Task5 – Elevate Labs Cyber Security Internship

Ahmad Ghraieb

**Wireshark:**

**Wireshark** is a free, open-source **network protocol analyzer**. It is the world's leading tool of its kind, allowing users to **capture and interactively inspect** the data traffic running on a computer network.

It works by capturing data packets traveling across a network interface (like Ethernet or Wi-Fi) and displaying the raw traffic in a human-readable format. This allows for deep inspection of network communications at the packet level.

**Key Uses of Wireshark**

Wireshark is an essential tool for:

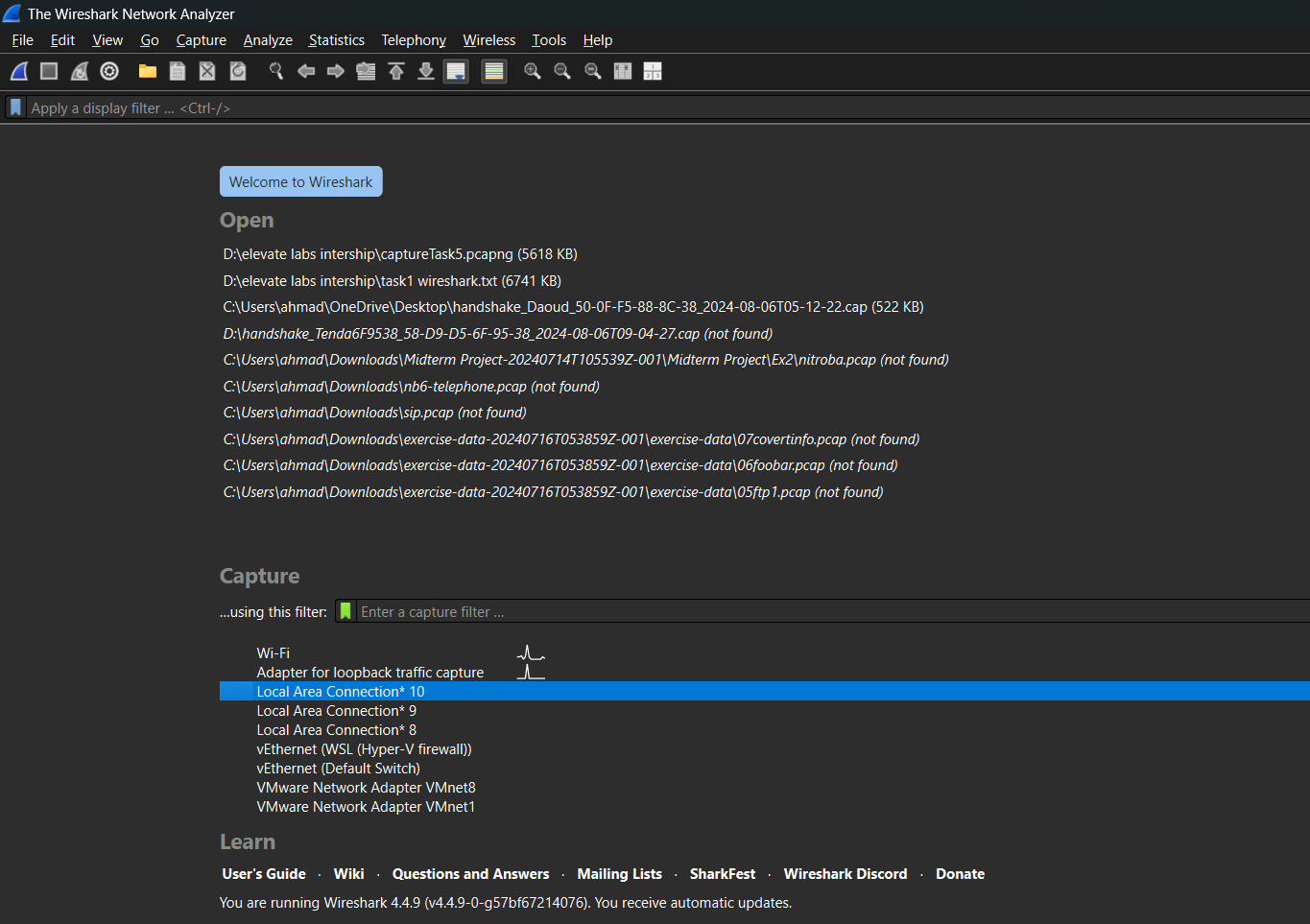
* **Network Troubleshooting:** Diagnosing issues like slow performance, connectivity problems, latency, and packet loss.
* **Security Analysis:** Detecting suspicious activity, investigating security breaches, and analyzing potential threats by examining communication patterns.
* **Protocol Development:** Debugging new network protocols or applications by observing their real-time network behavior.
* **Education and Training:** Providing a visual and detailed way for students and professionals to learn about network protocols and operations.

**Key Features**

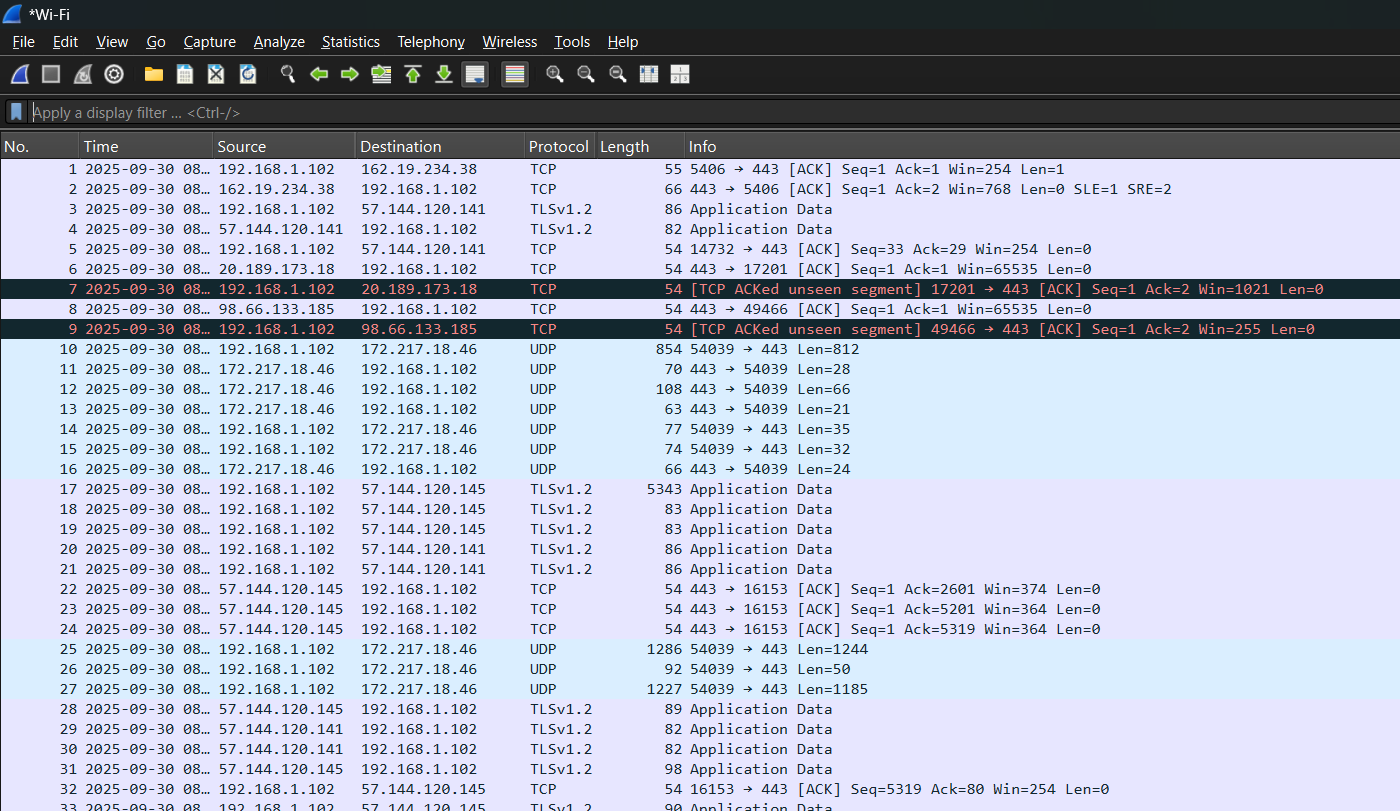
Wireshark offers a rich feature set, including:

* **Real-time Packet Capture and Offline Analysis:** It can capture live traffic or analyze saved packet capture files (PCAP).
* **Deep Protocol Support:** It recognizes and dissects thousands of protocols (e.g., TCP/IP, HTTP, DNS).
* **Filtering:** Powerful display filters allow users to isolate specific packets, sessions, or protocols for targeted analysis.
* **Cross-platform Compatibility:** It is available for Windows, macOS, Linux, and various other operating systems.
* **Visualization Tools:** It can generate statistics, graphs, and flow diagrams to help visualize network performance.

This is the initial interface after opening the app



Here is the display after adapter selection and start capturing



**Key Interface Components and Usage**

The main interface is typically divided into three main panes:

1. **Packet List Pane (The largest part visible in the image):** This pane displays a summary of each captured packet.
   * **Usage:** It provides a quick overview, including:
     + **No.**: The packet number.
     + **Time**: Timestamp of the capture.
     + **Source** and **Destination**: IP addresses or MAC addresses.
     + **Protocol**: The protocol used (e.g., TCP, UDP, TLSv1.2).
     + **Length**: The size of the packet in bytes.
     + **Info**: A concise summary of the packet's contents or status (e.g., ACK, SYN, Application Data, retransmitted).
2. **Display Filter Toolbar (Top, below the menus):** The field labeled "**Apply a display filter...**" is where users can enter filters to narrow down the visible packets based on criteria like protocol, source/destination, or specific data fields.
   * **Usage:** Essential for analyzing large captures by filtering out irrelevant traffic (e.g., typing tcp.port == 80 to see only HTTP traffic).
3. **Menus and Toolbars (Top):** Provide access to all Wireshark functions.
   * **File:** Open, save, and merge capture files.
   * **Edit:** Find packets, set time references, and manage profiles.
   * **View:** Control the display of the main window components.
   * **Go:** Navigate between packets.
   * **Capture:** Start, stop, and configure packet capture settings.
   * **Analyze:** Apply display filters, enable/disable protocols, and analyze expert information.
   * **Statistics:** Generate various statistics and summaries of the captured data.
   * **Telephony/Wireless/Tools/Help:** Other specialized functions.

**Capabilities and Functions**

Wireshark's core capabilities enable a wide range of network analyses:

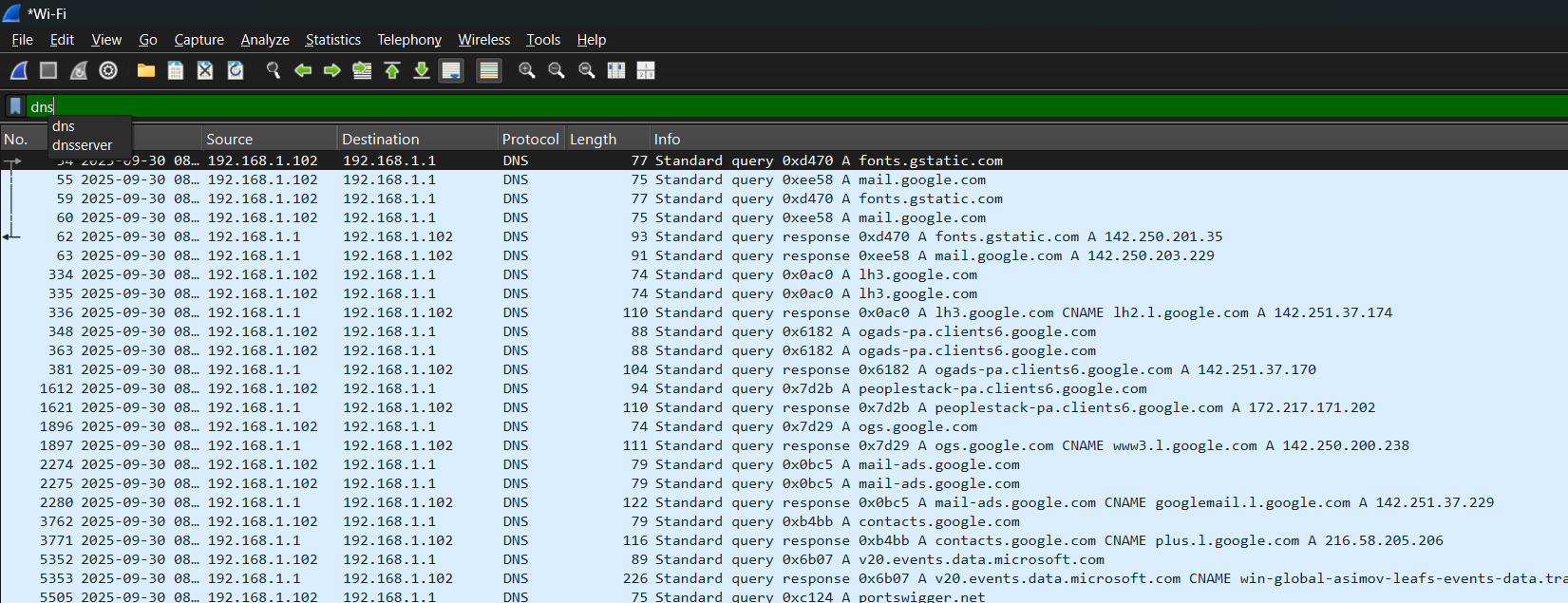
* **Troubleshooting:** Diagnosing network problems like latency, packet loss, connection issues (e.g., the highlighted packet shows TCP ACKed unseen segment indicating potential flow control or reordering issues).
* **Security Analysis:** Inspecting network traffic for suspicious activity, malware communication, or unauthorized data transfer.
* **Protocol Development:** Examining and debugging custom network protocols.
* **Performance Analysis:** Measuring network utilization, throughput, and response times.
* **Learning/Education:** Understanding how network protocols (TCP, IP, UDP, etc.) and applications (DNS, HTTP, TLS) work in real-time.
* **Deep Packet Inspection:** Viewing the actual data contents of a packet, often referred to as the **payload** (not fully visible in this image but available in the lower panes).

Using filters:

Filtering by DNS:

The **Domain Name System (DNS) protocol** acts as the **"phonebook of the internet."**

It is the core application-layer protocol responsible for **translating human-readable domain names** (like www.example.com) into the **numerical Internet Protocol (IP) addresses** (like 192.0.2.1) that computers use to locate and communicate with each other on the network. This translation is fundamental for web browsing, email, and other network services.



Filtering by TCP:

The **Transmission Control Protocol (TCP)** is a core, **connection-oriented** protocol in the Internet Protocol Suite (TCP/IP) that operates at the transport layer.

Its main function is to provide **reliable, ordered, and error-checked** delivery of data between applications on different devices. TCP achieves this reliability through mechanisms like the **three-way handshake** for connection establishment, **sequence numbers** for ordering packets, and **acknowledgments (ACKs)** with retransmission for handling lost data.

A screenshot of a computer

AI-generated content may be incorrect.

Filtering by UDP:

The **User Datagram Protocol (UDP)** is a **connectionless** transport layer protocol.

It's designed for speed and low overhead by sending data packets (**datagrams**) without first establishing a formal connection (no handshake) or guaranteeing delivery, order, or error-checking. This makes it ideal for **time-sensitive applications** like video streaming, online gaming, and DNS lookups, where speed is prioritized over absolute reliability.

A screenshot of a computer

AI-generated content may be incorrect.

Filtering by a specific ip:

A screenshot of a computer

AI-generated content may be incorrect.

Saving the capture as a pcap file for later examination

A screenshot of a computer

AI-generated content may be incorrect.

The task focuses on **using Wireshark** as part of the Cyber Security Internship. It introduces Wireshark as a free, open-source network protocol analyzer used for capturing and analyzing network traffic. The document explains its key uses, including **network troubleshooting, security analysis, protocol development, and education**. It also highlights main features like real-time and offline packet capture, filtering, protocol support, and visualization tools.

The report describes the **Wireshark interface** (packet list, filter toolbar, menus) and demonstrates filtering techniques for **DNS, TCP, UDP, and specific IPs**. Finally, it covers how to save captured traffic as a **PCAP file** for later analysis.