipkart.com

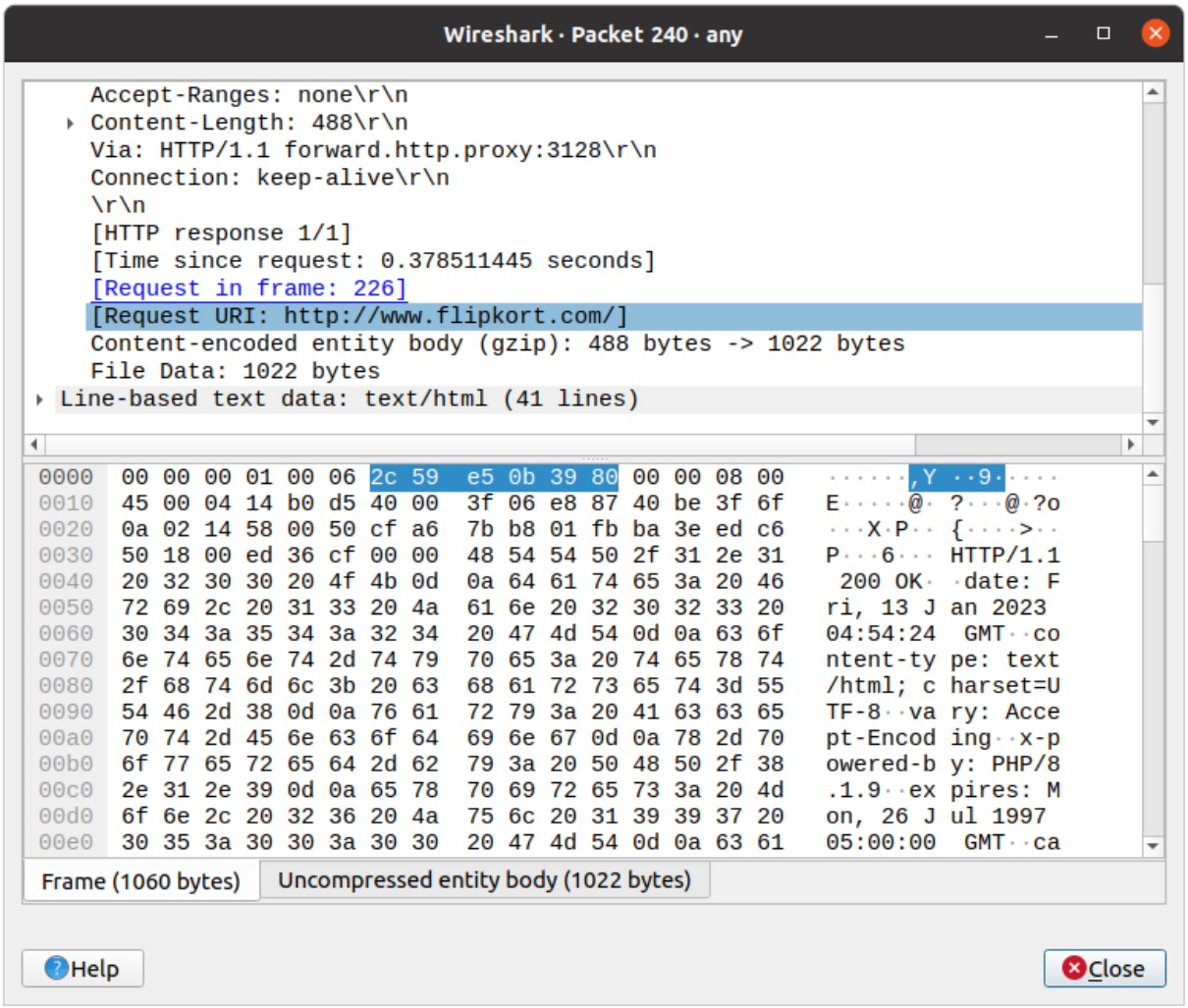

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
77 6.648186760 10.2.20.88 142.250.183.227 OCSP 481 Request
79 6.702000425 142.250.183.227 10.2.20.88 OCSP 842 Response
226 10.201694352 10.2.20.88 64.190.63.111 HTTP 391 GET / HTTP/1.1
240 10.580205797 64.190.63.111 10.2.20.88 HTTP 1060 HTTP/1.1 200 OK (text/ht
280 10.664157056 10.2.20.88 64.190.63.136 HTTP 447 GET /frmpark/flipkort.com
328 10.813504625 10.2.20.88 117.18.237.29 OCSP 478 Request
329 10.813634303 10.2.20.88 117.18.237.29 OCSP 478 Request
330 10.813742685 10.2.20.88 117.18.237.29 OCSP 478 Request
334 10.910271305 117.18.237.29 10.2.20.88 OCSP 917 Response
335 10.910271442 117.18.237.29 10.2.20.88 OCSP 917 Response
Frame 77: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.2.20.88, Dst: 142.250.183.227
Transmission Control Protocol, Src Port: 51348, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
Hypertext Transfer Protocol
Online Certificate Status Protocol
0000 00 04 00 01 00 06 90 8d 6e 8c 61 a4 00 00 08 00 ..... n a.....
0010 45 00 01 d1 9c 30 40 00 40 06 37 bf 0a 02 14 58 E....0@. @.7....X
0020 8e fa b7 e3 c8 94 00 50 2c 6c a6 83 3e 93 6e 90 .....P ,l..>.n.
0030 50 18 01 f6 66 fb 00 00 50 4f 53 54 20 2f 67 74 P...f... POST /gt
0040 73 31 63 33 20 48 54 54 50 2f 31 2e 31 0d 0a 48 s1c3 HTT P/1.1..H
0050 6f 73 74 3a 20 6f 63 73 70 2e 70 6b 69 2e 67 6f ost: ocs p.pki.go
0060 6f 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 og..User -Agent:
0070 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 Mozilla/ 5.0 (X11
0080 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 ; Ubuntu ; Linux
0090 78 38 36 5f 36 34 3b 20 72 76 3a 39 31 2e 30 29 x86_64; rv:91.0)
00a0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2 0100101
00b0 46 69 72 65 66 6f 78 2f 39 31 2e 30 0d 0a 41 63 Firefox/ 91.0..Ac


Wireshark · Packet 226 · any
Frame 226: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on int
Linux cooked capture
Internet Protocol Version 4, Src: 10.2.20.88, Dst: 64.190.63.111
Transmission Control Protocol, Src Port: 53158, Dst Port: 80, Seq: 1, Ack: 1,
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.flipkort.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
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
0030 50 18 01 f6 9f f0 00 00 47 45 54 20 2f 20 48 54 P····· GET / HT
0040 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 TP/1.1·· Host: ww
0050 77 2e 66 6c 69 70 6b 6f 72 74 2e 63 6f 6d 0d 0a w.flipko rt.com··
0060 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0070 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 62 lla/5.0 (X11; Ub
0080 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f untu; Li nux x86_
0090 36 34 3b 20 72 76 3a 39 31 2e 30 29 20 47 65 63 64; rv:9 1.0) Gec
00a0 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 ko/20100 101 Fire
00b0 66 6f 78 2f 39 31 2e 30 0d 0a 41 63 63 65 70 74 fox/91.0 ··Accept
00c0 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl
00d0 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm
00e0 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm
00f0 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 l;q=0.9, image/we
0100 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 bp,*/*;q =0.8··Ac
0110 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e
0120 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 n-US,en; q=0.5··A
Help
Close


Wireshark · Packet 226 · any
Transmission Control Protocol, Src Port: 53158, Dst Port: 80, Seq: 1, Ack: 1,
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.flipkort.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
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.flipkort.com/]
[HTTP request 1/1]
0030 50 18 01 f6 9f f0 00 00 47 45 54 20 2f 20 48 54 P····· GET / HT
0040 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 TP/1.1·· Host: ww
0050 77 2e 66 6c 69 70 6b 6f 72 74 2e 63 6f 6d 0d 0a w.flipko rt.com··
0060 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0070 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 62 lla/5.0 (X11; Ub
0080 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f untu; Li nux x86_
0090 36 34 3b 20 72 76 3a 39 31 2e 30 29 20 47 65 63 64; rv:9 1.0) Gec
00a0 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 ko/20100 101 Fire
00b0 66 6f 78 2f 39 31 2e 30 0d 0a 41 63 63 65 70 74 fox/91.0 ··Accept
00c0 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl
00d0 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm
00e0 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm
00f0 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 l;q=0.9, image/we
0100 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 bp,*/*;q =0.8··Ac
0110 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e
0120 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 n-US,en; q=0.5··A
Help
Close


Wireshark · Packet 240 · any
Frame 240: 1060 bytes on wire (8480 bits), 1060 bytes captured (8480 bits) on
Linux cooked capture
Internet Protocol Version 4, Src: 64.190.63.111, Dst: 10.2.20.88
Transmission Control Protocol, Src Port: 80, Dst Port: 53158, Seq: 1, Ack: 336,
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
date: Fri, 13 Jan 2023 04:54:24 GMT\r\n
content-type: text/html; charset=UTF-8\r\n
vary: Accept-Encoding\r\n
x-powered-by: PHP/8.1.9\r\n
expires: Mon, 26 Jul 1997 05:00:00 GMT\r\n
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
pragma: no-cache\r\n
0000 00 00 00 01 00 06 2c 59 e5 0b 39 80 00 00 08 00 ,Y 9
0010 45 00 04 14 b0 d5 40 00 3f 06 e8 87 40 be 3f 6f E@ ? @ ?o
0020 0a 02 14 58 00 50 cf a6 7b b8 01 fb ba 3e ed c6 X P { >
0030 50 18 00 ed 36 cf 00 00 48 54 54 50 2f 31 2e 31 P 6 HTTP/1.1
0040 20 32 30 30 20 4f 4b 0d 0a 64 61 74 65 3a 20 46 200 OK date: F
0050 72 69 2c 20 31 33 20 4a 61 6e 20 32 30 32 33 20 ri, 13 J an 2023
0060 30 34 3a 35 34 3a 32 34 20 47 4d 54 0d 0a 63 6f 04:54:24 GMT co
0070 6e 74 65 6e 74 2d 74 79 70 65 3a 20 74 65 78 74 ntent-ty pe: text
0080 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 /html; c harset=U
0090 54 46 2d 38 0d 0a 76 61 72 79 3a 20 41 63 63 65 TF-8 va ry: Acce
00a0 70 74 2d 45 6e 63 6f 64 69 6e 67 0d 0a 78 2d 70 pt-Encod ing x-p
00b0 6f 77 65 72 65 64 2d 62 79 3a 20 50 48 50 2f 38 owered-b y: PHP/8
00c0 2e 31 2e 39 0d 0a 65 78 70 69 72 65 73 3a 20 4d .1.9 ex pires: M
00d0 6f 6e 2c 20 32 36 20 4a 75 6c 20 31 39 39 37 20 on, 26 J ul 1997
00e0 30 35 3a 30 30 3a 30 30 20 47 4d 54 0d 0a 63 61 05:00:00 GMT ca
Frame (1060 bytes)
Uncompressed entity body (1022 bytes)
Help
Close


Wireshark · Packet 240 · any
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=
pragma: no-cache\r\n
last-modified: Fri, 13 Jan 2023 04:54:24 GMT\r\n
x-cache-miss-from: parking-75cd85f887-wgzf7\r\n
server: NginX\r\n
content-encoding: gzip\r\n
Accept-Ranges: none\r\n
Content-Length: 488\r\n
Via: HTTP/1.1 forward.http.proxy:3128\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.378511445 seconds]
0000 00 00 00 01 00 06 2c 59 e5 0b 39 80 00 00 08 00 ,Y 9
0010 45 00 04 14 b0 d5 40 00 3f 06 e8 87 40 be 3f 6f E@ ? @ ?o
0020 0a 02 14 58 00 50 cf a6 7b b8 01 fb ba 3e ed c6 X P { >
0030 50 18 00 ed 36 cf 00 00 48 54 54 50 2f 31 2e 31 P 6 HTTP/1.1
0040 20 32 30 30 20 4f 4b 0d 0a 64 61 74 65 3a 20 46 200 OK date: F
0050 72 69 2c 20 31 33 20 4a 61 6e 20 32 30 32 33 20 ri, 13 J an 2023
0060 30 34 3a 35 34 3a 32 34 20 47 4d 54 0d 0a 63 6f 04:54:24 GMT co
0070 6e 74 65 6e 74 2d 74 79 70 65 3a 20 74 65 78 74 ntent-ty pe: text
0080 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 /html; c harset=U
0090 54 46 2d 38 0d 0a 76 61 72 79 3a 20 41 63 63 65 TF-8 va ry: Acce
00a0 70 74 2d 45 6e 63 6f 64 69 6e 67 0d 0a 78 2d 70 pt-Encod ing x-p
00b0 6f 77 65 72 65 64 2d 62 79 3a 20 50 48 50 2f 38 owered-b y: PHP/8
00c0 2e 31 2e 39 0d 0a 65 78 70 69 72 65 73 3a 20 4d .1.9 ex pires: M
00d0 6f 6e 2c 20 32 36 20 4a 75 6c 20 31 39 39 37 20 on, 26 J ul 1997
00e0 30 35 3a 30 30 3a 30 30 20 47 4d 54 0d 0a 63 61 05:00:00 GMT ca
Frame (1060 bytes)
Uncompressed entity body (1022 bytes)
Help
Close



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	226	240
Source Port	53158	80
Destination Port	80	53158
Source IP address	10.2.20.88	64.190.63.111
Destination IP address	64.190.63.111	10.2.20.88
Source Ethernet Address	08:00:27:51:ee:52	52:54:00:12:35:02
Destination Ethernet Address	52:54:00:12:35:02	08:00:27:51:ee:52

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

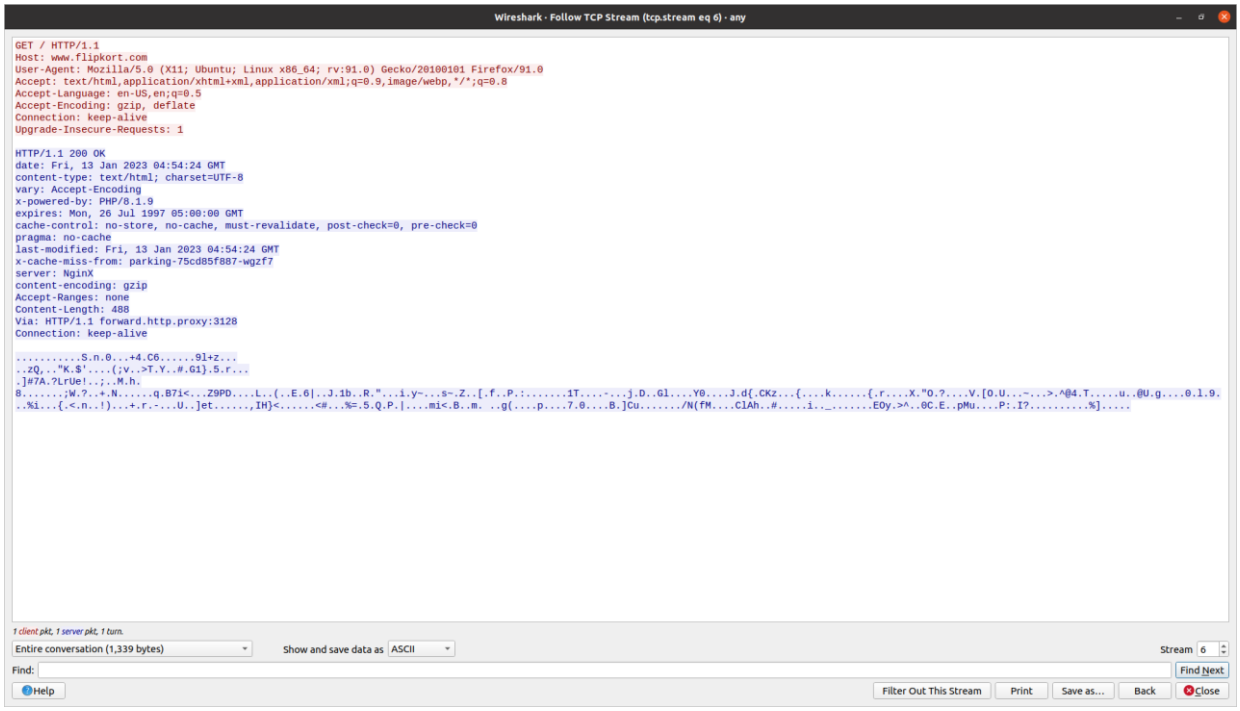
HTTP Request		HTTP Response	
Get	GET/HTTP/1.1\r\n	Server	nginx \r\n

Host	www.flipkart.com \r\n	Content-Type	text/html\r\n
User-Agent	Mozilla/5.0 (x11;Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0\r\n	Date	Fri,13 Jan 2023 4:54:24 GMT\r\n
Accept-Language	en-US,en;q=0.5\r\n	Location	https://www.flipkart.com \r\n
Accept-Encoding	gzip, deflate\r\n	Content-Length	488 \r\n
Connection	Keep-alive\r\n	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

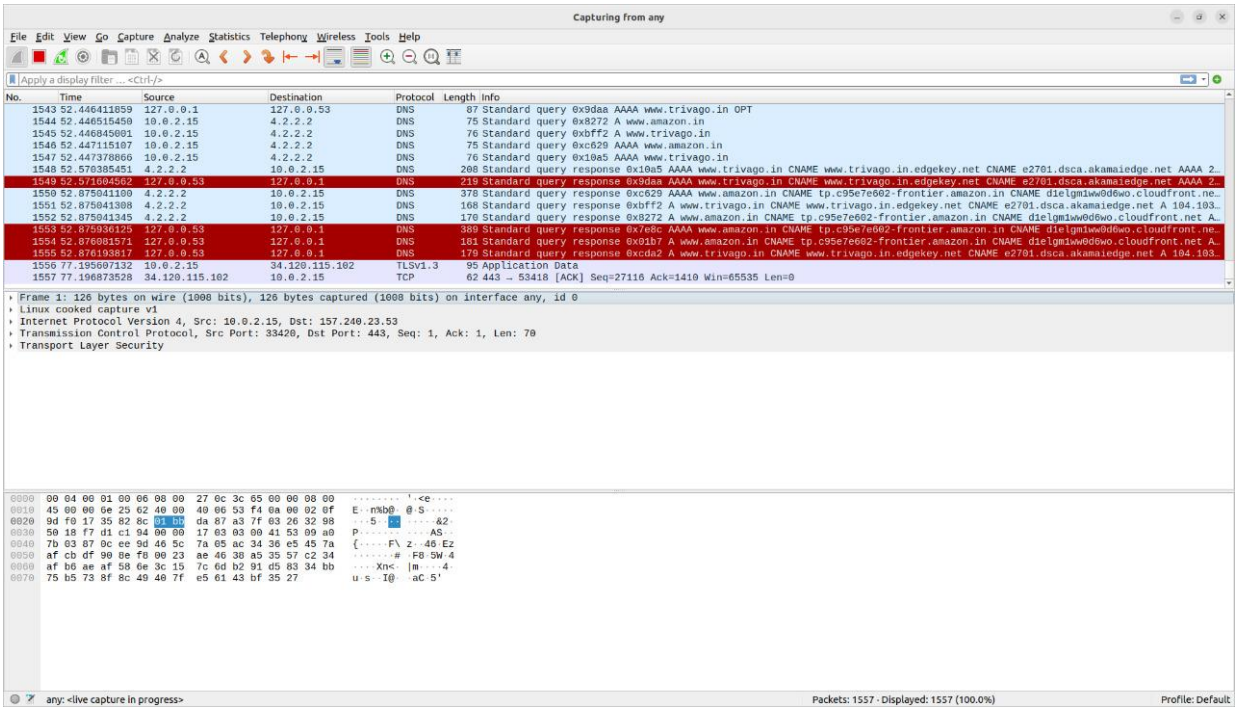
Step 1: Use the command **tcpdump -D** to see which interfaces are available for capture.

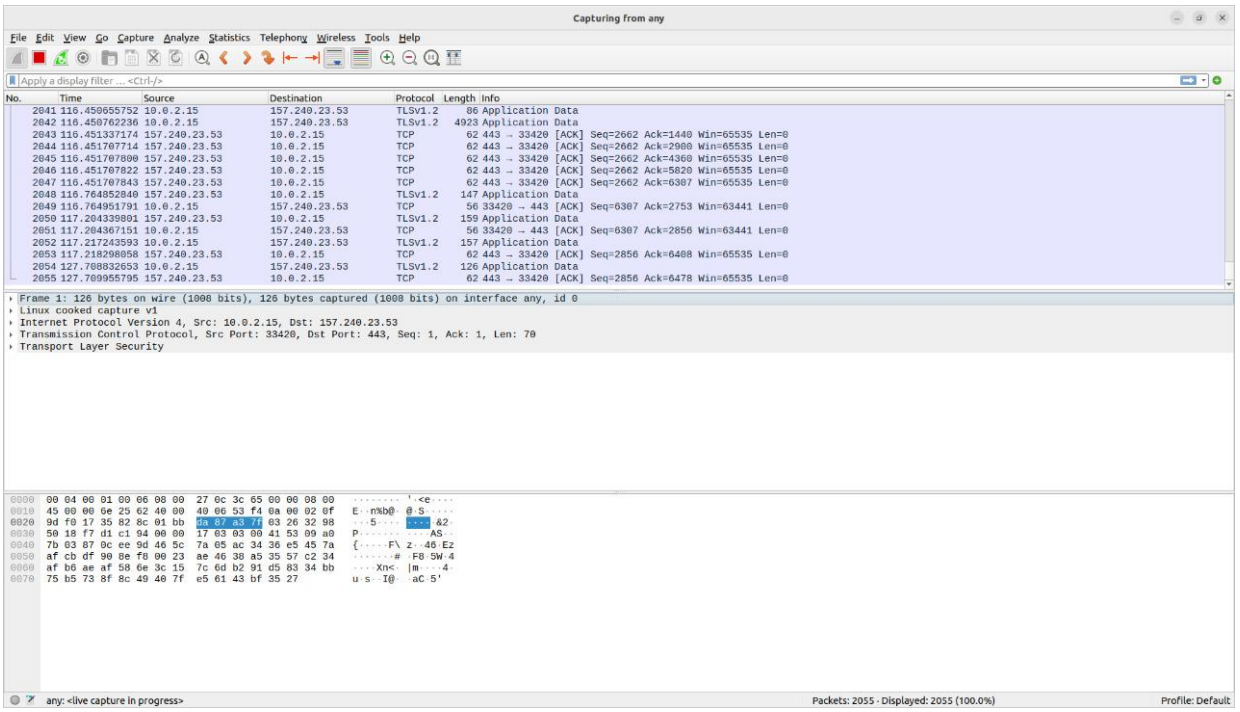
sudo tcpdump -D

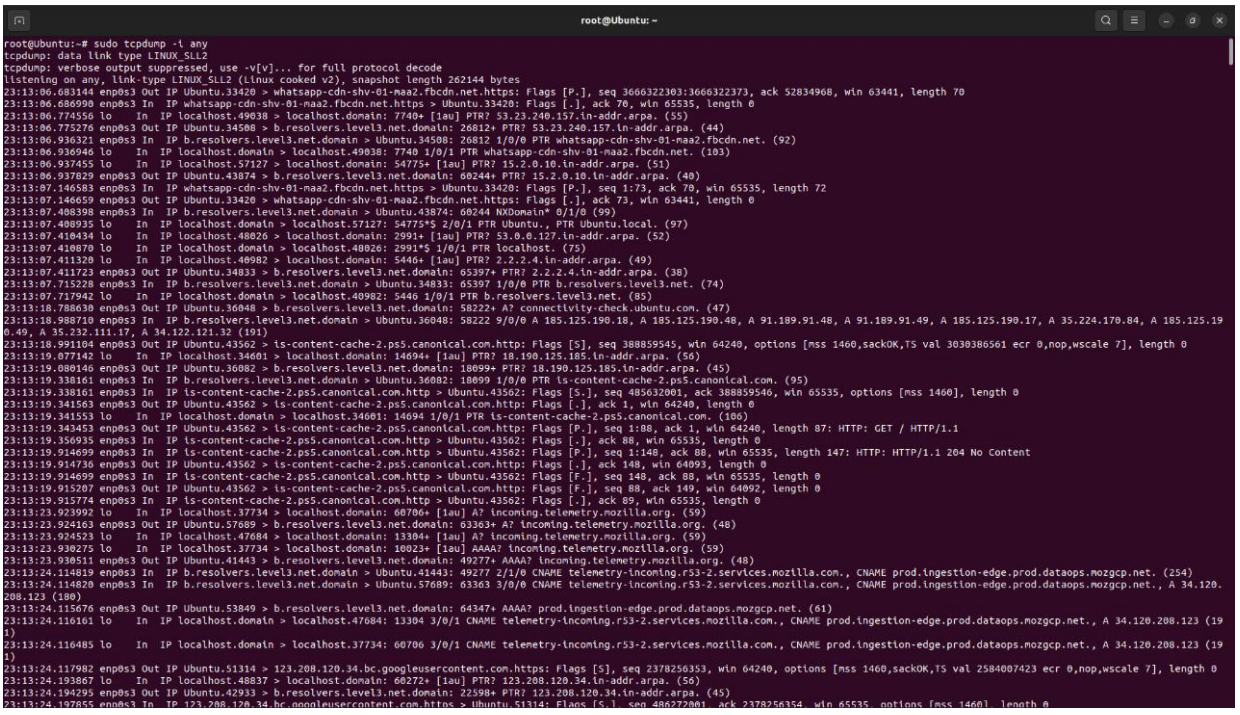
```
nagavenigowda@DELL:~$ sudo tcpdump -D
[sudo] password for nagavenigowda:
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.dummy0 [none]
5.tunl0 [none]
6.sit0 [none]
7.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
8.nflog (Linux netfilter log (NFLOG) interface) [none]
9.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
10.dbus-system (D-Bus system bus) [none]
11.dbus-session (D-Bus session bus) [none]
12.bond0 [none, Disconnected]
nagavenigowda@DELL:~$
```

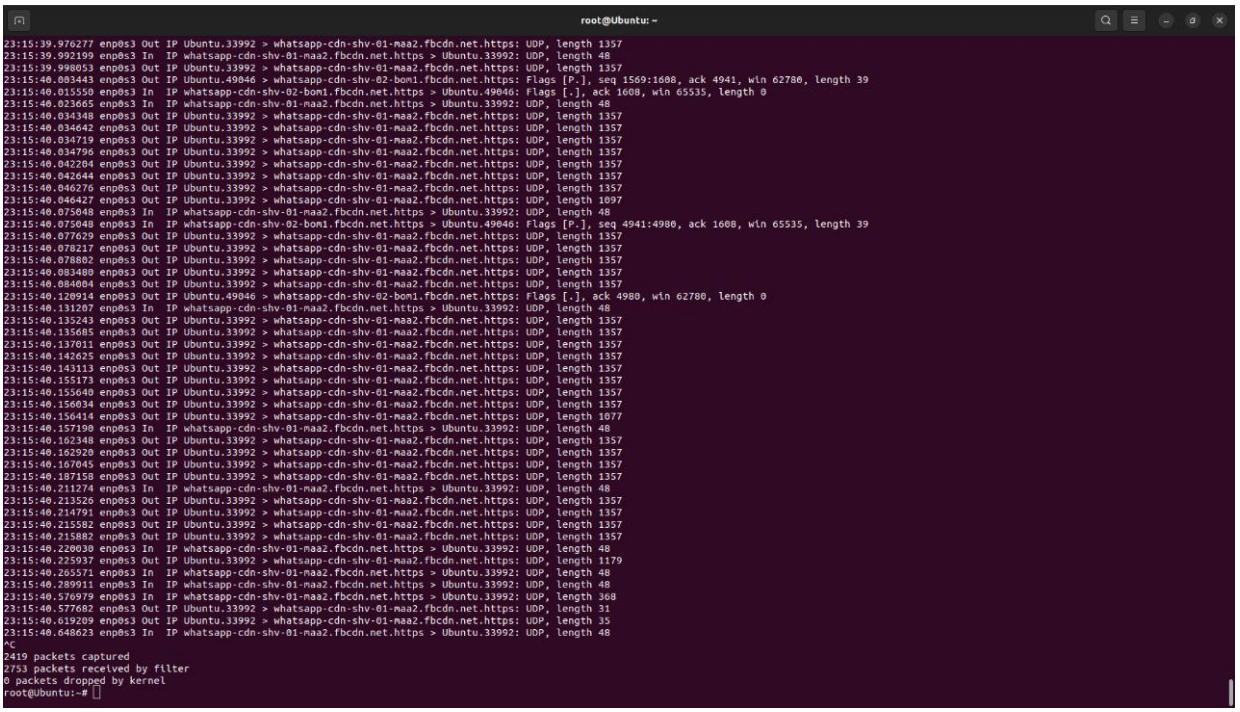
Step 2: Capture all packets in any interface by running this command:

sudo tcpdump -i any




Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2041 116.450655752 10.0.2.15 157.240.23.53 TLSv1.2 86 Application Data
2042 116.450762236 10.0.2.15 157.240.23.53 TLSv1.2 4923 Application Data
2043 116.451337174 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2662 Ack=1440 Win=65535 Len=0
2044 116.451707714 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2662 Ack=2900 Win=65535 Len=0
2045 116.451707800 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2662 Ack=4360 Win=65535 Len=0
2046 116.451707822 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2662 Ack=5820 Win=65535 Len=0
2047 116.451707843 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2662 Ack=6307 Win=65535 Len=0
2048 116.764852840 157.240.23.53 10.0.2.15 TLSv1.2 147 Application Data
2049 116.764951791 10.0.2.15 157.240.23.53 TCP 56 33420 → 443 [ACK] Seq=6307 Ack=2753 Win=63441 Len=0
2050 117.204339801 157.240.23.53 10.0.2.15 TLSv1.2 159 Application Data
2051 117.204367151 10.0.2.15 157.240.23.53 TCP 56 33420 → 443 [ACK] Seq=6307 Ack=2856 Win=63441 Len=0
2052 117.217243593 10.0.2.15 157.240.23.53 TLSv1.2 157 Application Data
2053 117.218298058 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2856 Ack=6488 Win=65535 Len=0
2054 127.708832653 10.0.2.15 157.240.23.53 TLSv1.2 126 Application Data
2055 127.709955795 157.240.23.53 10.0.2.15 TCP 62 443 → 33420 [ACK] Seq=2856 Ack=6478 Win=65535 Len=0
Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.23.53
Transmission Control Protocol, Src Port: 33420, Dst Port: 443, Seq: 1, Ack: 1, Len: 70
Transport Layer Security
0000 00 04 00 01 00 06 08 00 27 0c 3c 65 00 00 08 00 .... '·<e····
0010 45 00 00 6e 25 62 40 00 40 06 53 f4 0a 00 02 0f E··n%b@· @·S·····
0020 9d f0 17 35 82 8c 01 bb da 87 a3 7f 03 26 32 98 ···5···· ····&2·
0030 50 18 f7 d1 c1 94 00 00 17 03 03 00 41 53 09 a0 P····· ····AS··
0040 7b 03 87 0c ee 9d 46 5c 7a 05 ac 34 36 e5 45 7a {·····F\ z··46·Ez
0050 af cb df 90 8e f8 90 23 ae 46 30 a5 35 57 c2 34 ·····# ·F0·5W·4
0060 af b6 ae af 58 6e 3c 15 7c 6d b2 91 d5 83 34 bb ····Xn<· |m····4·
0070 75 b5 73 8f 8c 49 40 7f e5 61 43 bf 35 27 u·s··I@· ·aC·5'
any: <live capture in progress>
Packets: 2055 · Displayed: 2055 (100.0%)
Profile: Default


root@Ubuntu: ~
root@Ubuntu:~# sudo tcpdump -i any
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
23:13:06.683144 enp0s3 Out IP Ubuntu.33420 > whatsapp-cdn-shv-01-maa2.fbcdn.net.https: Flags [P.], seq 3666322303:3666322373, ack 52834968, win 63441, length 70
23:13:06.686990 enp0s3 In IP whatsapp-cdn-shv-01-maa2.fbcdn.net.https > Ubuntu.33420: Flags [.], ack 70, win 65535, length 0
23:13:06.774556 lo In IP localhost.49038 > localhost.domain: 7740+ [1au] PTR? 53.23.240.157.in-addr.arpa. (55)
23:13:06.775276 enp0s3 Out IP Ubuntu.34508 > b.resolvers.level3.net.domain: 26812+ PTR? 53.23.240.157.in-addr.arpa. (44)
23:13:06.936321 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.34508: 26812 1/0/0 PTR whatsapp-cdn-shv-01-maa2.fbcdn.net. (92)
23:13:06.936946 lo In IP localhost.domain > localhost.49038: 7740 1/0/1 PTR whatsapp-cdn-shv-01-maa2.fbcdn.net. (103)
23:13:06.937455 lo In IP localhost.57127 > localhost.domain: 54775+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
23:13:06.937829 enp0s3 Out IP Ubuntu.43874 > b.resolvers.level3.net.domain: 60244+ PTR? 15.2.0.10.in-addr.arpa. (40)
23:13:07.146583 enp0s3 In IP whatsapp-cdn-shv-01-maa2.fbcdn.net.https > Ubuntu.33420: Flags [P.], seq 1:73, ack 70, win 65535, length 72
23:13:07.146659 enp0s3 Out IP Ubuntu.33420 > whatsapp-cdn-shv-01-maa2.fbcdn.net.https: Flags [.], ack 73, win 63441, length 0
23:13:07.408398 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.43874: 60244 NXDomain* 0/1/0 (99)
23:13:07.408935 lo In IP localhost.domain > localhost.57127: 54775*$ 2/0/1 PTR Ubuntu., PTR Ubuntu.local. (97)
23:13:07.410434 lo In IP localhost.48026 > localhost.domain: 2991+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
23:13:07.410870 lo In IP localhost.domain > localhost.48026: 2991*$ 1/0/1 PTR localhost. (75)
23:13:07.411320 lo In IP localhost.40982 > localhost.domain: 5446+ [1au] PTR? 2.2.2.4.in-addr.arpa. (49)
23:13:07.411723 enp0s3 Out IP Ubuntu.34833 > b.resolvers.level3.net.domain: 65397+ PTR? 2.2.2.4.in-addr.arpa. (38)
23:13:07.715228 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.34833: 65397 1/0/0 PTR b.resolvers.level3.net. (74)
23:13:07.717942 lo In IP localhost.domain > localhost.40982: 5446 1/0/1 PTR b.resolvers.level3.net. (85)
23:13:18.788630 enp0s3 Out IP Ubuntu.36048 > b.resolvers.level3.net.domain: 58222+ A? connectivity-check.ubuntu.com. (47)
23:13:18.988710 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.36048: 58222 9/0/0 A 185.125.190.18, A 185.125.190.48, A 91.189.91.48, A 91.189.91.49, A 185.125.190.17, A 35.224.170.84, A 185.125.190.49, A 35.232.111.17, A 34.122.121.32 (191)
23:13:18.991104 enp0s3 Out IP Ubuntu.43562 > is-content-cache-2.ps5.canonical.com.http: Flags [S], seq 388859545, win 64240, options [mss 1460,sackOK,TS val 3030386561 ecr 0,nop,wscale 7], length 0
23:13:19.077142 lo In IP localhost.34601 > localhost.domain: 14694+ [1au] PTR? 18.190.125.185.in-addr.arpa. (56)
23:13:19.080146 enp0s3 Out IP Ubuntu.36082 > b.resolvers.level3.net.domain: 18099+ PTR? 18.190.125.185.in-addr.arpa. (45)
23:13:19.338161 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.36082: 18099 1/0/0 PTR is-content-cache-2.ps5.canonical.com. (95)
23:13:19.338161 enp0s3 In IP is-content-cache-2.ps5.canonical.com.http > Ubuntu.43562: Flags [S.], seq 485632001, ack 388859546, win 65535, options [mss 1460], length 0
23:13:19.341563 enp0s3 Out IP Ubuntu.43562 > is-content-cache-2.ps5.canonical.com.http: Flags [.], ack 1, win 64240, length 0
23:13:19.341553 lo In IP localhost.domain > localhost.34601: 14694 1/0/1 PTR is-content-cache-2.ps5.canonical.com. (106)
23:13:19.343453 enp0s3 Out IP Ubuntu.43562 > is-content-cache-2.ps5.canonical.com.http: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1.1
23:13:19.356935 enp0s3 In IP is-content-cache-2.ps5.canonical.com.http > Ubuntu.43562: Flags [.], ack 88, win 65535, length 0
23:13:19.914699 enp0s3 In IP is-content-cache-2.ps5.canonical.com.http > Ubuntu.43562: Flags [P.], seq 1:148, ack 88, win 65535, length 147: HTTP: HTTP/1.1 204 No Content
23:13:19.914736 enp0s3 Out IP Ubuntu.43562 > is-content-cache-2.ps5.canonical.com.http: Flags [.], ack 148, win 64093, length 0
23:13:19.914699 enp0s3 In IP is-content-cache-2.ps5.canonical.com.http > Ubuntu.43562: Flags [F.], seq 148, ack 88, win 65535, length 0
23:13:19.915207 enp0s3 Out IP Ubuntu.43562 > is-content-cache-2.ps5.canonical.com.http: Flags [F.], seq 88, ack 149, win 64092, length 0
23:13:19.915774 enp0s3 In IP is-content-cache-2.ps5.canonical.com.http > Ubuntu.43562: Flags [.], ack 89, win 65535, length 0
23:13:23.923992 lo In IP localhost.37734 > localhost.domain: 60706+ [1au] A? incoming.telemetry.mozilla.org. (59)
23:13:23.924163 enp0s3 Out IP Ubuntu.57689 > b.resolvers.level3.net.domain: 63363+ A? incoming.telemetry.mozilla.org. (48)
23:13:23.924523 lo In IP localhost.47684 > localhost.domain: 13304+ [1au] A? incoming.telemetry.mozilla.org. (59)
23:13:23.930275 lo In IP localhost.37734 > localhost.domain: 10023+ [1au] AAAA? incoming.telemetry.mozilla.org. (59)
23:13:23.930511 enp0s3 Out IP Ubuntu.41443 > b.resolvers.level3.net.domain: 49277+ AAAA? incoming.telemetry.mozilla.org. (48)
23:13:24.114819 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.41443: 49277 2/1/0 CNAME telemetry-incoming.r53-2.services.mozilla.com., CNAME prod.ingestion-edge.prod.dataops.mozgcp.net. (254)
23:13:24.114820 enp0s3 In IP b.resolvers.level3.net.domain > Ubuntu.57689: 63363 3/0/0 CNAME telemetry-incoming.r53-2.services.mozilla.com., CNAME prod.ingestion-edge.prod.dataops.mozgcp.net., A 34.120.208.123 (180)
23:13:24.115676 enp0s3 Out IP Ubuntu.53849 > b.resolvers.level3.net.domain: 64347+ AAAA? prod.ingestion-edge.prod.dataops.mozgcp.net. (61)
23:13:24.116161 lo In IP localhost.domain > localhost.47684: 13304 3/0/1 CNAME telemetry-incoming.r53-2.services.mozilla.com., CNAME prod.ingestion-edge.prod.dataops.mozgcp.net., A 34.120.208.123 (191)
23:13:24.116485 lo In IP localhost.domain > localhost.37734: 60706 3/0/1 CNAME telemetry-incoming.r53-2.services.mozilla.com., CNAME prod.ingestion-edge.prod.dataops.mozgcp.net., A 34.120.208.123 (191)
23:13:24.117982 enp0s3 Out IP Ubuntu.51314 > 123.208.120.34.bc.googleusercontent.com.https: Flags [S], seq 2378256353, win 64240, options [mss 1460,sackOK,TS val 2584007423 ecr 0,nop,wscale 7], length 0
23:13:24.193867 lo In IP localhost.48837 > localhost.domain: 60272+ [1au] PTR? 123.208.120.34.in-addr.arpa. (56)
23:13:24.194295 enp0s3 Out IP Ubuntu.42933 > b.resolvers.level3.net.domain: 22598+ PTR? 123.208.120.34.in-addr.arpa. (45)
23:13:24.197855 enp0s3 In IP 123.208.120.34.bc.googleusercontent.com.https > Ubuntu.51314: Flags [S.], seq 486272001, ack 2378256354, win 65535, options [mss 1460], length 0



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

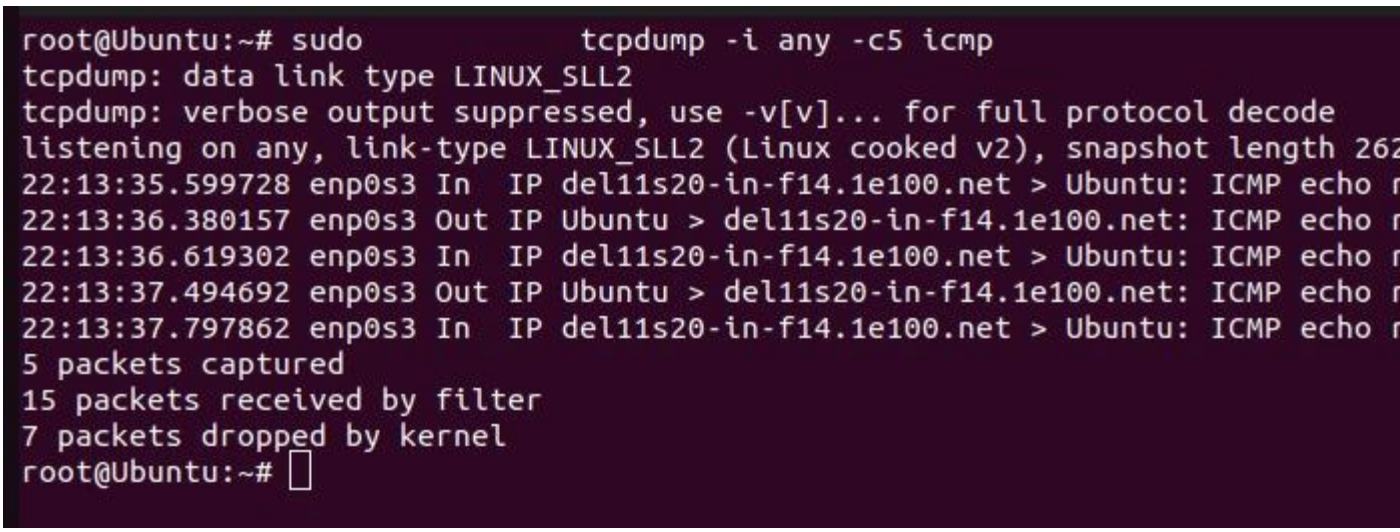
Observation

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



```
nagavenigowda@Ubuntu:~$ ping google.com
PING google.com (142.250.206.110) 56(84) bytes of data.
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=1 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=2 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=3 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=4 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=6 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=7 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=8 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=9 ttl=112
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=10 ttl=11
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=11 ttl=11
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=12 ttl=11
64 bytes from del11s20-in-f14.1e100.net (142.250.206.110): icmp_seq=13 ttl=11
```

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

```
root@Ubuntu:~# sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
22:17:03.426576 enp0s3 In  IP 34.104.35.123.80 > 10.0.2.15.34942: Flags [P.], seq 83056895:83076943, ack 212385
E.Nx6...@..."h#{
....P.~..X.~.zpP....\..aR...Pl...Jmh..).s...`U3K4.....................@...(v...l........=..u.....c.l...r.Zu.^.3T.
.9V$Z`....(..H.<.it     :.nFfo.)=......y..*.[$=..>"=r?<....z>.E...%...t..5^.;c..P......||<.._I.u ......2.'...:.
.....Q"..&.(.\....;<.
....b.@. .....j'I.+.X   .u.7..."..l..}-.....n-...>@..=I%1H.{....Id.c...HwV.1..G]Z.nac..{....;.34.Z./V....z.
M..sU.e......g3.......l..L.Z..C.....r..jR.h.i. ..".H.......9.....B&(.&.*......v9,..r.Ie.e.P.-.3.b.........\....
.Vi.V..iRVm.......*....Pe]...%..C..o...4-l.........R. A..i}..R..J........g.-t.,]..m..E.........._.R...-.....p...p.
..C.;.T.......KHB...a.[...[....`.j1...]..Mx.Ah...g...O.ZC.S.t....,.Y.t.(X....B.Z...Y?.U....!".x....=Dy_~...Ae.L
.|.@6@RZ.....3
..*.F...pnt....&..Sv..)3.b..;"IL.u.....o.F[.....u....f[o...+...iG.q.j...|V..aqn.@.I.....]+..X...hI....Fc%.....
..|SN.....z..1..V...d.S..(h...Pm"m.8<...:*..n..Gi.Z.c...l.H.u.>.|..h.&..vJ.|........k..s...Nh.Z....r\..gfiT....
..aoF.#...P..oU......Y.
=....o.Y>..l5... p@D....,W....jL.'....h*R....M...K..!.+.....b.x..'.........O.$k:...w"..Iq.p.M.R..Z..."...O..U..
Y.... .:..!..-......I.%U(......Q.o.KE ..&..*.."O...ul.#...{LB...$q..j#)O..t.i......../&I5f.SOmb........2c...VmC
R...     ......_.ord%\N.....P b....."..F.V;..^.e..?.e.T....Dl..EC.4.9..N.c.2...U
.,..p......B...._...a.. o.al...K.i......+...&...U...w.}.[....@a..R..=..x0.Z..........H(^..."q.mU..^....J...c...
,....U..<.3((
 .}.........)... 7.............'t...7..v...4.....2V..\.R..F..{..h.+.oz5.;Cx....u.Bq-2W...P..}.b'b...',]zx.
.....m....J...).!..R...8=:.A..y..q.G.._./...'. .1..FX...'.g..F..B..:...=M...."yc..l.TT/.Ha....=...c....)]...n..w
22:17:03.470271 enp0s3 Out IP 10.0.2.15.34942 > 34.104.35.123.80: Flags [.], ack 44392, win 65535, length 0
E..(    5@.@...
..."h#{.~.P~.zp...gP...R...
10 packets captured
17 packets received by filter
0 packets dropped by kernel
root@Ubuntu:~#
```

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

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnamesby 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 connectionto gather data more relevant to web server, you can use the -T flag.

sudo traceroute -T www.google.com

```
root@Ubuntu:~# sudo traceroute www.google.com
traceroute to www.google.com (142.251.42.100), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.654 ms  0.376 ms  5.557 ms
 2  _gateway (10.0.2.2)  4.212 ms  201.045 ms  199.667 ms
root@Ubuntu:~# sudo traceroute -n www.google.com
traceroute to www.google.com (142.251.42.100), 30 hops max, 60 byte packets
 1  10.0.2.2  0.536 ms  0.455 ms  0.408 ms
 2  10.0.2.2  4.245 ms  5.447 ms *
root@Ubuntu:~# sudo traceroute -I www.google.com
traceroute to www.google.com (142.251.42.100), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  1.024 ms  0.827 ms  0.775 ms
 2  172.16.1.1 (172.16.1.1)  181.903 ms * *
 3  * * *
 4  * * *
 5  * * *
 6  * 121.240.238.41.static-bangalore.vsnl.net.in (121.240.238.41)  9.311 ms *
 7  * * *
 8  121.240.1.46 (121.240.1.46)  16.173 ms  16.013 ms  16.521 ms
 9  108.170.253.97 (108.170.253.97)  15.809 ms  15.712 ms  15.611 ms
10  108.170.253.103 (108.170.253.103)  15.508 ms  15.998 ms  20.295 ms
11  142.250.56.38 (142.250.56.38)  135.800 ms  135.699 ms  135.599 ms
12  108.170.248.193 (108.170.248.193)  135.495 ms  30.117 ms  29.704 ms
13  142.251.77.95 (142.251.77.95)  46.277 ms  45.442 ms  44.705 ms
14  bom07s45-in-f4.1e100.net (142.251.42.100)  44.033 ms  43.598 ms  42.742 ms
root@Ubuntu:~# sudo traceroute -T  www.google.com
traceroute to www.google.com (142.251.42.100), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  11.143 ms  10.608 ms  10.128 ms
 2  bom07s45-in-f4.1e100.net (142.251.42.100)  85.098 ms  120.998 ms  117.129 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

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

```
root@Ubuntu:~# nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-14 11:45 IST
Nmap scan report for www.pes.edu (52.172.204.196)
Host is up (0.0086s latency).
Other addresses for www.pes.edu (not scanned): 64:ff9b::34ac:ccc4
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 6.03 seconds
root@Ubuntu:~# nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-14 11:46 IST
Nmap scan report for 163.53.78.128
Host is up (0.013s 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 5.92 seconds
```

```
root@Ubuntu:~# nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-14 11:52 IST
Nmap scan report for 192.168.1.1
Host is up (0.0069s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
53/tcp   open  domain
443/tcp  open  https
3128/tcp open  squid-http
4444/tcp open  krb524
8090/tcp open  opsmessaging

Nmap scan report for 192.168.1.2
Host is up (0.0052s latency).
All 1000 scanned ports on 192.168.1.2 are filtered

Nmap scan report for 192.168.1.3
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.1.3 are filtered

Nmap done: 3 IP addresses (3 hosts up) scanned in 27.50 seconds
root@Ubuntu:~#
```

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

```
nagavenigowda@Ubuntu:~$ nc 10.0.2.15 9380
Hello , This is NagaveniGowda
F sec
WEEK 1 CN LAB
PES2UG21CS315
```

```
root@Ubuntu:~# nc -l 9380
Hello , This is NagaveniGowda
F sec
WEEK 1 CN LAB
```

Note: 2 students can combine for the following tasks (switch and cables canbe taken from Lab technicians)

DONE USING WINDOWS

It did not work with VM to Remote Linux.

b) Inter system communication

Setup a simple switched network of 2 PCs with one acting as Web server. Assign IPaddresses for both PCs. Set the capture option as described above.

Step 1: Open terminal on Server machine (Machine 1).

Step 2: Type nc -l any_portnum

Step 3: Open terminal on the Client machine (Machine 2)

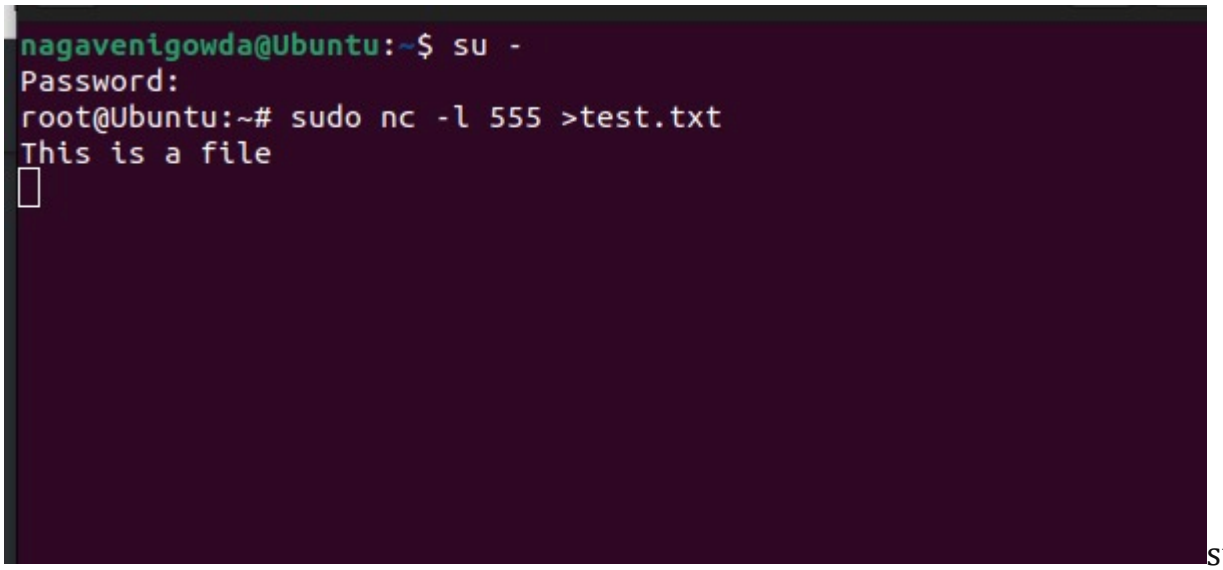
Step 4: Type nc <server-ip-address> portnum

Step 5: Type anything in client will appear in the server terminal

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’



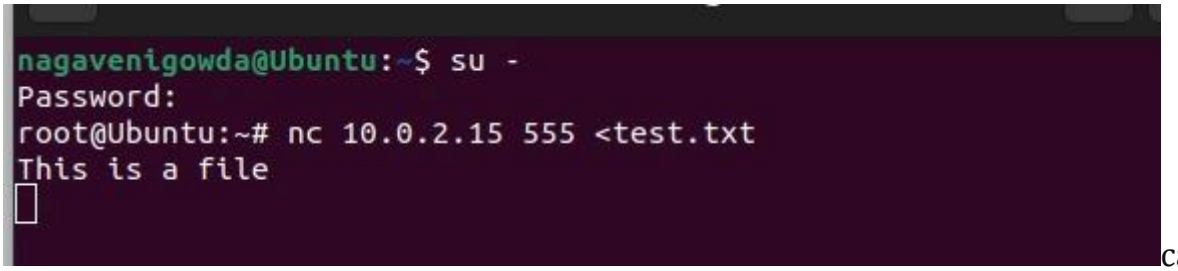
sudo nc -l 555 > test.txt

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

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



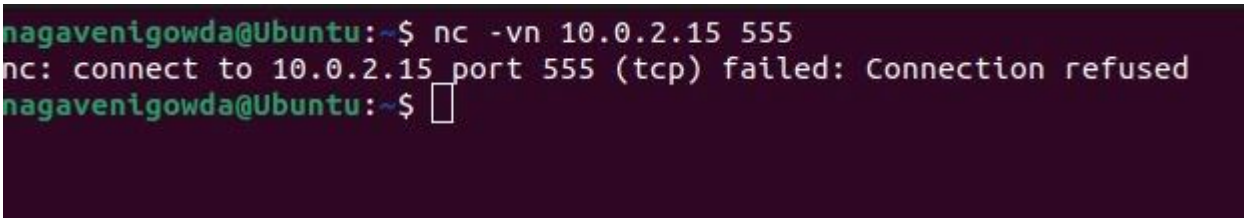
cat test.txt

Task 7 c): Other Commands

COULD NOT BE EXECUTED. PERMISSION DENIED.

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

   nc -vn 10.0.2.8 555



COULD NOT BE EXECUTED. PERMISSION DENIED.

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

COULD NOT BE EXECUTED. PERMISSION DENIED.

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

COULD NOT BE EXECUTED. PERMISSION DENIED.

Step 3: Observe the details on the terminal

COULD NOT BE EXECUTED. PERMISSION DENIED.

Questions on above observations:

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

1.1. The version of the server is 1.1 as well

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

2023-01-14 11:52 IST

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

Ans : $ ping -c <number of packets> <url>

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

Ans : Simply scan the entire subnet.

Eg:

$ nmap -sP 10.0.4.*

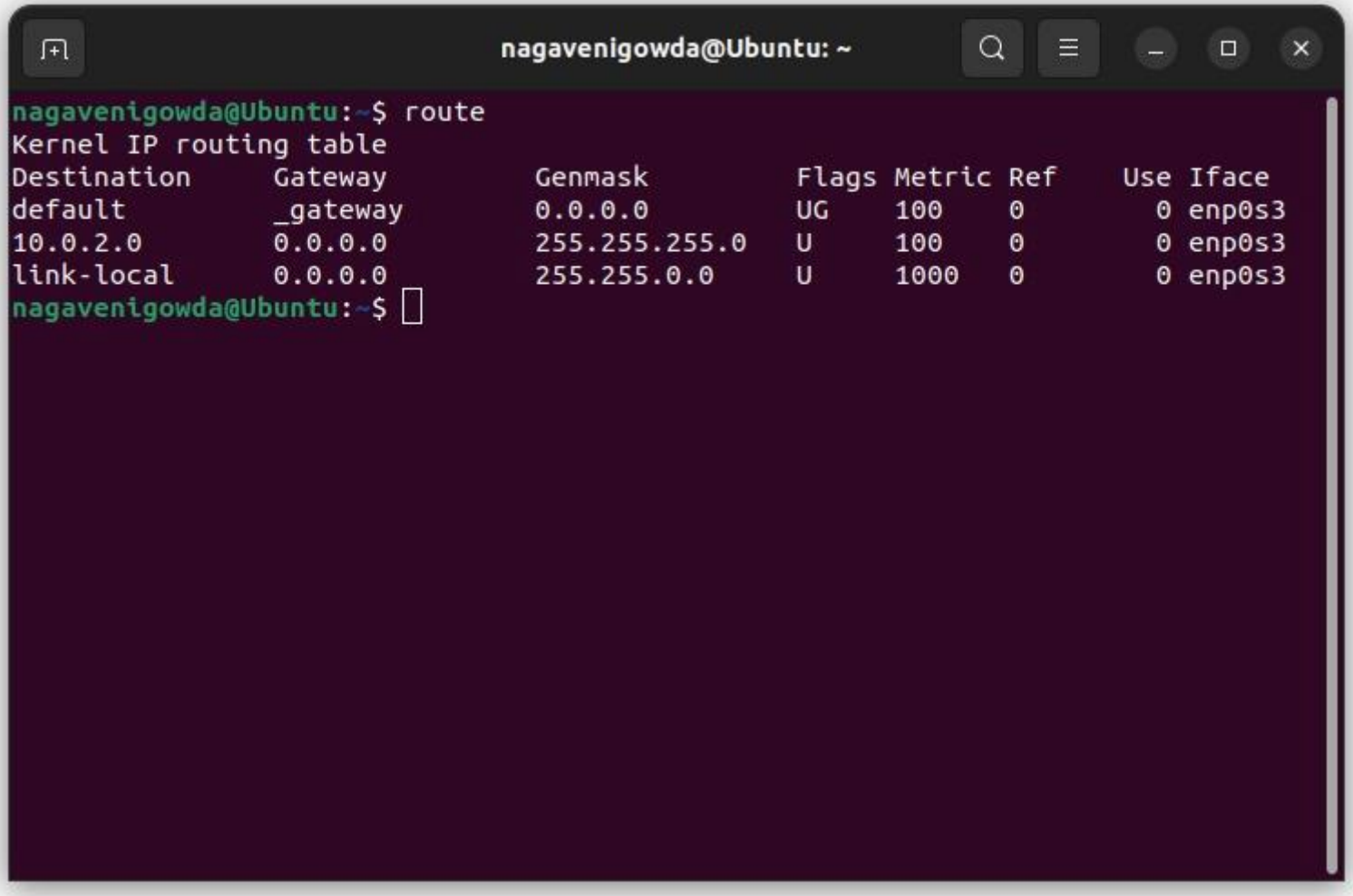
Exercises:

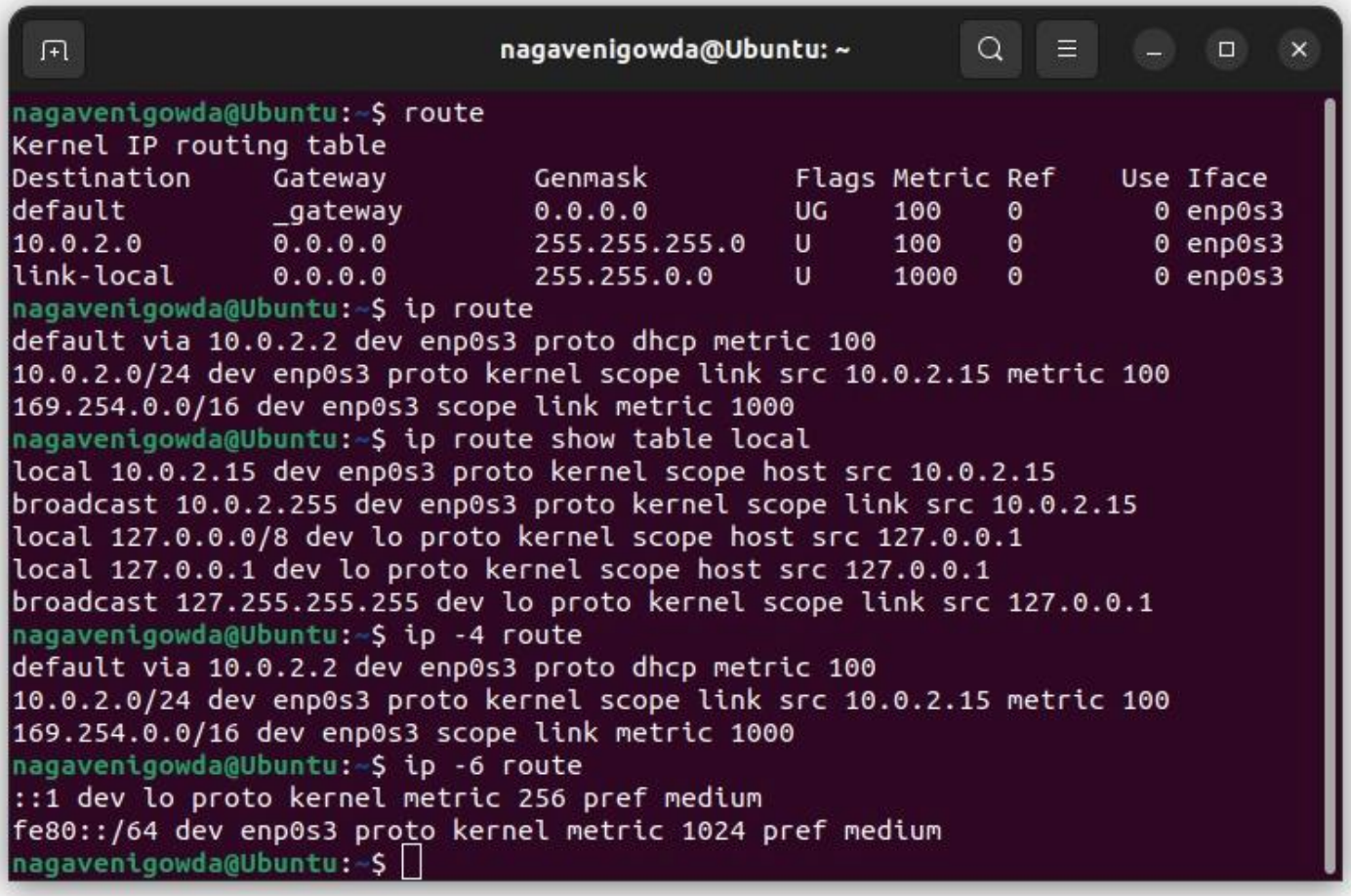
1) Capture and Analyze IPv4 / IPv6 packets

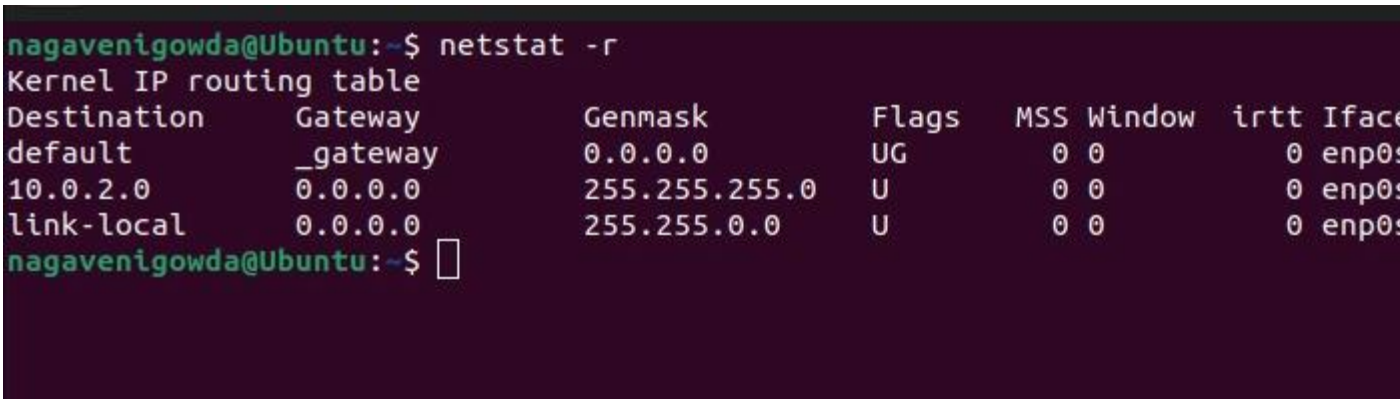
IPv4 / IPv6 packet header

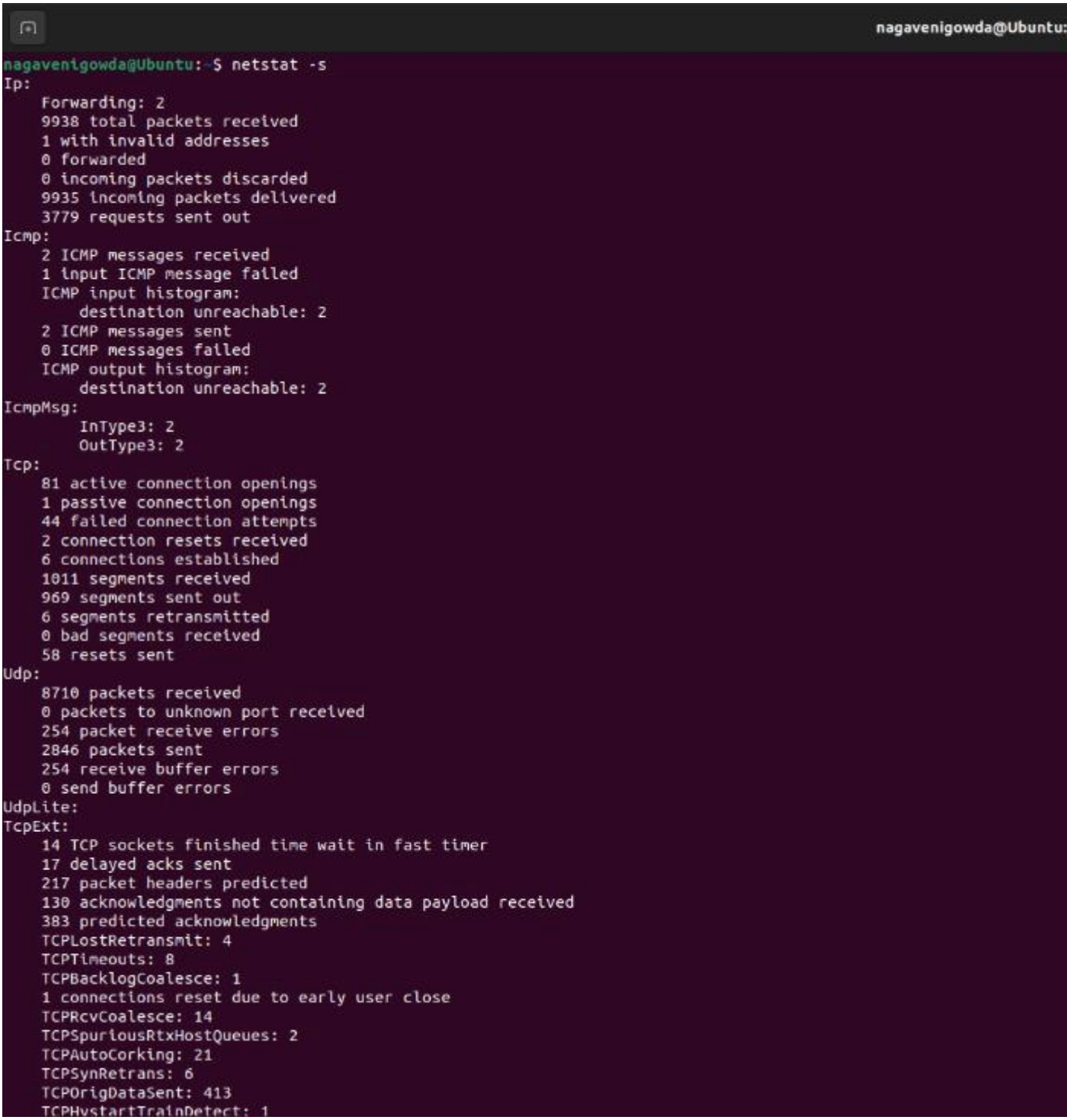
GET	./success.txt HTTP/1.1
HOST	detectportal.firefox.com
USER-AGENT	Mozilla/5.0
ACCEPT-LANGUAGE	en-US, en; q=0.5
CACHE-CONTROL	no-cache
PRAGMA	no-cache
CONNECTION	keep-alive

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


nagavenigowda@Ubuntu: ~
nagavenigowda@Ubuntu:~$ 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
nagavenigowda@Ubuntu:~$


nagavenigowda@Ubuntu: ~
nagavenigowda@Ubuntu:~$ 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
nagavenigowda@Ubuntu:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
nagavenigowda@Ubuntu:~$ ip route show table local
local 10.0.2.15 dev enp0s3 proto kernel scope host src 10.0.2.15
broadcast 10.0.2.255 dev enp0s3 proto kernel scope link src 10.0.2.15
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
nagavenigowda@Ubuntu:~$ ip -4 route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
nagavenigowda@Ubuntu:~$ ip -6 route
::1 dev lo proto kernel metric 256 pref medium
fe80::/64 dev enp0s3 proto kernel metric 1024 pref medium
nagavenigowda@Ubuntu:~$


nagavenigowda@Ubuntu:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 enp0s
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s
link-local 0.0.0.0 255.255.0.0 U 0 0 0 enp0s
nagavenigowda@Ubuntu:~$


nagavenigowda@Ubuntu:
nagavenigowda@Ubuntu: $ netstat -s
Ip:
Forwarding: 2
9938 total packets received
1 with invalid addresses
0 forwarded
0 incoming packets discarded
9935 incoming packets delivered
3779 requests sent out
Icmp:
2 ICMP messages received
1 input ICMP message failed
ICMP input histogram:
destination unreachable: 2
2 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
destination unreachable: 2
IcmpMsg:
InType3: 2
OutType3: 2
Tcp:
81 active connection openings
1 passive connection openings
44 failed connection attempts
2 connection resets received
6 connections established
1011 segments received
969 segments sent out
6 segments retransmitted
0 bad segments received
58 resets sent
Udp:
8710 packets received
0 packets to unknown port received
254 packet receive errors
2846 packets sent
254 receive buffer errors
0 send buffer errors
UdpLite:
TcpExt:
14 TCP sockets finished time wait in fast timer
17 delayed acks sent
217 packet headers predicted
130 acknowledgments not containing data payload received
383 predicted acknowledgments
TCPLostRetransmit: 4
TCPTimeouts: 8
TCPBacklogCoalesce: 1
1 connections reset due to early user close
TCPRcvCoalesce: 14
TCPSpuriousRtxHostQueues: 2
TCPAutoCorking: 21
TCPSynRetrans: 6
TCPOrigDataSent: 413
TCPHystartTrainDetect: 1