Wireshark Packet Analysis Report

1. Objective

To capture live network traffic, identify multiple protocols, and analyze packet details to improve protocol awareness.

2. Steps Performed

1. Installed Wireshark from the official website.
2. Launched Wireshark and selected the active network interface (Wi-Fi / Ethernet).
3. Started packet capture.
4. Generated traffic by visiting websites and running 'ping google.com'.
5. Stopped capture after 1 minute.
6. Applied filters: http, dns, tcp.
7. Identified at least three protocols.
8. Saved capture file as .pcap.
9. Summarized findings.

3. Protocols Identified

Protocol	Purpose	Observation
DNS	Resolves domain names to IP addresses	Multiple DNS queries to 8.8.8.8 and local DNS server
HTTP	Web page data transfer	GET requests to websites visited
TCP	Reliable data transport	Established sessions for HTTP communication
ARP	Address resolution in LAN	Broadcast requests to map IP to MAC address

4. Sample Packet Details

Time (s)	Source IP	Destination IP	Protocol	Length	Info
0.125	10.244.135.195	8.8.8.8	DNS	74	Standard query A google.com
0.432	10.244.135.195	142.250.183.14	TCP	66	TCP handshake SYN
0.678	10.244.135.195	142.250.183.14	HTTP	517	GET /index.html HTTP/1.1

Wireshark Packet Analysis Report

5. Findings & Insights

- The majority of captured packets were TCP due to web browsing activity.
- DNS lookups preceded most HTTP requests, showing name resolution before data transfer.
- ARP traffic appeared locally to maintain device communication on the LAN.
- No suspicious or malformed packets detected during this capture.

6. Outcome

Successfully:

- Captured live network traffic
- Filtered packets by protocol
- Identified 3+ protocols
- Gained practical packet analysis skills