

**HTTP (HyperText Transfer Protocol) Traffic**

This screenshot shows captured **HTTP traffic**, which is used for transmitting web pages and data over the internet. The packets displayed represent communication between a client (typically a browser) and a web server. The captured packets show details like the request method (e.g., GET), the requested resource (e.g., /index.html), and response codes (e.g., 200 OK). HTTP typically operates over **TCP port 80** and is not encrypted, so packet contents like URLs and headers are visible in plain text.

A screenshot of a computer

AI-generated content may be incorrect.

**DNS (Domain Name System) Traffic**

This screenshot captures **DNS query and response packets**, which are used to resolve human-readable domain names (e.g., google.com) into IP addresses (e.g., 142.250.190.78). The DNS protocol typically uses **UDP port 53**, though TCP may be used for larger responses. The packet details include the query name, query type (e.g., A, AAAA), and the resolved IP address in the response. DNS is essential for accessing websites and other internet services.

A screenshot of a computer

AI-generated content may be incorrect.

**TCP (Transmission Control Protocol) Traffic**

This screenshot shows general **TCP traffic**, which provides a reliable, connection-oriented protocol used by many applications, including HTTP, FTP, and email. Each TCP packet includes a sequence number, acknowledgment number, source and destination ports, and flags (like SYN, ACK, FIN). The TCP handshake process (SYN, SYN-ACK, ACK) is also visible when a new connection is established. TCP ensures error-checked, ordered delivery of data across networks.

**Interesting Observations from Packet Capture**

**IP Addresses Observed**

The capture revealed multiple IP addresses communicating over the network. These include:

* **Source IPs** (originating the requests)
* **Destination IPs** (receiving/responding)

These IPs help identify which devices or domains were involved in the communication.

**Ports Identified**

Commonly used ports observed during the capture:

* **TCP Port 80** – Used for HTTP traffic
* **UDP Port 53** – Used for DNS queries
* **Random high-numbered ports** – Used as ephemeral source ports

**Interesting Packets**

Below are some noteworthy observations from the traffic:

1. **DNS Query**:  
   A DNS request was made to resolve a domain name (e.g., www.example.com).  
   The response returned an IP address (e.g., 93.184.216.34).
2. **HTTP Request**:  
   An HTTP GET request was captured showing the URI path and Host header, revealing the exact resource the client tried to access (e.g., /index.html on example.com).
3. **TCP Handshake**:  
   The standard **three-way handshake** (SYN → SYN-ACK → ACK) was observed, indicating a new TCP connection was successfully established.



