Wireshark Packet Analysis

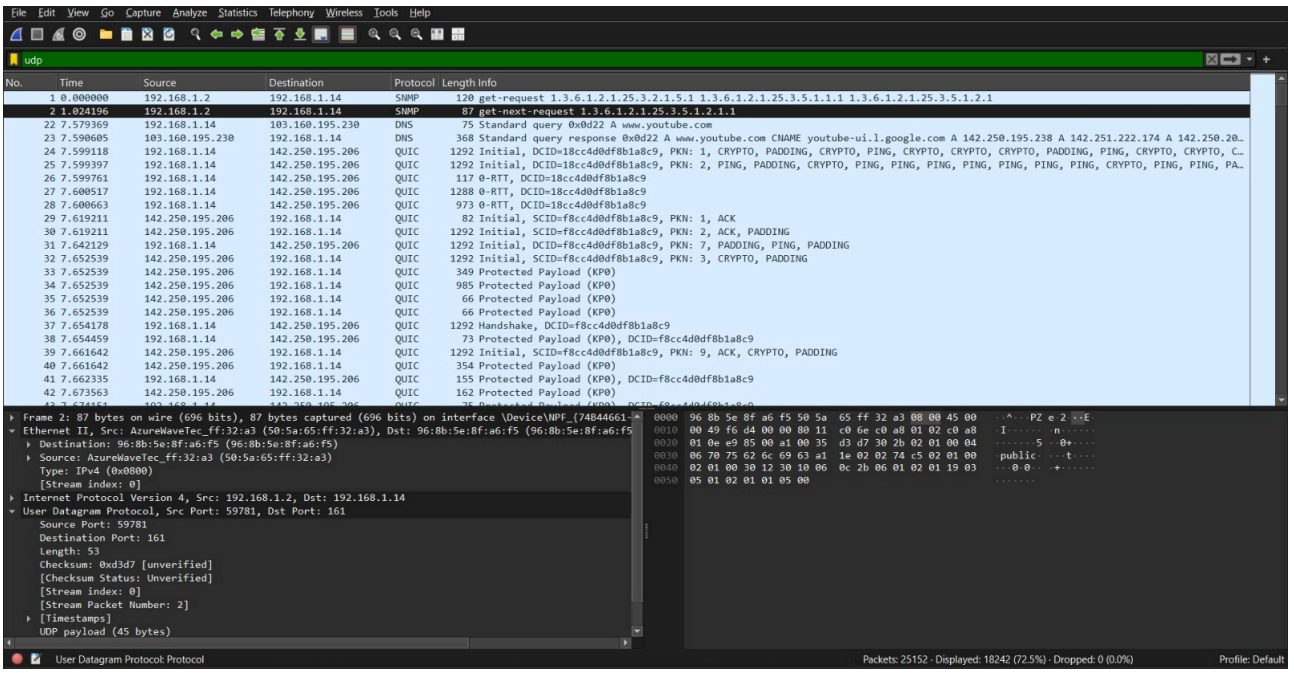
Types of protocols identified:

1. SNMP (Simple Network Management Protocol)

Port Used: UDP 161
Description:
SNMP is used for monitoring and managing network devices. It allows querying device information such as interface status, CPU load, etc.

Key Observations:

- Two SNMP packets between `192.168.1.2` and `192.168.1.14`.
- One packet is a **GET-NEXT request**, requesting OID: `1.3.6.1.2.1.25.3.5.1.2.1` (likely related to printer or system processes).
- SNMP community string observed: `"public"` (default; not secure).



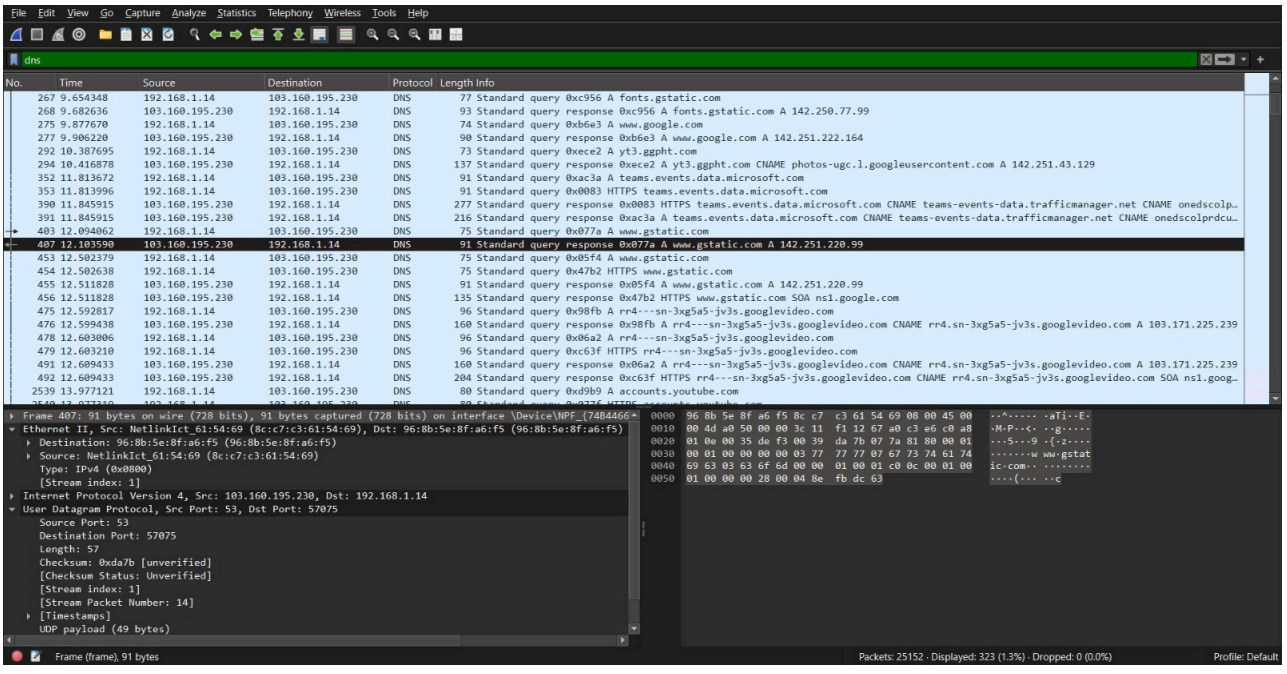
Screenshot of SNMP Protocol

2. DNS (Domain Name System)

Port Used: UDP 53
Description:
DNS resolves domain names (like `google.com`) to IP addresses.

Key Observations:

- Queries to domains such as:
  - `www.youtube.com`
  - `fonts.gstatic.com`
  - `google.com`
- DNS responses include multiple A-records (IPv4 addresses), indicating **load balancing** and **CDN use**.
- Source IP: `192.168.1.14` making requests to public DNS servers (e.g., `103.160.195.230`).



Screenshot of DNS Protocol

3. QUIC (Quick UDP Internet Connections)

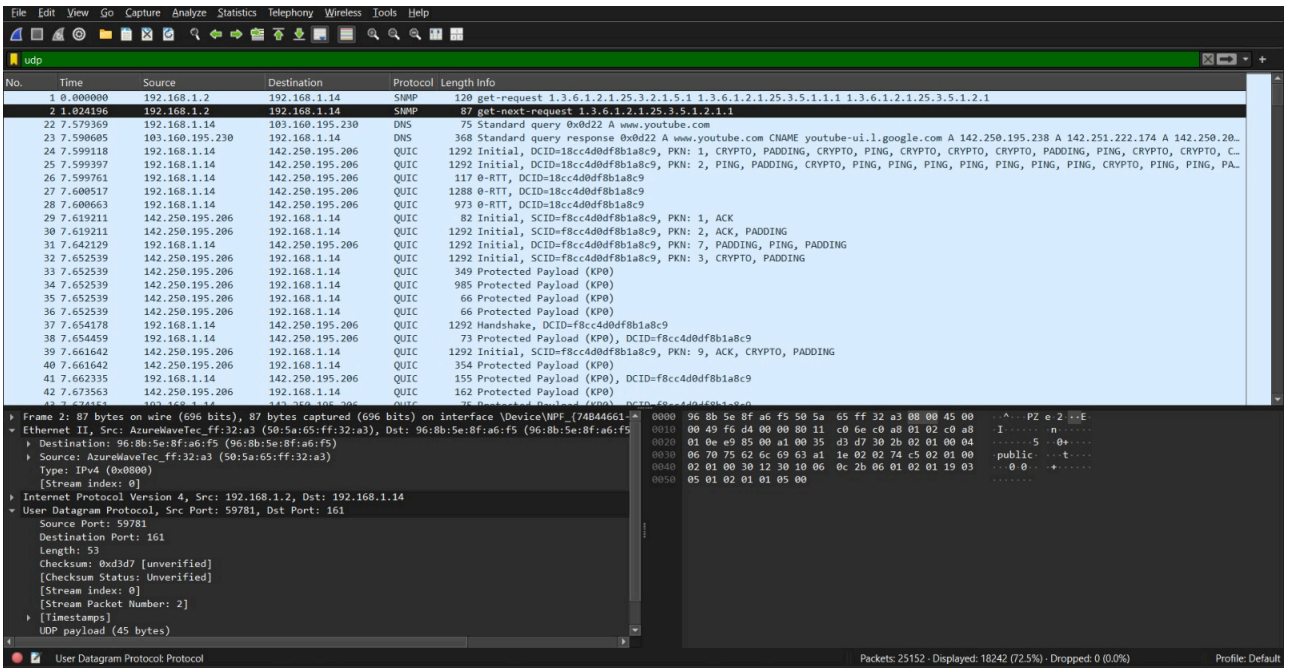
Port Used: UDP 443

Description:

A modern encrypted transport protocol developed by Google, used in HTTP/3, offering faster and more secure connections over UDP.

Key Observations:

- Multiple QUIC packets to `142.250.195.206` and similar Google IPs.
- Traffic includes:
  - **Initial**, **Handshake**, **0-RTT**, and **Protected Payloads**
  - Keywords like **CRYPTO**, **PING**, **ACK** indicate connection establishment and encrypted data transfer.
- Likely related to YouTube or Google traffic.



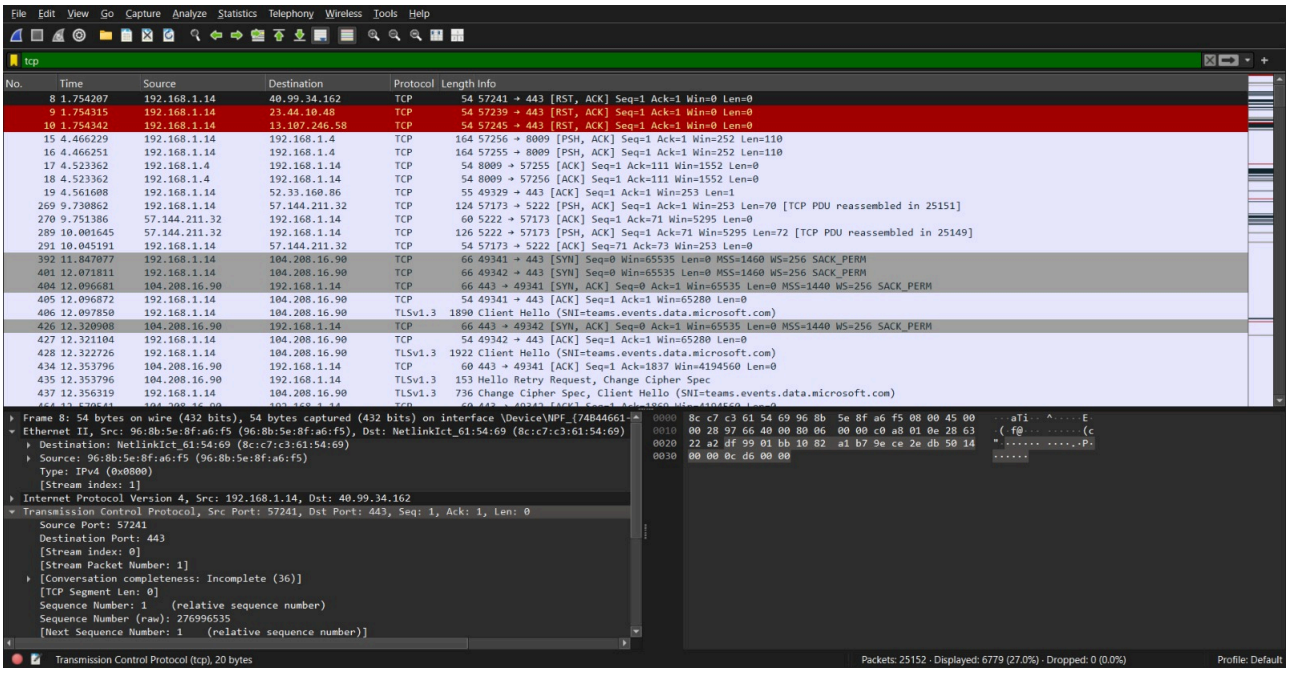
Screenshot of QUIC Protocol

4. TCP (Transmission Control Protocol)

Port Used: Various, including 443 (HTTPS), 8009, etc.
Description:
Reliable, connection-oriented protocol used in most traditional web traffic (including HTTPS).

Key Observations:

- Connections from `192.168.1.14` to Microsoft servers (`teams.events.data.microsoft.com`)
- Packets include:
  - **SYN**, **ACK**, **PSH**, **RST** flags
  - TLS handshakes visible (`Client Hello`, `Change Cipher Spec`)
- Some connections are **reset (RST)**—possibly blocked or failed.



Screenshot of TCP Protocol