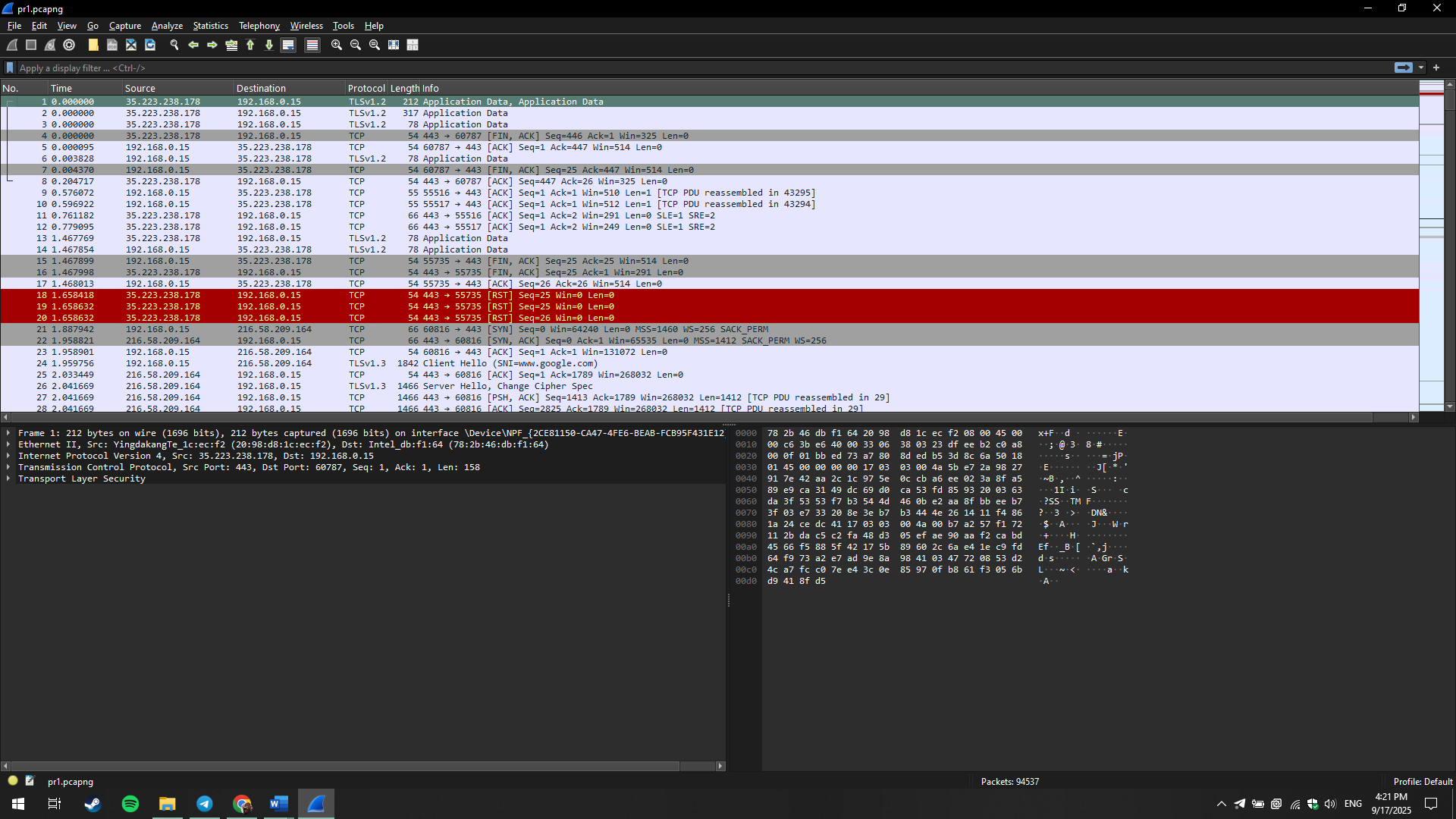
**Assignment 1**

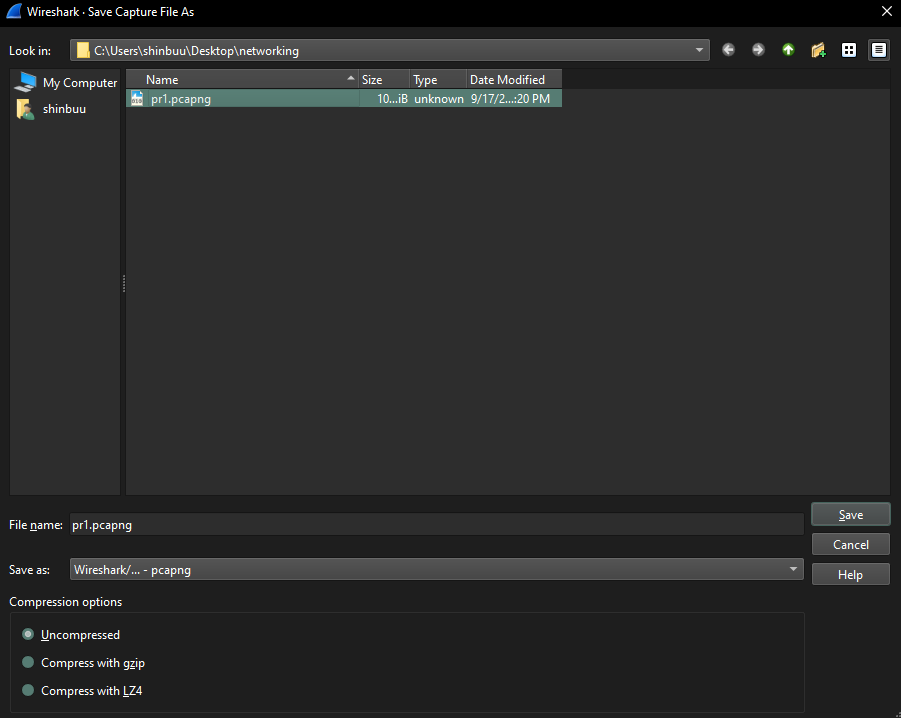
**Topic: Network Traffic Analysis: Packet Capture and Detection of Anomalies/Attacks**

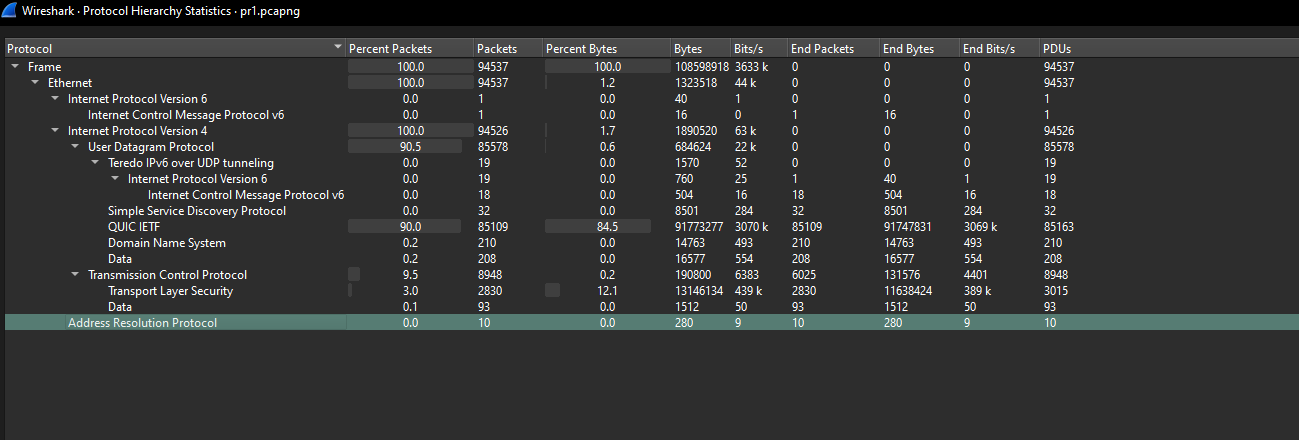
**Objective:**  
To gain hands-on experience in capturing and analyzing network traffic, identifying normal communication patterns, and detecting possible anomalies or malicious activities using professional tools.

**Tasks**

1. **Environment Setup**
   * Wireshark
2. **Traffic Capture**  
   Based on the data from the "Protocol Hierarchy Statistics", the percentage distribution of the main protocols in the traffic was determined:





1. **Protocol Analysis**  
   

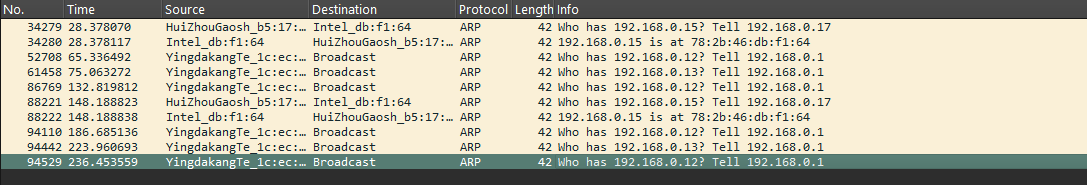
**QUIC IETF:** A modern protocol used to accelerate web traffic and provide a faster and more reliable connection. Its dominant position (90%) indicates that most of the traffic comes from modern web applications (e.g., Google Chrome).

**TCP (Transmission Control Protocol):** One of the fundamental Internet protocols that provides reliable and ordered data delivery. It is used for most standard web connections.

**TLSv1.3 (Transport Layer Security):** A security protocol that encrypts data transmitted over the network. It is used to protect the confidentiality of information, such as when browsing HTTPS sites.

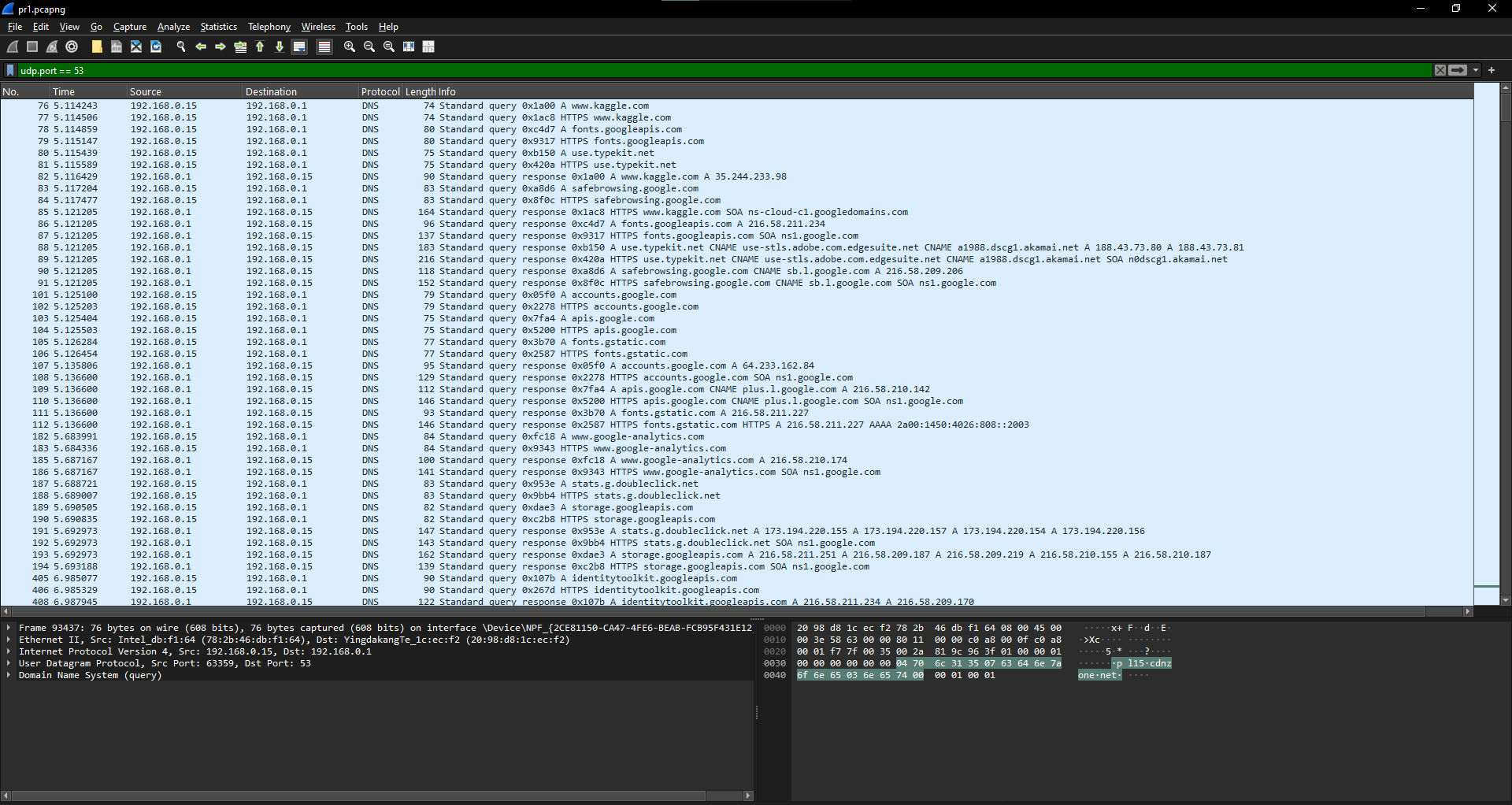
**DNS (Domain Name System):** A protocol that translates human-readable domain names (e.g., google.com) into machine-readable IP addresses, allowing computers to locate each other on the network.

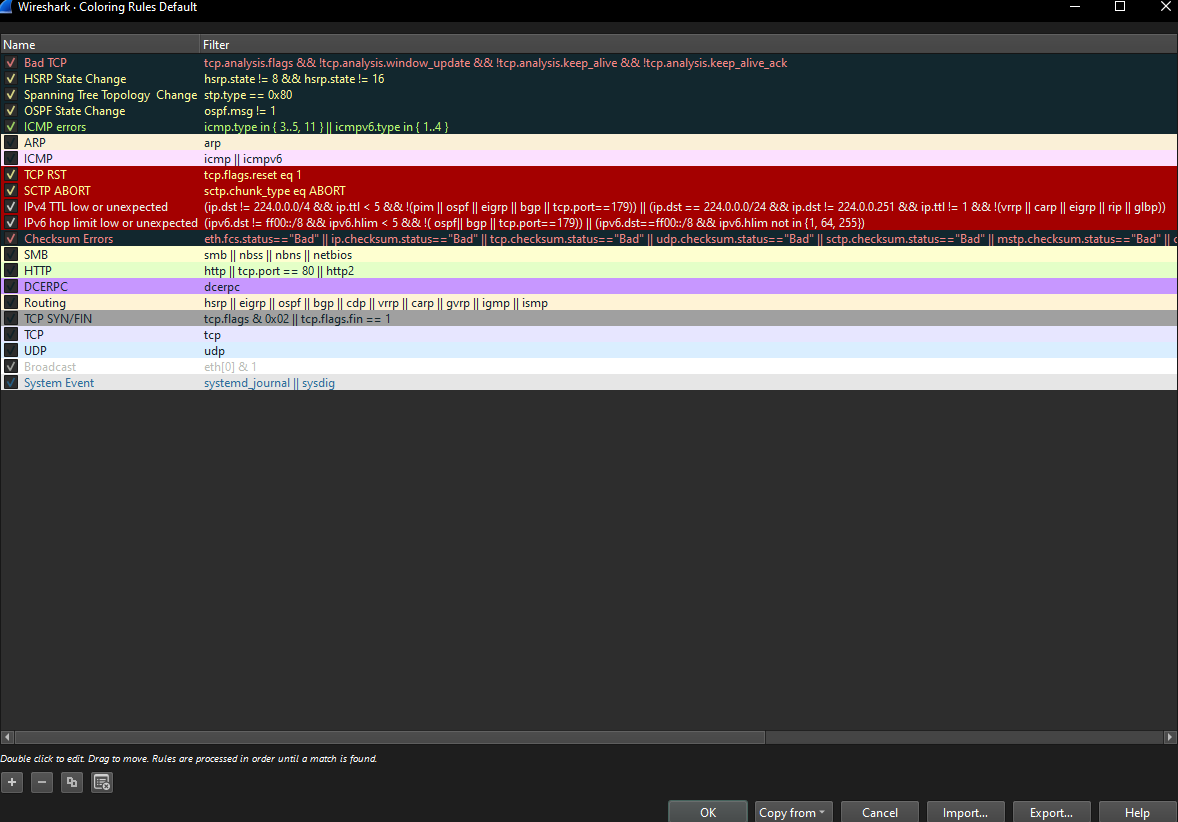
**ARP (Address Resolution Protocol):** A protocol used in a local network to map IP addresses to the MAC addresses of devices.

1. **Anomaly / Attack Detection**  
   

The screenshot with ARP traffic shows repeated requests from the same source (YingdakangTe\_1c:ec: Broadcast) to different IP addresses (192.168.0.12, 192.168.0.13, etc.). This behavior is suspicious and could be a sign of:

* **Network Scanning:** An attacker's attempt to gather information about the network topology.
* **ARP Spoofing:** Preparation for a "Man-in-the-Middle" attack, where the attacker tries to associate their MAC address with a gateway's IP address to intercept traffic.





The provided screenshot shows a list of packets with a focus on **TCP anomalies** highlighted by Wireshark's coloring rules. This indicates significant issues with the network connection's reliability.

**Key Observations:**

* **TCP Retransmissions:** Packets are being resent, which happens when the sender doesn't receive an acknowledgment for a previously sent packet within a set time. This is a clear sign of **packet loss**.
* **Duplicate Acknowledgements (Dup ACK):** The presence of multiple [TCP Dup ACK] flags means the receiver is repeatedly acknowledging the last successfully received in-order packet. This further confirms that one or more packets were lost or arrived out of order.
* **Out-of-Order Packets:** The [TCP Out-of-Order] flag indicates that a packet was received in an unexpected sequence. This can be a symptom of network congestion, unstable routing, or packet loss.

**Wireshark Coloring Rules:**

The coloring rules in Wireshark automatically highlight these issues, providing a visual cue for network analysis.

* **Red:** Marks **"Bad TCP"** traffic, including retransmissions, connection resets (RST), and other errors. This color indicates that something went wrong with the TCP session.
* **Black:** Used for packets with bad checksums, which means the data was corrupted during transmission.

**b) TCP Connection Issues**

The traffic contained packets with **[TCP Dup ACK]** (Duplicate Acknowledgement) and **[TCP Out-Of-Order]** (Out-of-Order) flags. These packets indicate **problems with connection reliability**, such as packet loss or out-of-order reception.

Additionally, a packet with **[TCP Retransmission]** was recorded, which confirms delivery issues: the sender retransmitted the packet because it did not receive an acknowledgment of its delivery. This could be caused by network congestion or high latency.

The network traffic analysis revealed both normal behavior and several anomalies that require attention. The presence of repeated ARP requests and TCP connection issues (retransmissions and Dup ACK) indicates potential vulnerabilities.

To improve network security, it is recommended to:

* **Use Intrusion Detection Systems (IDS)** to automatically monitor for suspicious traffic, such as mass ARP requests.
* Configure **static ARP entries** for critical devices to prevent ARP spoofing.
* Regularly update network device firmware and software to fix vulnerabilities.