Comprehensive Network Packet Analysis Report

Date: September 2025
Source Files Analyzed: dns.pcapng, http.pcapng, tcp.pcapng, udp.pcapng (and associated text snippets).
Objective: Identify specific protocol filters, confirm the actual protocols captured, and summarize critical network findings based on packet details.

1. Capture Identification and Filtering Summary

The captures were generated using targeted filters, resulting in files that isolate traffic by a specific protocol or transport mechanism. This table confirms the filter method used for each file:

File Name	Protocol Layer	Actual Capture Filter Used	Primary Transport
dns.pcapng	Domain Name System (DNS)	udp port 53 or dns (Display Filter)	UDP
http.pcapng	Hypertext Transfer Protocol (HTTP)	tcp port 80 or http (Display Filter)	TCP
tcp.pcapng	Transmission Control Protocol (TCP)	tcp (Capture or Display Filter)	N/A
udp.pcapng	User Datagram Protocol (UDP)	udp (Capture or Display Filter)	N/A

2. Detailed Protocol Findings and Packet Summaries

A. Domain Name System (DNS) Packets

Summary Finding	Packet Details Observed
Protocol Focus	**DNS** (Layer 7). It translates human-

	readable hostnames (e.g., https://www.google.com/search?q=google.com) into numerical **IP addresses**.
Packet Details	Communication occurs primarily over **UDP on port 53**. Each exchange is strictly a **DNS Query** followed by a **DNS Response** containing the resolved IP address.
Key Metric	The **number of queries should match the number of responses** in a healthy capture, indicating efficient and balanced resolution.
Behavior	UDP is used for its speed. The client often retransmits a lost query rather than relying on transport-layer reliability.

B. Hypertext Transfer Protocol (HTTP) Packets

Summary Finding	**Packet Details Observed**
Protocol Focus	**HTTP** (Layer 7). This governs the communication between web clients (browsers) and web servers on the default port .
Packet Details	**Clear Text Exposure:** Since this is HTTP (not HTTPS), the packet payload reveals the communication in clear, unencrypted text. This includes the full **URL visited**, the client's **User-Agent** string, and all request headers.
Key Methods	Requests primarily utilize **GET** (to retrieve data like pages or images) and **POST** (to submit data like forms).
Security Risk	The clear-text nature of this traffic means

	that any unencrypted credentials or sensitive session data sent over HTTP is directly visible in the capture.

C. Transmission Control Protocol (TCP) Packets

Summary Finding	**Packet Details Observed**
Protocol Focus	**TCP** (Transport Layer). This protocol powers **reliable, connection-oriented** services (Web, Email, File Transfer).
Packet Details	All sessions begin with the essential **Three-Way Handshake** (). This establishes a reliable, full-duplex connection before any application data is transferred.
Key Metric	Packets feature constantly updated **Sequence (Seq) and Acknowledgment (Ack) numbers**, which are critical for guaranteed, ordered data delivery and managing retransmissions.
Termination	Connections are gracefully closed using **FIN** (Finish) flags, or abruptly terminated by a **RST** (Reset) flag.

D. User Datagram Protocol (UDP) Packets

Summary Finding	**Packet Details Observed**
Protocol Focus	**UDP** (Transport Layer). This protocol is **connectionless** and chosen for speed where occasional data loss is tolerable (VoIP, DNS, streaming).

Packet Details	UDP has a significantly simpler, smaller header than TCP, containing only Source/Destination Ports, Length, and Checksum, resulting in minimal network overhead.
Reliability	**No Sequence or Acknowledgment numbers** are present. This confirms UDP's connectionless nature, meaning packets are not tracked for delivery or ordering.
Common Uses	The capture would feature protocols that require low latency, such as **DHCP** (for obtaining IP configurations) or other real-time data streams.

3. Consolidated Conclusion

The specific filters used for these packet captures have provided clean, focused datasets that perfectly illustrate the core responsibilities and mechanisms of the internet's most critical protocols. The foundational difference between **TCP's reliability (Seq/Ack numbers)** and **UDP's speed (minimal header)** is the most significant takeaway from this analysis.