## **Lab: 01**

Name: Muhammad Waqas Siddique

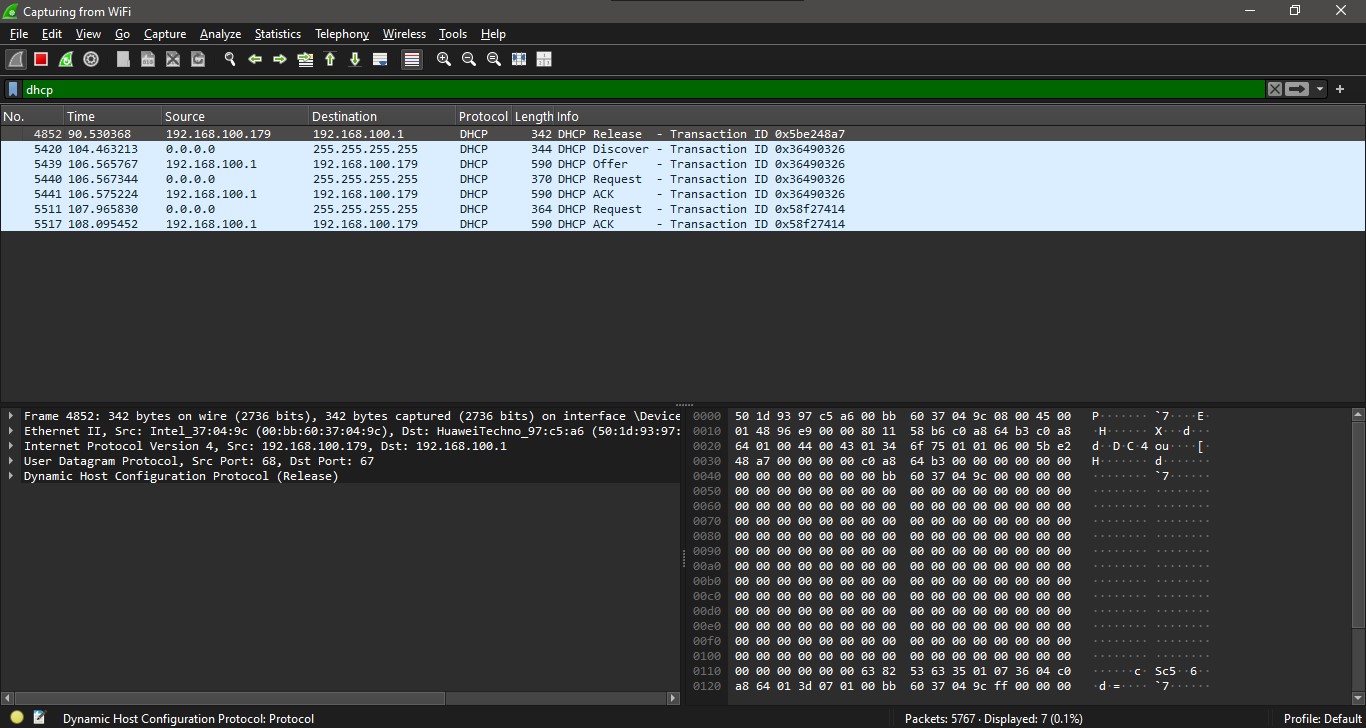
Class: BSCSev-IV-B

Roll No: 232441

Course: Computer Networks

## **DHCP (Dynamic Host Configuration Protocol):**

* **Purpose**: Automatically assigns IP addresses to devices.
* **Key Features**: Simplifies network setup and management.
* **Analyzing the Packets/Information Received:**
  + **Frame 35287**: 342 bytes captured on interface \Device\MPF\_([085850E1-31C0-4C50-9997-B0223AFRALBF], id 0.
  + **Ethernet II**: Src MAC: AzureMowTec\_71:77:8:C7 (94:bb:43:37:78:C7 ), Dst MAC: Cisco\_e8:84:40 (79:6e:64:c8:84:40).
  + **IPv4**: Src IP: 10.120.166.184, Dst IP: i.i.i.l (likely 1.1.1.1 or placeholder).
  + **UDP**: Src Port: 60, Dst Port: 67 (DHCP server port).
  + **DHCP**: Indicates a DHCP Release message, where the client releases its IP address.

****

**UDP (User Datagram Protocol)**

UDP is a connectionless protocol that sends data without error checking, making it faster but less reliable, commonly used in streaming and gaming.

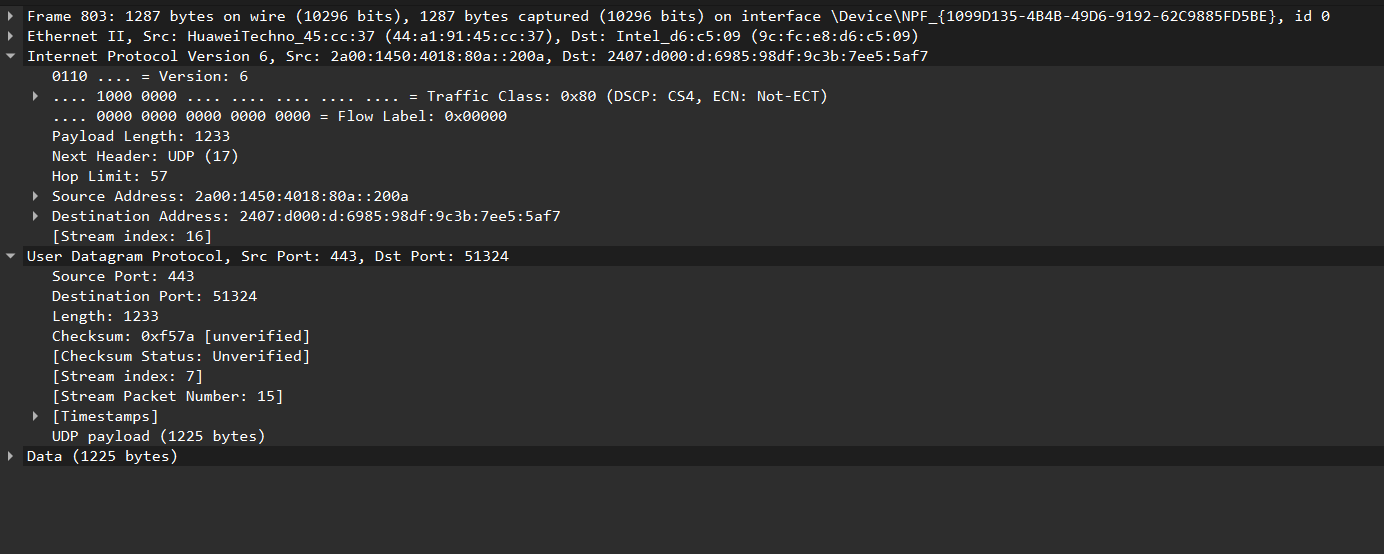
**Source Port**: 443

* This is the **HTTPS port** (indicating encrypted traffic).

**Destination Port**: 51324

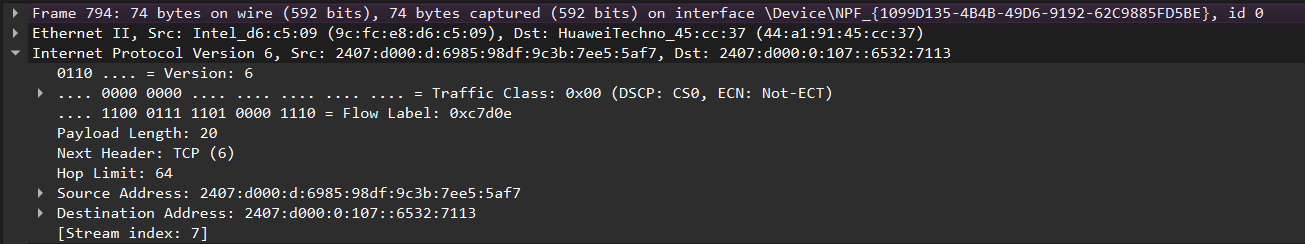
* This is a random **port** assigned to the client.

**Length**: 1233 bytes

This includes the UDP header + payload

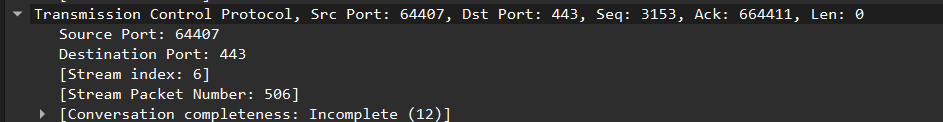
**TCP (Transmission Control Protocol)**

TCP is a connection-oriented protocol that ensures reliable data transfer by establishing a connection, sequencing packets, and retransmitting lost data.



**Source IP**: 2407:d000:d:6985:98df:9c3b:7ee5:5af7  
→ The sender’s IP address.

**Destination IP**: 2407:d000:0:107::6532:7113  
→ The receiver’s IP address.



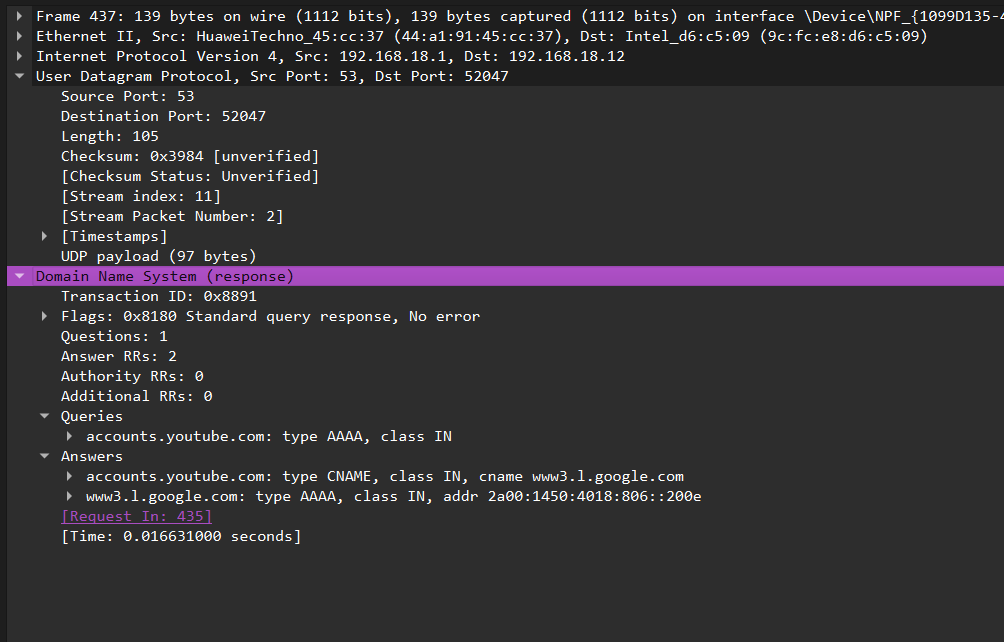
**Source Port**: 64407  
→ This is a random port assigned to the client.

**Destination Port**: 443  
→ This indicates the packet is going to an HTTPS web server.

**Sequence Number**: 3153 (relative)  
→ This is the sequence number of the first byte in this packet.

**DNS (Domain Name System)**

DNS translates human-readable domain names (e.g., google.com) into IP addresses so computers can communicate over the internet.



**CNAME Record (Canonical Name)**

* accounts.youtube.com is **aliased to** www3.l.google.com
* This means **Google manages YouTube's account subdomain via a CNAME**.

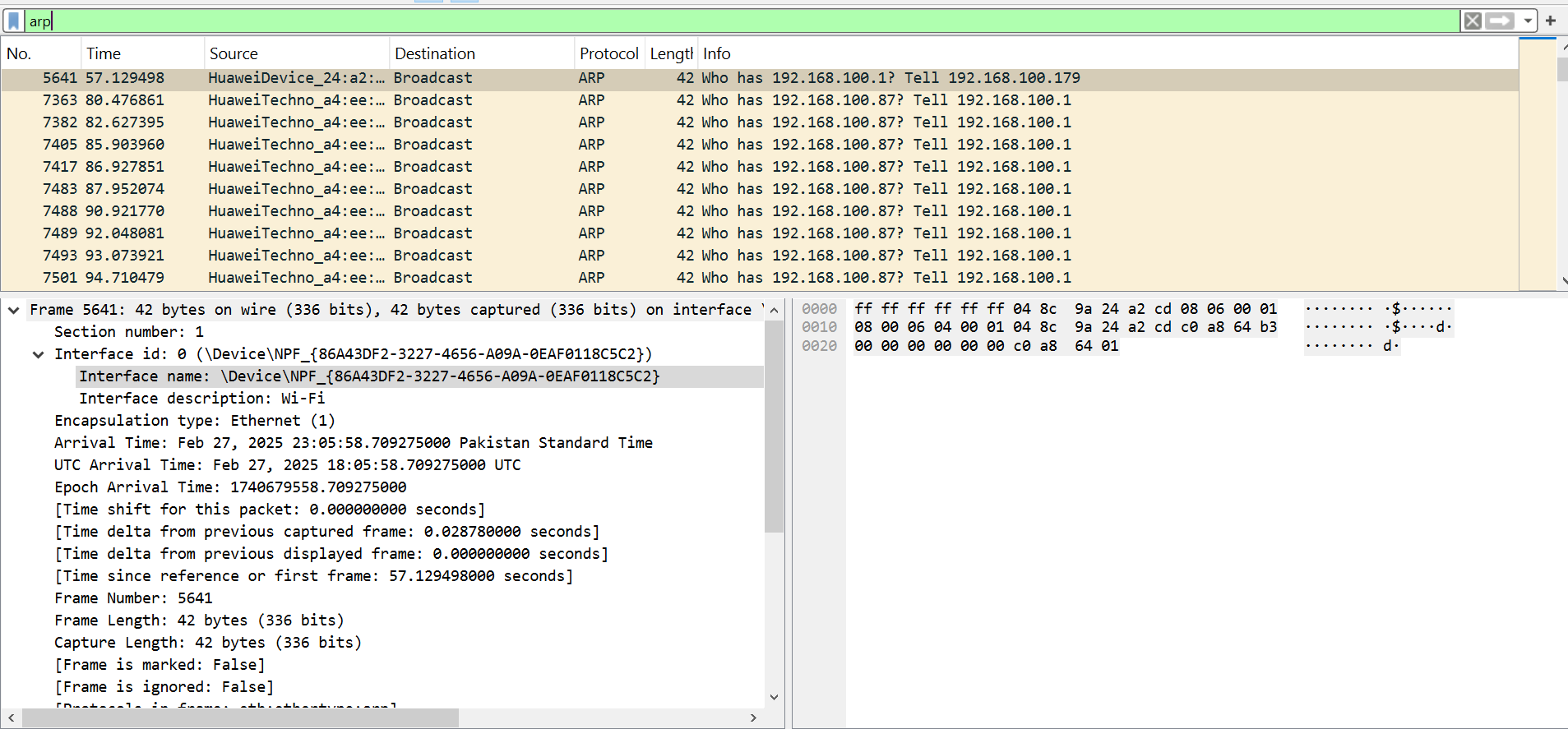
**AAAA Record (IPv6 Address)**

* www3.l.google.com resolves to 2a00:1450:4018:806::200e
* This is a **Google IPv6 address**.

**ARP:**

**ARP (Address Resolution Protocol)** is a network protocol used to map an **IP address** (logical address) to a **MAC address** (physical hardware address) within a local network (LAN).

**How ARP Works:**

1. **Device A wants to communicate** with Device B but only knows its IP address.
2. Device A **broadcasts an ARP request** on the network:
   * "Who has IP 192.168.1.2? Tell me your MAC address."
3. **Device B responds with its MAC address**.
4. Device A **saves the MAC address** in its ARP cache and sends the data.
5. **Hardware Type:** Specifies the network link layer protocol in use.

* **Ethernet (1)** indicates the ARP request is using Ethernet.

1. **Protocol Type:** Defines the upper-layer protocol ARP is resolving.

* **IPv4 (0x0800)** means it is mapping an IPv4 address to a MAC address.

1. **Hardware Size:** Specifies the size of the hardware (MAC) address in bytes.

* **Size: 6** (MAC addresses are 6 bytes long).

1. **Protocol Size:** Defines the size of the protocol address (IP) in bytes.

* **Size: 4** (IPv4 addresses are 4 bytes long).

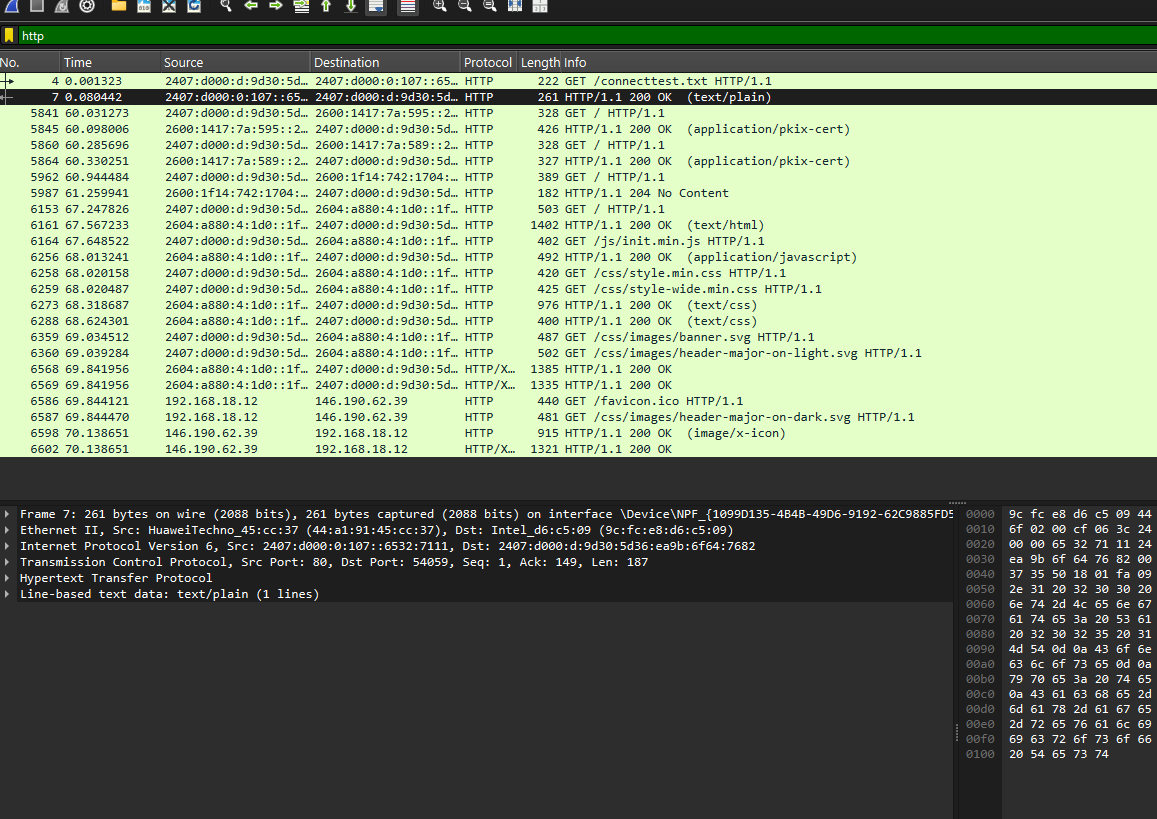
1. **Opcode:** Indicates the type of ARP message.

* **Request (1)** means the sender is asking for the MAC address of a given IP.

1. **Sender MAC Address:** The MAC address of the device making the request.
2. **Sender IP Address:** The IP address of the requesting device.
3. **Target MAC Address:** Initially set to **00:00:00:00:00:00** since the sender does not know it yet.
4. **Target IP Address:** The IP address whose MAC address is being requested.

**HTTP (Hypertext Transfer Protocol)**

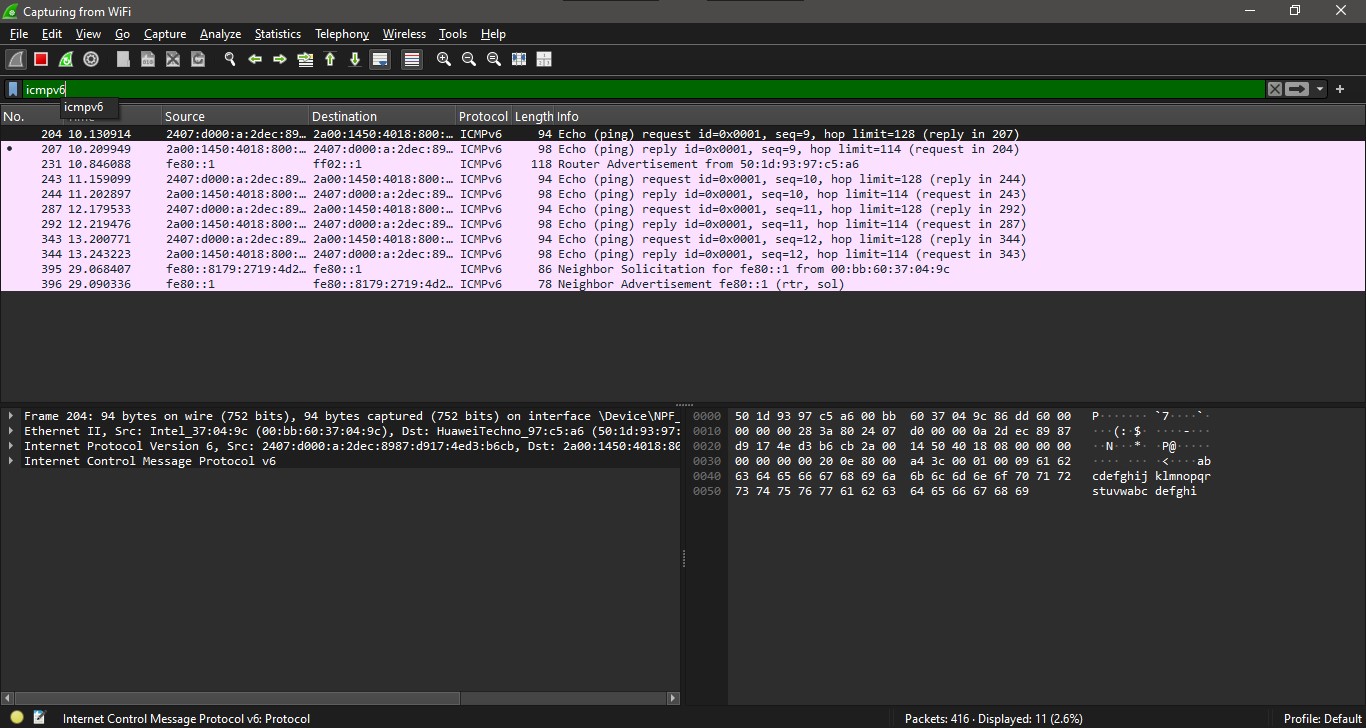
HTTP is used for communication between web browsers and servers, allowing users to request and view web pages.



## **ICMP (Internet Control Message Protocol)**:

* **Purpose**: Used for error reporting and diagnostic functions. Common utilities like ping and traceroute rely on ICMP.

**Key Features:** ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic purposes

****

**QUIC (Quick UDP Internet Connections)**

**It** is a **transport layer network protocol** developed by Google to improve the speed, security, and reliability of internet communications. Unlike traditional **TCP**, QUIC operates over **UDP** and integrates key features such as multiplexed streams, connection migration, and built-in encryption.

A screenshot of a computer

AI-generated content may be incorrect.

* 1. **PING (Frame Type: 0x01)**
* Used to check if the connection is still **alive**.
* Does not carry data, only confirms connectivity between client and server.
  1. **PADDING (Frame Type: 0x00)**
* Adds extra **bytes** to a QUIC packet to ensure a minimum size.
* Used to **prevent traffic analysis** or meet required packet size for security reasons.
  1. **CRYPTO (Frame Type: 0x06)**
* Used for **initial encryption handshakes** (similar to TLS handshake in TCP)