Practical 8: To analyze network traffic using Wireshark – Capture and Study TCP and UDP Packets

Objectives

1. Capture and analyze TCP and UDP packets using Wireshark.
2. Identify and interpret key fields in the TCP segment and UDP datagram headers.

Lab Task

Task 1: Generate UDP Packet using DNS and Analyze It

1. Open Wireshark and start capturing on the active network interface.
2. Flush the DNS cache to ensure fresh DNS queries:
   - **Windows:** `ipconfig /flushdns`
   - **Linux:** `sudo systemd-resolve -flush-caches` or `sudo service nscd restart`
   - **macOS:** `sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder`
3. Generate DNS A-record queries:
   - **Windows:** `nslookup -type=A www.google.com 8.8.8.8`
   - **Linux:** `dig +short A www.google.com @8.8.8.8`
   - **macOS:** `dig +short A www.google.com @1.1.1.1`
4. Analyze DNS over UDP:
   (a) Extract the hexadecimal dump of any captured UDP packet carrying a DNS query or response.
   (b) Prepare the **UDP datagram header** using the extracted hex dump.
   (c) Fill the **UDP Packet Analysis Table (Table 1)** in this exercise with the observed values.

Task 2: Generate TCP Packet using Web Browsing and Analyze It

1. Open Wireshark and start capturing on the active network interface.
2. Surf any website using a web browser to generate TCP traffic.
3. Extract the hexadecimal dump of any captured TCP segment.
4. Prepare the **TCP segment header** using the extracted hex dump and fill the **TCP Packet Analysis Table (Table 2)**.

Observation and Analysis

UDP Part

Table 1: UDP Packet Analysis

1	**a.** Source port number: **b.** Destination port number: **c.** Total length of UDP datagram: **d.** Length of data: **e.** Is the packet from client or server? **f.** Application-layer protocol: **g.** Is checksum calculated?
2	Are answers in No. 1 verified by the information in the detail pane?
3	Source and destination IP addresses in the query message: Source and destination IP addresses in the response message: Relation between IP addresses:
4	Source and destination port number in the query message: Source and destination port number in the response message: Relation between port numbers: Which port number is well-known?
5	Length of the first UDP packet: How many bytes of payload are carried by the first UDP packet?
6	Number of bytes in the DNS message: Does the count agree with the answer to question 5?
7	Is the checksum calculated for the first UDP packet? Value of the checksum:

TCP Part — General

Table 2: TCP Packet Analysis

1	**a.** Source port number: **b.** Destination port number: **c.** Sequence number: **d.** Acknowledgment number: **e.** Header length: **f.** Set flags: **g.** Window size: **h.** Urgent pointer:
2	Are answers in question 1 verified by the information in the detail pane?

Submission Requirements

1. Screenshot of captured **UDP (DNS)** packets in Wireshark.
2. Screenshot of captured **TCP (HTTP)** packets in Wireshark.
3. Prepare **UDP datagram header in hexadecimal format.**
4. Prepare **TCP segment header in hexadecimal format.**
5. Attach the completed UDP and TCP analysis tables with values filled from Wireshark.