

Name:- Ritesh Lakhani
Date:- 21/02/2025

EnrollmentNo:- 22010101099

Lab-11 : Wireshark Tool Exercises

1. Capturing Live Traffic – Use any website.

ip.addr == 103.102.166.224						
No.	Time	Source	Destination	Protocol	Length	Info
2077	24.113799058	10.20.53.68	103.102.166.224	TLSv1.2	171	Application Data
2081	24.196982055	103.102.166.224	10.20.53.68	TLSv1.2	2242	Application Data
2083	24.197049154	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=106 Ack=2177 Win=4503 Len=0 TSval=301961961...
2145	24.520742128	10.20.53.68	103.102.166.224	TLSv1.2	166	Application Data
2152	24.603805534	103.102.166.224	10.20.53.68	TLSv1.2	2216	Application Data
2153	24.603846512	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=206 Ack=4327 Win=4504 Len=0 TSval=301962001...
2270	25.477495192	10.20.53.68	103.102.166.224	TLSv1.2	150	Application Data
2277	25.560976478	103.102.166.224	10.20.53.68	TCP	5858	443 → 57014 [PSH, ACK] Seq=4327 Ack=290 Win=83 Len=5792 TSval=208...
2278	25.561048448	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=290 Ack=10119 Win=4480 Len=0 TSval=30196209...
2279	25.561127554	103.102.166.224	10.20.53.68	TCP	5858	443 → 57014 [PSH, ACK] Seq=10119 Ack=290 Win=83 Len=5792 TSval=20...
2280	25.561139201	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=290 Ack=15911 Win=4440 Len=0 TSval=30196209...
2281	25.561985697	103.102.166.224	10.20.53.68	TCP	2962	443 → 57014 [PSH, ACK] Seq=15911 Ack=290 Win=83 Len=2896 TSval=20...
2282	25.562021609	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=290 Ack=18807 Win=4500 Len=0 TSval=30196209...
2283	25.562649235	103.102.166.224	10.20.53.68	TLSv1.2	2962	Application Data
2284	25.562683724	10.20.53.68	103.102.166.224	TCP	66	57014 → 443 [ACK] Seq=290 Ack=21703 Win=4500 Len=0 TSval=30196209...

```
student@student: ~
--(student@student)-[~]
-$ ping www.wikipedia.org
PING dyna.wikimedia.org (103.102.166.224) 56(84) bytes of data.
64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=1 ttl=56 time=78.0 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=2 ttl=56 time=80.4 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=3 ttl=56 time=78.7 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=4 ttl=56 time=81.3 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=5 ttl=56 time=77.2 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=6 ttl=56 time=91.9 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=7 ttl=56 time=79.1 ms
4 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=8 ttl=56 time=82.0 ms
C
-- dyna.wikimedia.org ping statistics --
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
tt min/avg/max/mdev = 77.202/81.077/91.864/4.350 ms
```

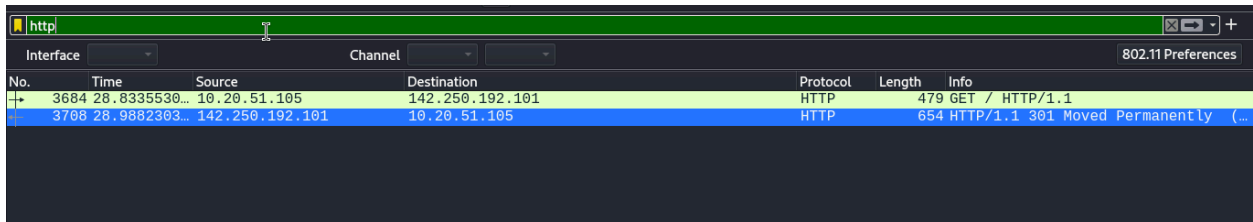
Capturing Wikipedia Traffic

1. Start Wireshark – Select the network interface and begin capturing.
2. Filter Traffic – Use `ip.addr == 103.102.166.224` for Wikipedia or `http/tcp.port == 443` for HTTP/HTTPS.
3. Analyze Packets – Inspect HTTP `GET` requests or TLS handshake for HTTPS.
4. Verify Connectivity – Use `ping www.wikipedia.org` to check response time and packet loss.

2. Applying Capture Filters:

a. HTTP traffic: hAp

- i. For HTTP - Inspect request and response headers, URLs, and status codes.
- ii. For HTTPS, observe the handshake process (TLS).



No.	Time	Source	Destination	Protocol	Length	Info
3684	28.8335530...	10.20.51.105	142.250.192.101	HTTP	479	GET / HTTP/1.1
3708	28.9882303...	142.250.192.101	10.20.51.105	HTTP	654	HTTP/1.1 301 Moved Permanently (...)

Description:-

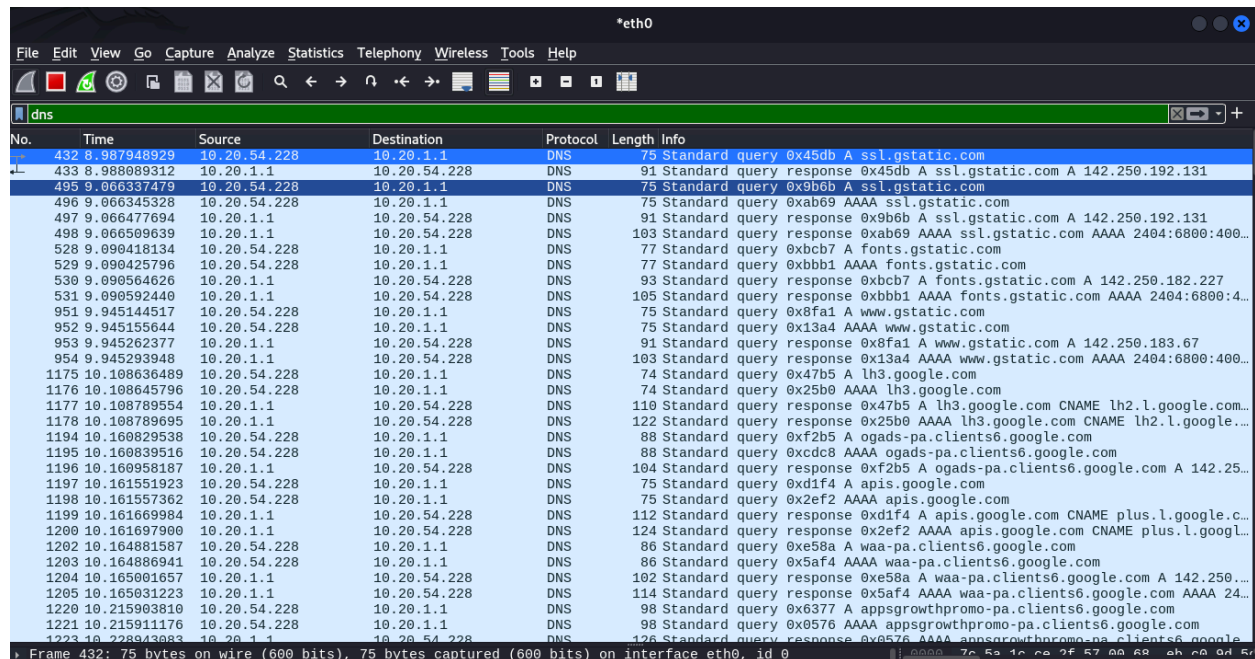
Request: The client (10.20.51.105) sends an HTTP GET request to 142.250.192.101.

Response: The server replies with HTTP 301 Moved Permanently, indicating redirection to another URL.

Observation: HTTP traffic is unencrypted, allowing inspection of headers, URLs, and status codes.

b. DNS requests: dns

- Observe how domain names are translated into IP addresses.
- Identify DNS request and response packets.



No.	Time	Source	Destination	Protocol	Length	Info
432	8.887948929	10.20.54.228	10.20.1.1	DNS	75	Standard query 0x45db A ssl.gstatic.com
433	8.989898312	10.20.1.1	10.20.54.228	DNS	91	Standard query response 0x45db A ssl.gstatic.com A 142.250.192.131
495	8.963374719	10.20.54.228	10.20.1.1	DNS	75	Standard query 0xab69 AAAA ssl.gstatic.com
496	8.96345328	10.20.54.228	10.20.1.1	DNS	75	Standard query 0xab69 AAAA ssl.gstatic.com
497	9.066477694	10.20.1.1	10.20.54.228	DNS	91	Standard query response 0xab69 AAAA ssl.gstatic.com A 142.250.192.131
498	9.066599639	10.20.1.1	10.20.54.228	DNS	103	Standard query response 0xab69 AAAA ssl.gstatic.com AAAA 2404:6800:400...
528	9.090418134	10.20.54.228	10.20.1.1	DNS	77	Standard query 0xbcb7 A fonts.gstatic.com
529	9.090425796	10.20.54.228	10.20.1.1	DNS	77	Standard query 0xbcb7 A fonts.gstatic.com
530	9.090564626	10.20.1.1	10.20.54.228	DNS	93	Standard query response 0xbcb7 A fonts.gstatic.com A 142.250.182.227
531	9.090592440	10.20.1.1	10.20.54.228	DNS	105	Standard query response 0xbcb7 AAAA fonts.gstatic.com AAAA 2404:6800:400...
951	9.945144517	10.20.54.228	10.20.1.1	DNS	75	Standard query 0x8fa1 A www.gstatic.com
952	9.945155644	10.20.54.228	10.20.1.1	DNS	75	Standard query 0x13a4 AAAA www.gstatic.com
953	9.945262377	10.20.1.1	10.20.54.228	DNS	91	Standard query response 0x8fa1 A www.gstatic.com A 142.250.183.67
954	9.945293948	10.20.1.1	10.20.54.228	DNS	103	Standard query response 0x13a4 AAAA www.gstatic.com AAAA 2404:6800:400...
1175	10.108636489	10.20.54.228	10.20.1.1	DNS	74	Standard query 0x47b5 A lh3.google.com
1176	10.108645796	10.20.54.228	10.20.1.1	DNS	74	Standard query 0x25b0 AAAA lh3.google.com
1177	10.108789554	10.20.1.1	10.20.54.228	DNS	110	Standard query response 0x47b5 A lh3.google.com CNAME lh2.l.google.com...
1178	10.108789695	10.20.1.1	10.20.54.228	DNS	122	Standard query response 0x25b0 AAAA lh3.google.com CNAME lh2.l.google.com...
1194	10.160829538	10.20.54.228	10.20.1.1	DNS	88	Standard query 0xf2b5 A ogads-pa.clients6.google.com
1195	10.160839516	10.20.54.228	10.20.1.1	DNS	88	Standard query 0xcdb8 AAAA ogads-pa.clients6.google.com
1196	10.160958187	10.20.1.1	10.20.54.228	DNS	104	Standard query response 0xf2b5 A ogads-pa.clients6.google.com A 142.250...
1197	10.161551923	10.20.54.228	10.20.1.1	DNS	75	Standard query 0xd1f4 A apis.google.com
1198	10.161557362	10.20.54.228	10.20.1.1	DNS	75	Standard query 0x2ef2 AAAA apis.google.com
1199	10.161669984	10.20.1.1	10.20.54.228	DNS	112	Standard query response 0xd1f4 A apis.google.com CNAME plus.l.google.com...
1200	10.161697900	10.20.1.1	10.20.54.228	DNS	124	Standard query response 0x2ef2 AAAA apis.google.com CNAME plus.l.google.com...
1202	10.164881587	10.20.54.228	10.20.1.1	DNS	86	Standard query 0xe58a A waa-pa.clients6.google.com
1203	10.164886941	10.20.54.228	10.20.1.1	DNS	86	Standard query 0x5af4 AAAA waa-pa.clients6.google.com
1204	10.165001657	10.20.1.1	10.20.54.228	DNS	102	Standard query response 0xe58a A waa-pa.clients6.google.com A 142.250...
1205	10.165031223	10.20.1.1	10.20.54.228	DNS	114	Standard query response 0x5af4 AAAA waa-pa.clients6.google.com AAAA 24...
1220	10.215903810	10.20.54.228	10.20.1.1	DNS	98	Standard query 0x6377 A appsgrowthpromo-pa.clients6.google.com
1221	10.215911176	10.20.54.228	10.20.1.1	DNS	98	Standard query 0x0576 AAAA appsgrowthpromo-pa.clients6.google.com
1223	10.228043683	10.20.1.1	10.20.54.228	DNS	126	Standard query response 0x0576 AAAA appsgrowthpromo-pa.clients6.google.com

Description:-

DNS Requests and Responses Overview:

- DNS Request:** The client (10.20.54.228) queries the DNS server (10.20.1.1) for domain name resolution (e.g., `ssl.gstatic.com`).
- DNS Response:** The server replies with the corresponding IP address (e.g., `142.250.192.131`).
- Process:** Converts domain names to IP addresses for network communication.

c. TCP packets: tcp

- Observe the 3-way handshake (SYN, SYN-ACK, ACK).
- Identify sequence numbers and acknowledgment numbers.

The image shows a Wireshark packet capture on interface eth0. The filter is set to 'tcp'. The packet list shows several TCP packets. The first three packets (No. 351, 355, 382) represent the 3-way handshake:

No.	Time	Source	Destination	Protocol	Length	Info
351	4.113653720	10.20.54.228	23.58.95.160	TCP	66	59564 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=1504316511 TSecr=...
355	4.147452921	23.58.95.160	10.20.54.228	TCP	66	45142 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=355132844 TSecr=...
382	4.625459951	10.20.54.228	23.58.95.250	TCP	66	45148 → 80 [ACK] Seq=1 Ack=1 Win=249 Len=0 TSval=355132844 TSecr=...

The status bar at the bottom indicates: Frame 138: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0.

Description:-

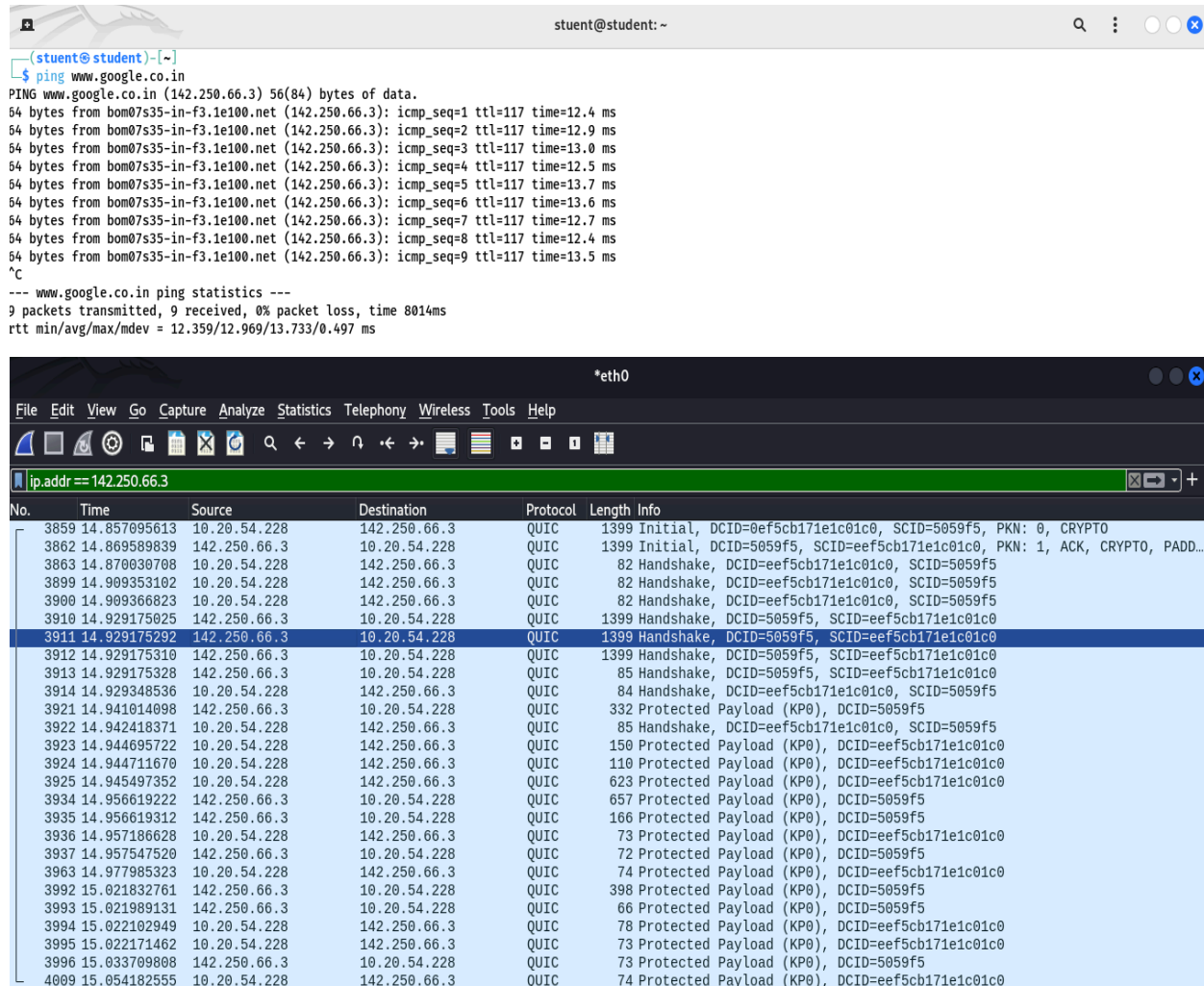
In the Wireshark capture, the **TCP 3-way handshake** is observed with the following steps:

- SYN:** The client (IP **10.20.54.228**) sends a SYN packet to initiate the connection.
- SYN-ACK:** The server (IP **23.58.95.160**) responds with a SYN-ACK packet to acknowledge the request.
- ACK:** The client sends an ACK packet to confirm the connection.

Additionally, **sequence numbers** (Seq) track the data being sent, starting from **Seq=1** for the SYN packet, and **acknowledgment numbers** (Ack) confirm the receipt of data, such as **Ack=249** to acknowledge the data received. This process ensures reliable and ordered data exchange in TCP communication.

d. ICMP (ping): icmp

i. Send ping requests (ping google.com) and observe request/reply packets.



The first screenshot shows a terminal window with the command `ping www.google.co.in` executed. The output displays 9 successful ICMP Echo Request and Reply packets with varying round-trip times and TTL values. The statistics at the bottom show 9 packets transmitted, 9 received, 0% packet loss, and a total time of 8014ms.

```
(student@student)-[~]
$ ping www.google.co.in
PING www.google.co.in (142.250.66.3) 56(84) bytes of data:
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=1 ttl=117 time=12.4 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=2 ttl=117 time=12.9 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=3 ttl=117 time=13.0 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=4 ttl=117 time=12.5 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=5 ttl=117 time=13.7 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=6 ttl=117 time=13.6 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=7 ttl=117 time=12.7 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=8 ttl=117 time=12.4 ms
54 bytes from bom07s35-in-f3.1e100.net (142.250.66.3): icmp_seq=9 ttl=117 time=13.5 ms
^C
--- www.google.co.in ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8014ms
rtt min/avg/max/mdev = 12.359/12.969/13.733/0.497 ms
```

The second screenshot shows a Wireshark packet capture on the `eth0` interface, filtered for `ip.addr == 142.250.66.3`. The capture shows a series of QUIC packets (Initial, Handshake, and Protected Payload) between the local host and the destination IP. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
3859	14.857095613	10.20.54.228	142.250.66.3	QUIC	1399	Initial, DCID=0ef5cb171e1c01c0, SCID=5059f5, PKN: 0, CRYPTO
3862	14.869589839	142.250.66.3	10.20.54.228	QUIC	1399	Initial, DCID=5059f5, SCID=eef5cb171e1c01c0, PKN: 1, ACK, CRYPTO, PADD...
3863	14.870030708	10.20.54.228	142.250.66.3	QUIC	82	Handshake, DCID=eef5cb171e1c01c0, SCID=5059f5
3899	14.909353102	10.20.54.228	142.250.66.3	QUIC	82	Handshake, DCID=eef5cb171e1c01c0, SCID=5059f5
3900	14.909366823	10.20.54.228	142.250.66.3	QUIC	82	Handshake, DCID=eef5cb171e1c01c0, SCID=5059f5
3910	14.929175025	142.250.66.3	10.20.54.228	QUIC	1399	Handshake, DCID=5059f5, SCID=eef5cb171e1c01c0
3911	14.929175292	142.250.66.3	10.20.54.228	QUIC	1399	Handshake, DCID=5059f5, SCID=eef5cb171e1c01c0
3912	14.929175310	142.250.66.3	10.20.54.228	QUIC	1399	Handshake, DCID=5059f5, SCID=eef5cb171e1c01c0
3913	14.929175328	142.250.66.3	10.20.54.228	QUIC	85	Handshake, DCID=5059f5, SCID=eef5cb171e1c01c0
3914	14.929348536	10.20.54.228	142.250.66.3	QUIC	84	Handshake, DCID=eef5cb171e1c01c0, SCID=5059f5
3921	14.941014098	142.250.66.3	10.20.54.228	QUIC	332	Protected Payload (KP0), DCID=5059f5
3922	14.942418371	10.20.54.228	142.250.66.3	QUIC	85	Handshake, DCID=eef5cb171e1c01c0, SCID=5059f5
3923	14.944695722	10.20.54.228	142.250.66.3	QUIC	150	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3924	14.944711670	10.20.54.228	142.250.66.3	QUIC	110	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3925	14.945497352	10.20.54.228	142.250.66.3	QUIC	623	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3934	14.956619222	142.250.66.3	10.20.54.228	QUIC	657	Protected Payload (KP0), DCID=5059f5
3935	14.956619312	142.250.66.3	10.20.54.228	QUIC	166	Protected Payload (KP0), DCID=5059f5
3936	14.957186628	10.20.54.228	142.250.66.3	QUIC	73	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3937	14.957547520	142.250.66.3	10.20.54.228	QUIC	72	Protected Payload (KP0), DCID=5059f5
3963	14.977985323	10.20.54.228	142.250.66.3	QUIC	74	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3992	15.021832761	142.250.66.3	10.20.54.228	QUIC	398	Protected Payload (KP0), DCID=5059f5
3993	15.021989131	142.250.66.3	10.20.54.228	QUIC	66	Protected Payload (KP0), DCID=5059f5
3994	15.022102949	10.20.54.228	142.250.66.3	QUIC	78	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3995	15.022171462	10.20.54.228	142.250.66.3	QUIC	73	Protected Payload (KP0), DCID=eef5cb171e1c01c0
3996	15.033709808	142.250.66.3	10.20.54.228	QUIC	73	Protected Payload (KP0), DCID=5059f5
4009	15.054182555	10.20.54.228	142.250.66.3	QUIC	74	Protected Payload (KP0), DCID=eef5cb171e1c01c0

Description:-

ICMP (ping) Packets:

The first image demonstrates the use of the `ping` command to test connectivity with `google.co.in`. The system sends ICMP Echo Request packets, and Google's server responds with ICMP Echo Reply packets. Each response includes sequence numbers (`icmp_seq`), Time-to-Live (`ttl`), and round-trip time (`time`). The ping statistics at the end indicate no packet loss, confirming successful communication.