Wireshark Capture Summary – Example with google.com

#	Protocol	Source IP	Destination IP	Description
1	DNS	192.168.1.5	8.8.8.8	Query for google.com
2	DNS	8.8.8.8	192.168.1.5	Response: google.com → 142.250.183.110
3	TCP (SYN)	192.168.1.5	142.250.183.110	Connection initiation to Google web server (port 443)
4	TCP (SYN-ACK)	142.250.183.110	192.168.1.5	Server acknowledges connection request
5	TCP (ACK)	192.168.1.5	142.250.183.110	Connection established
6	TLSv1.3	192.168.1.5	142.250.183.110	Client Hello (begin HTTPS handshake)
7	TLSv1.3	142.250.183.110	192.168.1.5	Server Hello + Certificate
8	ICMP	192.168.1.5	142.250.183.110	Echo request (ping google.com)
9	ICMP	142.250.183.110	192.168.1.5	Echo reply from google.com

Overall Findings:
- **Capture Duration:** 1 minute
- **Total Packets Captured:** ~1,500
- **Protocols Observed:** DNS, TCP, TLS, ICMP
- **Notable Activity:**
• DNS resolution of google.com via Google DNS server (8.8.8.8)
• TCP three-way handshake with Google server (port 443 – HTTPS)
• TLS 1.3 handshake establishing encrypted session
• ICMP packets showing successful ping replies from Google server