Lab Session 1: Wireshark

Objective: Capture, filter, and interpret basic network traffic, connecting it to the concepts learned in class.

0. Wrap-Up Report

- During the lab, write your answer in a short report (1-2 pages max) in addition to:
  - One example each of ARP, DHCP, DNS, and TCP packets from your capture.
  - Key extracted details (MAC, IP, mask/prefix, ports, etc.).
  - A simple diagram of a captured packet showing its PDU structure.
  - One TCP stream you isolated and explain the synchronization process.

1. Setup

- Open **Wireshark**.
- Identify the correct network interface to capture traffic.
- Quick interface overview:
  - Capture Interfaces List: select where to capture.
  - Start / Stop / Clear buttons.
  - Packet list (top), packet details (bottom left), hex view (bottom right).

2. First Capture and Observation

- Start capturing on the active network interface.
- Open a browser and visit a simple webpage (e.g., `http://httpforever.com/`).
- Stop the capture.

Questions:

- Which protocols appear in your capture? (DNS, TCP, HTTP...)
- Locate a DNS packet:
  - What domain name is being queried?
  - What IP address is returned?
- Locate a TCP packet:

  - What are the source and destination ports?

3. ARP and DHCP Analysis

- **ARP – Address Resolution Protocol**
  - Clear your ARP cache:
    - Windows: `arp -d`
    - Linux: `ip neigh flush all`
  - Start capturing and ping another host on the same LAN.
  - Identify the ARP **request** and **reply**.

  Questions:
  - What MAC address corresponds to the target IP?
  - At which OSI layer does ARP operate?
- **DHCP – Dynamic Host Configuration Protocol**
  - Disable and re-enable your network interface (or run `ipconfig /renew`).
  - Capture the Discover → Offer → Request → ACK sequence.

  Questions:
  - What IP address was assigned to your machine?
  - What subnet mask and gateway were provided?

4. IPv4 and IPv6 Filtering

- Apply filters in Wireshark:
  - IPv4: `ip`
  - IPv6: `ipv6`

IPv4:

- Identify the source and destination IPs.
- From your machine's configuration or DHCP, find the subnet mask.
- Determine the broadcast address.

IPv6:

- Identify the IPv6 address and its prefix length.
- Observe if multicast addresses appear in the capture.

5. PDU Layer Analysis

- Select a TCP or UDP packet.
- Expand the headers: Ethernet → IP → TCP/UDP → Application.

Tasks:

- Note the source and destination MAC addresses.
- Note the source and destination IP addresses.
- Note the source and destination ports.
- Identify any application-layer data (e.g., HTTP request).

Checkpoint: Call the lab supervisor and show your findings.

6. Display Filter Practice

- Essay different display filters by:
  - IP address (source, destination, any).
  - TCP/UDP ports (e.g., HTTP, DNS).
  - Specific protocol fields (e.g., DNS queries only, ARP requests).
  - Combining conditions (AND, OR, NOT).

Questions:

- How would you filter only packets sent *to* your default gateway?
- How could you display only the first packet of a TCP connection?
- Write a filter to see DNS queries *from* your machine only.

7. Capture vs Display Filters

- Start a capture with a *capture filter* (e.g., only DNS, only your host, only your subnet).
- Compare the results to using a display filter on a full capture.

Questions:

- What changes when you use a capture filter instead of a display filter?
- Give one case where a capture filter would be the better choice.

8. TCP 3-Way Handshake and Stream Isolation

- Open a simple HTTP-only website (no HTTPS).

- Apply the display filter: `tcp.flags.syn == 1 || tcp.flags.ack == 1`.
- Look for a pattern of three packets: one from your computer, one from the server, then another from your computer.
- Right-click on one of these packets → `Follow` → `TCP Stream`.
- Use the filter `tcp.stream ==` *N* (replace *N* with the stream number) to see only that conversation.

Questions:

- How many packets are exchanged before any web page content is sent?
- Can you guess/recall why these packet exist in TCP?
- After these first packets, what type of information starts to appear in the stream?

9. Using Wireshark Statistics Panels

- `Statistics` → `Protocol Hierarchy`: identify dominant protocols.
- `Statistics` → `Conversations`: sort by bytes/packets, find top talkers.

Tasks:

- Export a screenshot of the Protocol Hierarchy and describe it.
- Identify the top 2 conversations by bytes.