Wireshark Network Traffic Analysis Report

Date of Capture: 29/09/2025
Tool Used: Wireshark
Capture Duration: ~1 minute

Protocols Identified

DNS (Domain Name System)

Example: github.com

Source: Local machine → DNS server

Source:10.191.24.143→140.82.114.22(github)

Purpose: Resolves domain names to IP addresses.

ICMP (Internet Control Message Protocol)

Example: ping google.com

Observed Echo Request (Type 8) and Echo Reply (Type 0).

Purpose: Connectivity testing and troubleshooting.

TCP

Example: TCP request to github.com

Source 10.191.24.143 → 140.82.114.22

Purpose: Standard web traffic for loading web pages.

QUIC (Quick UDP Internet Connections)

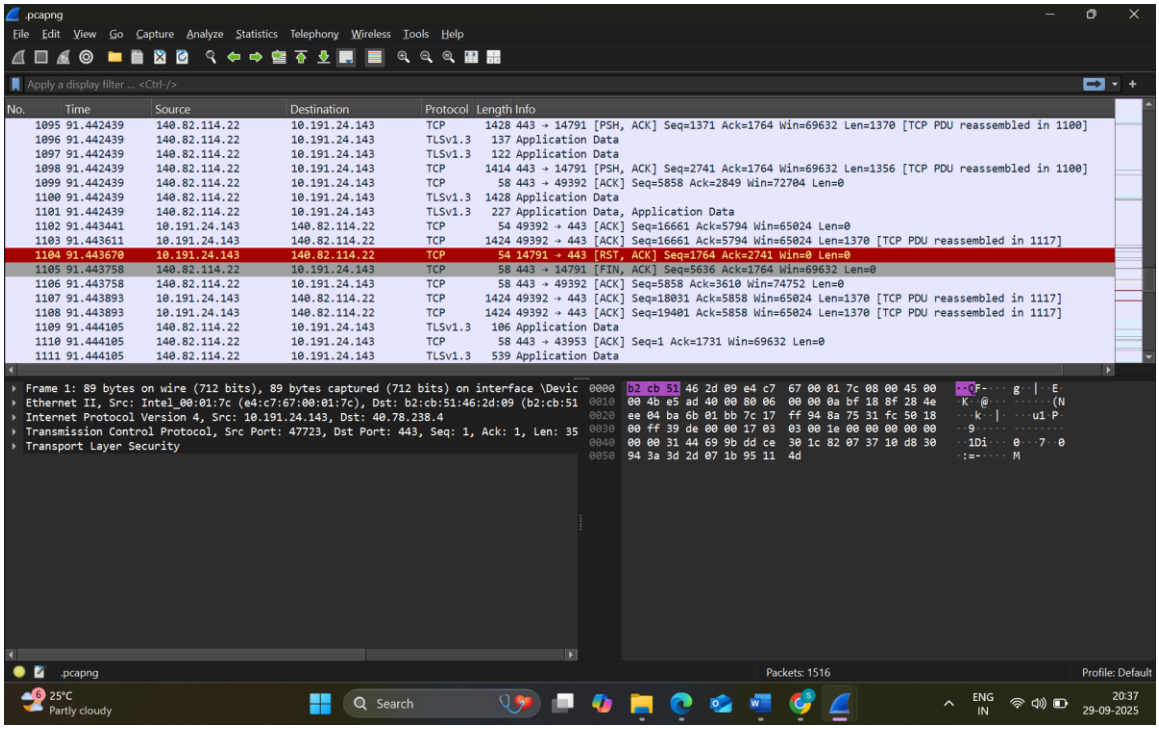
Example: Connection to www.youtube.com over port 443/UDP.

Transport: UDP-based protocol used for HTTP/3.

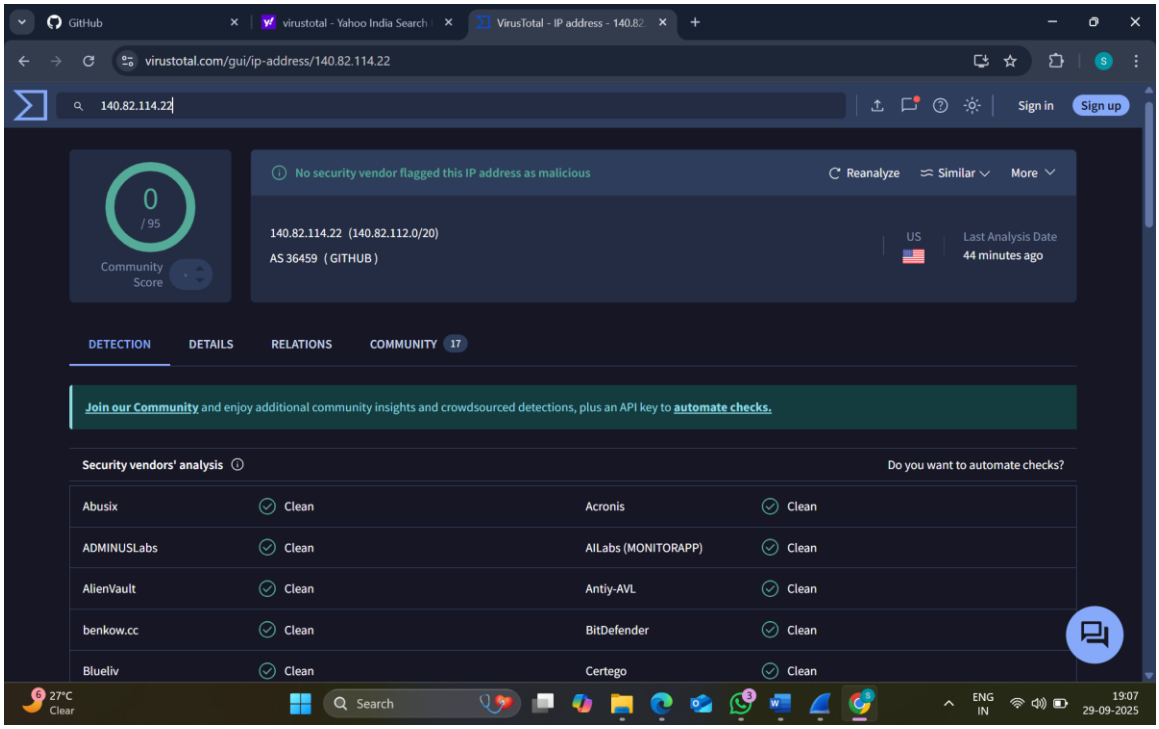
Features: Provides faster connection setup, improved performance over high-latency networks, and built-in encryption.

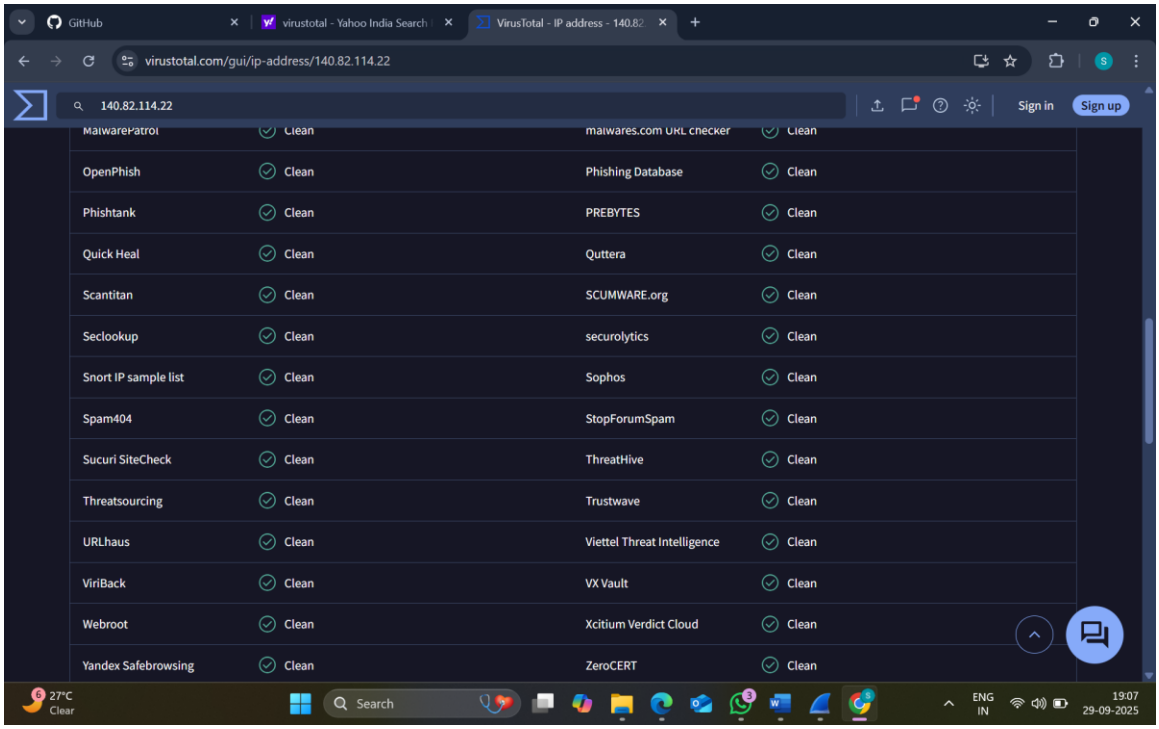
Purpose: Modern alternative to TCP+TLS for secure web traffic.

Browsed github.com



Identified in virustotal by source ip address and destination ip adress





Peroformed other filters like tcp and dns separately and saved as dns.pcap and tcp.pcap files that should added in github repo along with full packet capture by my wife connection

Summary

The packet capture successfully recorded multiple types of traffic, including DNS lookups, ICMP ping messages, TCP-based HTTP browsing, and QUIC connections. The presence of QUIC highlights the shift from traditional TCP-based HTTPS to HTTP/3 over UDP, showing how modern browsers optimize performance and security. This exercise improved understanding of how various protocols operate together in real-time communication.