1.Install Wireshark.

sudo apt update

sudo apt install -y wireshark tshark tcpdump

2.Start capturing on your active network interface.

ip route get 8.8.8.8 | awk '{print $5; exit}' # Check for Interface

ip link show # or

ifconfig -a

3.Browse a website or ping a server to generate traffic.

Browse 2 websites (GUI Based Approach)

Google.com

https://db-ip.com/all/192.168.171

terminal: ping and a curl request (CLI Based Approach)

ping -c 4 google.com

curl -I https://www.google.com

5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

Using (CLI):

show DNS packets

tshark -r ~/capture.pcap -Y dns

show HTTP packets

tshark -r ~/capture.pcap -Y http

show ICMP

tshark -r ~/capture.pcap -Y icmp

To extract just the top protocols seen:

tshark -r ~/capture.pcap -q -z io,phs

or use protocol hierarchy:

```
tshark -r ~/capture.pcap -q -z proto,colinfo,0

# simpler: protocol hierarchy summary

tshark -r ~/capture.pcap -q -z io,phs,0,ip
```

6.Identify at least 3 different protocols in the capture.

- TCP
- DNS
- TLS
- UDP
- QUIC

8.Summarize your findings and packet details.

Protocols Observed

- **TCP (Transmission Control Protocol)** – The dominant protocol, responsible for reliable data transfer between hosts.
- **DNS (Domain Name System)** – Used to resolve domain names into IP addresses.
- **QUIC / TLS** – Present during secure web browsing; indicates encrypted HTTPS communication over UDP.
- **UDP (User Datagram Protocol)** – Used by QUIC and some DNS traffic for faster, connectionless delivery.

Key Observations

- **Handshake and Termination:**
    - Multiple SYN, SYN-ACK, and ACK packets confirm several TCP connection establishments.
    - FIN packets show graceful connection termination.
- **Retransmissions:**
    - A few packets were marked as **"suspected retransmissions"**, typical of network latency or temporary packet loss.

- **RST (Reset) Packets:**
    - Some sessions ended abruptly, possibly due to timeouts or closed connections.
- **QUIC/TLS Handshake:**
    - TLS handshake messages and deprecated legacy version warnings confirm encrypted HTTPS traffic.
- **DNS Queries:**
    - Several DNS packets show hostname lookups for visited websites.

Packet Summary (from Expert Info)

Severity	Description / Event	Protocol	Count
Warning	TCP segment not captured / RST / Handshake failure	TCP	574
Note	Retransmissions, Keep-alive, Coalesced segments	TCP	20+
Chat	SYN, SYN-ACK, FIN – connection start and end	TCP	51 each
Deprecated	Legacy TLS version field ignored	TLS	146
Protocol	Standard DNS request/response	DNS	131
Info	QUIC / UDP packets in encrypted traffic	QUIC / UDP	9 + 4

Interpretation

- The traffic primarily consists of **web-related communication**, where TCP manages reliable sessions and QUIC/TLS provides encrypted data exchange.
- DNS lookups occur prior to establishing web sessions.
- Retransmissions and RSTs are normal in short captures due to session resets or packet loss.
- Presence of **TLS** and **QUIC** confirms that most browsing occurred over **secure HTTPS**.

Conclusion

The Wireshark capture demonstrates active network behavior with multiple concurrent TCP and QUIC sessions, DNS resolution, and encrypted communication. The packet flow reflects a typical secure web-browsing session. Minor retransmissions and resets are expected in normal network conditions.