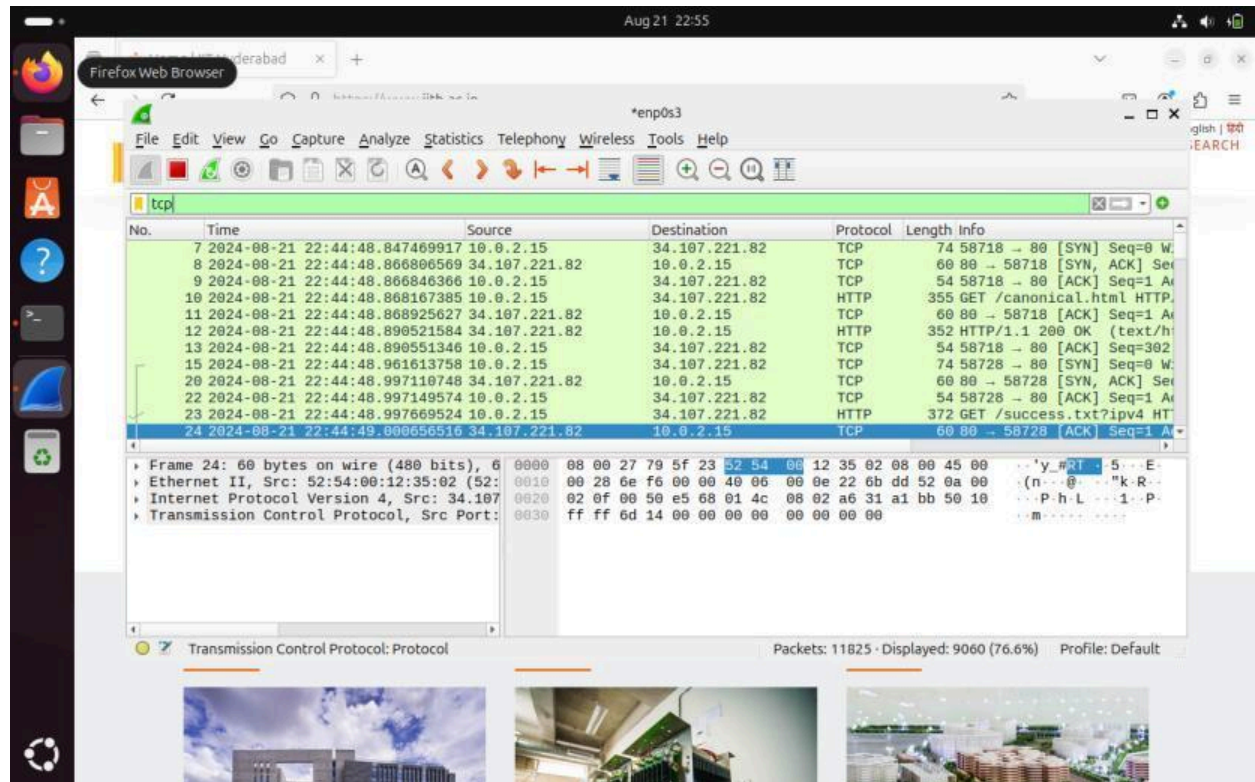


Roll No- CS24MTECH14006

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 .

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows a GET request (packet 10) and a 200 OK response (packet 11). The packet details pane for packet 11 shows the HTTP response structure, including the status bar '200 OK'.

No.	Time	Source	Destination	Protocol	Length	Info
10	22:44:48.868167385	10.0.2.15	34.107.221.82	HTTP	355	GET /canonical.html HTTP/1.1
11	22:44:48.868925627	34.107.221.82	10.0.2.15	TCP	60	80 → 58718 [ACK] Seq=1 Ack=302 Win=65535 Len=0
12	22:44:48.890521584	34.107.221.82	10.0.2.15	HTTP	352	HTTP/1.1 200 OK (text/html)

Packet 11 details:

- Frame 10: 355 bytes on wire (2840 bits), 355 captured (PCAPSession: 79:5f:23) (08:00:00:00:00:00) → 10.0.2.15:80
- Ethernet II, Src: PCSSystemtec_79:5f:23 (08:00:00:00:00:00), Dst: 10.0.2.15
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
- Transmission Control Protocol, Src Port: 58718, Dst Port: 80
- Hypertext Transfer Protocol
 - GET /canonical.html HTTP/1.1
 - Host: detectportal.firefox.com
 - User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
 - Accept: */* Accept-Language: en

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows a GET request (packet 10) and a 200 OK response (packet 11). The packet details pane for packet 11 shows the structure of the HTTP response, including the status bar '200 OK'.

No.	Time	Source	Destination	Protocol	Length	Info
10	22:44:48.868167385	10.0.2.15	34.107.221.82	HTTP	355	GET /canonical.html HTTP/1.1
11	22:44:48.868925627	34.107.221.82	10.0.2.15	TCP	60	60 → 58718 [ACK] Seq=1 Ack=302 Win=65535 Len=0
12	22:44:48.890521584	34.107.221.82	10.0.2.15	HTTP	352	HTTP/1.1 200 OK (text/html)

The packet details pane for packet 11 shows the structure of the HTTP response:

- Frame 10: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface eth0
- Ethernet II, Src: PCSSystemtec_79:5f:23 (08:00:27:9f:5f:23), Dst: VirtualBox__enp0s3 (08:00:27:9f:5f:23)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
- Transmission Control Protocol, Src Port: 58718, Dst Port: 80
- Hypertext Transfer Protocol
 - GET /canonical.html HTTP/1.1
 - Host: 10.0.2.15
 - User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
 - Accept: */* Accept-Encoding: gzip, deflate, br

Solution 3)

The screenshot shows a web browser window with the address bar displaying `https://gaia.cs.umass.edu`. The page content features the CNRG logo and navigation links: People, Research, Publications, Collaborations, Search, Education, and Resources. Below the logo, a paragraph describes the group's research focus.

The developer tools are open, showing the Network tab with a list of requests. The selected request is a GET request for `qumember.gif` from `www.scalable-networks.com`. The request details show the status as 200, the type as image, and the size as 36.9 KB. The response headers indicate the scheme is https, the host is `gaia.cs.umass.edu`, and the filename is `/`.

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list shows a GET request for `/favicon.ico` from `10.0.2.15` to `34.223.124.45`. The packet details pane shows the Hypertext Transfer Protocol section, and the packet bytes pane shows the raw data of the request.

The packet list shows the following details:

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

The packet details pane shows the following details for the selected packet:

- Frame 676: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits) on interface `eth0`
- Ethernet II, Src: PCSysmtec_79:5f:23 (08:00:07:79:5f:23), Dst: Realtek_88:6b:45:43:00:00 (08:00:00:08:00:00:00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.223.124.45
- Transmission Control Protocol, Src Port: 5623, Dst Port: 80
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the request, including the HTTP method, version, and headers.

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)

The image shows a Wireshark packet capture interface. The top pane displays a list of network packets. Packet 11 is highlighted, showing an HTTP GET request from source 10.0.2.15 to destination 34.197.221.82. The bottom pane shows the expanded details of this packet, including the Hypertext Transfer Protocol section with the following information:

- Host: detectportal.firefox.com
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
- Accept: */*
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Cache-Control: no-cache
- Pragma: no-cache
- Connection: keep-alive
- Full request URI: http://detectportal.firefox.com/canonical.html

The packet list pane shows the following details for packet 11:

No.	Time	Source	Destination	Protocol	Length	Info
11	18:42:37.0001920.15	10.0.2.15	34.197.221.82	HTTP	391	GET /canonical.html HTTP/1.1

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 image shows a Wireshark network traffic capture. The main packet list pane displays a series of packets. Packet 11 is highlighted, showing an HTTP GET request to 34.107.221.82 on port 80. The packet details pane for packet 11 shows the following information:

- [Header checksum status: Unverified]
- Source Address: 10.0.2.15
- Destination Address: 34.107.221.82
- Transmission Control Protocol, Src Port: 50484, Dst Port: 80, Seq: 1, Ack: 1, Len: 301
- Source Port: 50484
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 301]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 3426643694
- [Next Sequence Number: 302 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 78208902
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]

The packet bytes pane shows the raw data of the packet, starting with 0020 dd 52 c5 34 00 50 cc 3e 6e ee 04 a9 8a 0030 fa f0 0d 14 00 00 47 45 54 20 2f 63 6e 0040 69 63 61 6c 2e 68 74 6d 6c 20 48 54 55 0050 2e 31 0d 0a 48 6f 73 74 3a 20 64 65 77 0060 70 6f 72 74 61 6c 2e 66 69 72 65 66 6e 0070 6f 6d 00 0a 55 73 65 72 2d 41 67 65 6e 0080 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 26 0090 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 00a0 78 38 36 5f 36 34 3b 20 72 76 3a 31 33 00b0 29 20 47 65 63 6b 6f 2f 32 30 31 30 33 00c0 20 46 69 72 65 66 6f 78 2f 31 32 39 22 00d0 41 63 63 65 70 74 3a 29 2a 2f 2a 0d 6e 00e0 65 70 74 2d 4c 61 6e 67 75 61 67 65 63 00f0 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 6e 0100 63 65 70 74 2d 45 6e 63 6f 64 69 6e 6e 0110 7a 69 70 2c 20 64 65 66 6e 61 74 65 6e 0120 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 2e 0130 63 61 63 68 65 0d 0a 50 72 61 67 6d 6e

At the bottom of the Wireshark window, it shows "Packets: 18319 · Displayed: 12164 (66.4%) Profile: Default".

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)

The image shows a Wireshark packet capture window titled "wireshark_enp0s342PT52.pcapng" with the filter "http.get_ok". The interface includes a packet list on the left, a packet details pane in the middle, and a packet bytes pane on the right. The top status bar shows the date and time as "Aug 25 16:33".

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
13	18.42:37.823805166	34.107.221.82	10.0.2.15	HTTP	352	HTTP/1.1 200 OK (text/html)

Packet Details:

- Frame 13: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface enp0s3, id 0
- Ethernet II, Src: PC03systeme_78:5f:23 (08:00:27:79:5f:23), Dst: 10.0.2.15
- Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.0.2.15
- TCP, Src Port: 80, Dst Port: 50484, Seq: 1, Ack: 298, Len: 298
- HTTP, Method: GET, URI: http://detectportal.firefox.com/canonical.html

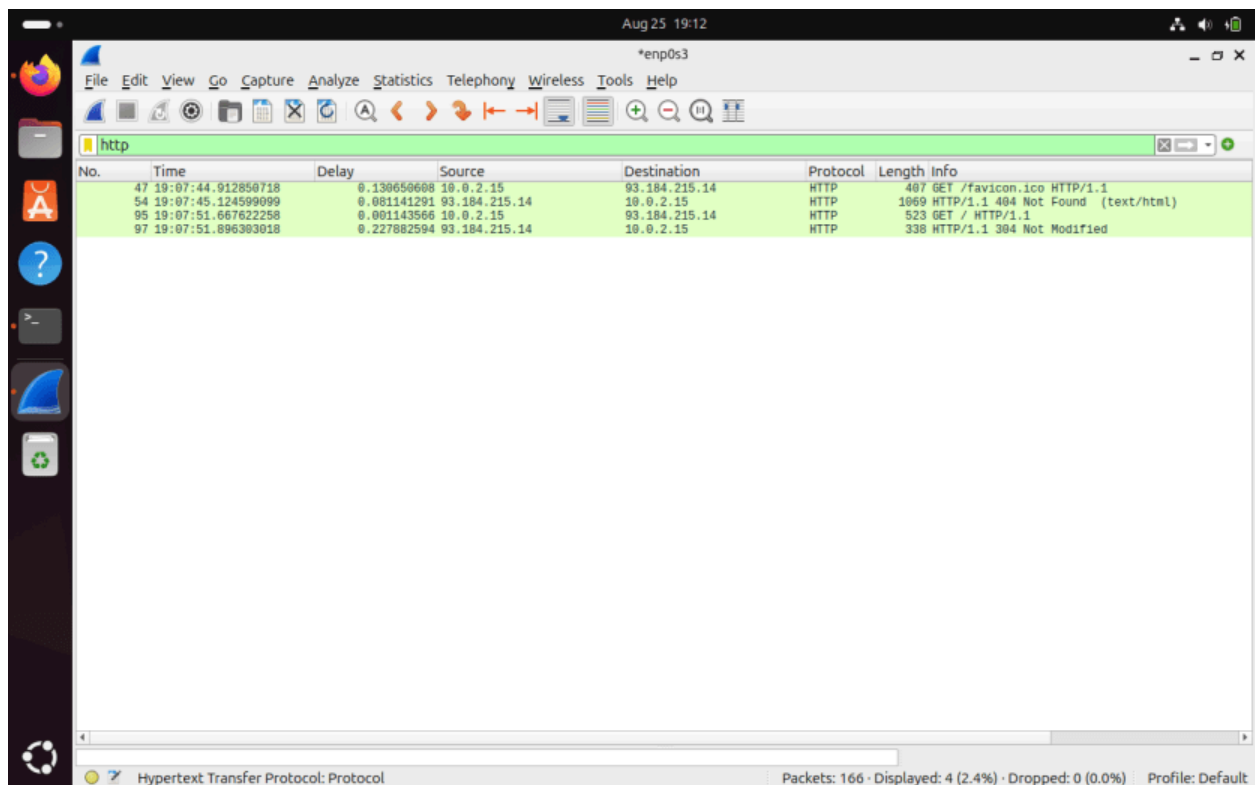
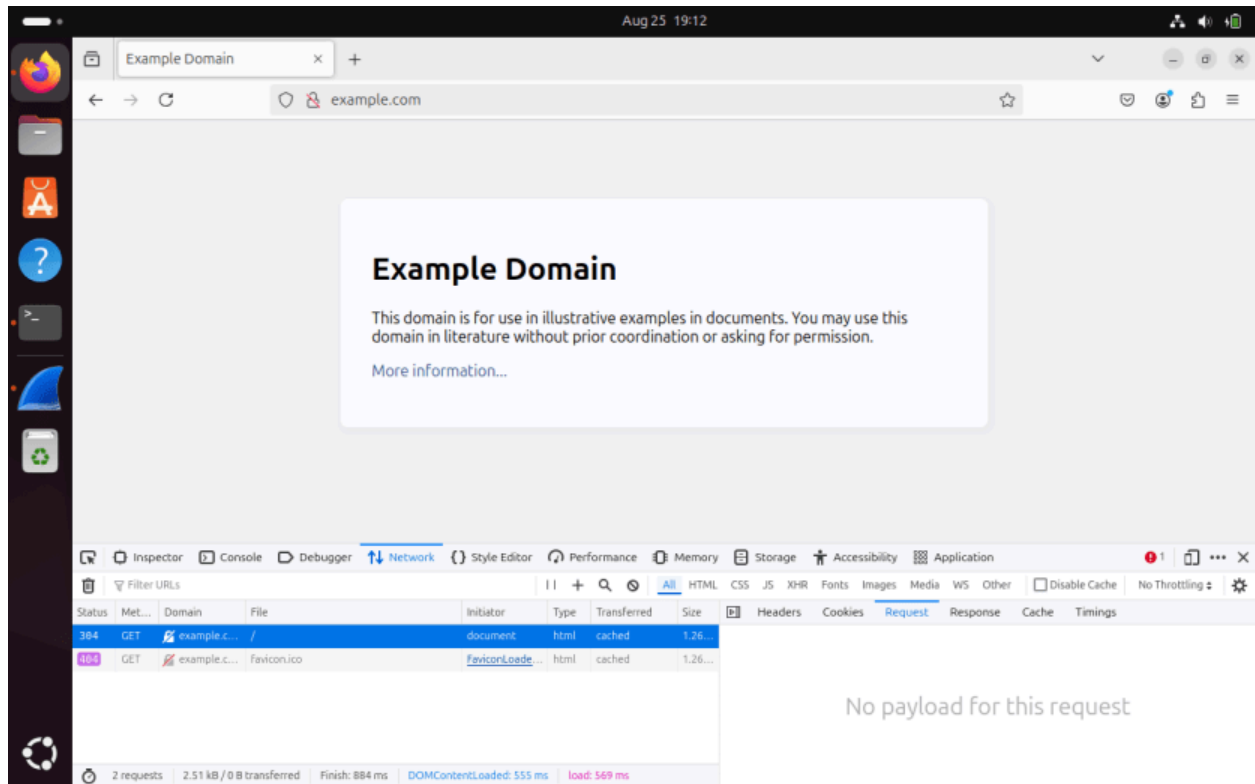
Packet Bytes:

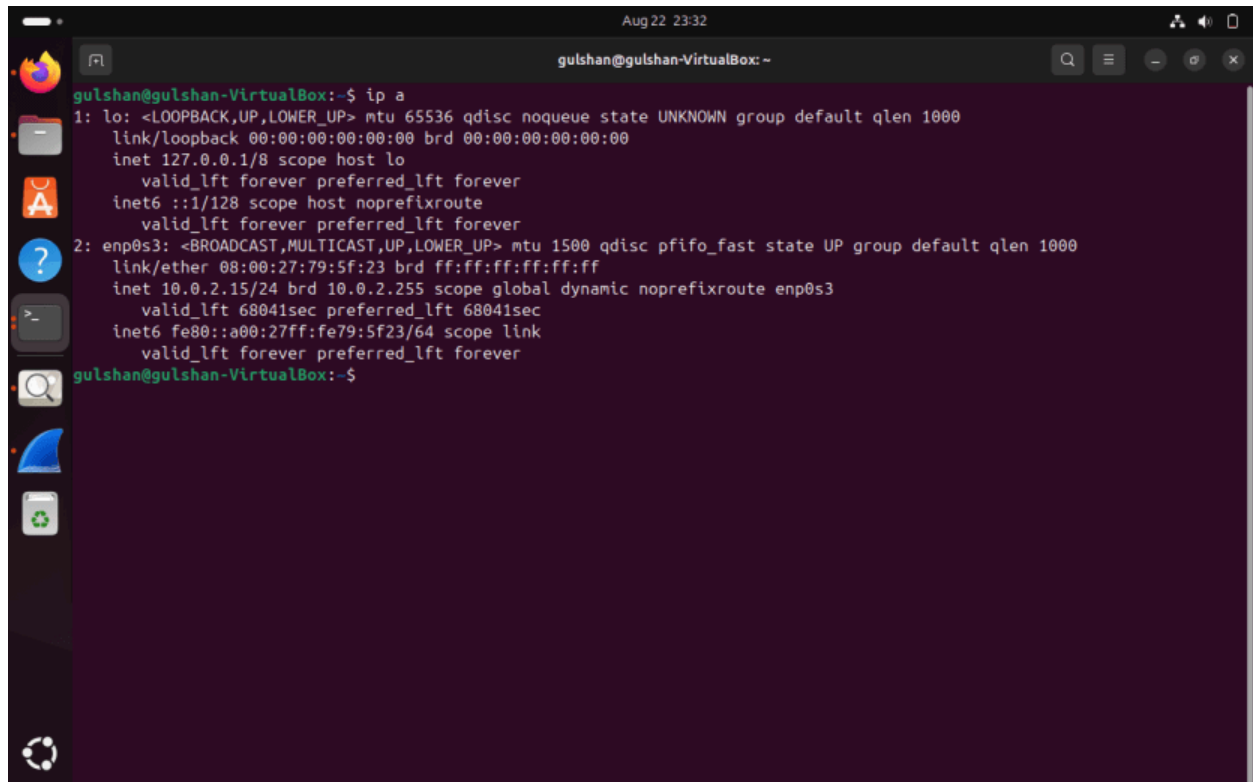
```
Source Port: 80
Destination Port: 50484
[Stream index: 0]
[Conversation completeness: Complete, WITH DATA (31)]
[TCP Segment Len: 298]
Sequence Number: 1 (relative sequence number)
[Next Sequence Number: 299 (relative sequence number)]
Acknowledgment Number: 302 (relative ack number)
[ACK Number: 302 (relative ack number)]
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
[Time stamps]
[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: 79753\r\n
Content-Type: text/html\r\n
Cache-Control: public,max-age=0,s-maxage=3600\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.823805166 seconds]
[Request in frame: 11]
[Next request in frame: 1149]
[Next response in frame: 1151]
[Request URI: http://detectportal.firefox.com/canonical.html]
File Data: 90 bytes
Live-based text data: text/html (1 lines)
```



Solution 7)

7.1) For <http://example.com>





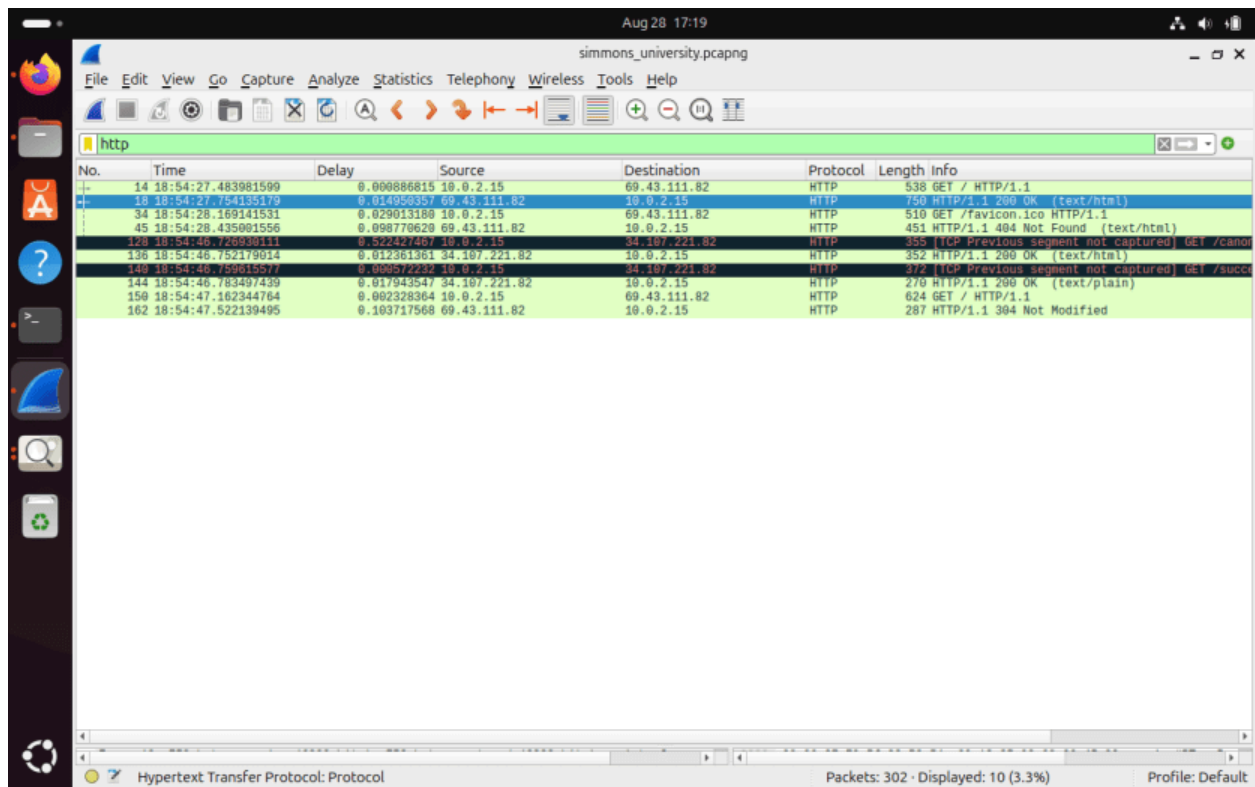
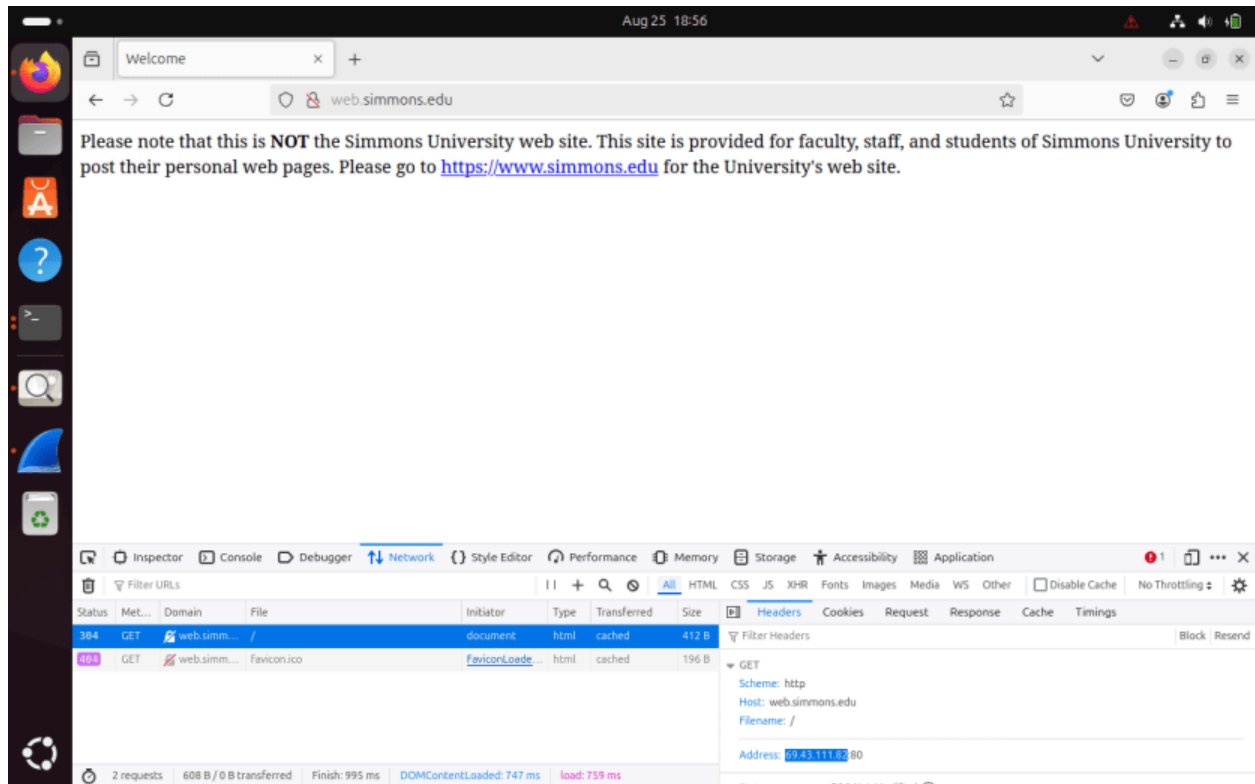
```
Aug 22 23:32
gulshan@gulshan-VirtualBox: ~
gulshan@gulshan-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:79:5f:23 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 68041sec preferred_lft 68041sec
   inet6 fe80::a00:27ff:fe79:5f23/64 scope link
       valid_lft forever preferred_lft forever
gulshan@gulshan-VirtualBox:~$
```

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>

The screenshot shows a web browser displaying the NAAC (National Assessment and Accreditation Council) website. The browser's address bar shows the URL naac.gov.in/index.php/en/. The website header includes a language selector, accessibility options (A, A+, Screen Reader), a login button, and quick links. The main content area features the NAAC logo, its name in English and Hindi, and a large group photo of staff members. Below the website content, the browser's developer tools are open, showing the Network tab. The network log displays several requests, including a GET request for the main document (55.35 kB) and various JavaScript files (jQuery, custom.js, popper.min.js). The right-hand pane of the developer tools shows the 'Headers' tab for the selected document, displaying the 'GET' method, 'http' scheme, 'naac.gov.in' host, and '/index.php/en/' filename. The address bar also shows the IP address 164.100.228.235:80.

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
200	GET	naac.gov.in	/index.php/en/	document	html	55.35 kB	264...
200	POST	translate...	log?hasfast=true&authuser=0&format=json	mvel_main?...	plain	615 B	0 B
200	GET	naac.gov.in	caption.js?070f6215ab446db3422e741c64;	script	js	678 B	491 B
200	GET	naac.gov.in	jquery-3.3.1.min.js	script	js	30.65 kB	86.9...
200	GET	naac.gov.in	custom.js	script	js	1.24 kB	3.12...
200	GET	naac.gov.in	popper.min.js	script	html	489 B	273 B

80 requests 5.62 MB / 2.46 MB transferred Finish: 13.62 s DOMContentLoaded: 1.79 s load: 10.43 s

No.	Time	Delay	Source	Destination	Protocol	Length	Info
13	19:00:42.806755603	0.001279867	10.0.2.15	164.100.228.235	HTTP	439	GET / HTTP/1.1
17	19:00:42.809488896	0.075386114	164.100.228.235	10.0.2.15	HTTP	654	HTTP/1.1 301 Moved Permanently
19	19:00:43.019622390	0.004523338	10.0.2.15	164.100.228.235	HTTP	521	GET /index.php?cn=/http/1.1
47	19:00:43.219622390	0.004523338	164.100.228.235	10.0.2.15	HTTP	2853	HTTP/1.1 200 OK (text/html)
52	19:00:43.442779286	0.015740999	10.0.2.15	164.100.228.235	HTTP	471	GET /media/system/js/caption.js?070f6f
54	19:00:43.468928246	0.023417271	10.0.2.15	164.100.228.235	HTTP	434	GET /templates/naac/js/jquery-3.3.1.mi
60	19:00:43.510219638	0.004039904	164.100.228.235	10.0.2.15	HTTP	732	HTTP/1.1 200 OK (text/javascript)
62	19:00:43.514062842	0.003723473	10.0.2.15	164.100.228.235	HTTP	456	GET /administrator/chatbot/fab.css HTTP
81	19:00:43.537009354	0.004298036	10.0.2.15	164.100.228.235	HTTP	431	GET /templates/naac/js/bootstrap.min.js
85	19:00:43.538059806	0.000188878	10.0.2.15	164.100.228.235	HTTP	458	GET /administrator/chatbot/style.css H
91	19:00:43.541635593	0.001072666	10.0.2.15	164.100.228.235	HTTP	457	GET /administrator/chatbot/chat.css HT
96	19:00:43.556888681	0.002567846	10.0.2.15	164.100.228.235	HTTP	424	GET /templates/naac/js/custom.js HTTP:
100	19:00:43.575571573	0.007244420	164.100.228.235	10.0.2.15	HTTP	544	HTTP/1.1 200 OK (text/html)
105	19:00:43.581453765	0.000000276	164.100.228.235	10.0.2.15	HTTP	1426	HTTP/1.1 200 OK (text/css)
109	19:00:43.588768759	0.000749273	164.100.228.235	10.0.2.15	HTTP	7347	HTTP/1.1 200 OK (text/javascript)
111	19:00:43.589863322	0.001085351	10.0.2.15	164.100.228.235	HTTP	428	GET /templates/naac/js/popper.min.js H
113	19:00:43.593112810	0.002277482	164.100.228.235	10.0.2.15	HTTP	2189	HTTP/1.1 200 OK (text/css)
115	19:00:43.594771129	0.000354399	10.0.2.15	164.100.228.235	HTTP	459	GET /administrator/chatbot/social.css i
119	19:00:43.596299013	0.000159895	10.0.2.15	164.100.228.235	HTTP	466	GET /templates/naac/css/font-awesome.m
132	19:00:43.609166153	0.004893748	164.100.228.235	10.0.2.15	HTTP	1297	HTTP/1.1 200 OK (text/javascript)
134	19:00:43.626439575	0.017223635	164.100.228.235	10.0.2.15	HTTP	543	HTTP/1.1 404 Not Found (text/html)
146	19:00:43.649073140	0.001063926	164.100.228.235	10.0.2.15	HTTP	3346	HTTP/1.1 200 OK (text/css)
148	19:00:43.653122227	0.006228544	164.100.228.235	10.0.2.15	HTTP	543	HTTP/1.1 404 Not Found (text/html)
157	19:00:43.662470125	0.001735725	164.100.228.235	10.0.2.15	HTTP	834	HTTP/1.1 200 OK (text/css)
164	19:00:43.668622227	0.000000000	10.0.2.15	142.250.183.227	OCSP	454	HTTP/1.1 200 OK (text/css)
168	19:00:43.751689582	0.001801527	10.0.2.15	142.250.183.227	OCSP	489	Request
168	19:00:43.834075166	0.036863248	142.250.183.227	10.0.2.15	OCSP	755	Response
174	19:00:43.849467714	0.002945058	142.250.183.227	10.0.2.15	OCSP	755	Response
214	19:00:43.977181288	0.000587712	10.0.2.15	164.100.228.235	HTTP	466	GET /templates/naac/css/font-awesome.m
225	19:00:44.026585543	0.028038445	164.100.228.235	10.0.2.15	HTTP	543	HTTP/1.1 404 Not Found (text/html)
227	19:00:44.027819639	0.000400447	10.0.2.15	164.100.228.235	HTTP	513	GET /images/button.Accred.Results.png
228	19:00:44.027568857	0.000558218	10.0.2.15	164.100.228.235	HTTP	507	GET /images/button_assessor.png HTTP/1
229	19:00:44.027954146	0.000385289	10.0.2.15	164.100.228.235	HTTP	510	GET /images/docs/Binary/FAQNew.png HT
230	19:00:44.028318338	0.000364192	10.0.2.15	164.100.228.235	HTTP	511	GET /templates/naac/images/logo.png HT
235	19:00:44.029747110	0.000259590	10.0.2.15	164.100.228.235	HTTP	513	GET /images/ministry_of_education.png
236	19:00:44.030352642	0.000605532	10.0.2.15	184.18.23.19	HTTP	418	GET /Icons/valid-css-blue HTTP/1.1
239	19:00:44.031869647	0.006821549	10.0.2.15	184.18.23.19	HTTP	422	GET /Icons/valid-xhtml10-blue HTTP/1.1
240	19:00:44.032254072	0.000304425	10.0.2.15	164.100.228.235	HTTP	506	GET /images/inflibnet-logo.png HTTP/1.
254	19:00:44.970806419	0.001073968	184.18.23.19	10.0.2.15	HTTP	827	HTTP/1.1 301 Moved Permanently (text/
264	19:00:44.981225527	0.001978197	184.18.23.19	10.0.2.15	HTTP	831	HTTP/1.1 301 Moved Permanently (text/

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.

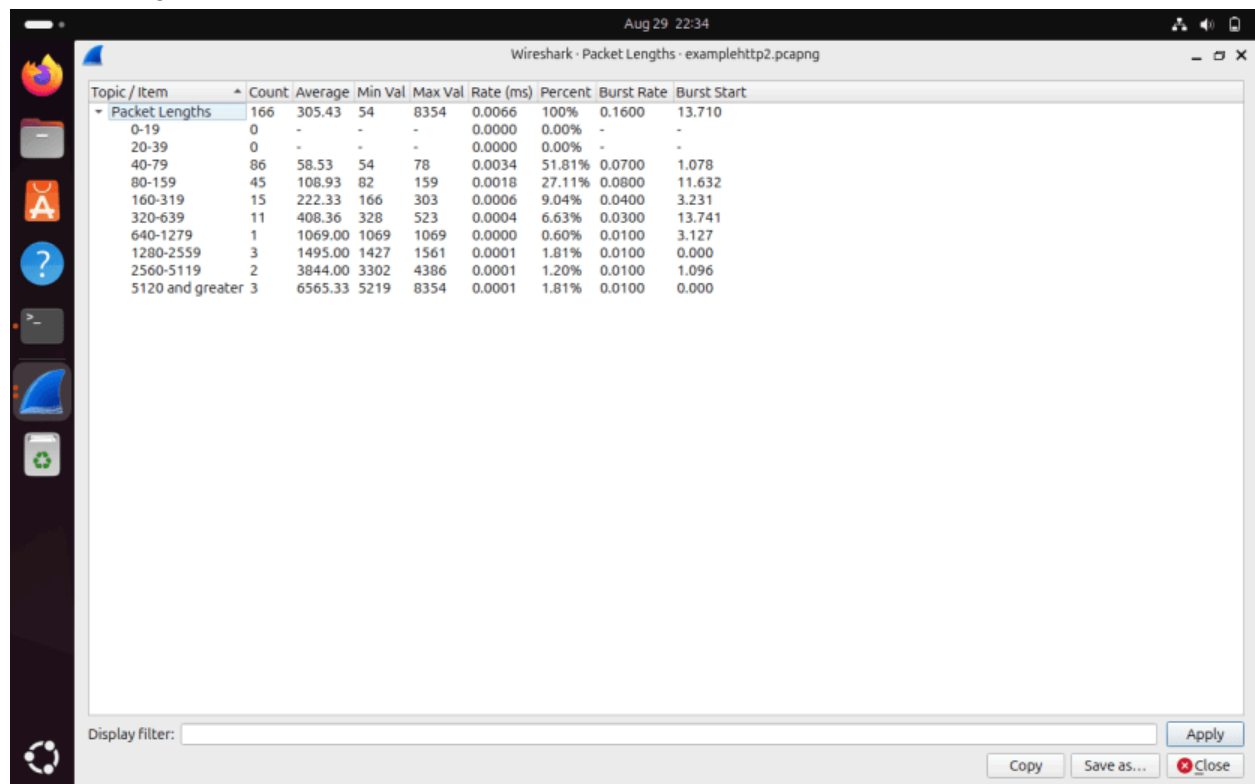
4) <http://naac.gov.in>

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:



Total Packets - 166

Average packet length- 305.43 bytes

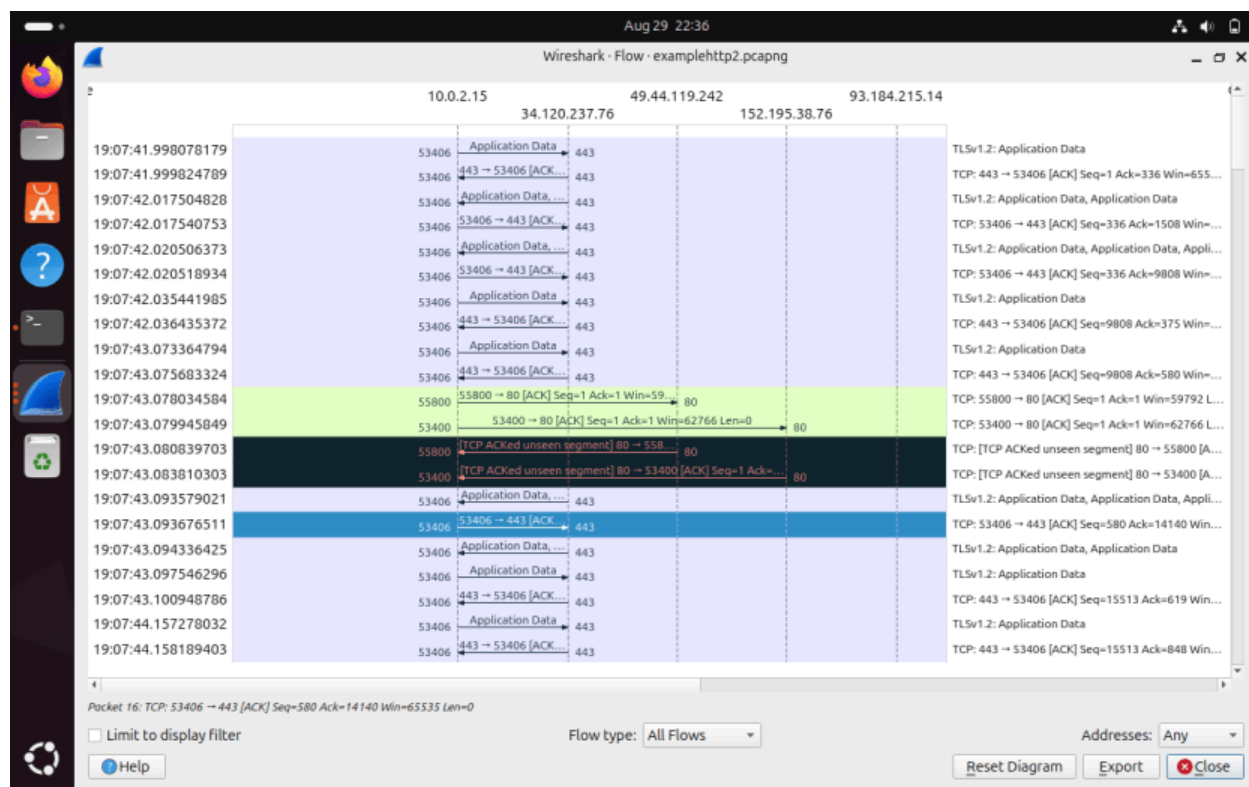
Minimum packet length-54 bytes

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



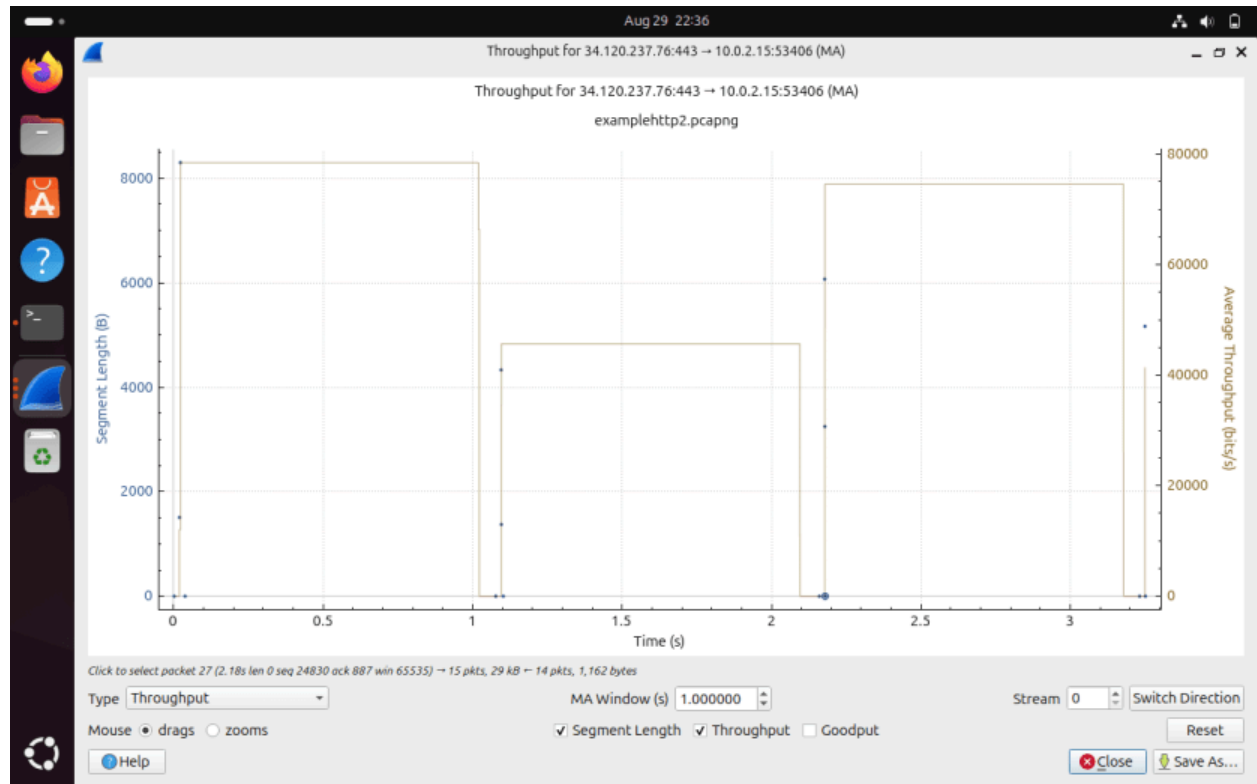
The communication between multiple IP addresses 10.0.2.15, 49.44.119.242, 93.184.215.14, 34.120.237.76, 152.195.38.76 is shown in the flow graph.

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

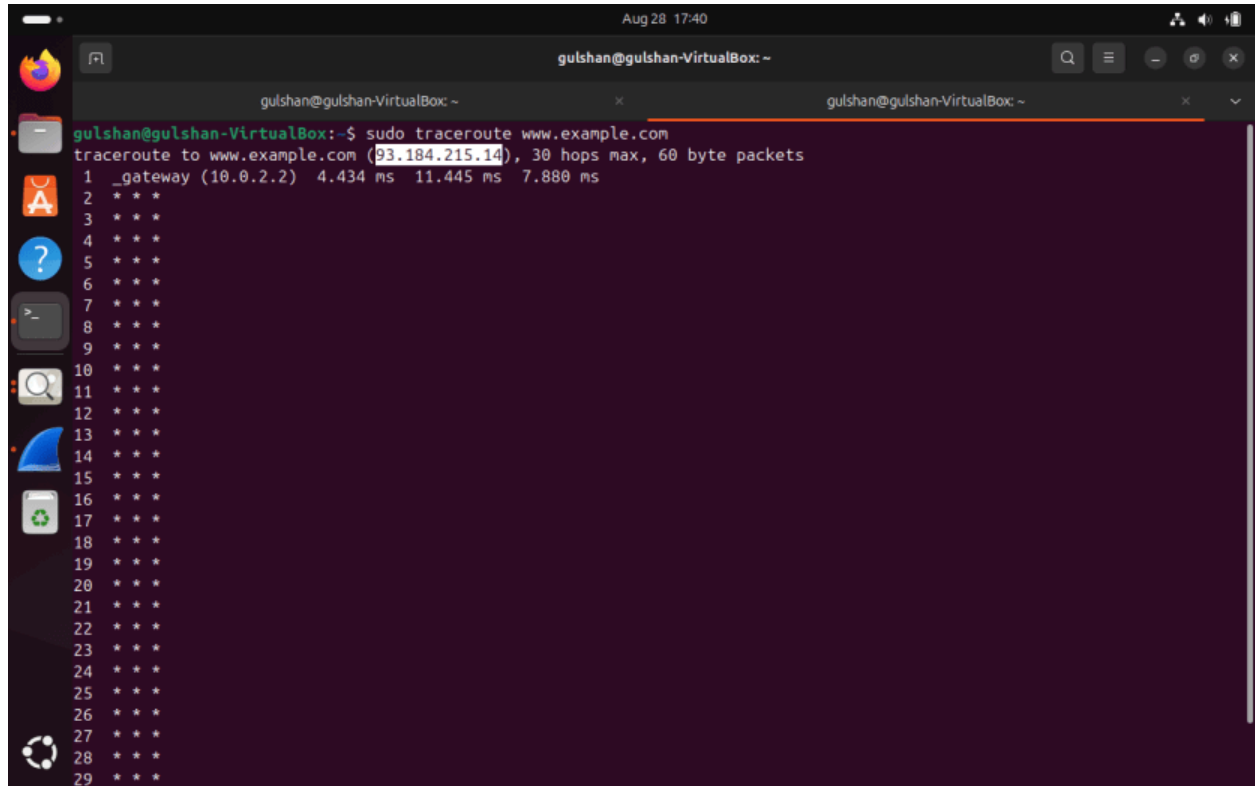


For large data transfer the burst of high throughput is observed from the graph. Throughput gets fluctuated, which could be due to network congestion. The overall measure of the data transfer rate is the average throughput.

Part B) Analyze packet trace of traceroute session

Task 1)

Solution 1)



The screenshot shows a terminal window titled "gulshan@gulshan-VirtualBox: ~" with a dark background. The user has executed the command `sudo traceroute www.example.com`. The output shows the traceroute path to `www.example.com` (IP `93.184.215.14`), indicating 30 hops max and 60 byte packets. The first hop is the gateway at `10.0.2.2` with round-trip times of 4.434 ms, 11.445 ms, and 7.880 ms. Subsequent hops (2 through 29) are marked with three asterisks (***) indicating timeouts.

```
gulshan@gulshan-VirtualBox:~$ sudo traceroute www.example.com
traceroute to www.example.com (93.184.215.14), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  4.434 ms  11.445 ms  7.880 ms
 2  ***
 3  ***
 4  ***
 5  ***
 6  ***
 7  ***
 8  ***
 9  ***
10  ***
11  ***
12  ***
13  ***
14  ***
15  ***
16  ***
17  ***
18  ***
19  ***
20  ***
21  ***
22  ***
23  ***
24  ***
25  ***
26  ***
27  ***
28  ***
29  ***
```

Aug 28 17:40

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

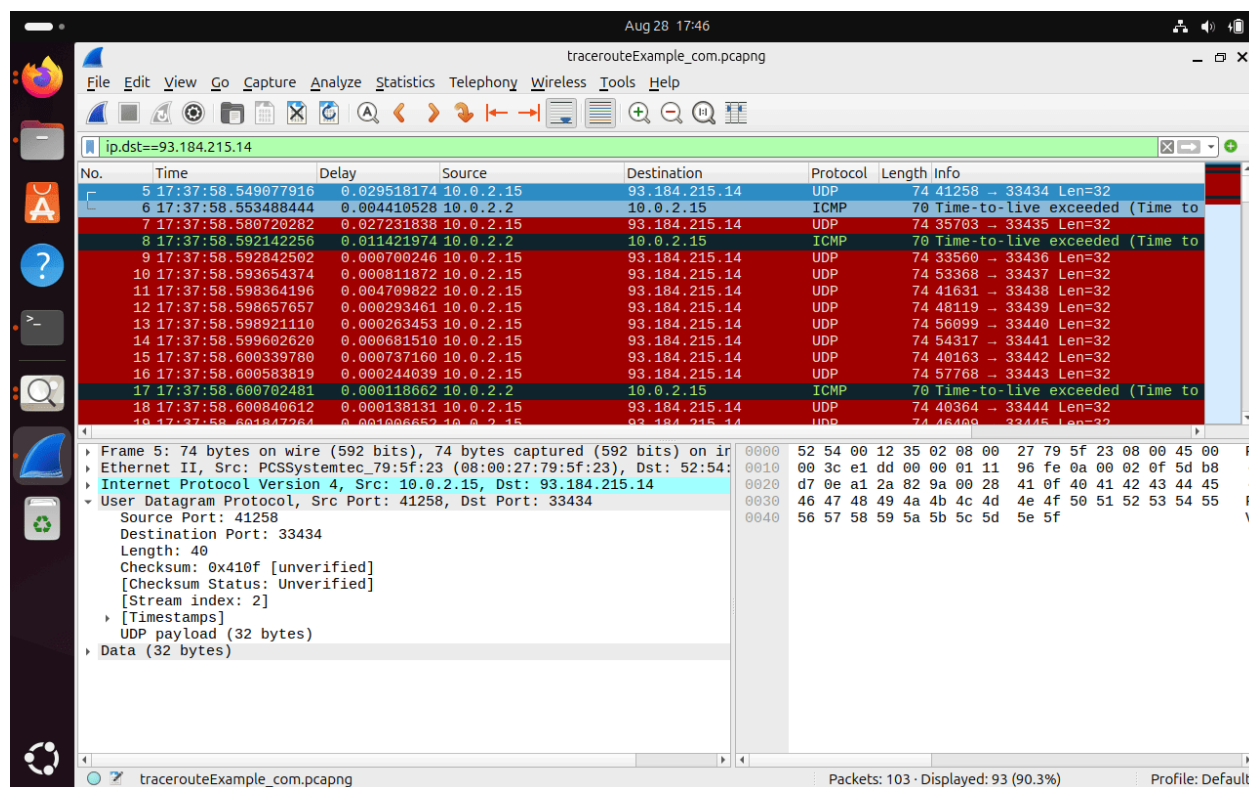
ip.src==10.0.2.15 && ip.dst==93.184.215.14

No.	Time	Delay	Source	Destination	Protocol	Length	Info
5	17:37:58.549077916	0.029518174	10.0.2.15	93.184.215.14	UDP	74	41258 - 33434 Len=32
6	17:37:58.553488444	0.004410528	10.0.2.15	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live ex
7	17:37:58.589729282	0.027221839	10.0.2.15	93.184.215.14	UDP	74	35769 - 33455 Len=32
8	17:37:58.592142265	0.011421974	10.0.2.15	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live ex
9	17:37:58.592842582	0.000789248	10.0.2.15	93.184.215.14	UDP	74	33568 - 33436 Len=32
10	17:37:58.593654374	0.000811872	10.0.2.15	93.184.215.14	UDP	74	53368 - 33437 Len=32
11	17:37:58.598364196	0.004789822	10.0.2.15	93.184.215.14	UDP	74	41631 - 33438 Len=32
12	17:37:58.598657657	0.000293461	10.0.2.15	93.184.215.14	UDP	74	48119 - 33439 Len=32
13	17:37:58.598921110	0.000203453	10.0.2.15	93.184.215.14	UDP	74	56999 - 33440 Len=32
14	17:37:58.599682626	0.000681519	10.0.2.15	93.184.215.14	UDP	74	54317 - 33441 Len=32
15	17:37:58.600397780	0.000737168	10.0.2.15	93.184.215.14	UDP	74	49163 - 33442 Len=32
16	17:37:58.600583819	0.000244839	10.0.2.15	93.184.215.14	UDP	74	57768 - 33443 Len=32
17	17:37:58.600782481	0.000118662	10.0.2.15	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live ex
18	17:37:58.600840612	0.000138131	10.0.2.15	93.184.215.14	UDP	74	40364 - 33444 Len=32
19	17:37:58.601847264	0.001086652	10.0.2.15	93.184.215.14	UDP	74	46409 - 33445 Len=32
20	17:37:58.602619425	0.000772161	10.0.2.15	93.184.215.14	UDP	74	57975 - 33446 Len=32
21	17:37:58.602856864	0.000227239	10.0.2.15	93.184.215.14	UDP	74	42494 - 33447 Len=32
22	17:37:58.603714567	0.000857982	10.0.2.15	93.184.215.14	UDP	74	34350 - 33448 Len=32
23	17:37:58.603985283	0.000270636	10.0.2.15	93.184.215.14	UDP	74	45951 - 33449 Len=32
26	17:37:58.603987514	0.043151528	10.0.2.15	93.184.215.14	UDP	74	56503 - 33450 Len=32
27	17:37:58.606084846	0.002177332	10.0.2.15	93.184.215.14	UDP	74	60385 - 33451 Len=32
28	17:37:58.606840863	0.000756017	10.0.2.15	93.184.215.14	UDP	74	47025 - 33452 Len=32
31	17:38:03.657464684	0.018361448	10.0.2.15	93.184.215.14	UDP	74	45325 - 33453 Len=32
32	17:38:03.662735051	0.005278447	10.0.2.15	93.184.215.14	UDP	74	50634 - 33454 Len=32
33	17:38:03.666313443	0.003578392	10.0.2.15	93.184.215.14	UDP	74	49672 - 33455 Len=32
34	17:38:03.666980761	0.000667318	10.0.2.15	93.184.215.14	UDP	74	36298 - 33456 Len=32
35	17:38:03.679316384	0.003335543	10.0.2.15	93.184.215.14	UDP	74	37415 - 33457 Len=32
36	17:38:03.672179685	0.001863391	10.0.2.15	93.184.215.14	UDP	74	58735 - 33458 Len=32
37	17:38:03.675544477	0.003364872	10.0.2.15	93.184.215.14	UDP	74	57576 - 33459 Len=32
38	17:38:03.677541029	0.001990552	10.0.2.15	93.184.215.14	UDP	74	33560 - 33460 Len=32
39	17:38:03.680525338	0.002984309	10.0.2.15	93.184.215.14	UDP	74	43798 - 33461 Len=32
40	17:38:03.681618587	0.001093249	10.0.2.15	93.184.215.14	UDP	74	50484 - 33462 Len=32
41	17:38:03.686456845	0.004838258	10.0.2.15	93.184.215.14	UDP	74	51439 - 33463 Len=32
42	17:38:03.688483369	0.002026524	10.0.2.15	93.184.215.14	UDP	74	43779 - 33464 Len=32
43	17:38:03.692617041	0.004133672	10.0.2.15	93.184.215.14	UDP	74	41283 - 33465 Len=32
44	17:38:03.700249261	0.007632220	10.0.2.15	93.184.215.14	UDP	74	34565 - 33466 Len=32
45	17:38:03.702825228	0.002575967	10.0.2.15	93.184.215.14	UDP	74	34799 - 33467 Len=32
46	17:38:03.704598531	0.001773393	10.0.2.15	93.184.215.14	UDP	74	57779 - 33468 Len=32
47	17:38:08.688296862	4.983698331	10.0.2.15	93.184.215.14	UDP	74	48238 - 33469 Len=32
48	17:38:08.688835341	0.000538479	10.0.2.15	93.184.215.14	UDP	74	50983 - 33470 Len=32

wireshark_enp0s3N9K352.pcapng

Packets: 103 · Displayed: 93 (90.3%) · Dropped: 0 (0.0%) Profile: Default

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.

- 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.
- 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.
- Length- Length is the total size of UDP packet (including both header and payload). Here the length is 40.
- 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.
- Timestamps- When the packet is captured that time is timestamp.
- 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:~$ 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

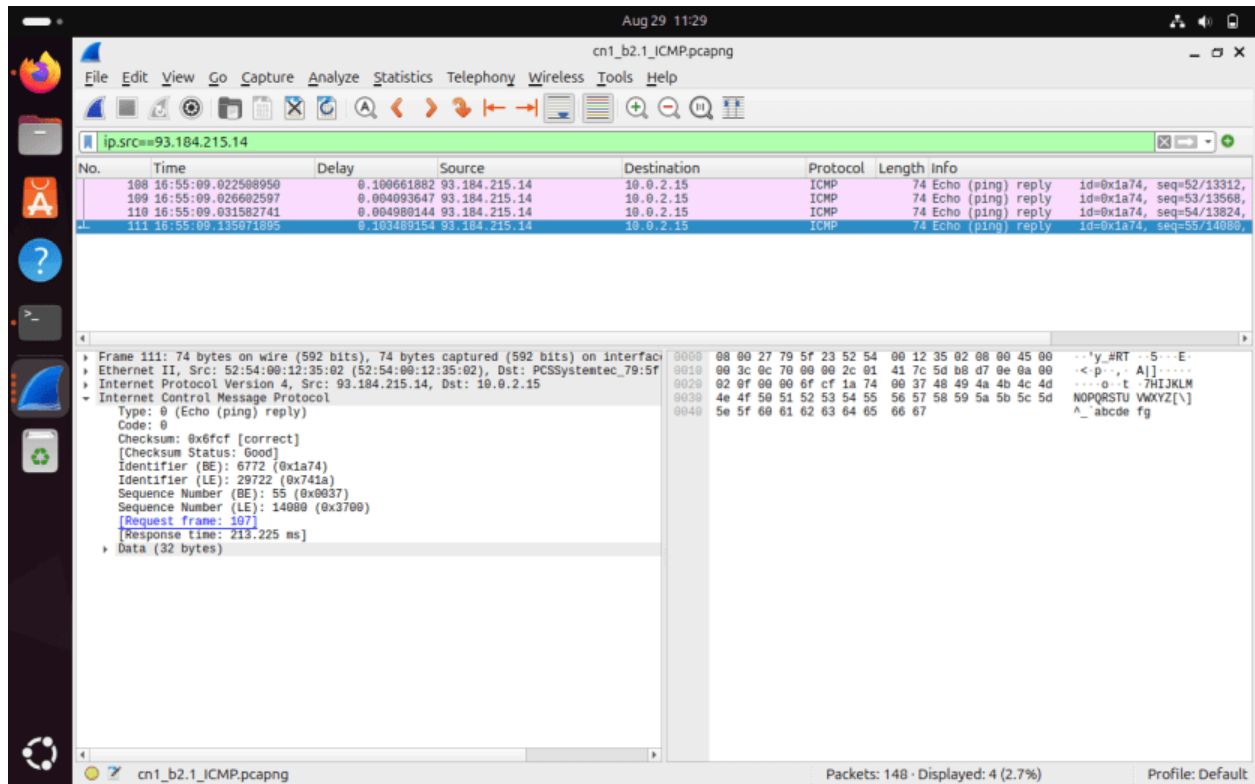
No.	Time	Source	Destination	Protocol	Length	Info
3	16:55:08.234106910	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a74, seq=1/256, ttl=1 (no response)
4	16:55:08.234433962	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a74, seq=2/512, ttl=1 (no response)
5	16:55:08.234510708	10.0.2.15	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 response)
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 response)
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 response)
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 response)
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 response)
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 response)
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 response)
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 response)
17	16:55:08.235093385	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a74, seq=12/3072, ttl=4 (no response)
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 response)
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 response)
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 response)
21	16:55:08.235929981	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a74, seq=16/4096, ttl=5 (no response)
22	16:55:08.237712241	192.168.0.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	16:55:08.237772071	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: PCSysntec_79:5f:23 (08:00:27:79:5f:23), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
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: 0x6005 [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)

wireshark_enp0s3211252.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	17:00:48.717995761	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	17:00:48.719840619	10.0.2.15	93.184.215.14	TCP	74	48423 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva
8	17:00:48.719815307	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	17:00:48.720739197	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	17:00:48.723138025	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	17:00:48.723579287	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
19	17:00:48.725398195	10.0.2.15	93.184.215.14	TCP	74	41205 → 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: PCSysNetec 79:5f:23 (08:00:27:79:5f:23), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)

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]

wireshark_enp0s34RCU52.pcapng

Packets: 84 · Displayed: 38 (45.2%)

Profile: Default

Aug 29 11:46

cn1_b2_TCP_pcapng

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
27	17:00:48.927848956	0.181705596	93.184.215.14	10.0.2.15	TCP	60	80 → 39215 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
29	17:00:48.939890275	0.000981826	93.184.215.14	10.0.2.15	TCP	60	80 → 37227 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
30	17:00:48.939890604	0.000000329	93.184.215.14	10.0.2.15	TCP	60	80 → 40765 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
31	17:00:48.939890646	0.000000042	93.184.215.14	10.0.2.15	TCP	60	80 → 47563 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
32	17:00:48.939890772	0.000000126	93.184.215.14	10.0.2.15	TCP	60	80 → 37269 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
37	17:00:48.940784454	0.000659459	93.184.215.14	10.0.2.15	TCP	60	80 → 50119 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
39	17:00:48.941773215	0.000972846	93.184.215.14	10.0.2.15	TCP	60	80 → 41745 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
42	17:00:48.944324471	0.001521822	93.184.215.14	10.0.2.15	TCP	60	80 → 41385 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
43	17:00:48.944325016	0.000000545	93.184.215.14	10.0.2.15	TCP	60	80 → 34061 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
46	17:00:48.948226351	0.002740874	93.184.215.14	10.0.2.15	TCP	60	80 → 59633 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
47	17:00:48.948226568	0.000000217	93.184.215.14	10.0.2.15	TCP	60	80 → 44017 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
50	17:00:48.957441541	0.009097574	93.184.215.14	10.0.2.15	TCP	60	80 → 43381 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
51	17:00:48.957441708	0.000000167	93.184.215.14	10.0.2.15	TCP	60	80 → 55895 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
54	17:00:48.960865137	0.003337314	93.184.215.14	10.0.2.15	TCP	60	80 → 55901 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
55	17:00:48.960865256	0.000000119	93.184.215.14	10.0.2.15	TCP	60	80 → 59001 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
59	17:00:48.968703596	0.005861569	93.184.215.14	10.0.2.15	TCP	60	80 → 54433 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le

cn1_b2_TCP_pcapng

Packets: 84 · Displayed: 16 (19.0%)

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)

Aug 29 12:25
cn1_b2.1_ICMPPcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

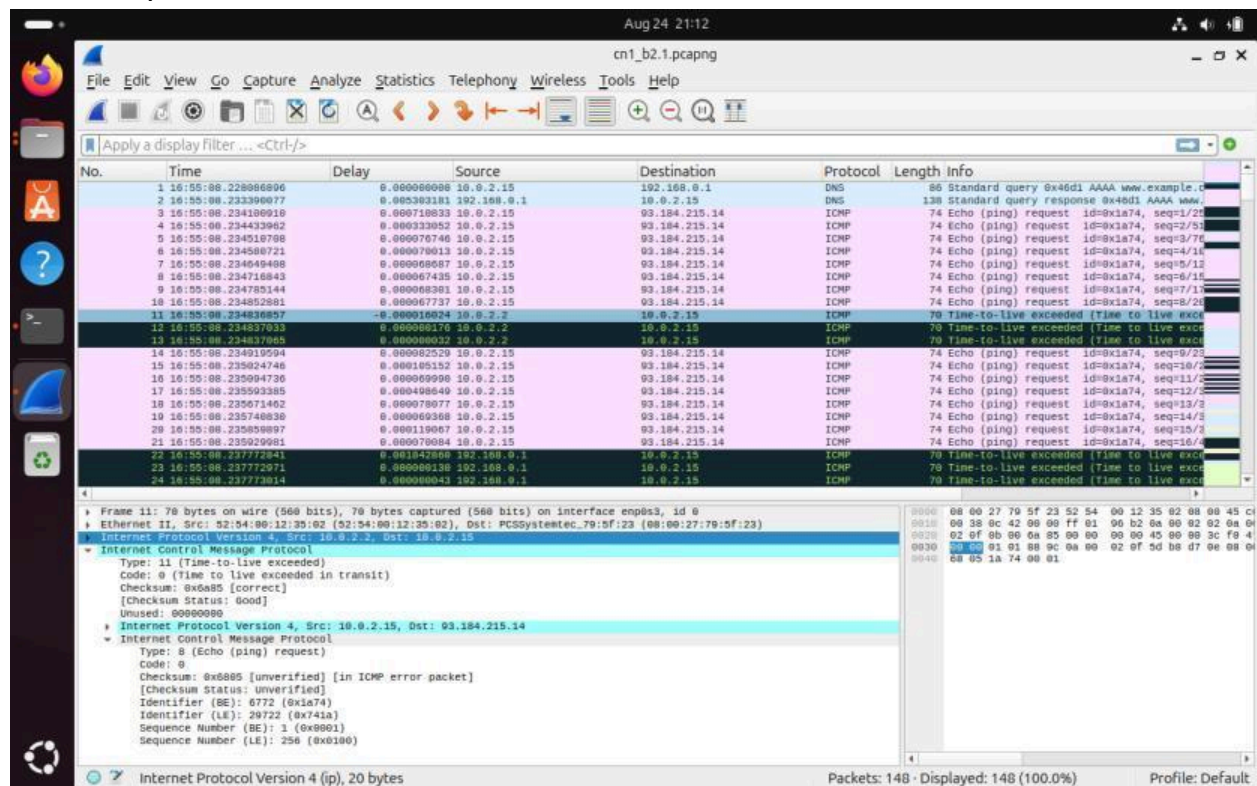
icmp

No.	Time	Delay	Source	Destination	Protocol	Length	Info
3	16:55:00.234100910	0.000718033	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=1/250, ttl=1 (no)
4	16:55:00.234433962	0.000333862	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=2/251, ttl=1 (no)
5	16:55:00.234810706	0.000670746	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=3/252, ttl=1 (no)
6	16:55:00.235100723	0.000660111	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=4/253, ttl=1 (no)
7	16:55:00.235494900	0.000660507	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=5/254, ttl=2 (no)
8	16:55:00.235718043	0.000667400	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=6/255, ttl=2 (no)
9	16:55:00.236102145	0.000652138	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=7/256, ttl=3 (no)
10	16:55:00.236521081	0.000667737	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=8/257, ttl=3 (no)
11	16:55:00.236937007	0.000664064	10.0.2.15	93.184.215.14	ICMP	74	Time-to-Live exceeded Time to live exceeded in trans
12	16:55:00.236937035	0.000661176	10.0.2.15	93.184.215.14	ICMP	74	Time-to-Live exceeded Time to live exceeded in trans
13	16:55:00.236937045	0.000660552	10.0.2.15	93.184.215.14	ICMP	74	Time-to-Live exceeded Time to live exceeded in trans
14	16:55:00.236937054	0.000663520	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=9/258, ttl=3 (no)
15	16:55:00.237321621	0.000663271	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=10/259, ttl=3 (no)
16	16:55:00.237694730	0.000660900	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=11/260, ttl=4 (no)
17	16:55:00.238093385	0.000660449	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=12/261, ttl=4 (no)
18	16:55:00.238518115	0.000660781	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=13/262, ttl=4 (no)
19	16:55:00.239140030	0.000660368	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=14/263, ttl=5 (no)
20	16:55:00.239595587	0.000661067	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=15/264, ttl=5 (no)
21	16:55:00.240020713	0.000660527	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=16/265, ttl=5 (no)
22	16:55:00.237772041	0.001842860	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
23	16:55:00.237772071	0.000660130	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
24	16:55:00.237772084	0.000660043	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
25	16:55:00.237772095	0.000660041	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
26	16:55:00.237772087	0.000660052	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
27	16:55:00.238083764	0.001203131	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
28	16:55:00.238083764	0.000660141	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
29	16:55:00.238101025	0.000660042	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
30	16:55:00.238101067	0.000660042	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
31	16:55:00.238101096	0.000660032	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
32	16:55:00.238101069	0.000660070	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
33	16:55:00.242683269	0.001460958	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=17/265, ttl=6 (no)
34	16:55:00.243000813	0.000725353	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=18/266, ttl=6 (no)
35	16:55:00.243180871	0.000662050	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=19/267, ttl=6 (no)
36	16:55:00.244705443	0.000667062	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
37	16:55:00.245001806	0.001126007	192.168.0.1	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
38	16:55:00.246032114	0.000801264	10.119.254.121	10.0.2.15	ICMP	78	Time-to-Live exceeded Time to live exceeded in trans
39	16:55:00.247237483	0.000554132	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=20/268, ttl=7 (no)
40	16:55:00.247690922	0.000580189	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=21/269, ttl=7 (no)
41	16:55:00.247774312	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=22/270, ttl=7 (no)
42	16:55:00.247774312	0.000513757	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=23/271, ttl=7 (no)
43	16:55:00.247903087	0.000590319	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=24/272, ttl=8 (no)
44	16:55:00.247903087	0.000590319	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=25/273, ttl=8 (no)
45	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=26/274, ttl=8 (no)
46	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=27/275, ttl=8 (no)
47	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=28/276, ttl=8 (no)
48	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=29/277, ttl=8 (no)
49	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=30/278, ttl=8 (no)
50	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=31/279, ttl=8 (no)
51	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=32/280, ttl=8 (no)
52	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=33/281, ttl=8 (no)
53	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=34/282, ttl=8 (no)
54	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=35/283, ttl=8 (no)
55	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=36/284, ttl=8 (no)
56	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=37/285, ttl=8 (no)
57	16:55:00.248042039	0.000599105	10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=38/286, ttl=8 (no)

Internet Control Message Protocol: Protocol Packets: 148 · Displayed: 95 (64.2%) · Selected: 10 (6.8%) Profile: Default

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

Solution 4)



- 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.
- 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.
- 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.

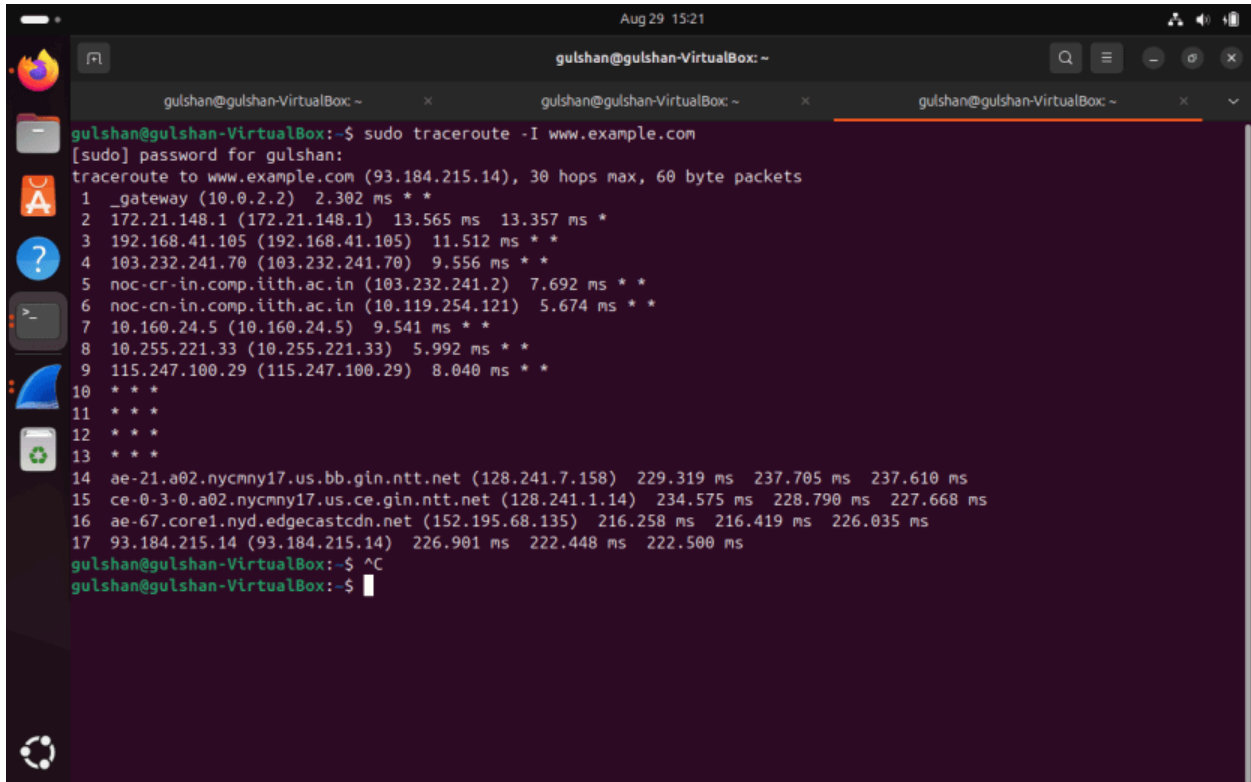
The TTL value at beginning is 1, later each subsequent probe send has TTL value incremented by 1.

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.



```
Aug 29 15:21
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)  2.302 ms  *  *
 2 172.21.148.1 (172.21.148.1)  13.565 ms  13.357 ms  *
 3 192.168.41.105 (192.168.41.105)  11.512 ms  *  *
 4 103.232.241.70 (103.232.241.70)  9.556 ms  *  *
 5 noc-cr-in.comp.iith.ac.in (103.232.241.2)  7.692 ms  *  *
 6 noc-cn-in.comp.iith.ac.in (10.119.254.121)  5.674 ms  *  *
 7 10.160.24.5 (10.160.24.5)  9.541 ms  *  *
 8 10.255.221.33 (10.255.221.33)  5.992 ms  *  *
 9 115.247.100.29 (115.247.100.29)  8.040 ms  *  *
10 *  *  *
11 *  *  *
12 *  *  *
13 *  *  *
14 ae-21.a02.nycmny17.us.bb.gin.ntt.net (128.241.7.158)  229.319 ms  237.705 ms  237.610 ms
15 ce-0-3-0.a02.nycmny17.us.ce.gin.ntt.net (128.241.1.14)  234.575 ms  228.790 ms  227.668 ms
16 ae-67.core1.nyd.edgecastcdn.net (152.195.68.135)  216.258 ms  216.419 ms  226.035 ms
17 93.184.215.14 (93.184.215.14)  226.901 ms  222.448 ms  222.500 ms
gulshan@gulshan-VirtualBox:~$ ^C
gulshan@gulshan-VirtualBox:~$
```

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
107	14:58:14.873905817	0.058888812	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=8x22d3, seq=40/12644, ttl=46 (request in 36)
108	14:58:14.682058261	0.000593184	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=8x22d3, seq=50/12806, ttl=46 (request in 36)
109	14:58:14.689312696	0.002254897	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=8x22d3, seq=61/13006, ttl=46 (request in 36)
170	14:58:14.843217239	0.157904512	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=8x22d3, seq=92/13312, ttl=46 (request in 36)

4

Frame 170: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 8

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)

Destination: PCSsystemtec_79:5f:23 (08:00:27:79:5f:23)

Source: 52:54:00:12:35:02 (52:54:00:12:35:02)

Type: IPv4 (8000)

Internet Protocol Version 4, Src: 93.184.215.14, Dst: 10.0.2.15

Internet Control Message Protocol

0000 08 00 27 79 5f 23 52 54 00 12 35 02 08 00 45 00 ..y..HT..S..E

0010 00 3c b1 7a 00 00 2e 01 9a 71 5d b8 d7 0e 0a 00 <.Z...q]....

0020 02 0f 00 00 07 73 23 03 00 34 48 49 4a 4b 4c 4d ..gs*..4H1KLM

0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\

0040 5e 5f 60 61 62 63 64 65 66 67 ^..abcde fg

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.

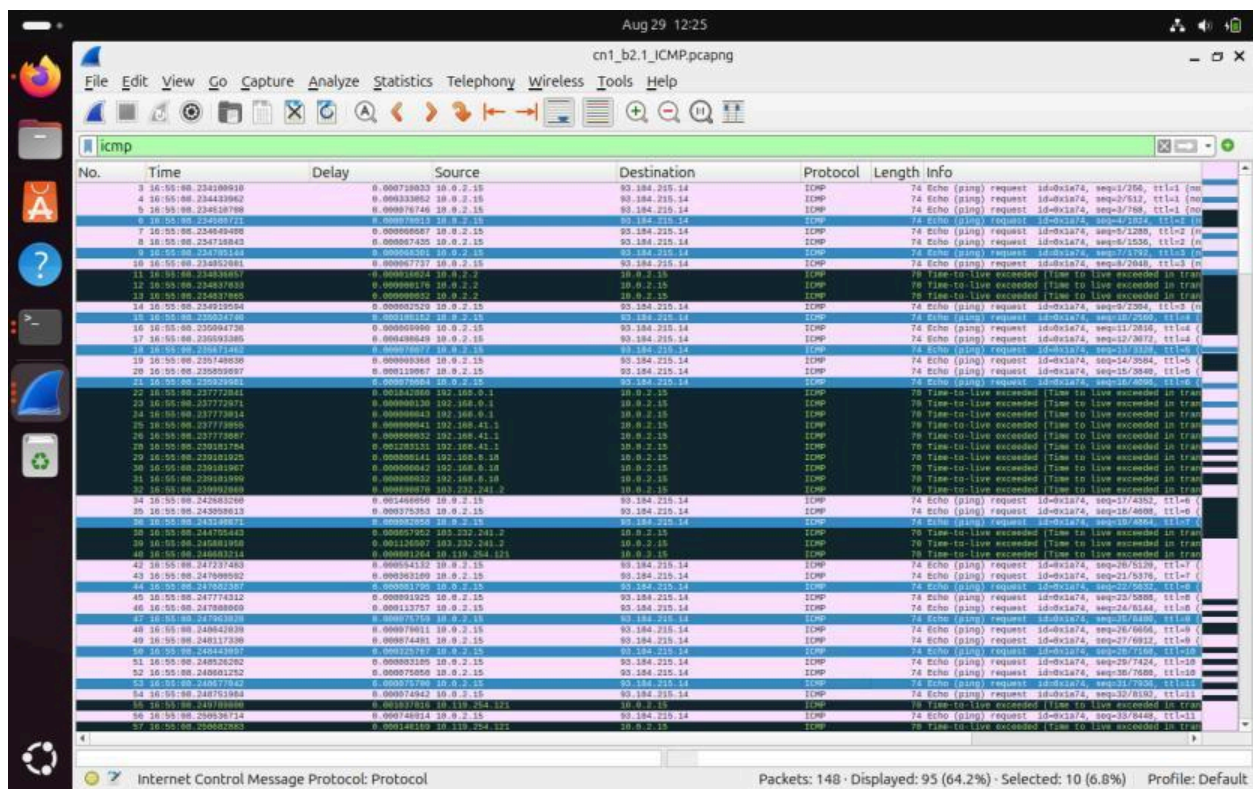
Congestion in network can delay responses is also the one of the reason.

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)



No.	Time	Delay	Source	Destination	Protocol	Length	Info
3	16:55:08.234108818	0.000718833	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=1/256, ttl=1 (m)
4	16:55:08.234433962	0.000333852	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=2/256, ttl=1 (m)
5	16:55:08.234518789	0.000076746	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=3/256, ttl=1 (m)
7	16:55:08.234648495	0.000066057	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=5/256, ttl=2 (m)
8	16:55:08.234718843	0.000067435	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=6/256, ttl=2 (m)
10	16:55:08.234852081	0.000077377	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=8/256, ttl=3 (m)
11	16:55:08.234838857	0.000018824	10.0.2.15	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
12	16:55:08.234877433	0.000001819	10.0.2.15	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
13	16:55:08.234837865	0.000000452	10.0.2.15	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
14	16:55:08.234919554	0.000007529	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=9/256, ttl=3 (m)
15	16:55:08.234937471	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=10/256, ttl=4 (m)
16	16:55:08.235004736	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=11/256, ttl=4 (m)
17	16:55:08.235033385	0.000488849	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=12/256, ttl=4 (m)
18	16:55:08.235118811	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=13/256, ttl=5 (m)
19	16:55:08.235148930	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=14/256, ttl=5 (m)
20	16:55:08.235059597	0.000110957	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=15/256, ttl=5 (m)
21	16:55:08.235070528	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=16/256, ttl=5 (m)
22	16:55:08.237772841	0.001420860	192.168.0.1	10.0.2.15	ICMP	74	Echo (ping) request id=0x1a7d, seq=17/256, ttl=5 (m)
23	16:55:08.237772871	0.000000130	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
24	16:55:08.237772914	0.000000043	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
25	16:55:08.237772956	0.000000041	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
26	16:55:08.237773067	0.000000032	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
28	16:55:08.236181794	0.001269131	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
29	16:55:08.236181825	0.000000141	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
30	16:55:08.236181867	0.000000042	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
31	16:55:08.236181909	0.000000032	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
32	16:55:08.236181949	0.000000076	192.168.0.1	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
34	16:55:08.242683268	0.001466950	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=17/4352, ttl=6 (m)
35	16:55:08.242683313	0.000375353	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=18/4608, ttl=6 (m)
37	16:55:08.242707743	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=19/5120, ttl=6 (m)
38	16:55:08.242707785	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
39	16:55:08.242707827	0.001126507	103.232.241.2	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
40	16:55:08.242707869	0.000001264	10.159.264.171	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
42	16:55:08.247237483	0.000054132	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=20/5120, ttl=7 (m)
43	16:55:08.247237525	0.000000109	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=21/5376, ttl=7 (m)
44	16:55:08.247237567	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=22/5376, ttl=7 (m)
45	16:55:08.247774312	0.000000105	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=23/5376, ttl=7 (m)
46	16:55:08.247774354	0.000113757	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=24/5184, ttl=8 (m)
48	16:55:08.248042038	0.000078811	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=25/5376, ttl=8 (m)
49	16:55:08.248117339	0.000074481	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=27/6912, ttl=8 (m)
50	16:55:08.248117381	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=28/7168, ttl=9 (m)
51	16:55:08.248536282	0.000000105	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=29/7424, ttl=9 (m)
52	16:55:08.248601252	0.000075858	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=30/7680, ttl=10 (m)
53	16:55:08.248719972	0.000000000	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=31/8256, ttl=10 (m)
54	16:55:08.248751384	0.000074943	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=32/8130, ttl=11 (m)
55	16:55:08.249000000	0.001070106	10.119.254.121	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran
56	16:55:08.249036174	0.000148214	10.0.2.15	80.184.215.14	ICMP	74	Echo (ping) request id=0x1a7d, seq=33/8400, ttl=11 (m)
57	16:55:08.250002863	0.000148159	10.119.254.121	10.0.2.15	ICMP	74	Time-to-live exceeded (Time to live exceeded in tran

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

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
3	*REF*		*REF* 10.0.2.15	93.184.215.14	ICMP	74	Echo (ping) request id=0xia74, seq=1/256, ttl=1 (no res
108	16:55:09.022508950	0.100661882	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=0xia74, seq=52/13312, ttl=44 (re
109	16:55:09.026602597	0.004093647	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=0xia74, seq=53/13568, ttl=44 (re
110	16:55:09.031582741	0.004988144	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=0xia74, seq=54/13824, ttl=44 (re
111	16:55:09.135071895	0.103489154	93.184.215.14	10.0.2.15	ICMP	74	Echo (ping) reply id=0xia74, seq=55/14080, ttl=44 (re
<div> <div> <div>Frame 108: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3,</div> <div>Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemec_79:5f:23 (08:00:00:00:00:00)</div> <div>Destination: PCSSystemec_79:5f:23 (08:00:27:79:5f:23)</div> <div>Source: 52:54:00:12:35:02 (52:54:00:12:35:02)</div> <div>Type: IPv4 (0x0800)</div> <div>Internet Protocol Version 4, Src: 93.184.215.14, Dst: 10.0.2.15</div> <div>Internet Control Message Protocol</div> </div> <div> <div>0000 08 00 27 79 5f 23 52 54 00 12 35 02 08 00 45 00 ..y_#RT..S...E-</div> <div>0010 00 3c 0c 6d 00 00 2c 01 41 7f 5d b8 d7 0e 0a 00 <B...A].....</div> <div>0020 02 0f 00 00 6f d2 1a 74 00 34 48 49 4a 4b 4c 4d ...o...t-4H1JKLM</div> <div>0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\]</div> <div>0040 5e 5f 60 61 62 63 64 65 66 67 ^_ abcde fg</div> </div> </div>							
			cn1_b2.1_ICMP.pcapng				
			Packets: 148 · Displayed: 5 (3.4%)				
			Profile: Default				

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

Solution 6(Task2)

The screenshot shows a Kali Linux desktop environment. A VirtualBox window titled 'gulshan@gulshan-VirtualBox: ~' is open, displaying a terminal window. The terminal shows the command 'tcpdump -r capture_tcpdump.pcap tcp' and its output, which is a list of captured packets. The packets include WhatsApp traffic and Google search traffic. The output is as follows:

```

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 11267573:11267612, 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 62780, length 0
00:51:28.648311 IP gulshan-VirtualBox.39632 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [P.], seq 1740298018:1740298057, 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 3474216453:3474216492, 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, length 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 65535, 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, win 63950, length 24
00:51:28.658054 IP 191.144.160.34.bc.googleusercontent.com.https > gulshan-VirtualBox.46328: Flags [.], ack 46, win 65535, length 0
00:51:28.658055 IP whatsapp-cdn-shv-03-bom2.fbcdn.net.https > gulshan-VirtualBox.39632: Flags [.], ack 63, win 65535, length 0
00:51:28.658431 IP gulshan-VirtualBox.39632 > whatsapp-cdn-shv-03-bom2.fbcdn.net.https: Flags [F.], seq 63, ack 1, win 63950, length 0

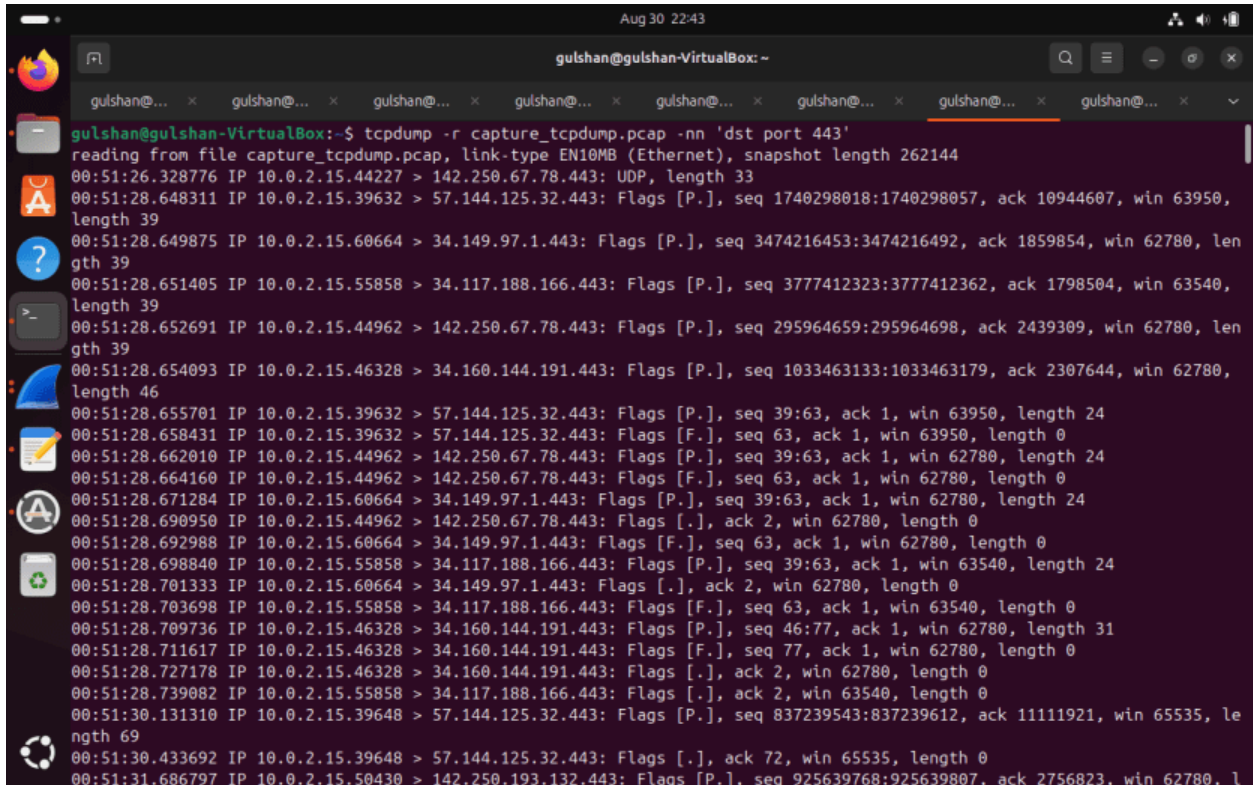
```

```
Aug 30 21:12
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, a
ck 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, a
ck 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 655
35, length 0
00:52:03.950184 IP gulshan-VirtualBox.43082 > www.iith.ac.in.https: Flags [S], seq 3660948202, win 64240, options [mss 1
460,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 29
20
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, lengt
h 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, lengt
h 274
00:52:04.043715 IP gulshan-VirtualBox.32774 > 49.44.119.242.http: Flags [S], seq 3492724101, win 64240, options [mss 146
0,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, o
ptions [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: ~
00:52:11.285202 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [P.], seq 1670:1785, a
ck 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, a
ck 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 655
35, length 0
00:52:12.311890 IP gulshan-VirtualBox.36322 > 76.237.120.34.bc.googleusercontent.com.https: Flags [P.], seq 4080:4328, a
ck 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 655
35, length 0
00:52:12.336169 IP 76.237.120.34.bc.googleusercontent.com.https > gulshan-VirtualBox.36322: Flags [P.], seq 1785:1900, a
ck 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, a
ck 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 655
35, length 0
00:52:12.613110 IP www.iith.ac.in.https > gulshan-VirtualBox.43082: Flags [P.], seq 90081:90112, ack 7867, win 65535, le
ngth 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, len
gth 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, l
ength 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.