**Network Packet Analysis Report**

**1. TCP (Transmission Control Protocol)**

* TCP is one of the core protocols of the Internet Protocol Suite. It ensures reliable, ordered, and error-checked delivery of data between applications.
* Used by most applications that require guaranteed data delivery—e.g., web browsing (HTTP/HTTPS), file transfers (FTP), emails (SMTP, IMAP), and more.
* **Connection-oriented**: Establishes a session with a 3-way handshake (SYN, SYN-ACK, ACK).
* **Reliable**: Retransmits lost packets, maintains order.
* **Port-based**: Communicates using port numbers (e.g., port 80 for HTTP, port 443 for HTTPS).
* **Observed Behavior**: In the capture, TCP was used as the transport layer for HTTP and possibly HTTPS traffic.

**2. HTTP (Hypertext Transfer Protocol)**

* HTTP is the foundation of any data exchange on the Web and is a protocol used for transmitting hypermedia documents, such as HTML.
* Used in browsers and web servers for accessing web pages and APIs over port 80 (unsecured).
* **Text-based protocol**: Easy to read and debug.
* **Request/Response model**: Clients send requests (GET, POST), servers respond with headers and content.
* **Limitations**: Does not include encryption (unlike HTTPS).
* **Observed Behavior**: HTTP GET requests and responses were visible in plaintext during website access.

**3. DNS (Domain Name System)**

* DNS translates human-readable domain names into machine-readable IP addresses .
* Every time a domain is accessed, a DNS query is made. This is a critical first step in most web connections.
* **Protocol type**: Application layer, typically uses UDP on port 53.
* **Query types**: A (IPv4), AAAA (IPv6), MX (mail), CNAME, etc.
* **Fast and lightweight**: Designed for quick lookups.
* **Observed Behavior**: DNS queries for domains like example.com or google.com, followed by corresponding responses with IP addresses

**Summary of Findings**

* Protocols Identified: TCP, HTTP, DNS
* Traffic Behavior:
  + DNS queries occurred prior to any web access.
  + TCP 3-way handshake established connection sessions.
  + HTTP traffic followed with actual web page data requests.

**Security Considerations**

* DNS and HTTP traffic are unencrypted; they can be observed and manipulated unless secured (e.g., DNS over HTTPS, HTTPS).
* TCP is reliable but can be exploited (e.g., SYN flood attacks) if not protected with firewalls or rate limiting.

**Conclusion**

This packet capture exercise illustrates how fundamental protocols—DNS, TCP, and HTTP—work together to enable basic web functionality. Understanding these protocols is crucial for network troubleshooting, security monitoring, and performance optimization.