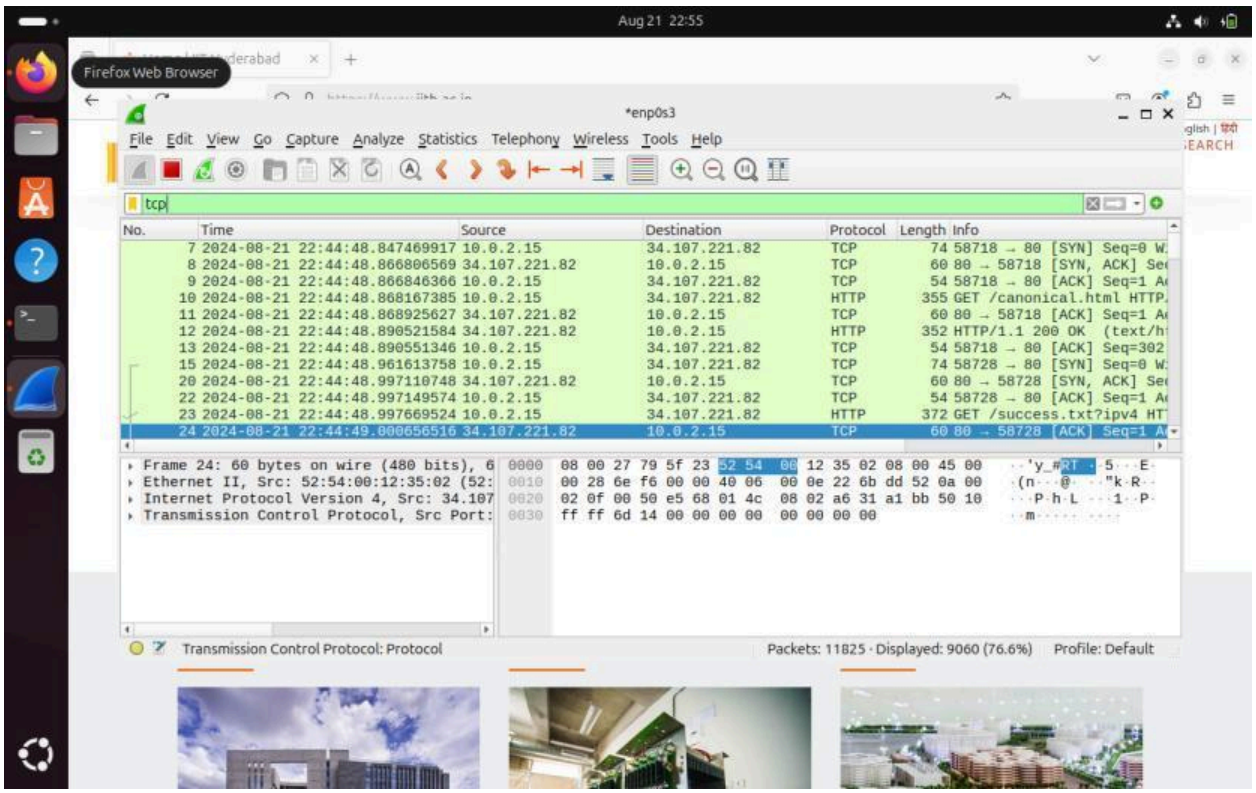
Roll No- CS24MTECH14006

Assignment 1

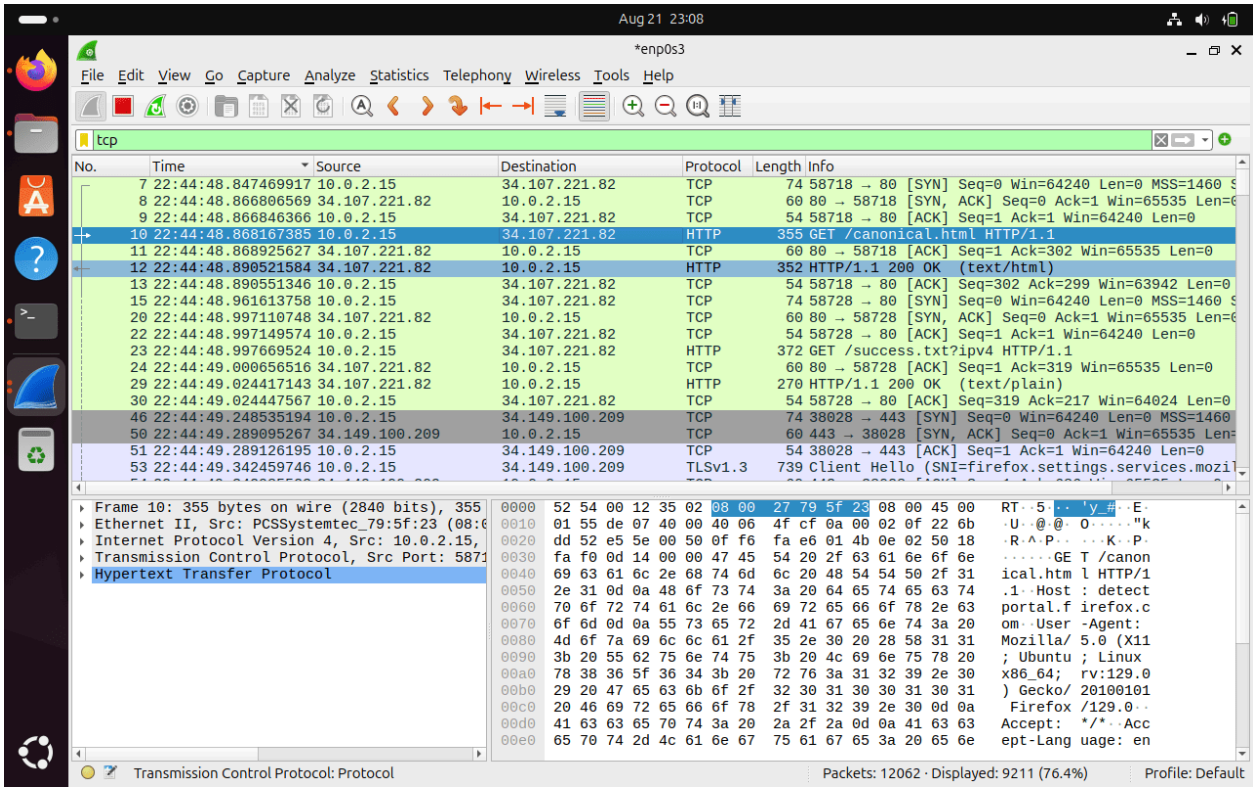
PART A: Analyze packet trace of your browsing session

Solution 1)



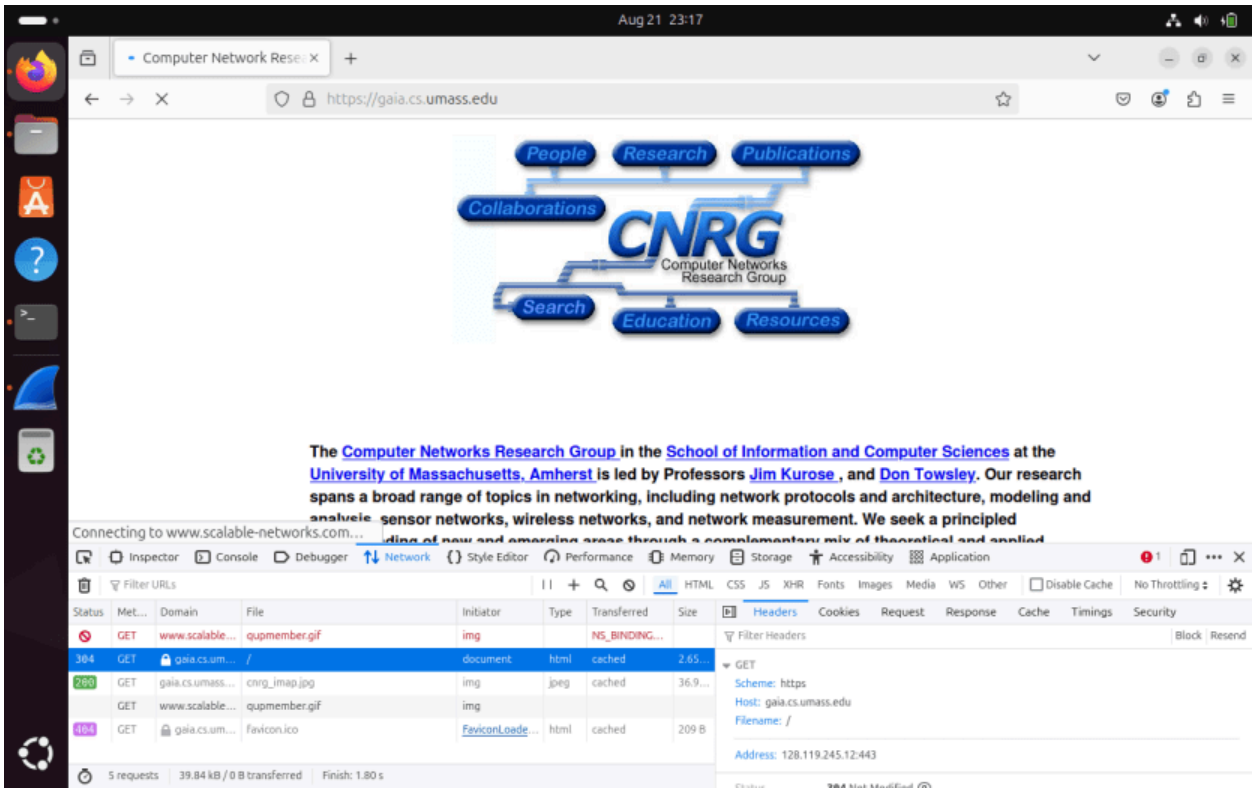
In the wireshark “protocol” column the protocols shown as appearing are: TCP, QUIC, HTTP, DNS, TLSv1.3 .

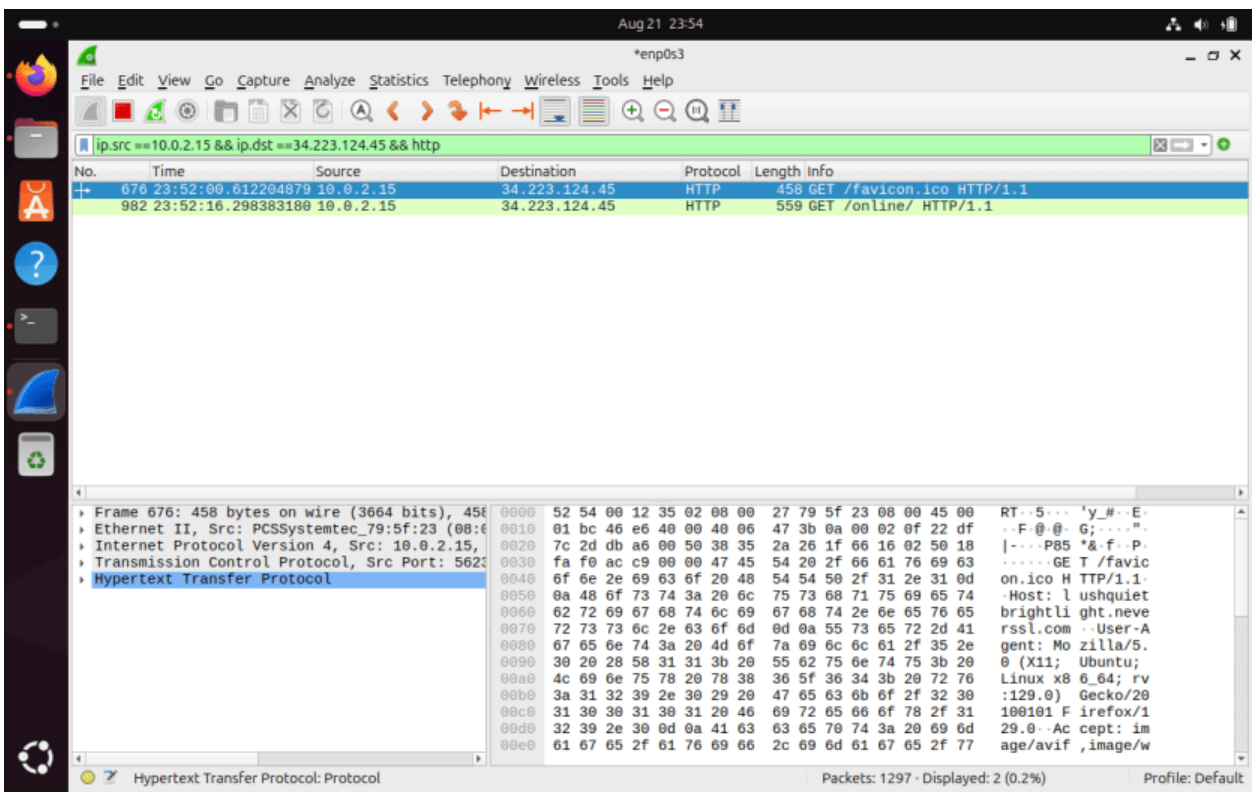
Solution 2)



The source with IP address 10.0.2.15 with number 10 sends HTTP GET message to the destination with IP address 34.107.221.82 at time 22.44.48.868167385 s. In response to that packet the HTTP OK reply comes at time 22.44.48.890521584 s. So the time difference between HTTP GET message sent until the HTTP OK message received is 0.02235419845 seconds.

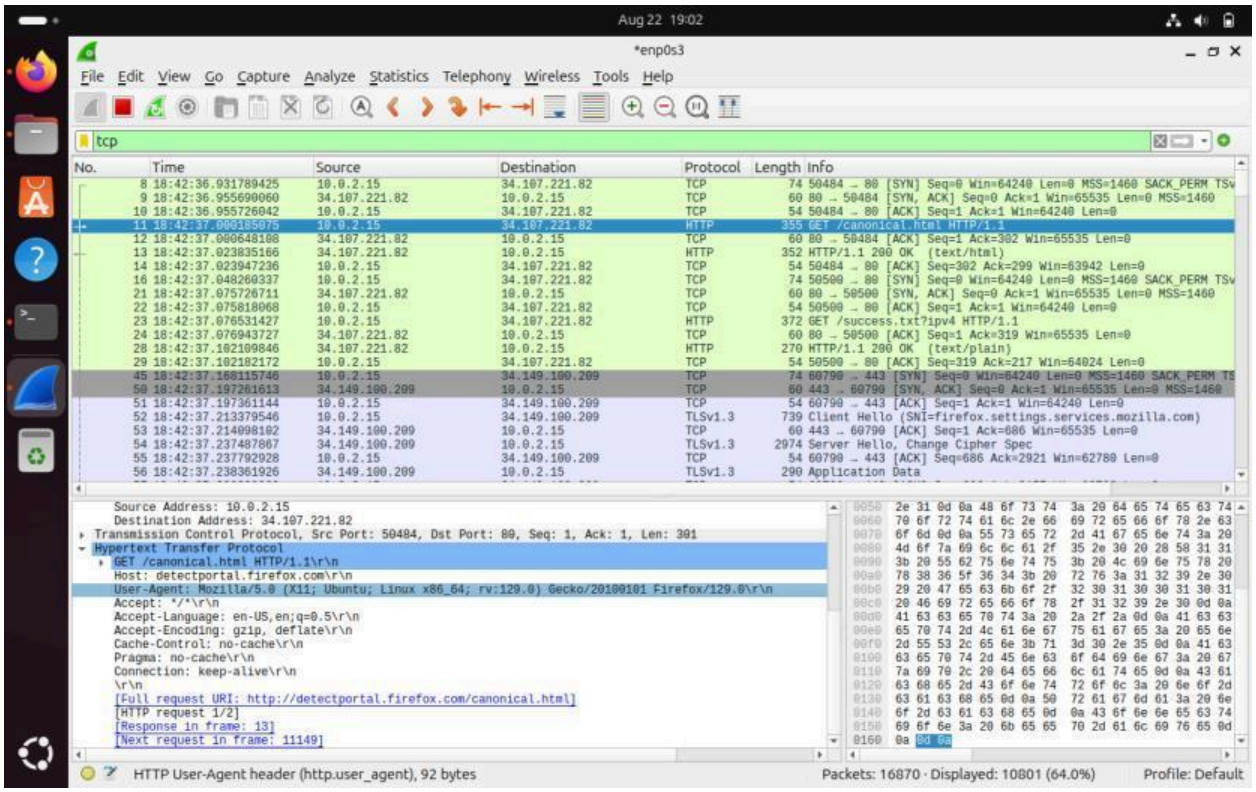
Solution 3)


Aug 21 23:17
Computer Network Rese
https://gaia.cs.umass.edu
People
Research
Publications
Collaborations
CNRG
Computer Networks Research Group
Search
Education
Resources
The Computer Networks Research Group in the School of Information and Computer Sciences at the University of Massachusetts, Amherst is led by Professors Jim Kurose , and Don Towsley. Our research spans a broad range of topics in networking, including network protocols and architecture, modeling and
sensor networks, wireless networks, and network measurement. We seek a principled
Connecting to www.scalable-networks.com...
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Status Met... Domain File Initiator Type Transferred Size
GET www.scalable... qupmember.gif img NS_BINDING...
304 GET gaia.cs.um... / document html cached 2.65...
200 GET gaia.cs.umass... cnrg_imap.jpg img jpeg cached 36.9...
GET www.scalable... qupmember.gif img
404 GET gaia.cs.um... favicon.ico FaviconLoade... html cached 209 B
5 requests 39.84 kB / 0 B transferred Finish: 1.80 s
Headers Cookies Request Response Cache Timings Security
Filter Headers
Block Resend
GET
Scheme: https
Host: gaia.cs.umass.edu
Filename: /
Address: 128.119.245.12:443


Aug 21 23:54
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src ==10.0.2.15 && ip.dst ==34.223.124.45 && http
No. Time Source Destination Protocol Length Info
676 23:52:00.612204879 10.0.2.15 34.223.124.45 HTTP 458 GET /favicon.ico HTTP/1.1
982 23:52:16.298383180 10.0.2.15 34.223.124.45 HTTP 559 GET /online/ HTTP/1.1
Frame 676: 458 bytes on wire (3664 bits), 458
Ethernet II, Src: PCSSystemtec_79:5f:23 (08:6
Internet Protocol Version 4, Src: 10.0.2.15,
Transmission Control Protocol, Src Port: 562
Hypertext Transfer Protocol
0000 52 54 00 12 35 02 08 00 27 79 5f 23 08 00 45 00 RT··5··· 'y_#··E·
0010 01 bc 46 e6 40 00 40 06 47 3b 0a 00 02 0f 22 df ··F·@·@· G;····"·
0020 7c 2d db a6 00 50 38 35 2a 26 1f 66 16 02 50 18 |-····P85 *&·f··P·
0030 fa f0 ac c9 00 00 47 45 54 20 2f 66 61 76 69 63 ····· GE T /favic
0040 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d on.ico H TTP/1.1·
0050 0a 48 6f 73 74 3a 20 6c 75 73 68 71 75 69 65 74 ·Host: l ushquiet
0060 62 72 69 67 68 74 6c 69 67 68 74 2e 6e 65 76 65 brightli ght.neve
0070 72 73 73 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 rssl.com ··User-A
0080 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
0090 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 3b 20 0 (X11; Ubuntu;
00a0 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76 Linux x8 6_64; rv
00b0 3a 31 32 39 2e 30 29 20 47 65 63 6b 6f 2f 32 30 :129.0) Gecko/20
00c0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 100101 F irefox/1
00d0 32 39 2e 30 0d 0a 41 63 63 65 70 74 3a 20 69 6d 29.0··Ac cept: im
00e0 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 age/avif ,image/w
Hypertext Transfer Protocol: Protocol
Packets: 1297 · Displayed: 2 (0.2%)
Profile: Default

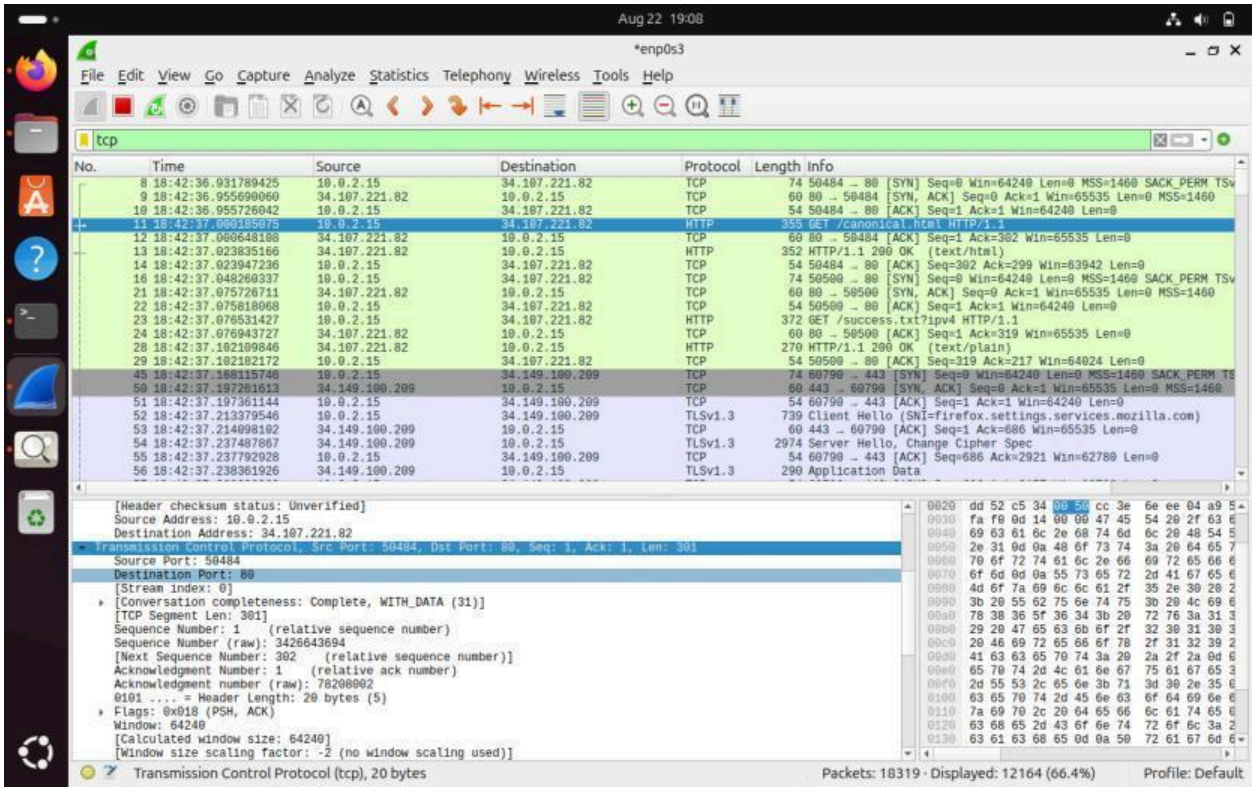
The Internet address of gaia.cs.umass.edu is 128.119.245.12 and the Internet address of my device is 10.0.2.15 .

Solution 4)



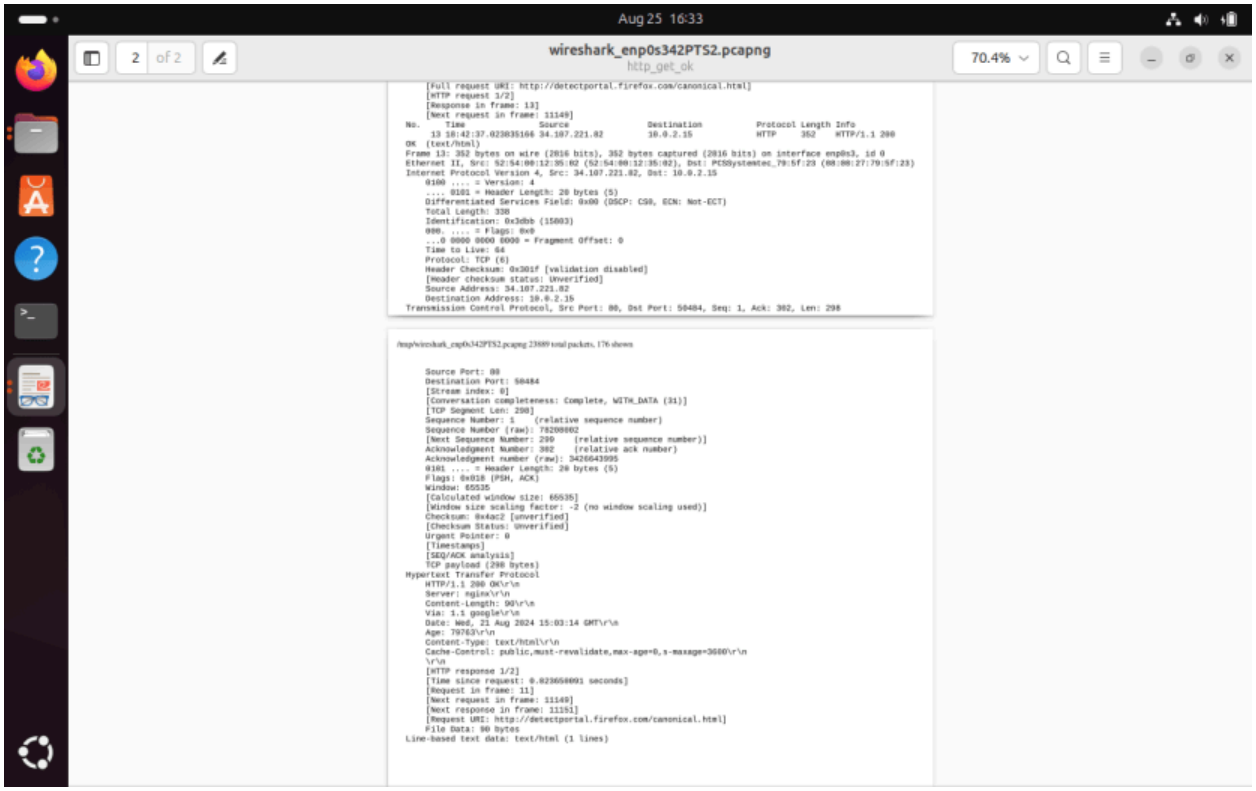
By expanding the packet highlighted in the above image containing HTTP GET request message the HTTP information is visible in the screen. The User agent shown is Firefox.

Solution 5)



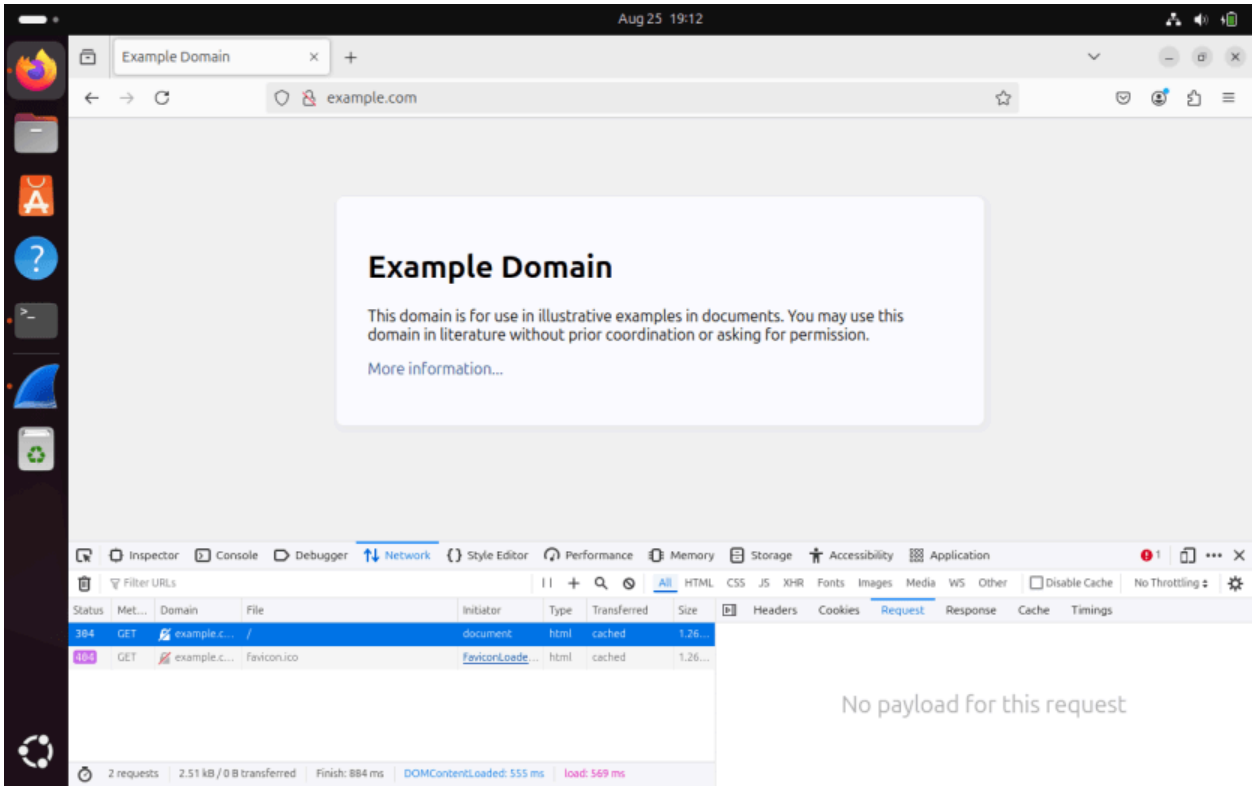
The destination port number to which the HTTP request is send is port number 80. HTTP (Hyper text transfer portorcol by default uses port number 80).

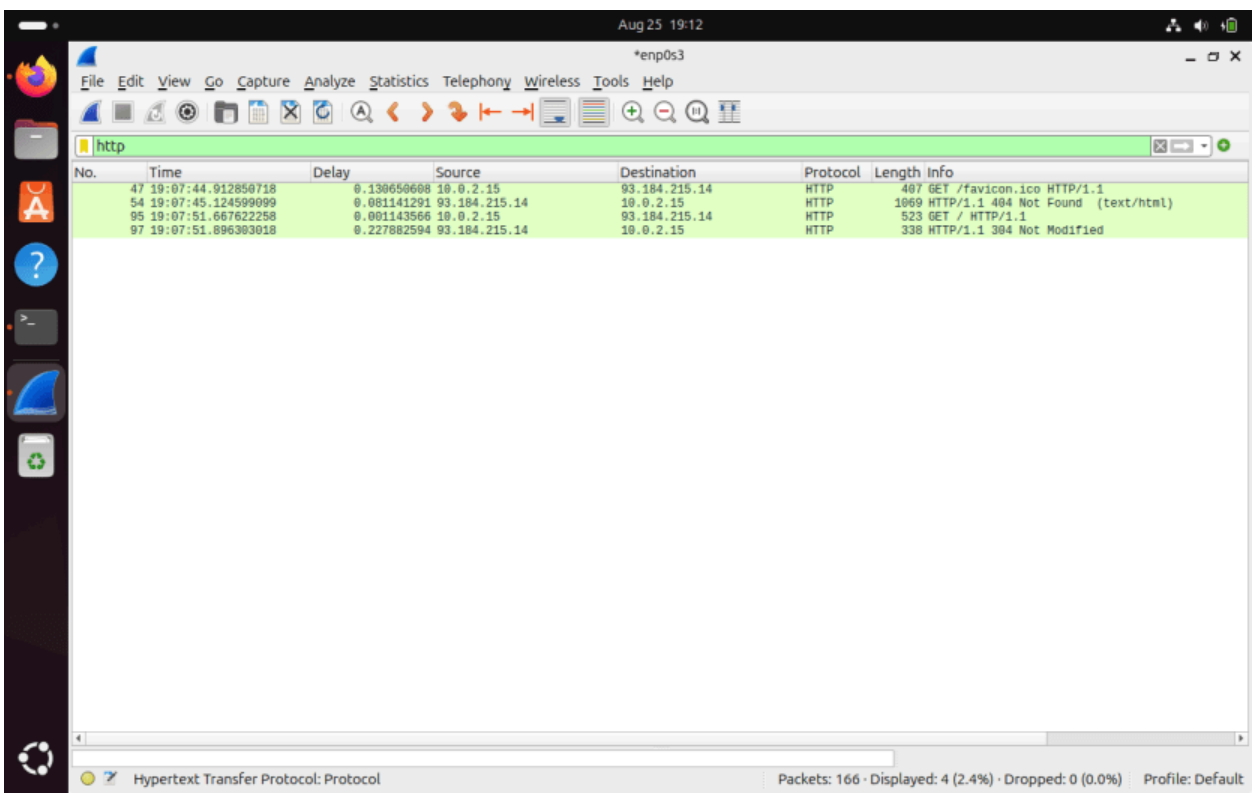
Solution 6)

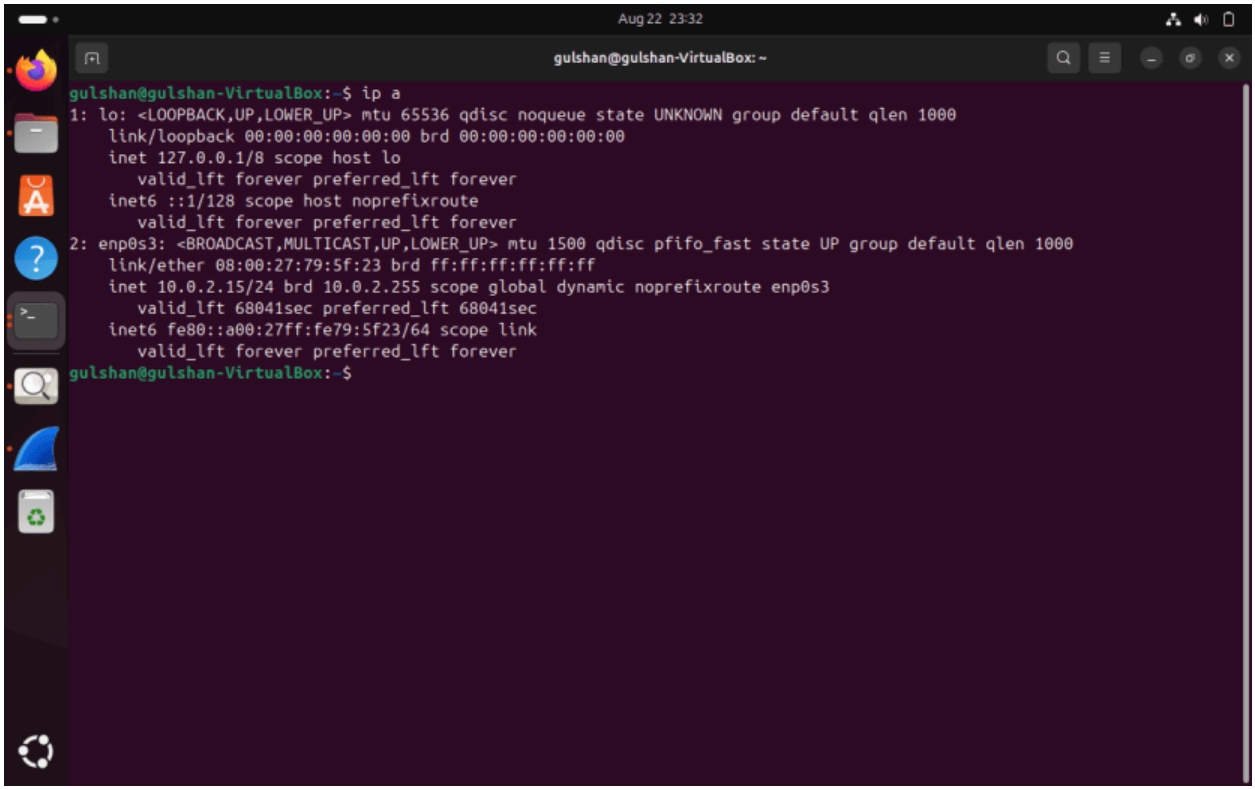

Aug 25 16:33
2 of 2
wireshark_enp0s342PTS2.pcapng
http_get_ok
70.4%
[Full request URI: http://detectportal.firefox.com/canonical.html]
[HTTP request 1/2]
[Response in frame: 13]
[Next request in frame: 11149]
No. Time Source Destination Protocol Length Info
13 16:42:37.023835166 34.107.221.82 10.0.2.15 HTTP 352 HTTP/1.1 200
OK (text/html)
Frame 13: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface enp0s3, id 0
Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_79:5f:23 (08:00:27:79:5f:23)
Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.0.2.15
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 338
Identification: 0x3dbb (15803)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x301f [validation disabled]
[Header checksum status: Unverified]
Source Address: 34.107.221.82
Destination Address: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 50484, Seq: 1, Ack: 302, Len: 298
/tmp/wireshark_enp0s342PTS2.pcapng 23889 total packets, 176 shown
Source Port: 80
Destination Port: 50484
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 298]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 78209802
[Next Sequence Number: 299 (relative sequence number)]
Acknowledgment Number: 302 (relative ack number)
Acknowledgment number (raw): 3426643995
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x4ac2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (298 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx\r\n
Content-Length: 90\r\n
Via: 1.1 google\r\n
Date: Wed, 21 Aug 2024 15:03:14 GMT\r\n
Age: 79763\r\n
Content-Type: text/html\r\n
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.023658091 seconds]
[Request in frame: 11]
[Next request in frame: 11149]
[Next response in frame: 11151]
[Request URI: http://detectportal.firefox.com/canonical.html]
File Data: 90 bytes
Line-based text data: text/html (1 lines)

Solution 7)

7.1) For http://example.com

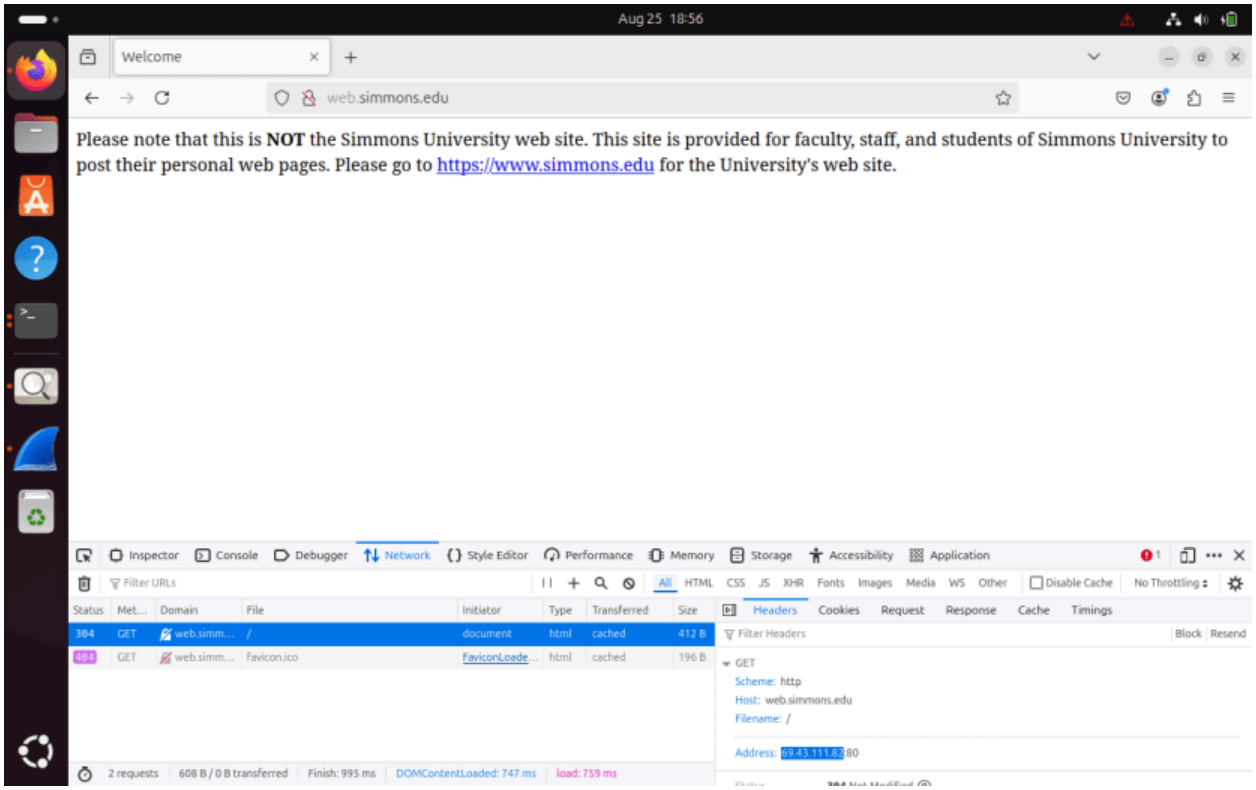

Aug 25 19:12
Example Domain
example.com
Example Domain
This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.
More information...
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Status Met... Domain File Initiator Type Transferred Size
Headers Cookies Request Response Cache Timings
304 GET example.c... / document html cached 1.26...
404 GET example.c... favicon.ico FaviconLoade... html cached 1.26...
No payload for this request
2 requests 2.51 kB / 0 B transferred Finish: 884 ms DOMContentLoaded: 555 ms load: 569 ms

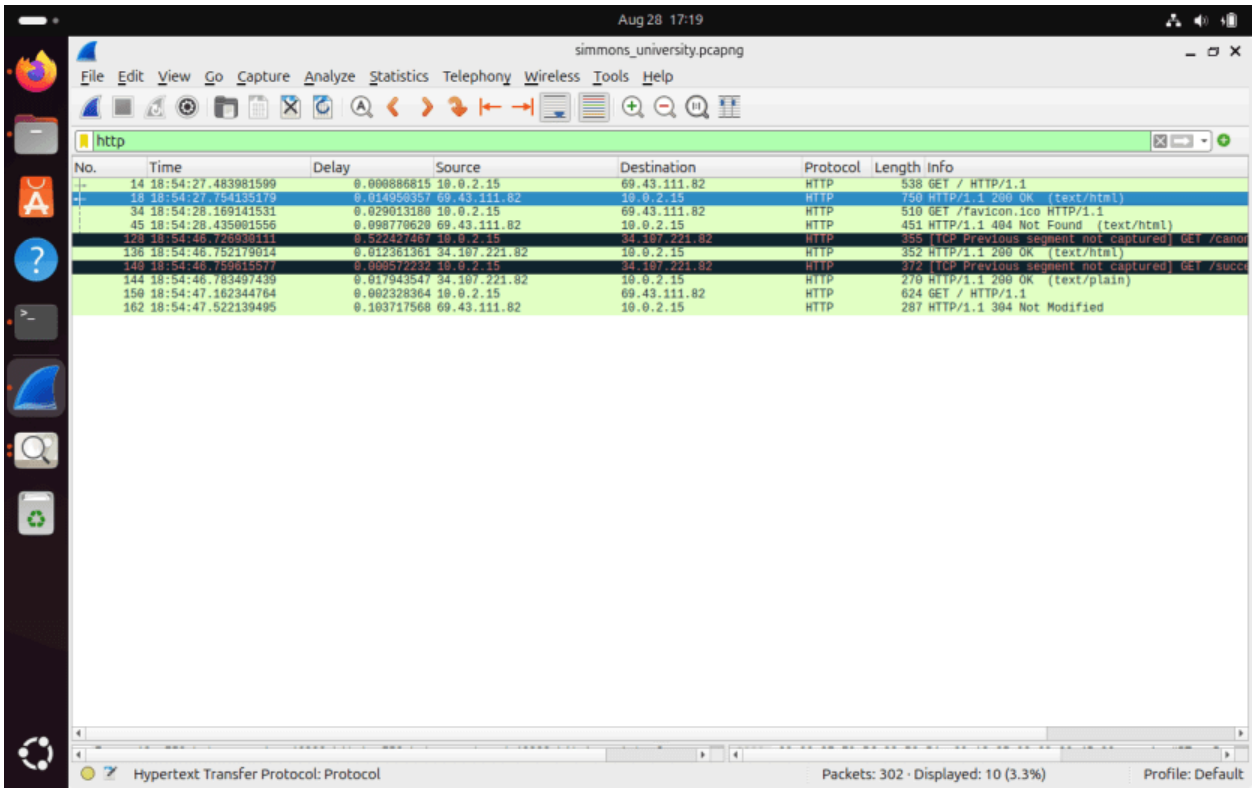

Aug 25 19:12
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Delay Source Destination Protocol Length Info
47 19:07:44.912850718 0.130650608 10.0.2.15 93.184.215.14 HTTP 407 GET /favicon.ico HTTP/1.1
54 19:07:45.124599099 0.081141291 93.184.215.14 10.0.2.15 HTTP 1069 HTTP/1.1 404 Not Found (text/html)
95 19:07:51.667622258 0.001143566 10.0.2.15 93.184.215.14 HTTP 523 GET / HTTP/1.1
97 19:07:51.896303018 0.227882594 93.184.215.14 10.0.2.15 HTTP 338 HTTP/1.1 304 Not Modified
Hypertext Transfer Protocol: Protocol
Packets: 166 · Displayed: 4 (2.4%) · Dropped: 0 (0.0%)
Profile: Default



7.1.1) TCP,QUIC, HTTP,DNS, TLSv1.3 are the protocols present in the protocol field for http://example.com .
7.1.2) 0.211748381 seconds required to get HTTP response from the point when the HTTP get message sent by the source.
7.1.3) The internet address of my sending device is 10.0.2.15 and the internet address of http://example.com is 93.184..215.14 .

Solution 7.2) For http://web.simmons.edu

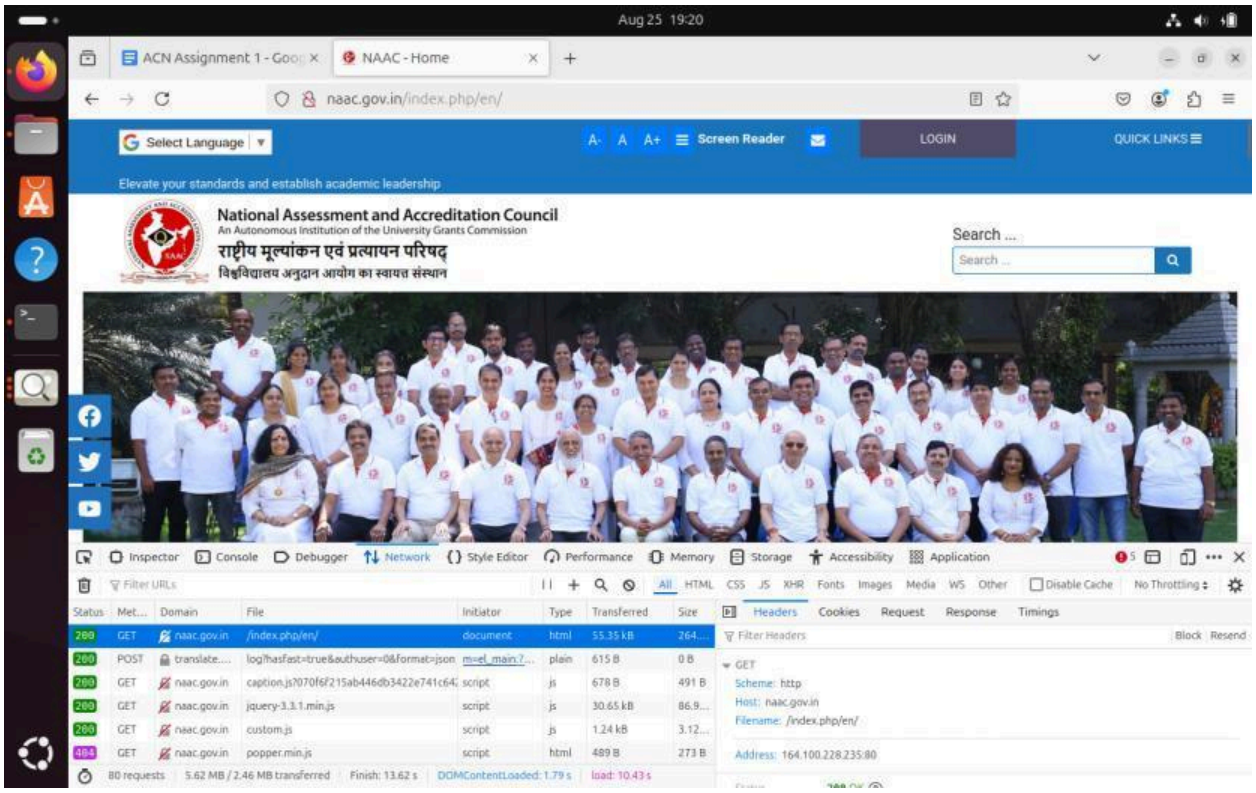


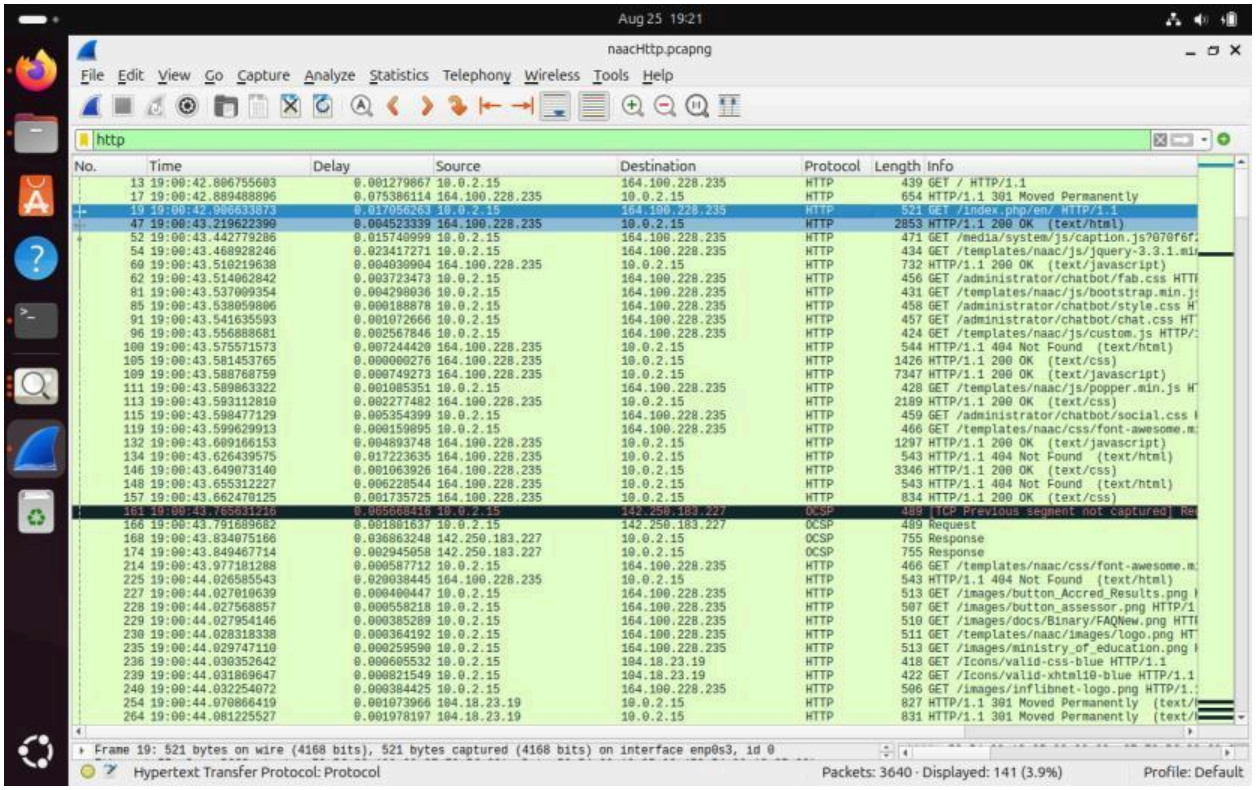


7.2.1) The protocols present in the protocols column are HTTP, TCP,DNS, TLSv1.3, QUIC.

7.2.2) Time required to receive HTTP OK from when the HTTP GET message was sent by the source is 0.27015358 seconds.
7.2.3) The IP(Internet Protocol) address of my computer is 10.0.2.15 and the IP(Internet Protocol) address of http://web.simmons.edu is 69.43.111.82 .

Solution 7.3) NAAC http://naac.gov.in





7.3.1)For http://naac.gov.in the protocols present in the protocols column are HTTP, DNS, TLSv1.3, TCP, QUIC.
7.3.2) Time required to receive HTTP OK from when the HTTP GET message was sent by the source is 0.3129885147 seconds.
7.3.3) The IP(Internet Protocol) address of my computer is 10.0.2.15 and the IP(Internet Protocol) address of http://naac.gov.in is 164.100.228.235 .

Solution 8)

When I visited this websites there is some similarities and differences in network traffic.

1) http://web.simmons.edu
   Here firstly initial HTTP GET request are send to fetch the main page. HTTP 200 OK responses for the successfully loaded resources. The latency is moderate in that case.
2) http://example.com
   The protocol used here is HTTP. Traffic is very less in this website and it is static website. The response is a single HTTP OK response with the page content and the latency is low because of simplicity and small size of the page.
3) www.youtube.com
   In this website the protocol used is HTTPS and here from multiple protocols including TCP, DNS, TLSv1.3, QUIC high volume of traffic is observed. For resolving multiple domain name the initial burst of DNS queries are used, then

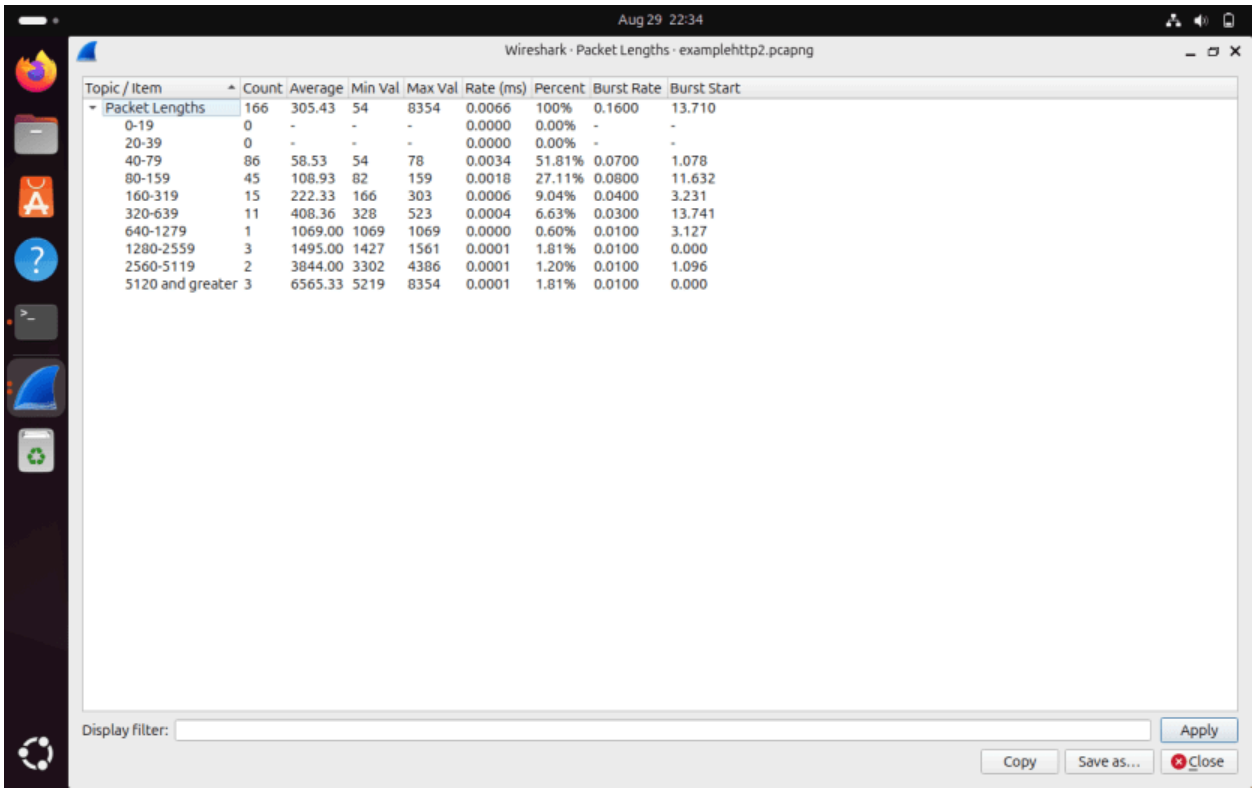
TCP handshakes and for secure connections TLS handshakes. It sends many encrypted packets with frequent HTTPs responses for content delivery.

4) http://naac.gov.in
   Here HTTP GET requests to retrieve the main HTML page is observed followed by multiple HTTP requests for additional resources. The latency is high here.The mentioned website uses HTTP. For successful content retrieval HTTP 200 OK response will be sent,.

Yes, the output vary when revisiting the same site due to caching, network availability, server changes,dynamic content. Due to these factors output is not same when revisiting the same.

Solution 9)

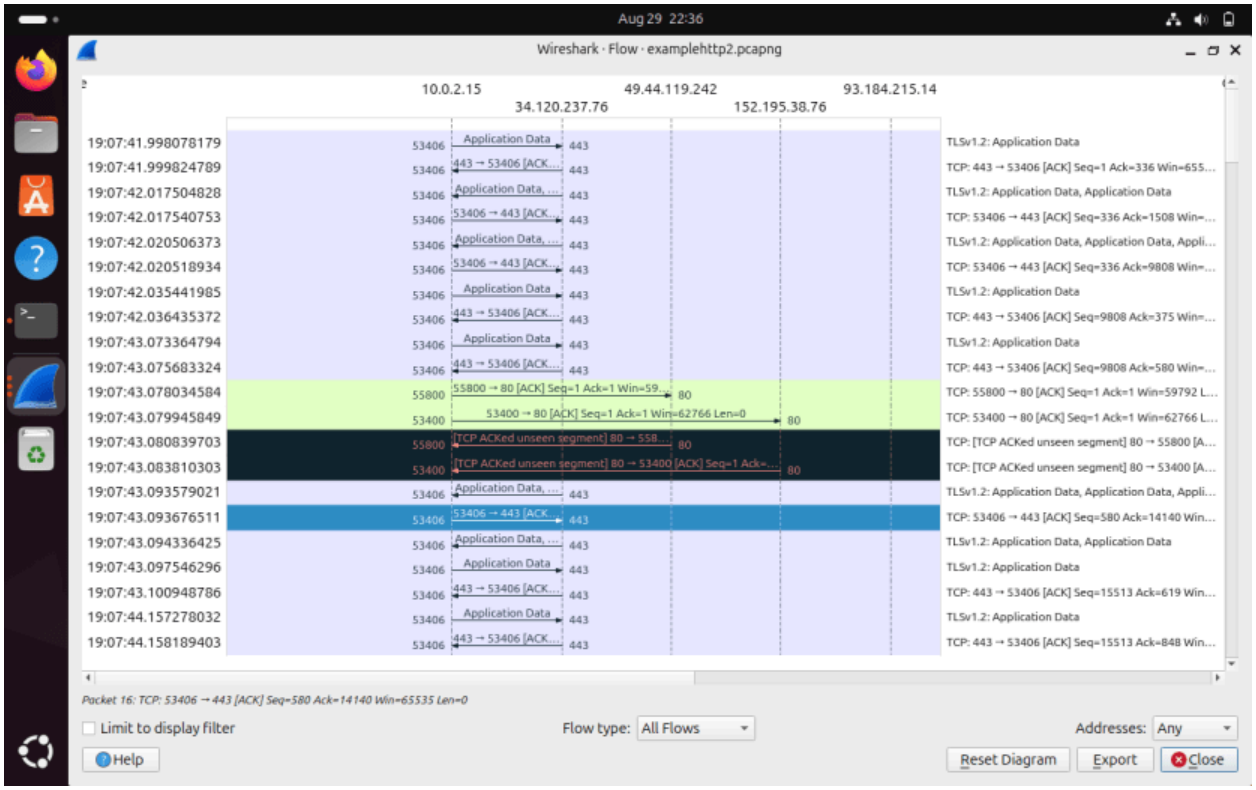
Packet Length:



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	166	305.43	54	8354	0.0066	100%	0.1600	13.710
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	86	58.53	54	78	0.0034	51.81%	0.0700	1.078
80-159	45	108.93	82	159	0.0018	27.11%	0.0800	11.632
160-319	15	222.33	166	303	0.0006	9.04%	0.0400	3.231
320-639	11	408.36	328	523	0.0004	6.63%	0.0300	13.741
640-1279	1	1069.00	1069	1069	0.0000	0.60%	0.0100	3.127
1280-2559	3	1495.00	1427	1561	0.0001	1.81%	0.0100	0.000
2560-5119	2	3844.00	3302	4386	0.0001	1.20%	0.0100	1.096
5120 and greater	3	6565.33	5219	8354	0.0001	1.81%	0.0100	0.000

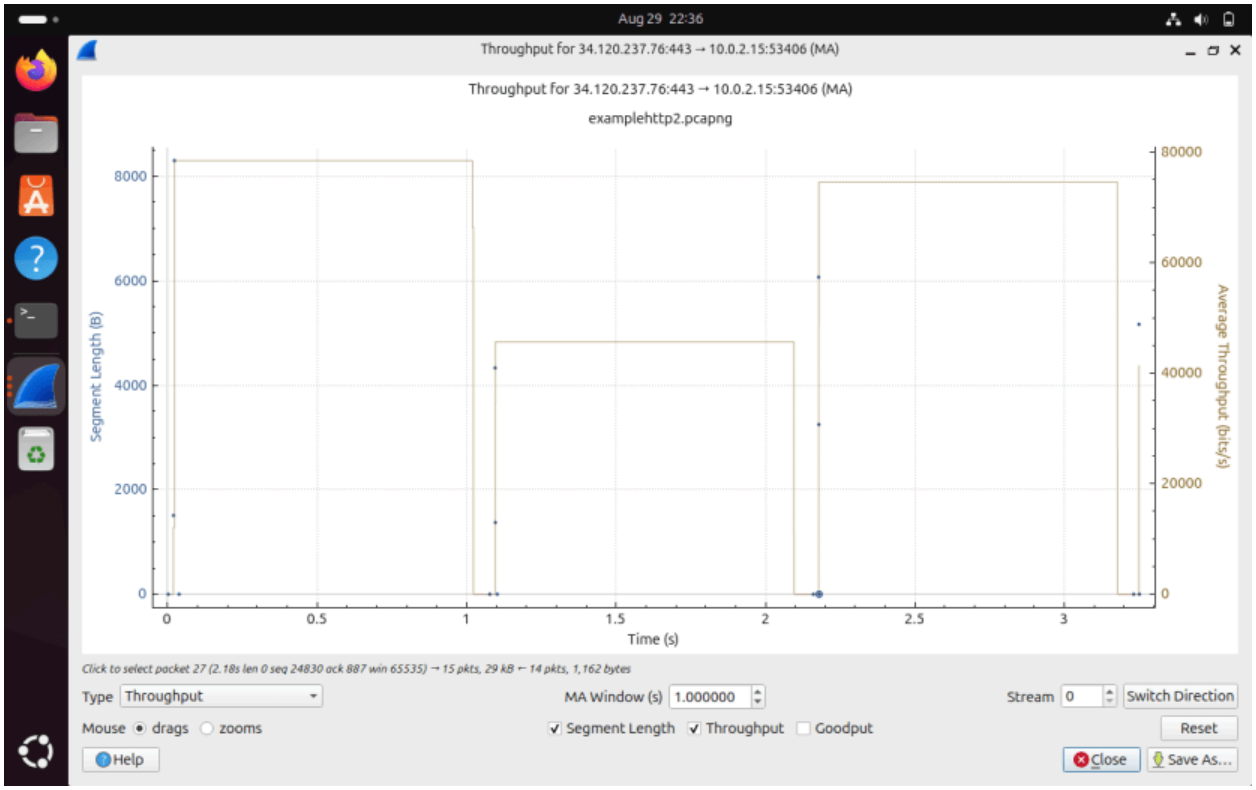
Total Packets - 166
Average packet length- 305.43 bytes
Minimum packet length-54 bytes
Maximum packet length- 8354 bytes
Here 51.81% of the packets are having the length between 40-79 which indicates small data transfers or frequent control messages.
Some larger packets like the one with 8354 bytes represents data transfer.

Flow graph



The communication between multiple IP addresses 10.0.2.15, 49.44.119.242, 93.184.215.14, 34.120.237.76, 152.195.38.76 is shown in the flow graph.
Encrypted communication - TLSv1.2 indicates that data being transmitted is encrypted for secure communication.
Sequence of application data packets followed by acknowledgements is shown in flow graph which is TCP communication.
Communication involves several hosts is justified by the presence of multiple IP addresses.

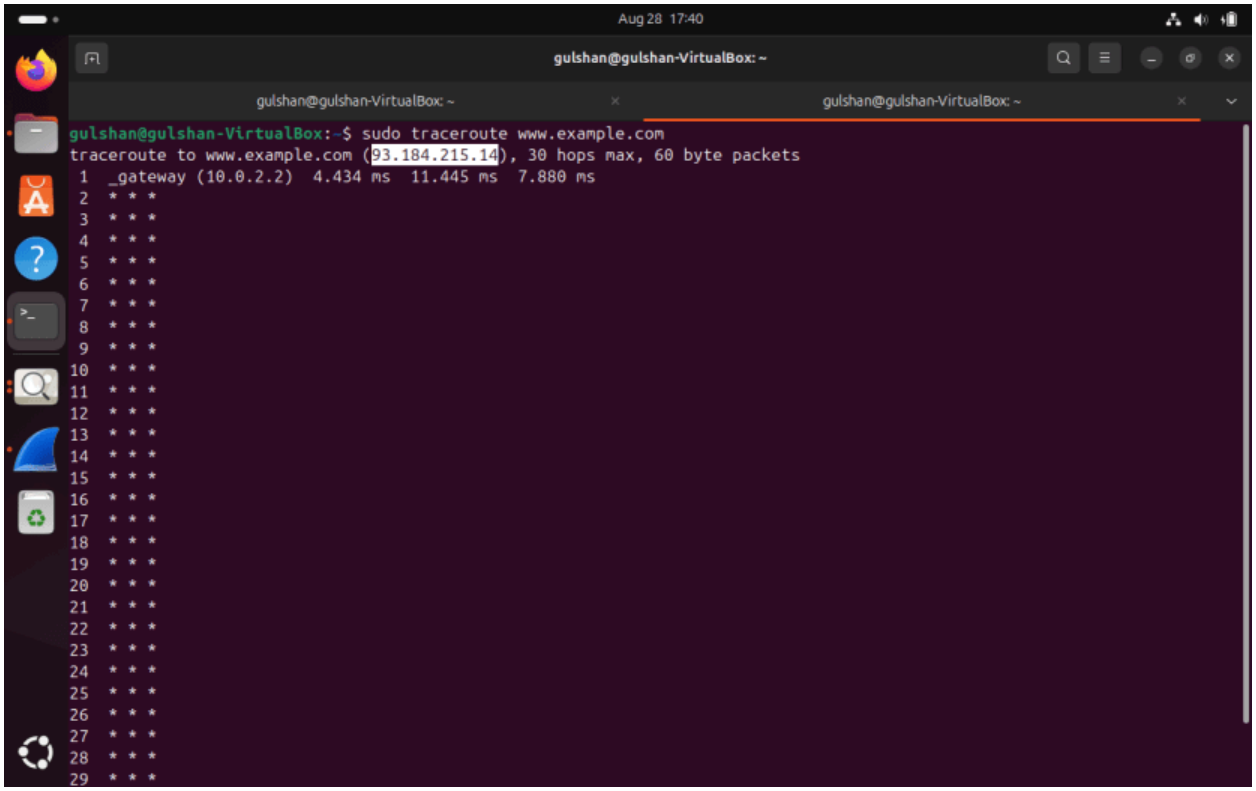
Throughput

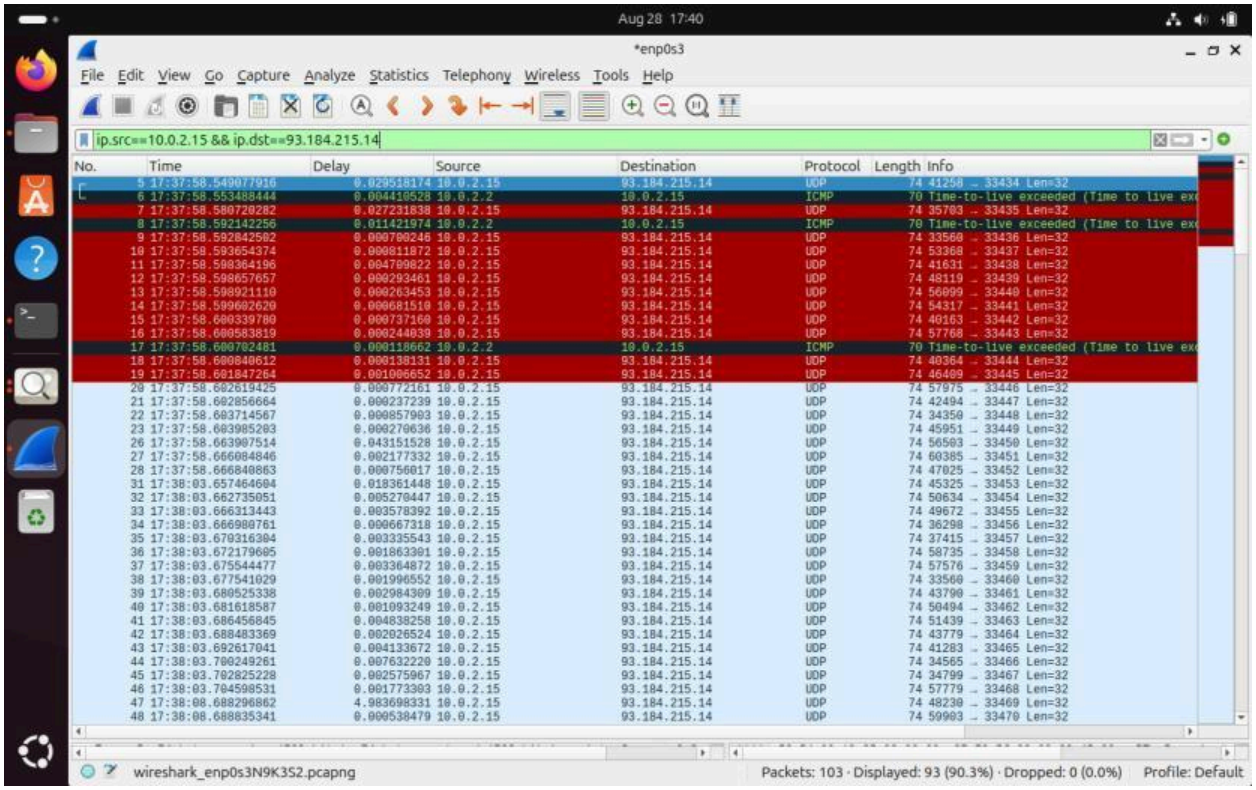


For large data transfer the burst of high throughput in observed from the graph. Throughput get fluctuated could be due to network congestion. THe overall measure of the data transfer rate is the average throughput.

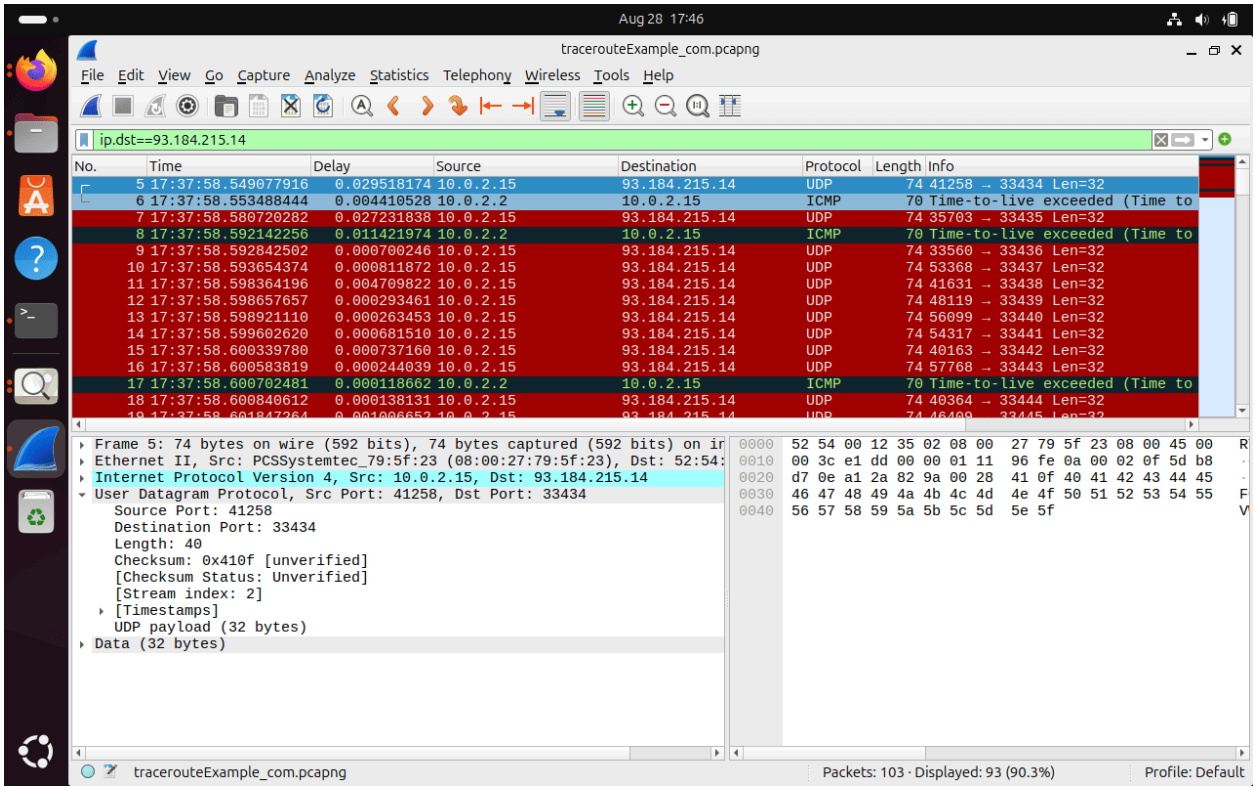
Part B) Analyze packet trace of traceroute session

Task 1)
Solution 1)





UDP is the protocol which is used to send probe packets as visible in the above screenshot where I used http://www.example.com website to capture traceroute traffic.



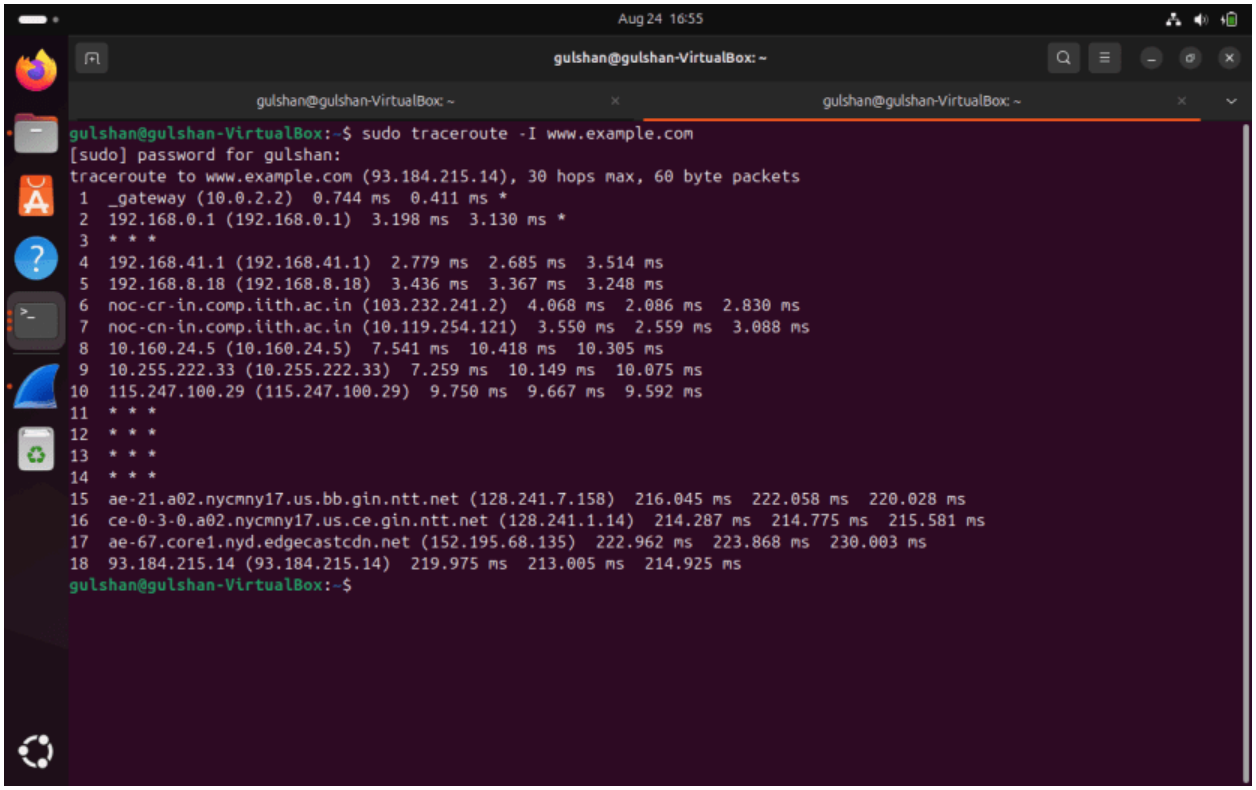
The key fields in the UDP protocol are source port, destination port, checksum, length, timestamps and the last one payload.

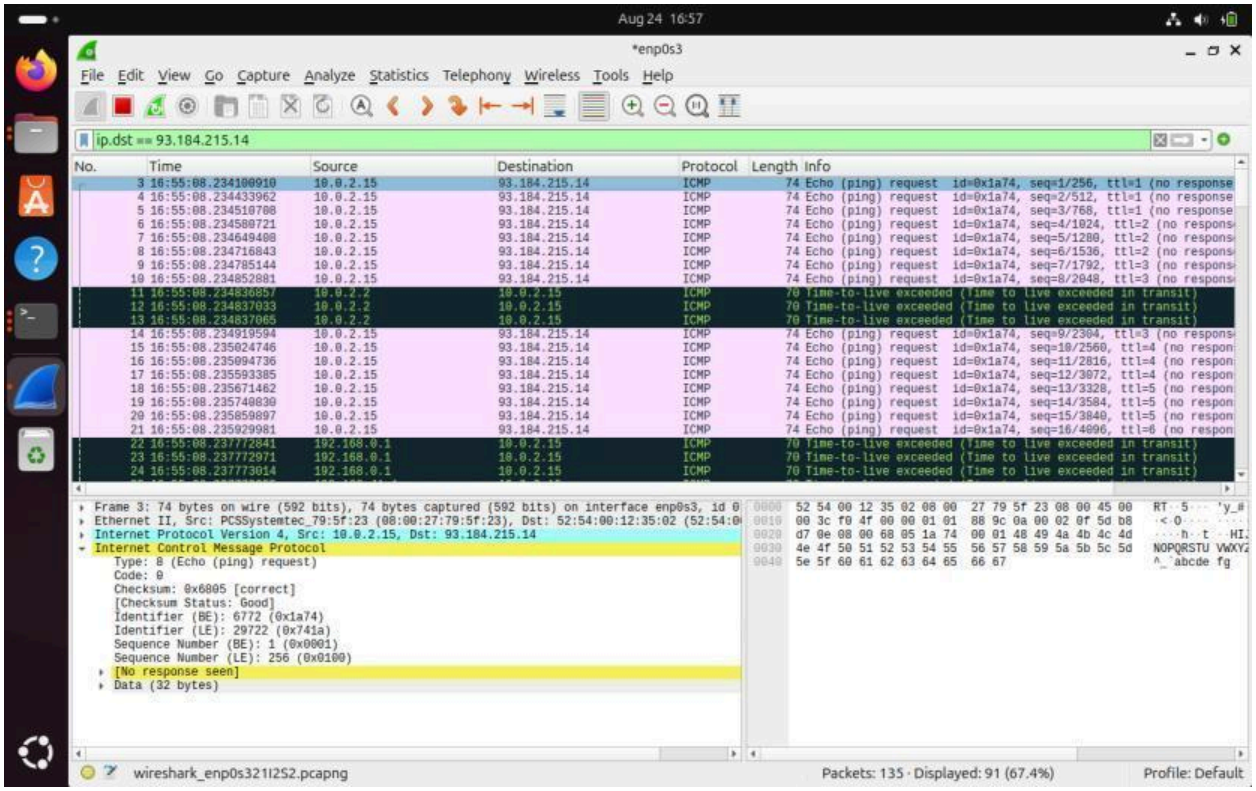
a) Source Port- It shows the port from which UDP packet originated and it corresponds to a specific application or service. Here the source port is 41258.
b) Destination port- Destination port is the port to which the UDP packet is directed. In my wireshark the destination port for the selected packet is 33434.
c) Length- Length is the total size of UDP packet (including both header and payload). Here the length is 40.
d) Checksum- It is used for detecting the errors. Checksum is calculated by sender and is verified by receiver. The checksum value is 0x410f in this packet.
e) Timestamps- When the packet is captured that time is timestamp.
f) UDP payload- The actual information which is to be transmitted is the UDP payload.

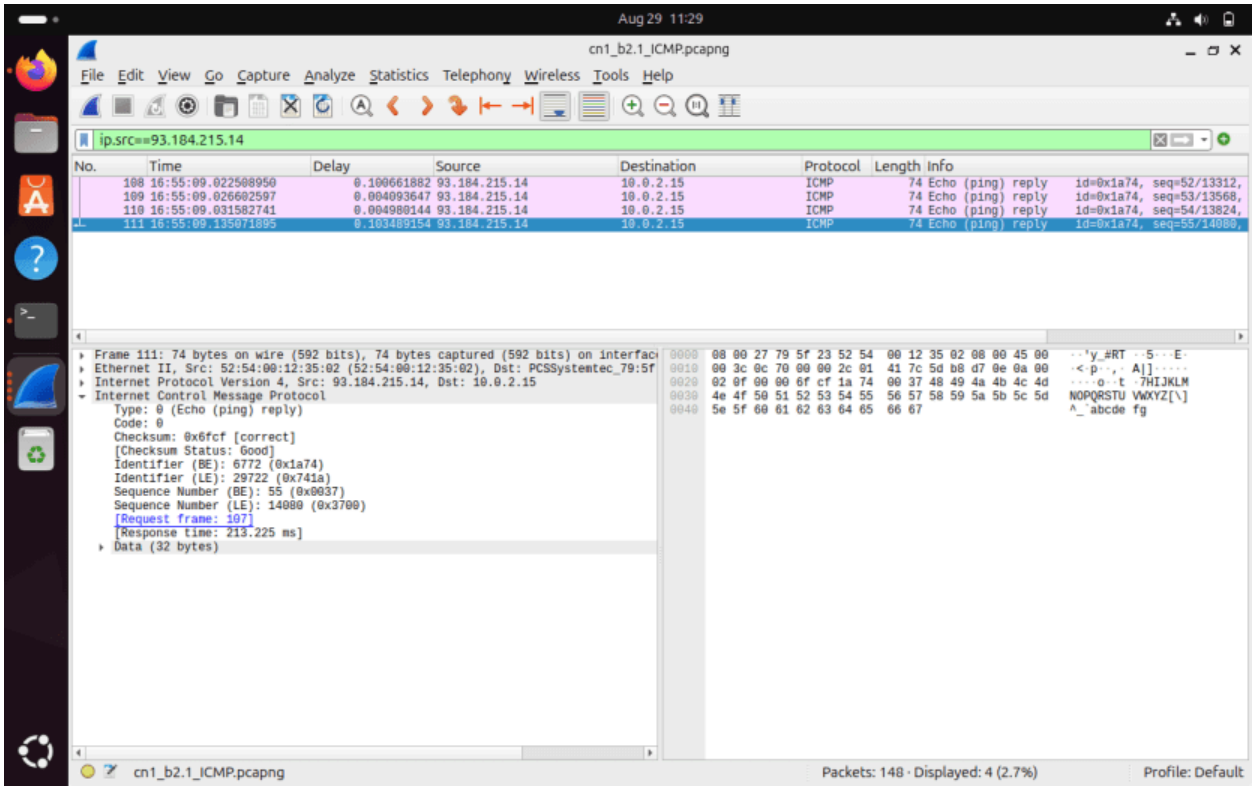
Solution 2)

Yes, we can change the default protocol which is used to send probes.

1) ICMP
   For using ICMP as protocol for sending the probes the command is “sudo traceroute -I www.example.com”. The response for ICMP probe is ICMP echo reply with Type 0 as it is visible in the 3rd screenshot and code 0. This reply comes directly from destination when the destination host is reachable.

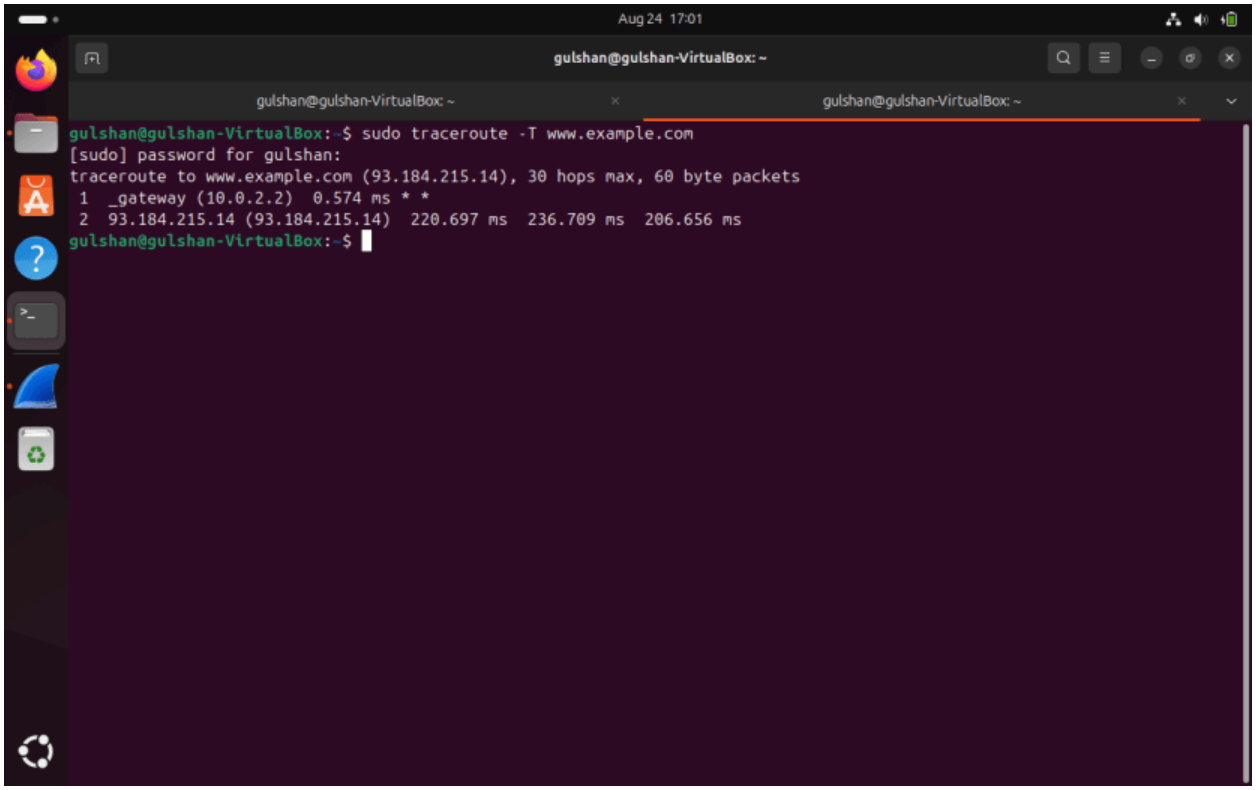

Aug 24 16:55
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox:~$ sudo traceroute -I www.example.com
[sudo] password for gulshan:
traceroute to www.example.com (93.184.215.14), 30 hops max, 60 byte packets
1 _gateway (10.0.2.2) 0.744 ms 0.411 ms *
2 192.168.0.1 (192.168.0.1) 3.198 ms 3.130 ms *
3 * * *
4 192.168.41.1 (192.168.41.1) 2.779 ms 2.685 ms 3.514 ms
5 192.168.8.18 (192.168.8.18) 3.436 ms 3.367 ms 3.248 ms
6 noc-cr-in.comp.iith.ac.in (103.232.241.2) 4.068 ms 2.086 ms 2.830 ms
7 noc-cn-in.comp.iith.ac.in (10.119.254.121) 3.550 ms 2.559 ms 3.088 ms
8 10.160.24.5 (10.160.24.5) 7.541 ms 10.418 ms 10.305 ms
9 10.255.222.33 (10.255.222.33) 7.259 ms 10.149 ms 10.075 ms
10 115.247.100.29 (115.247.100.29) 9.750 ms 9.667 ms 9.592 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 ae-21.a02.nycmny17.us.bb.gin.ntt.net (128.241.7.158) 216.045 ms 222.058 ms 220.028 ms
16 ce-0-3-0.a02.nycmny17.us.ce.gin.ntt.net (128.241.1.14) 214.287 ms 214.775 ms 215.581 ms
17 ae-67.core1.nyd.edgecastcdn.net (152.195.68.135) 222.962 ms 223.868 ms 230.003 ms
18 93.184.215.14 (93.184.215.14) 219.975 ms 213.005 ms 214.925 ms
gulshan@gulshan-VirtualBox:~$

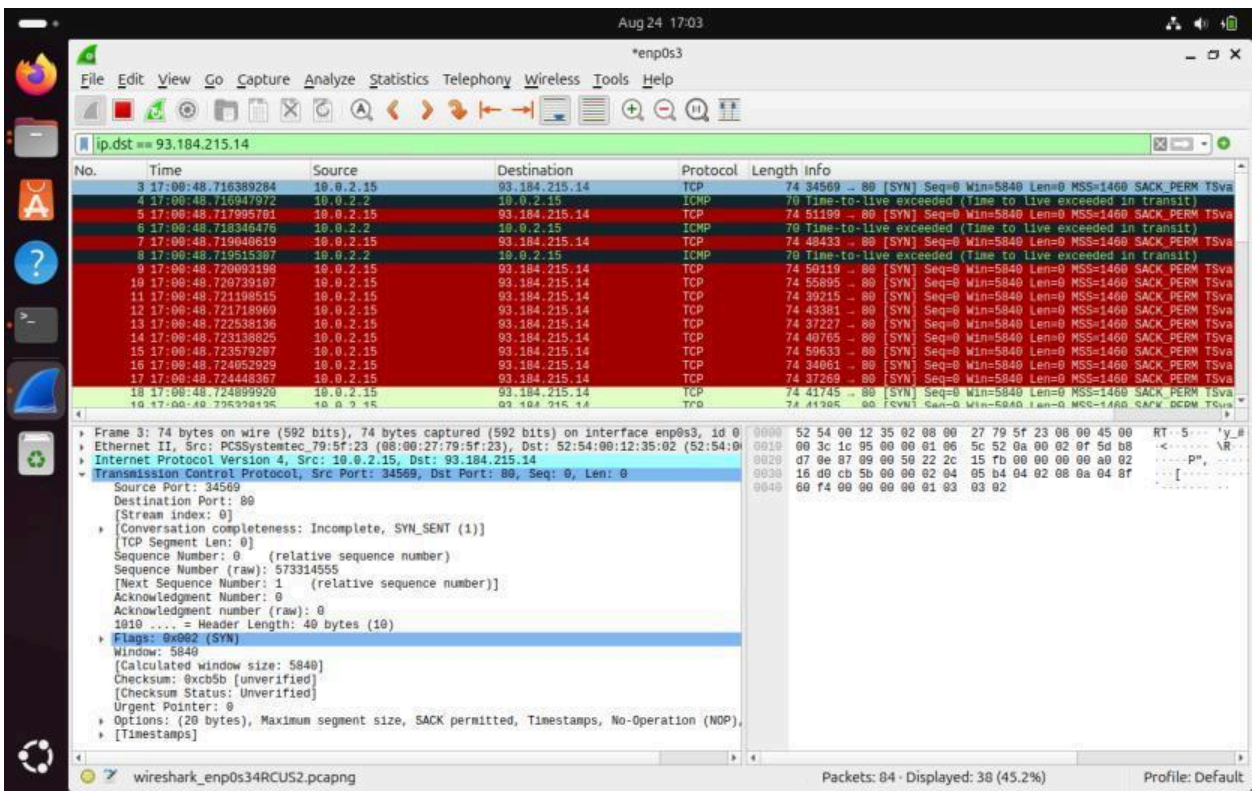

Aug 24 16:57
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 93.184.215.14
No. Time Source Destination Protocol Length Info
3 16:55:08.234100910 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=1/256, ttl=1 (no response
4 16:55:08.234433962 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=2/512, ttl=1 (no response
5 16:55:08.234510708 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=3/768, ttl=1 (no response
6 16:55:08.234580721 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=4/1024, ttl=2 (no respons
7 16:55:08.234649408 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=5/1280, ttl=2 (no respons
8 16:55:08.234716843 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=6/1536, ttl=2 (no respons
9 16:55:08.234785144 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=7/1792, ttl=3 (no respons
10 16:55:08.234852881 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=8/2048, ttl=3 (no respons
11 16:55:08.234836857 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
12 16:55:08.234837033 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
13 16:55:08.234837065 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
14 16:55:08.234919594 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=9/2304, ttl=3 (no respons
15 16:55:08.235024746 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=10/2560, ttl=4 (no respon
16 16:55:08.235094736 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=11/2816, ttl=4 (no respon
17 16:55:08.235593385 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=12/3072, ttl=4 (no respon
18 16:55:08.235671462 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=13/3328, ttl=5 (no respon
19 16:55:08.235740830 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=14/3584, ttl=5 (no respon
20 16:55:08.235859897 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=15/3840, ttl=5 (no respon
21 16:55:08.235929981 10.0.2.15 93.184.215.14 ICMP 74 Echo (ping) request id=0x1a74, seq=16/4096, ttl=6 (no respon
22 16:55:08.237772841 192.168.0.1 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
23 16:55:08.237772971 192.168.0.1 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
24 16:55:08.237773014 192.168.0.1 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PCSSystemtec_79:5f:23 (08:00:27:79:5f:23), Dst: 52:54:00:12:35:02 (52:54:0
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.215.14
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x6805 [correct]
[Checksum Status: Good]
Identifier (BE): 6772 (0x1a74)
Identifier (LE): 29722 (0x741a)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[No response seen]
Data (32 bytes)
0000 52 54 00 12 35 02 08 00 27 79 5f 23 08 00 45 00
0010 00 3c f0 4f 00 00 01 01 88 9c 0a 00 02 0f 5d b8
0020 d7 0e 08 00 68 05 1a 74 00 01 48 49 4a 4b 4c 4d
0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d
0040 5e 5f 60 61 62 63 64 65 66 67
wireshark_enp0s321I2S2.pcapng
Packets: 135 · Displayed: 91 (67.4%)
Profile: Default

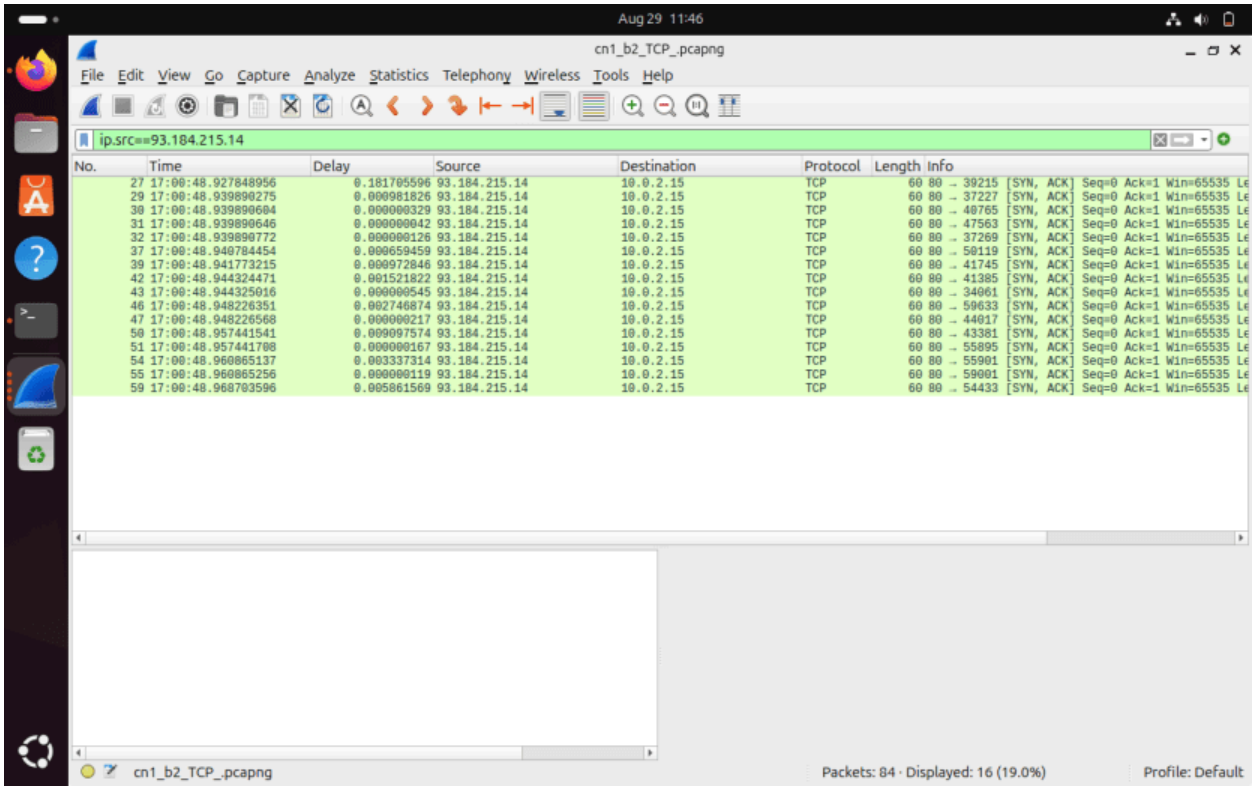


2) TCP

If we want to use TCP for sending probes then we have we use “-T” and the command will be ‘sudo traceroute -T ‘www.example.com ’ . The last probe response is TCP SYN-ACK if destination port is open and TCP RST if destination is closed.

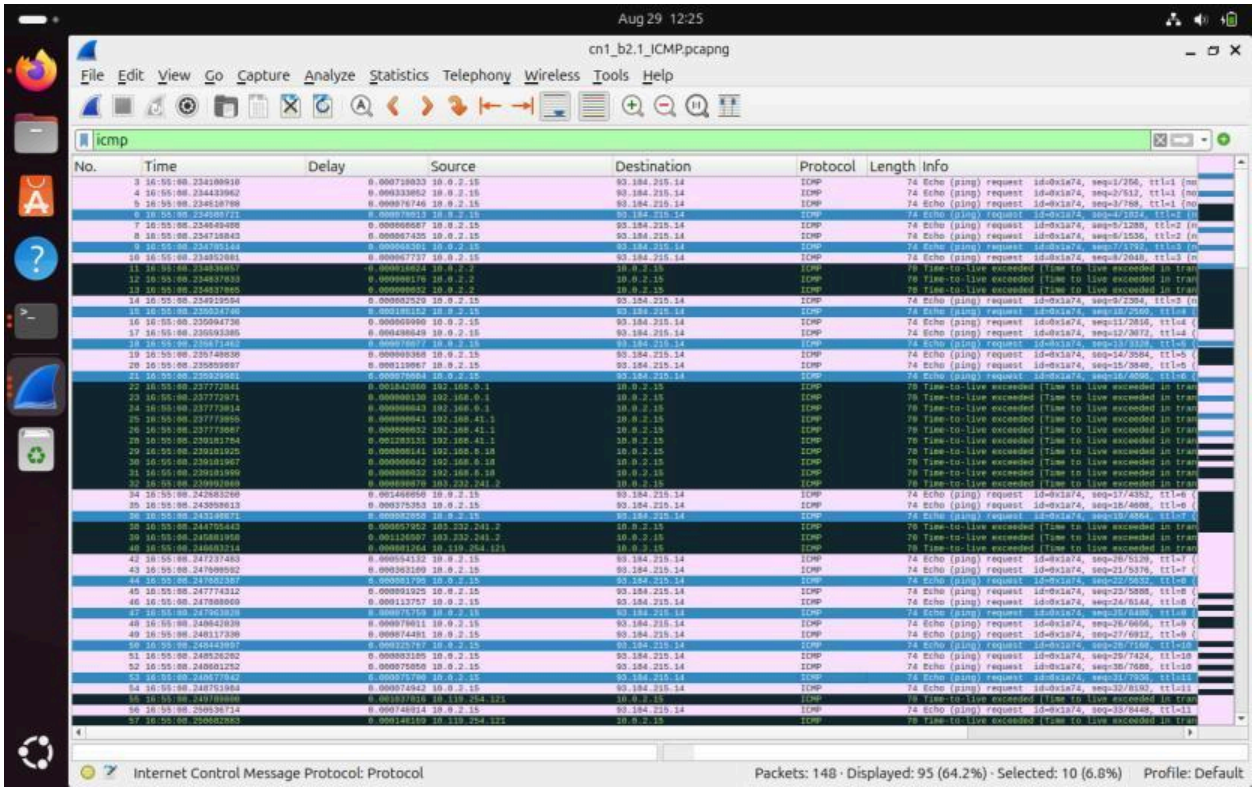

Aug 24 17:01
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox:~$ sudo traceroute -T www.example.com
[sudo] password for gulshan:
traceroute to www.example.com (93.184.215.14), 30 hops max, 60 byte packets
1 _gateway (10.0.2.2) 0.574 ms * *
2 93.184.215.14 (93.184.215.14) 220.697 ms 236.709 ms 206.656 ms
gulshan@gulshan-VirtualBox:~$


Aug 24 17:03
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 93.184.215.14
No. Time Source Destination Protocol Length Info
3 17:00:48.716389284 10.0.2.15 93.184.215.14 TCP 74 34569 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
4 17:00:48.716947972 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
5 17:00:48.717995701 10.0.2.15 93.184.215.14 TCP 74 51199 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
6 17:00:48.718346476 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
7 17:00:48.719040619 10.0.2.15 93.184.215.14 TCP 74 48433 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
8 17:00:48.719515307 10.0.2.2 10.0.2.15 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
9 17:00:48.720093198 10.0.2.15 93.184.215.14 TCP 74 50119 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
10 17:00:48.720739107 10.0.2.15 93.184.215.14 TCP 74 55895 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
11 17:00:48.721198515 10.0.2.15 93.184.215.14 TCP 74 39215 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
12 17:00:48.721718969 10.0.2.15 93.184.215.14 TCP 74 43381 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
13 17:00:48.722538136 10.0.2.15 93.184.215.14 TCP 74 37227 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
14 17:00:48.723138825 10.0.2.15 93.184.215.14 TCP 74 40765 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
15 17:00:48.723579207 10.0.2.15 93.184.215.14 TCP 74 59633 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
16 17:00:48.724052929 10.0.2.15 93.184.215.14 TCP 74 34061 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
17 17:00:48.724448367 10.0.2.15 93.184.215.14 TCP 74 37269 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
18 17:00:48.724899920 10.0.2.15 93.184.215.14 TCP 74 41745 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PCSSystemtec_79:5f:23 (08:00:27:79:5f:23), Dst: 52:54:00:12:35:02 (52:54:0
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 93.184.215.14
Transmission Control Protocol, Src Port: 34569, Dst Port: 80, Seq: 0, Len: 0
Source Port: 34569
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 573314555
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window: 5840
[Calculated window size: 5840]
Checksum: 0xcb5b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP),
[Timestamps]
0000 52 54 00 12 35 02 08 00 27 79 5f 23 08 00 45 00
0010 00 3c 1c 95 00 00 01 06 5c 52 0a 00 02 0f 5d b8
0020 d7 0e 87 09 00 50 22 2c 15 fb 00 00 00 00 a0 02
0030 16 d0 cb 5b 00 00 02 04 05 b4 04 02 08 0a 04 8f
0040 60 f4 00 00 00 00 01 03 03 02
wireshark_enp0s34RCUS2.pcapng
Packets: 84 · Displayed: 38 (45.2%)
Profile: Default



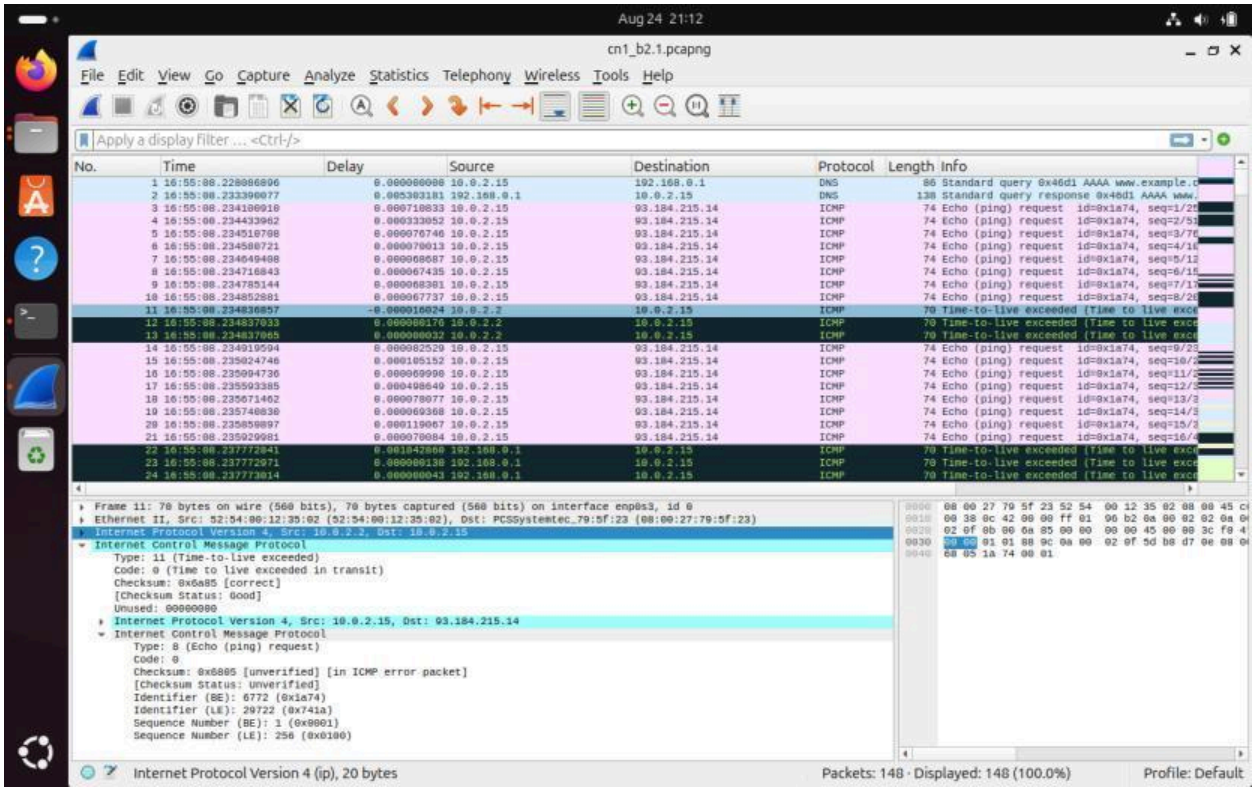
For UDP (which is default protocol in linux) the last probe response is ICMP ‘Port Unreachable ’ message which is of Type 3 and code 3.

Solution 3)



The typical gap between probe packets is 0.00007 seconds as in above screenshot.

Solution 4)



a) ICMP probes- For ICMP probes responses the contains are type, code, checksum. The type is 11 with time exceeded info when it is returned by intermediate router when TTL(time to live) becomes 0. Type 0 echo reply is sent by final destination. Code 0 for both echo reply and time exceeded message.
   It uses ICMP protocol for probe responses.
b) TCP probes- The contained in the probe responses for TCP are TCP flag, sequence and acknowledgement numbers, TCP header information. TCP flag - If the TCP port is open then SYN- ACK is sent by the destination. If the TCP port is closed the RST is sent by the destination. Sequence and acknowledgement numbers- This are used to reset or establish connection.
   It uses TCP protocols for probe responses.
c) UDP probes: The contained in the UDP probe response is ICMP type and ICMP code. It uses ICMP protocol for probe responses.

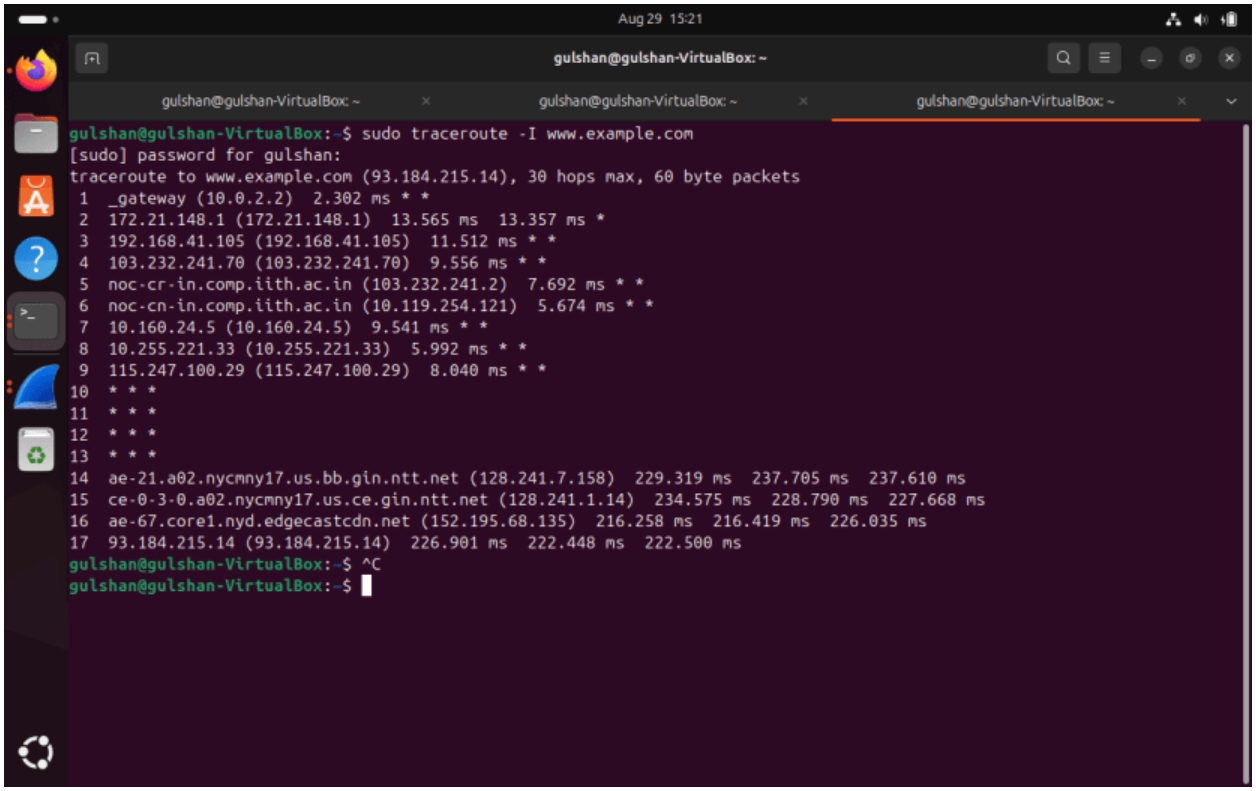
Solution 5)

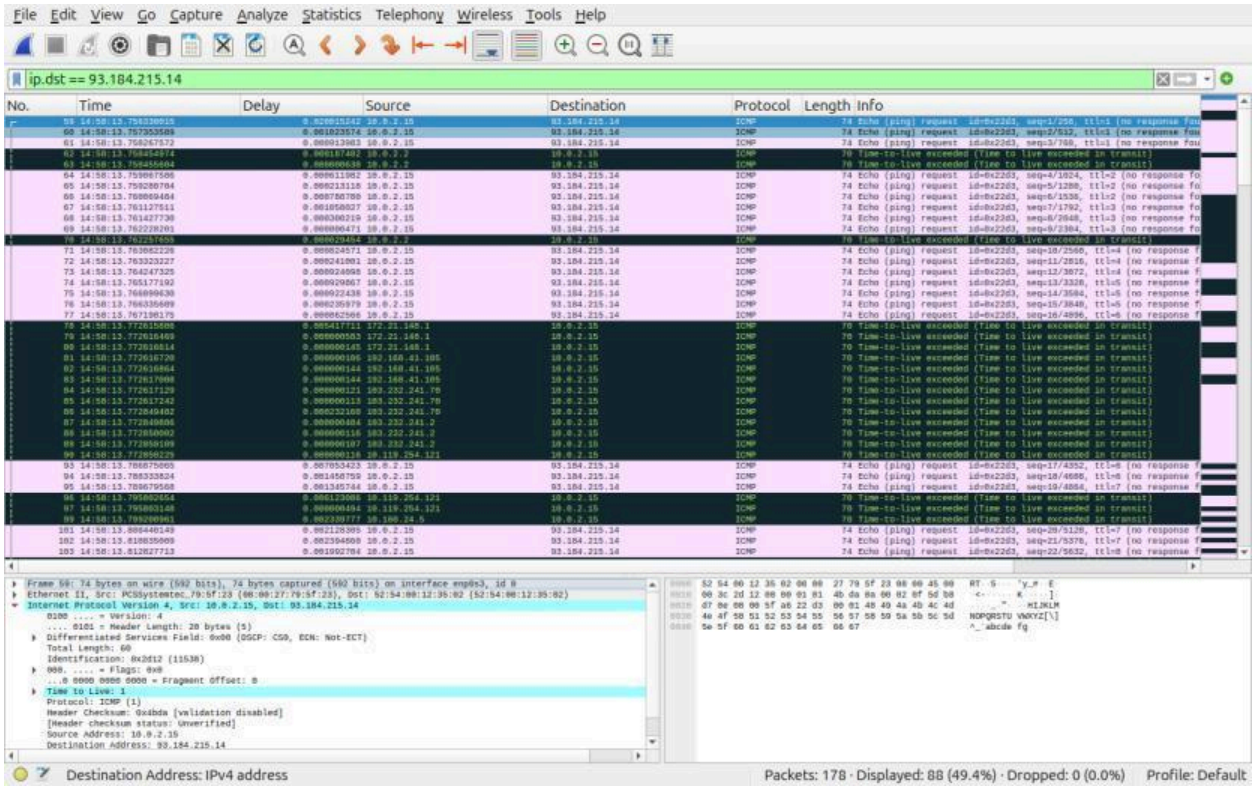
The Time To Live field present in ICMP, TCP and also UDP.
The TTL value at beginning is 1, later each subsequent probe send has TTL value incremented by 1.
The remaining hops from the destination to source is indicated by TTL value in the responses.
In responses the TTL value decreases by 1 at each hop.

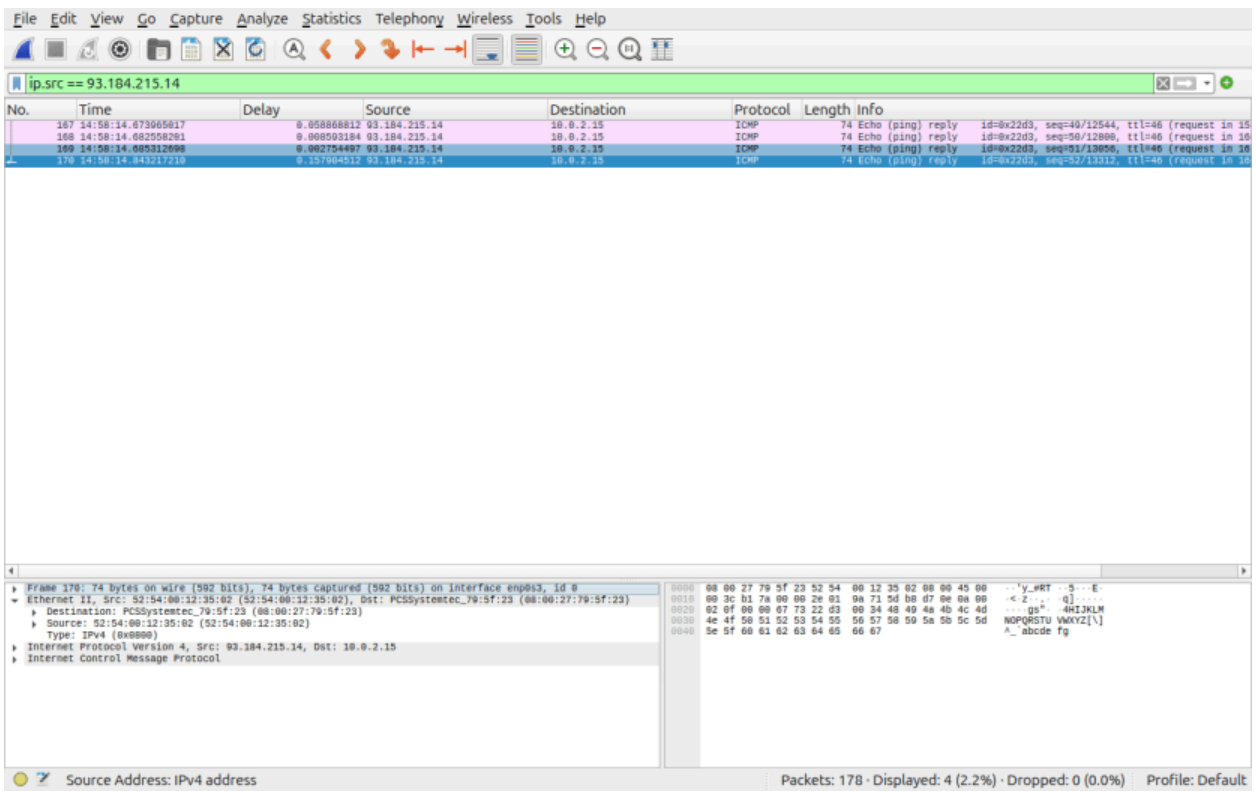
Solution 6)

To get the output of traceroute session the time required is the difference between 1st probe send to the last response which is equal to 1.086887195 seconds.

The bottleneck router is hop 17 with IP address 93.184.215.14 with highest latency around 222-227 ms.



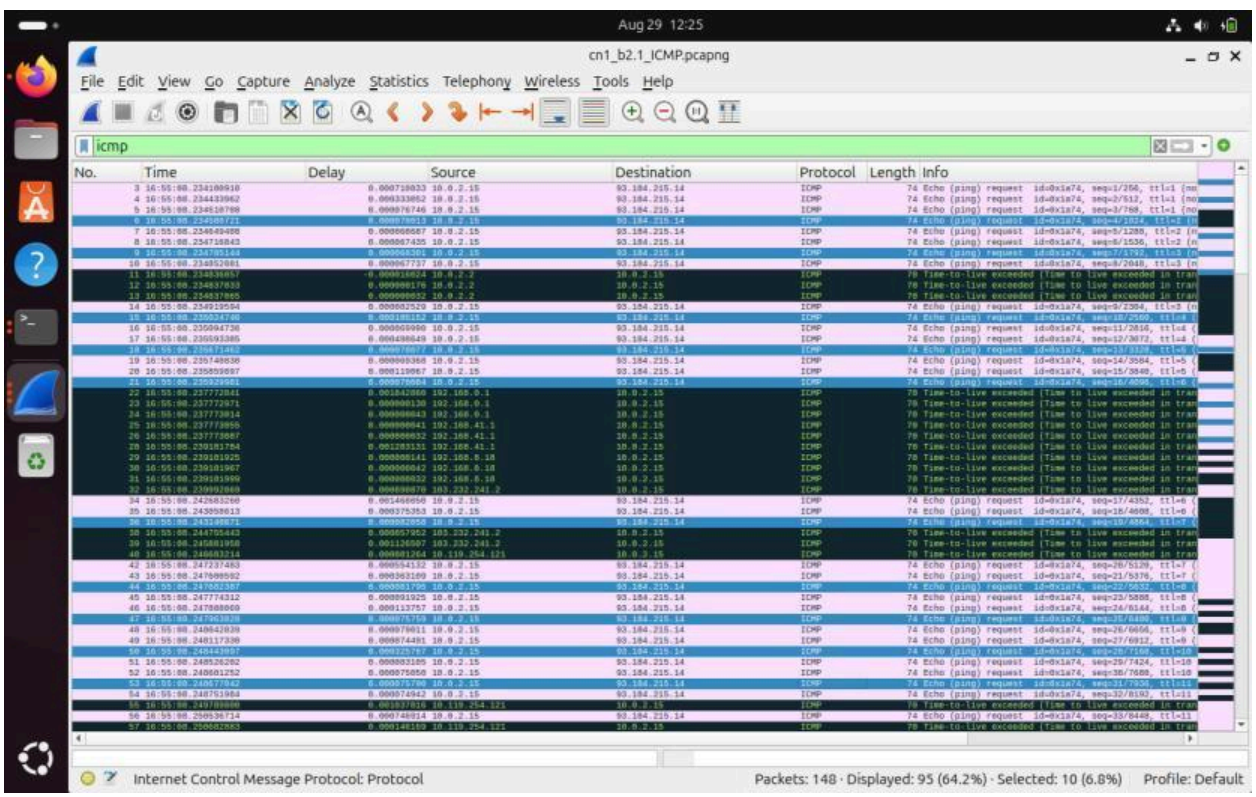

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 93.184.215.14
No. Time Delay Source Destination Protocol Length Info
Destination Address: IPv4 address
Packets: 178 · Displayed: 88 (49.4%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 93.184.215.14
No. Time Delay Source Destination Protocol Length Info
Source Address: IPv4 address
Packets: 178 · Displayed: 4 (2.2%) · Dropped: 0 (0.0%)
Profile: Default

Solution 7)

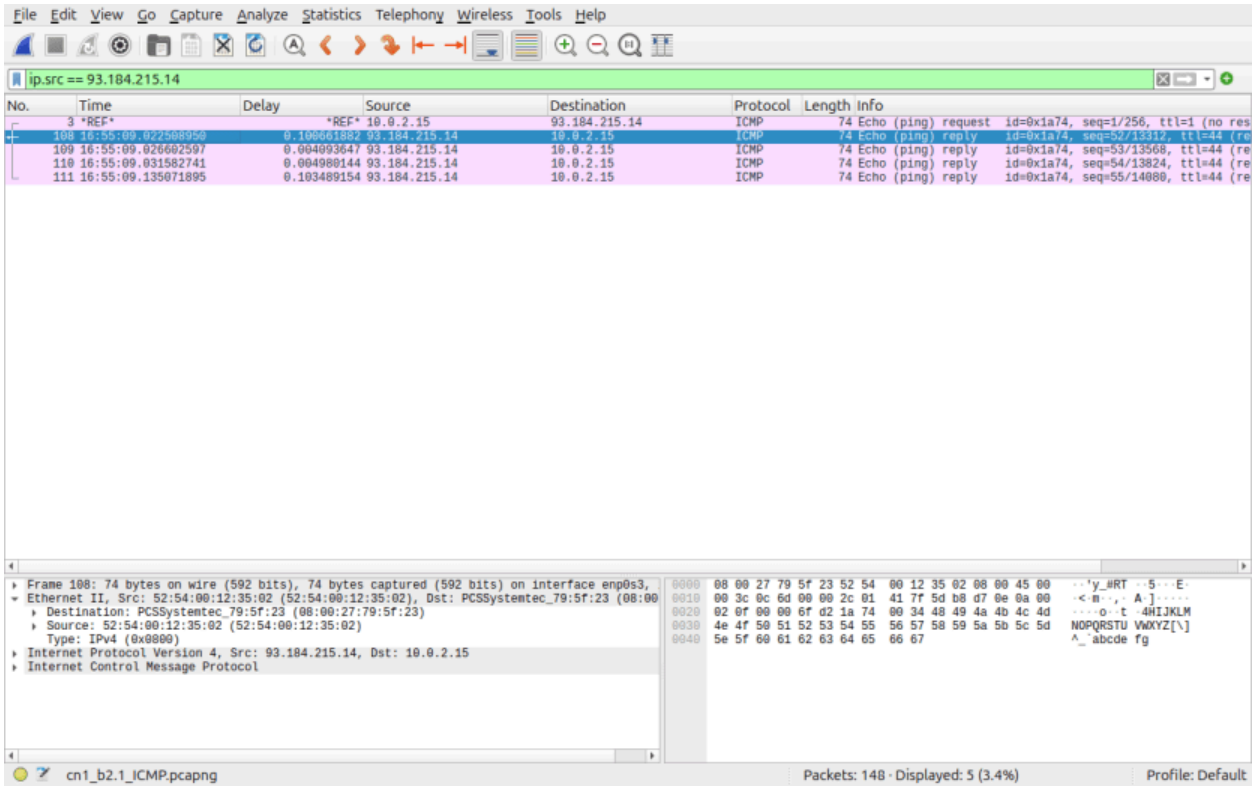
Yes, stars are present in the output of the traceroute session. The potential reasons behind this are discussed below
Firewall Rules or Filtering is one of the reason because some routers may be configured to block ICMP request and when router respond it result in timeout and stars are seen.
If the router received much packets then it will drop some packets leading to timeouts.
Congestion in network can delay responses is also the one of the reason.
Router misconfiguration- If the router is misconfigured then it may not respond probes which leads to stars.
Load balanced server- Sometimes multiple load balancer handle requests for a single IP then only one server responds to it which results in stars.
No route- If probe packet is not forwarded by router then probe times out.

Solution 8)



Three probe packets are sent in bursts.
For the first burst the inter packet time difference between the consecutive packets as follows

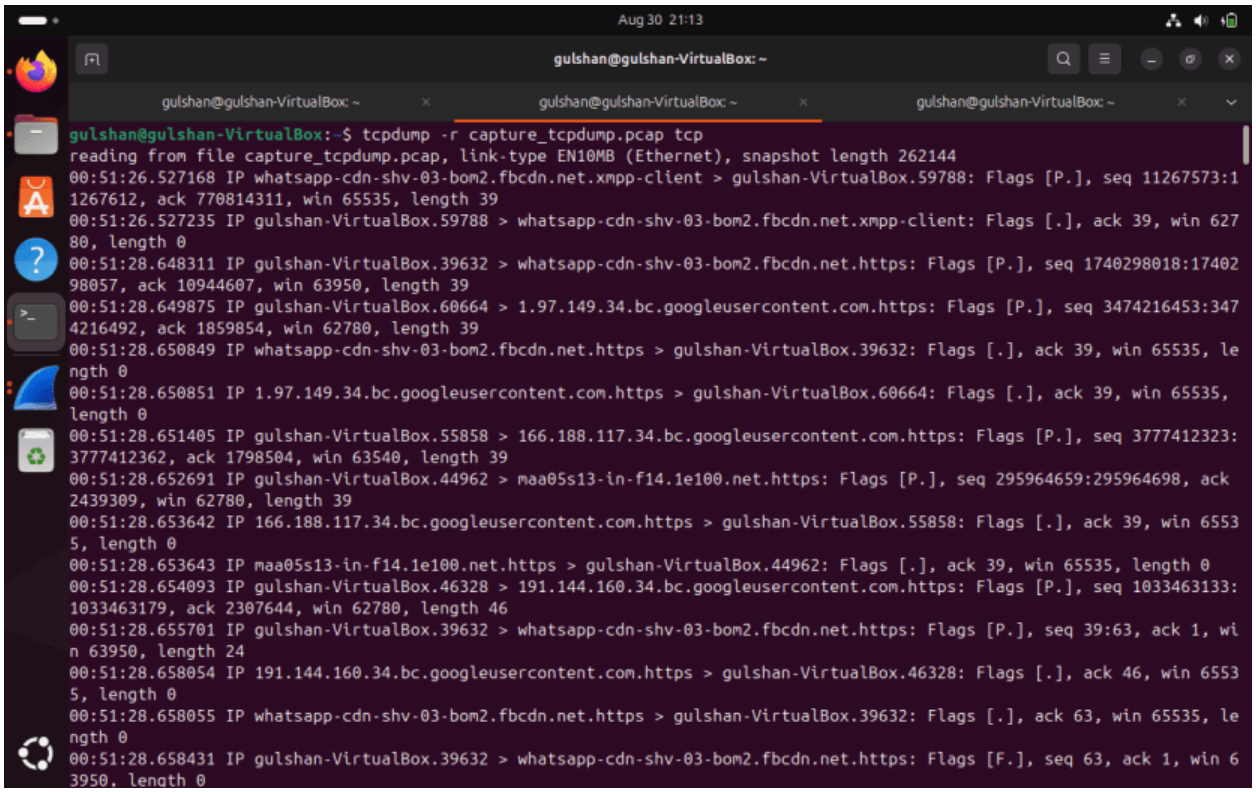
Between 1 and 2: 0.000333852 seconds
Between 2 and 3: 0.000070812 seconds



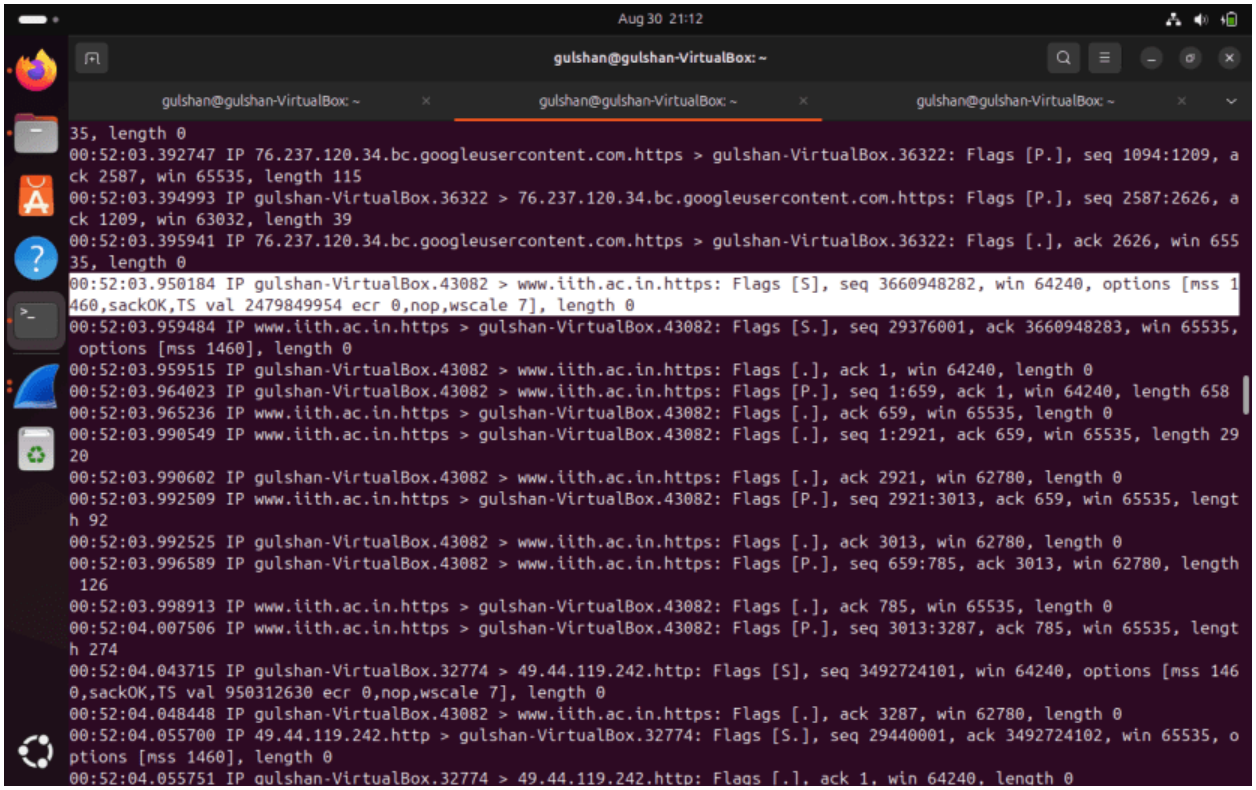
The time elapsed between first request and its response is 0.100661882 seconds.

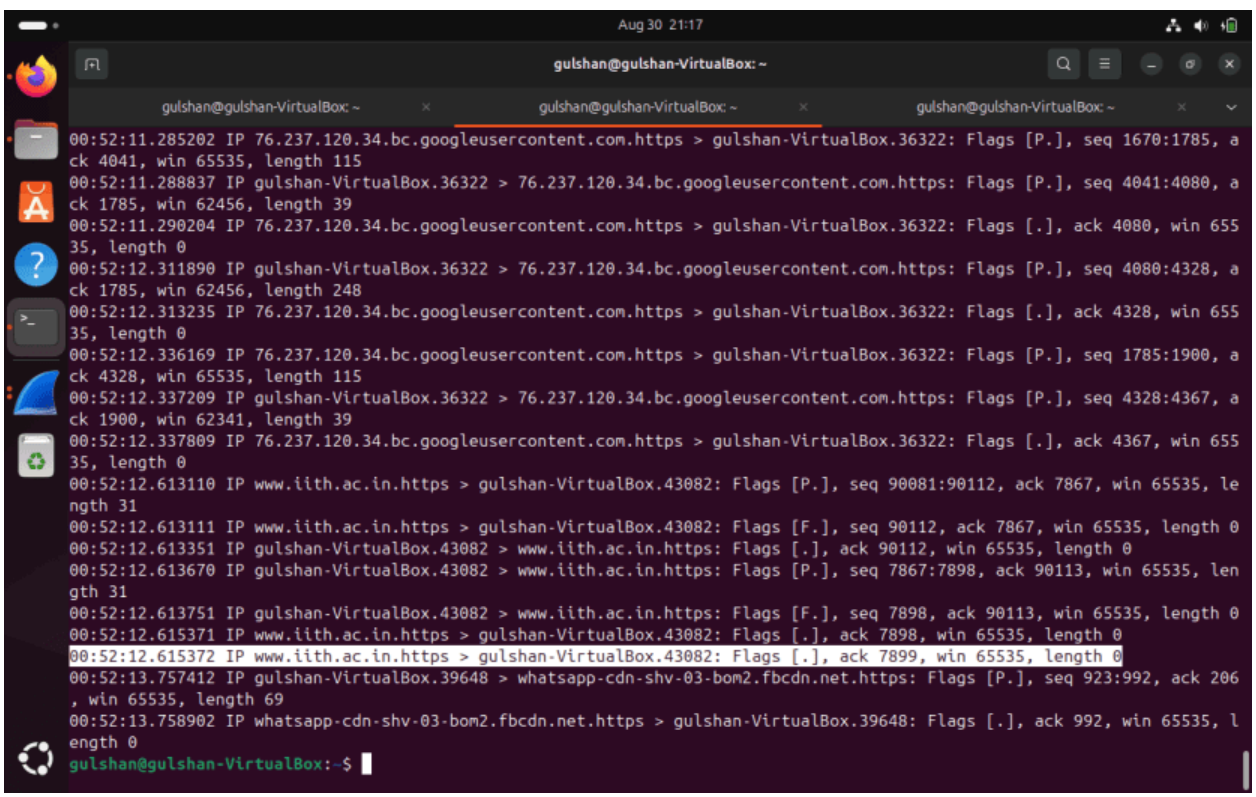
TASK-2

Solution 6(Task2)



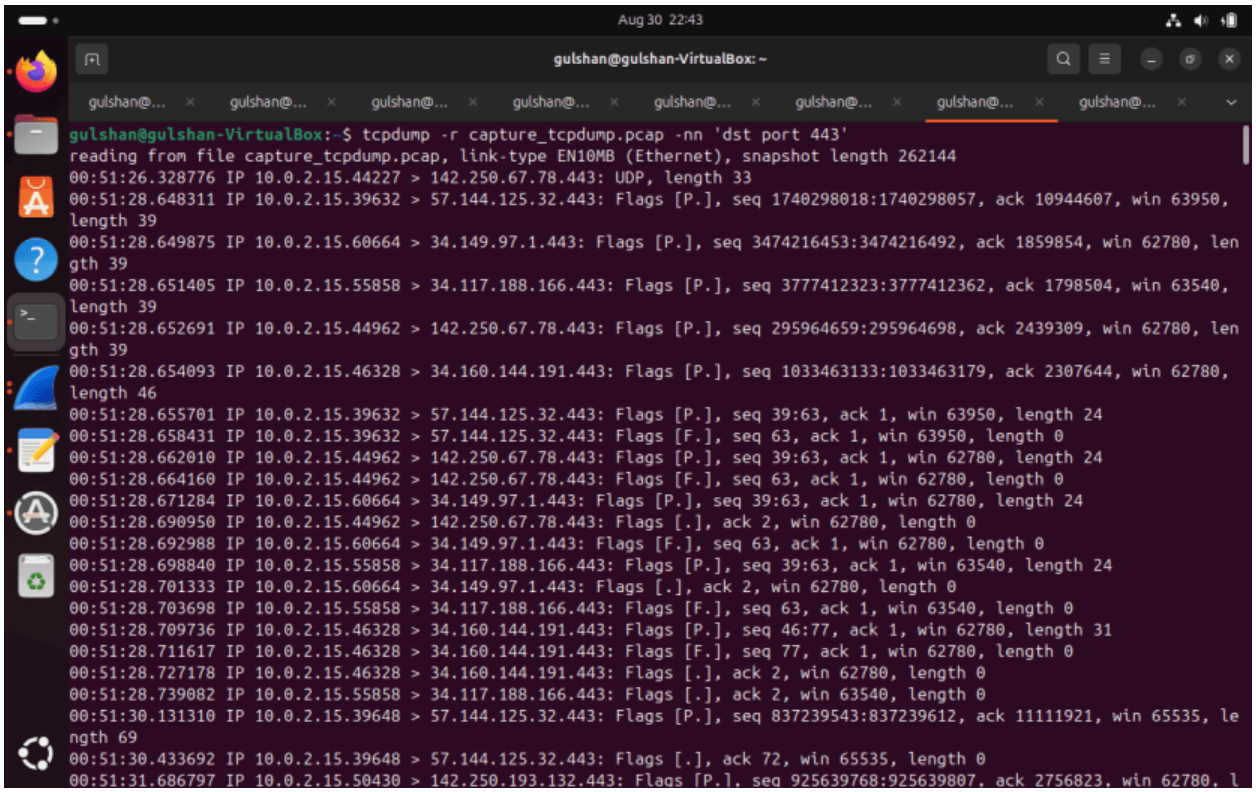
```
gulshan@gulshan-VirtualBox:~$ tcpdump -r capture_tcpdump.pcap tcp
reading from file capture_tcpdump.pcap, link-type EN10MB (Ethernet), snapshot length 262144
00:51:26.527168 IP whatsapp-cdn-shv-03-bom2.fbcdn.net.xmpp-client > gulshan-VirtualBox.59788: Flags [P.], seq 11267573:1
1267612, ack 770814311, win 65535, length 39
00:51:26.527235 IP gulshan-VirtualBox.59788 > whatsapp-cdn-shv-03-bom2.fbcdn.net.xmpp-client: Flags [.], ack 39, win 627
80, length 0
00:51:28.648311 IP gulshan-VirtualBox.39632 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [P.], seq 1740298018:17402
98057, ack 10944607, win 63950, length 39
00:51:28.649875 IP gulshan-VirtualBox.60664 > 1.97.149.34.bc.googleusercontent.com.https: Flags [P.], seq 3474216453:347
4216492, ack 1859854, win 62780, length 39
00:51:28.650849 IP whatsapp-cdn-shv-03-bom2.fbcdn.net.https > gulshan-VirtualBox.39632: Flags [.], ack 39, win 65535, le
ngth 0
00:51:28.650851 IP 1.97.149.34.bc.googleusercontent.com.https > gulshan-VirtualBox.60664: Flags [.], ack 39, win 65535,
length 0
00:51:28.651405 IP gulshan-VirtualBox.55858 > 166.188.117.34.bc.googleusercontent.com.https: Flags [P.], seq 3777412323:
3777412362, ack 1798504, win 63540, length 39
00:51:28.652691 IP gulshan-VirtualBox.44962 > maa05s13-in-f14.1e100.net.https: Flags [P.], seq 295964659:295964698, ack
2439309, win 62780, length 39
00:51:28.653642 IP 166.188.117.34.bc.googleusercontent.com.https > gulshan-VirtualBox.55858: Flags [.], ack 39, win 6553
5, length 0
00:51:28.653643 IP maa05s13-in-f14.1e100.net.https > gulshan-VirtualBox.44962: Flags [.], ack 39, win 65535, length 0
00:51:28.654093 IP gulshan-VirtualBox.46328 > 191.144.160.34.bc.googleusercontent.com.https: Flags [P.], seq 1033463133:
1033463179, ack 2307644, win 62780, length 46
00:51:28.655701 IP gulshan-VirtualBox.39632 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [P.], seq 39:63, ack 1, wi
n 63950, length 24
00:51:28.658054 IP 191.144.160.34.bc.googleusercontent.com.https > gulshan-VirtualBox.46328: Flags [.], ack 46, win 6553
5, length 0
00:51:28.658055 IP whatsapp-cdn-shv-03-bom2.fbcdn.net.https > gulshan-VirtualBox.39632: Flags [.], ack 63, win 65535, le
ngth 0
00:51:28.658431 IP gulshan-VirtualBox.39632 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [F.], seq 63, ack 1, win 6
3950, length 0
```


Aug 30 21:12
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
35, length 0
00:52:03.392747 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [P.], seq 1094:1209, ack 2587, win 65535, length 115
00:52:03.394993 IP gulshan-VirtualBox.36322 > 76.237.120.34.bc.googleusercontent.com.https: Flags [P.], seq 2587:2626, ack 1209, win 63032, length 39
00:52:03.395941 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [.], ack 2626, win 65535, length 0
00:52:03.950184 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [S], seq 3660948282, win 64240, options [mss 1460,sackOK,TS val 2479849954 ecr 0,nop,wscale 7], length 0
00:52:03.959484 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [S.], seq 29376001, ack 3660948283, win 65535, options [mss 1460], length 0
00:52:03.959515 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [.], ack 1, win 64240, length 0
00:52:03.964023 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [P.], seq 1:659, ack 1, win 64240, length 658
00:52:03.965236 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [.], ack 659, win 65535, length 0
00:52:03.990549 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [.], seq 1:2921, ack 659, win 65535, length 2920
00:52:03.990602 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [.], ack 2921, win 62780, length 0
00:52:03.992509 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [P.], seq 2921:3013, ack 659, win 65535, length 92
00:52:03.992525 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [.], ack 3013, win 62780, length 0
00:52:03.996589 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [P.], seq 659:785, ack 3013, win 62780, length 126
00:52:03.998913 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [.], ack 785, win 65535, length 0
00:52:04.007506 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [P.], seq 3013:3287, ack 785, win 65535, length 274
00:52:04.043715 IP gulshan-VirtualBox.32774 > 49.44.119.242.http: Flags [S], seq 3492724101, win 64240, options [mss 1460,sackOK,TS val 950312630 ecr 0,nop,wscale 7], length 0
00:52:04.048448 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [.], ack 3287, win 62780, length 0
00:52:04.055700 IP 49.44.119.242.http > gulshan-VirtualBox.32774: Flags [S.], seq 29440001, ack 3492724102, win 65535, options [mss 1460], length 0
00:52:04.055751 IP gulshan-VirtualBox.32774 > 49.44.119.242.http: Flags [.], ack 1, win 64240, length 0


Aug 30 21:17
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox: ~
00:52:11.285202 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [P.], seq 1670:1785, ack 4041, win 65535, length 115
00:52:11.288837 IP gulshan-VirtualBox.36322 > 76.237.120.34.bc.googleusercontent.com.https: Flags [P.], seq 4041:4080, ack 1785, win 62456, length 39
00:52:11.290204 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [.], ack 4080, win 65535, length 0
00:52:12.311890 IP gulshan-VirtualBox.36322 > 76.237.120.34.bc.googleusercontent.com.https: Flags [P.], seq 4080:4328, ack 1785, win 62456, length 248
00:52:12.313235 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [.], ack 4328, win 65535, length 0
00:52:12.336169 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [P.], seq 1785:1900, ack 4328, win 65535, length 115
00:52:12.337209 IP gulshan-VirtualBox.36322 > 76.237.120.34.bc.googleusercontent.com.https: Flags [P.], seq 4328:4367, ack 1900, win 62341, length 39
00:52:12.337809 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [.], ack 4367, win 65535, length 0
00:52:12.613110 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [P.], seq 90081:90112, ack 7867, win 65535, length 31
00:52:12.613111 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [F.], seq 90112, ack 7867, win 65535, length 0
00:52:12.613351 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [.], ack 90112, win 65535, length 0
00:52:12.613670 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [P.], seq 7867:7898, ack 90113, win 65535, length 31
00:52:12.613751 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [F.], seq 7898, ack 90113, win 65535, length 0
00:52:12.615371 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [.], ack 7898, win 65535, length 0
00:52:12.615372 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [.], ack 7899, win 65535, length 0
00:52:13.757412 IP gulshan-VirtualBox.39648 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [P.], seq 923:992, ack 206, win 65535, length 69
00:52:13.758902 IP whatsapp-cdn-shv-03-bom2.fbcdn.net.https > gulshan-VirtualBox.39648: Flags [.], ack 992, win 65535, length 0
gulshan@gulshan-VirtualBox:~$

To get the output of the traceroute session 8.665188 seconds for required and the bottleneck router is 172.21.148.1 .

Solution 8(Task 2)



```
gulshan@gulshan-VirtualBox:~$ tcpdump -r capture_tcpdump.pcap -nn 'dst port 443'
reading from file capture_tcpdump.pcap, link-type EN10MB (Ethernet), snapshot length 262144
00:51:26.328776 IP 10.0.2.15.44227 > 142.250.67.78.443: UDP, length 33
00:51:28.648311 IP 10.0.2.15.39632 > 57.144.125.32.443: Flags [P.], seq 1740298018:1740298057, ack 10944607, win 63950,
length 39
00:51:28.649875 IP 10.0.2.15.60664 > 34.149.97.1.443: Flags [P.], seq 3474216453:3474216492, ack 1859854, win 62780, len
gth 39
00:51:28.651405 IP 10.0.2.15.55858 > 34.117.188.166.443: Flags [P.], seq 3777412323:3777412362, ack 1798504, win 63540,
length 39
00:51:28.652691 IP 10.0.2.15.44962 > 142.250.67.78.443: Flags [P.], seq 295964659:295964698, ack 2439309, win 62780, len
gth 39
00:51:28.654093 IP 10.0.2.15.46328 > 34.160.144.191.443: Flags [P.], seq 1033463133:1033463179, ack 2307644, win 62780,
length 46
00:51:28.655701 IP 10.0.2.15.39632 > 57.144.125.32.443: Flags [P.], seq 39:63, ack 1, win 63950, length 24
00:51:28.658431 IP 10.0.2.15.39632 > 57.144.125.32.443: Flags [F.], seq 63, ack 1, win 63950, length 0
00:51:28.662010 IP 10.0.2.15.44962 > 142.250.67.78.443: Flags [P.], seq 39:63, ack 1, win 62780, length 24
00:51:28.664160 IP 10.0.2.15.44962 > 142.250.67.78.443: Flags [F.], seq 63, ack 1, win 62780, length 0
00:51:28.671284 IP 10.0.2.15.60664 > 34.149.97.1.443: Flags [P.], seq 39:63, ack 1, win 62780, length 24
00:51:28.690950 IP 10.0.2.15.44962 > 142.250.67.78.443: Flags [.], ack 2, win 62780, length 0
00:51:28.692988 IP 10.0.2.15.60664 > 34.149.97.1.443: Flags [F.], seq 63, ack 1, win 62780, length 0
00:51:28.698840 IP 10.0.2.15.55858 > 34.117.188.166.443: Flags [P.], seq 39:63, ack 1, win 63540, length 24
00:51:28.701333 IP 10.0.2.15.60664 > 34.149.97.1.443: Flags [.], ack 2, win 62780, length 0
00:51:28.703698 IP 10.0.2.15.55858 > 34.117.188.166.443: Flags [F.], seq 63, ack 1, win 63540, length 0
00:51:28.709736 IP 10.0.2.15.46328 > 34.160.144.191.443: Flags [P.], seq 46:77, ack 1, win 62780, length 31
00:51:28.711617 IP 10.0.2.15.46328 > 34.160.144.191.443: Flags [F.], seq 77, ack 1, win 62780, length 0
00:51:28.727178 IP 10.0.2.15.46328 > 34.160.144.191.443: Flags [.], ack 2, win 62780, length 0
00:51:28.739082 IP 10.0.2.15.55858 > 34.117.188.166.443: Flags [.], ack 2, win 63540, length 0
00:51:30.131310 IP 10.0.2.15.39648 > 57.144.125.32.443: Flags [P.], seq 837239543:837239612, ack 11111921, win 65535, le
ngth 69
00:51:30.433692 IP 10.0.2.15.39648 > 57.144.125.32.443: Flags [.], ack 72, win 65535, length 0
00:51:31.686797 IP 10.0.2.15.50430 > 142.250.193.132.443: Flags [P.], seq 925639768:925639807, ack 2756823, win 62780, l
```

There are three packets send in bursts.

For the first burst the inter packet time difference between the consecutive packets as follows

Between 1 and 2: 0.000030 seconds

Between 2 and 3: 0.000053 seconds.

The time elapsed between first request and its response is 0.095847 seconds.