**Task 5: Capture and Analyse Network Traffic Using Wireshark**

ICMP Ping (8.8.8.8)

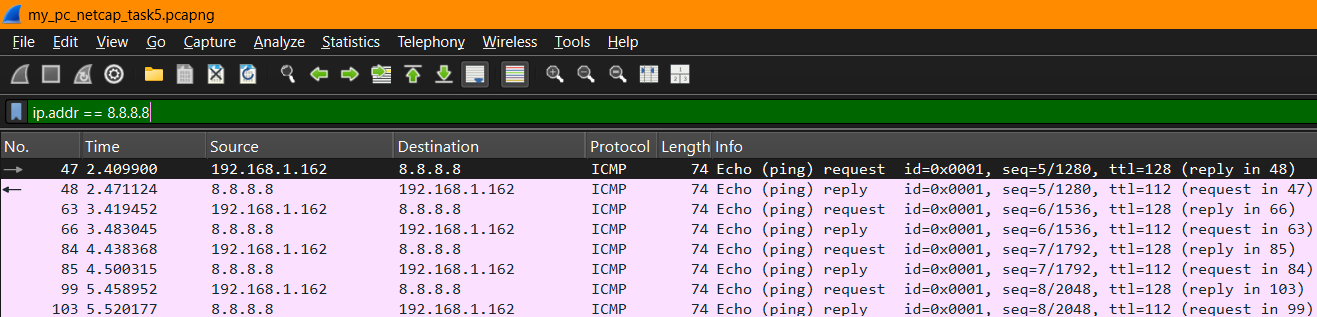


Figure 1 - ICMP Ping packets captured in Wireshark

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2 - Analysing packet 47 of ICMP reply in Wireshark

The red line indicates information to look for ICMP packet 47. ICMP used for network diagnostics and error reporting, not data transfer. It's essential for tools like ping and traceroute.

ICMP Process Example: ping Command

1. You type ping google.com
2. DNS resolves google.com to an IP address.
3. Your computer sends an ICMP Echo Request (Type 8) to that IP.
4. Google’s server replies with an ICMP Echo Reply (Type 0).
5. You see round-trip time (RTT), packet loss, etc.

DNS (Domin Name System) – Port 53

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 - DNS packets of personal computer captured in Wireshark

DNS (Domain Name System) plays a crucial role in packet transfer by translating human-readable domain names (like www.example.com) into IP addresses (like 93.184.216.34) that computers use to identify each other on the network.

**Summary of packet 8651 in figure 3**

**Field Value**

**Type** DNS Response

**Query** raw.githubusercontent.com (Type A)

**Response IPs** 185.199.109.133, 110.133, 108.133, 111.133

**TTL** 2427 seconds

**Error Code** No error (rcode: 0)

**Source** 192.168.1.1 (DNS server)

**Destination** 192.168.1.162 (your computer)

TCP/TLS (Transmission Control Protocol / Transport Layer Security) and QUIC (Quick UDP Internet Connection) – Port 443

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 - TCP packets captured in Wireshark

TCP provides a reliable connection before encryption by TLS.

**TCP Key Functions:**

* 3-Way Handshake: Client → Server: SYN Server → Client: SYN-ACK Client → Server: ACK
* Segmentation & Reassembly
* Error Detection
* Flow Control & Retransmission

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5 - TSL packet capture in Wireshark

As per Wireshark packet capture in figure 5:

1. TCP Handshake:

* SYN, SYN-ACK, ACK packets

1. TLS Handshake (over TCP):

* Client Hello
* Server Hello
* Certificate, Key Exchange, etc.

1. Encrypted Data:

* After the handshake, packets are marked as **"Application Data"**, and payload is encrypted

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6 - QUIC packet capture in Wireshark

**Summary of the Packet 427 in figure 6**

* Protocol: QUIC
* QUIC Version: IETF QUIC v1 (RFC 9000)
* Port: 443 (HTTPS)
* Source IP: Server (2404:6800:4009:80c::200a)
* Destination IP: Client (2409:40c1:3084:8612:...)
* QUIC Packet Type: Initial
* Payload: Contains TLS 1.3 Server Hello inside a CRYPTO frame
* Packet Number: 5
* Frame Length: 1292 bytes
* Encrypted? Yes (partially visible due to decryption support)

QUIC operates at the **Transport Layer**, just like TCP, **but it includes TLS inside itself** — unlike TCP, which layers TLS separately.

**ARP (Address Resolution Protocol)**

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7 - ARP packet capture in Wireshark

ARP bridges the **Internet Layer** (IP addresses) with the **Link Layer** (MAC addresses) on local networks.

**ARP Packet Analysis (Frame 9)**

**Ethernet Layer**

* Source MAC: 3c:ef:8c:05:3e:93 (ZhejiangDahu device)
* Destination MAC: ff:ff:ff:ff:ff:ff → Broadcast
* Type: 0x0806 (ARP)

**ARP Packet Details**

* Opcode: 1 → Request Sender
* MAC: 3c:ef:8c:05:3e:93
* Sender IP: 192.168.1.221
* Target MAC: 00:00:00:00:00:00 (Unknown – that's why it's a request)
* Target IP: 192.168.1.222

**Meaning**

The device at IP 192.168.1.221 is asking: “Who has IP address 192.168.1.222? Tell me (192.168.1.221).”

This is the core function of ARP — mapping an IP to its corresponding MAC address on the local subnet.

**TCP/IP Model Overview**

1. **Application Layer -** Interface with user apps (what you use)

* Protocol - HTTP, DNS, FTP, TLS, QUIC

1. **Transport -** Ensures delivery and flow control

* TCP, UDP, QUIC

1. **Internet -** Logical addressing and routing

* IP (IPv4/IPv6), ICMP

1. **Network Access** - Physical transmission of data on link

* Ethernet, Wi-Fi, ARP