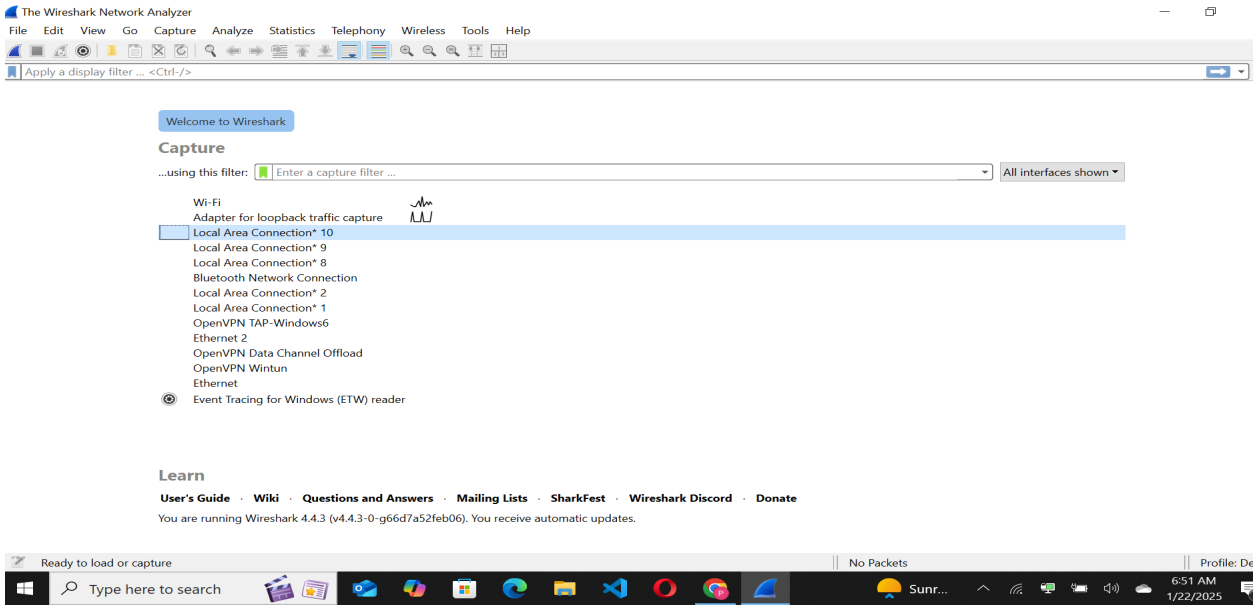
Report on Network Traffic Analysis Using Wireshark

1. Introduction

Network traffic analysis is essential for understanding how data flows within a network, diagnosing performance issues, and identifying potential security vulnerabilities. Wireshark is a powerful and widely used network protocol analyzer that allows for deep inspection of packets traversing a network.

2. Methodology

2.1. Setup:

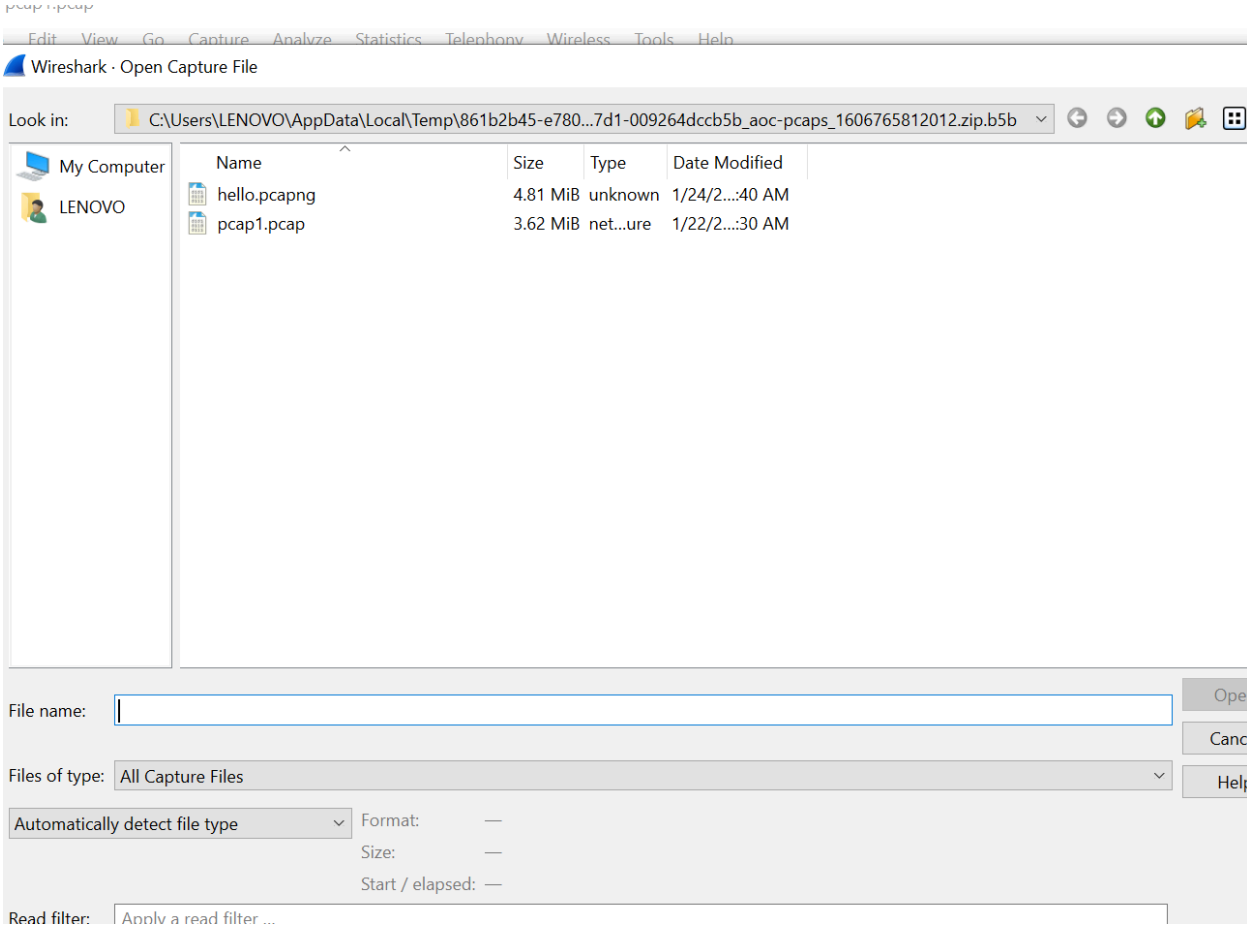
1. **Tool Used:** Wireshark
2. 

3. **Environment:** A standard local area network (LAN) with internet connectivity.
4. **Data Captured:** Network packets over a 10-minute period during regular office hours.
5. **Filters Applied:**
    - Captured traffic from all devices in the network.
    - Focused on TCP, UDP, HTTP, HTTPS, and DNS traffic.

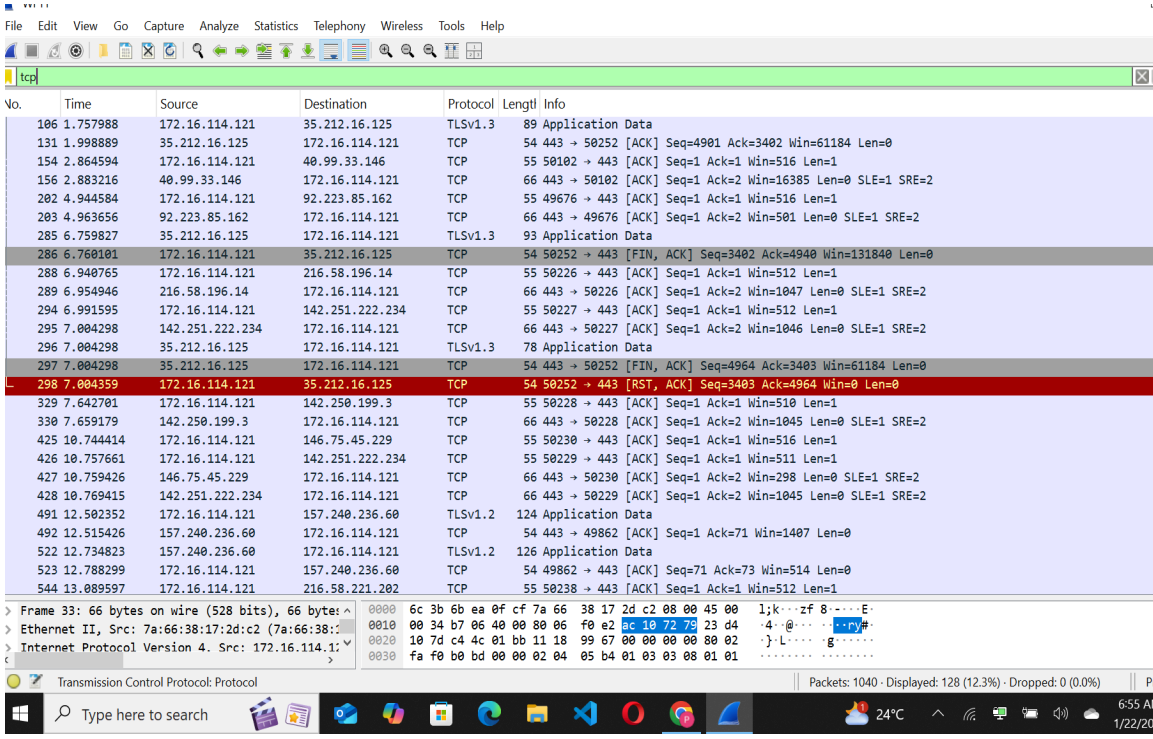
-

2.2. Procedure:

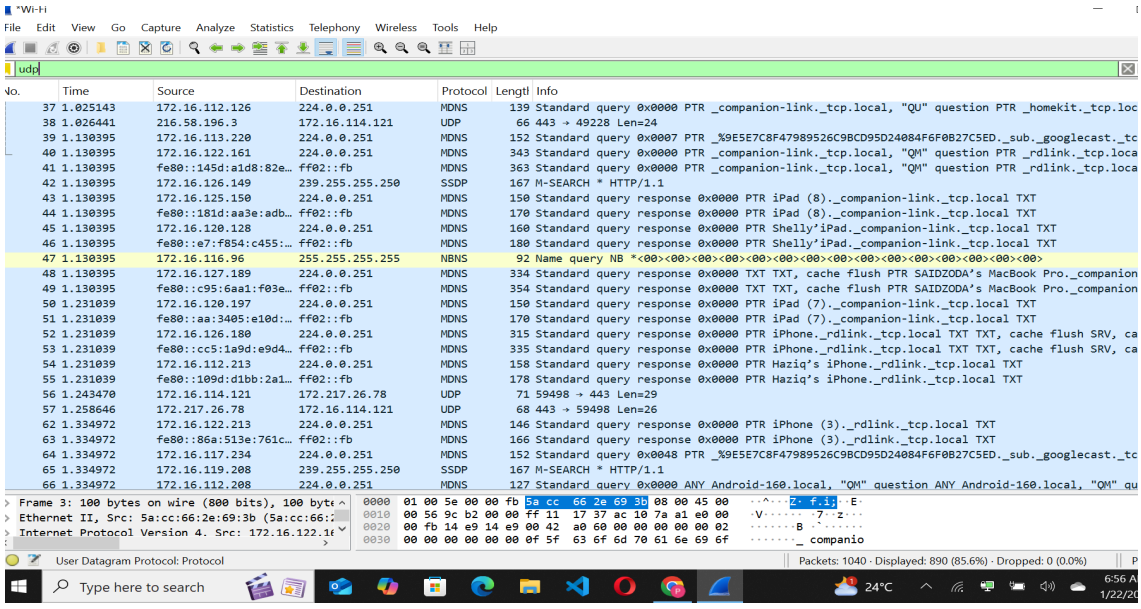
1. **Packet Capture:**
    - Wireshark was started, and a specific network interface wifi was selected for monitoring.
    - Captures were saved as hello.pcap and pcap1.pcap files for further analysis.



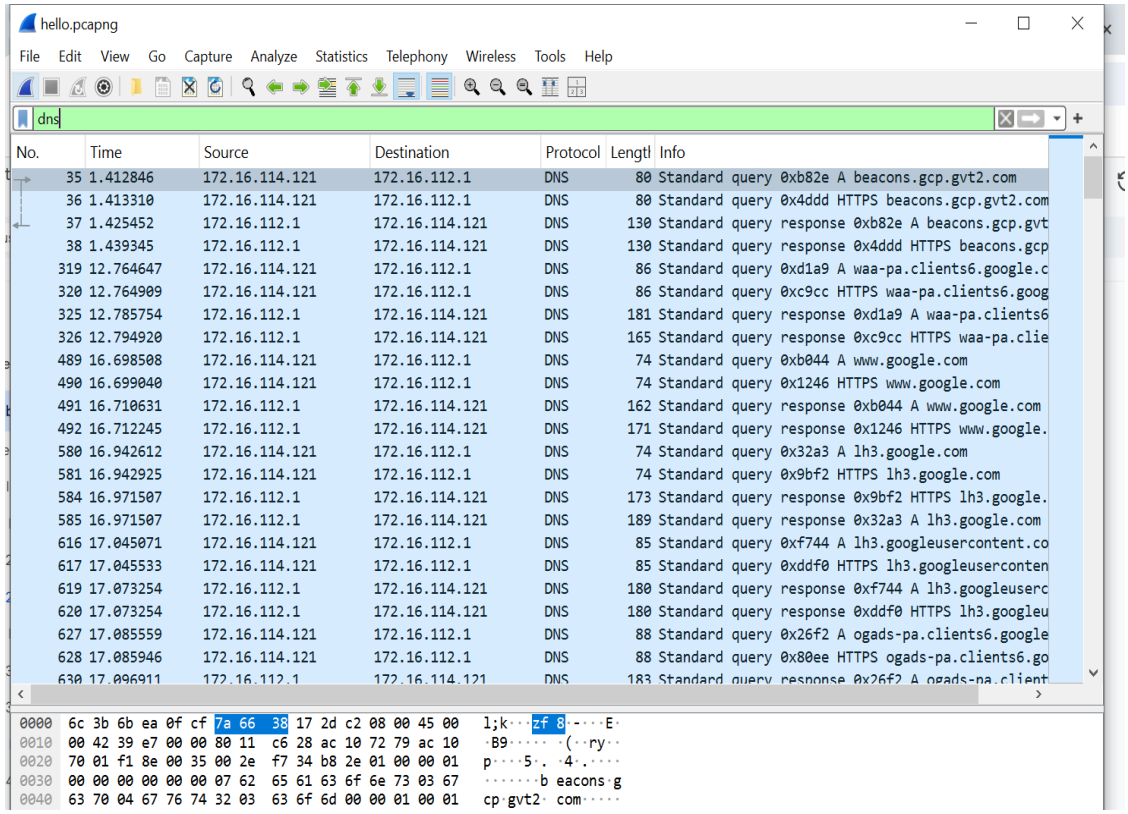
2. **Protocol Filtering:**
    - Applied filters to identify specific protocols:
        - tcp for Transmission Control Protocol.

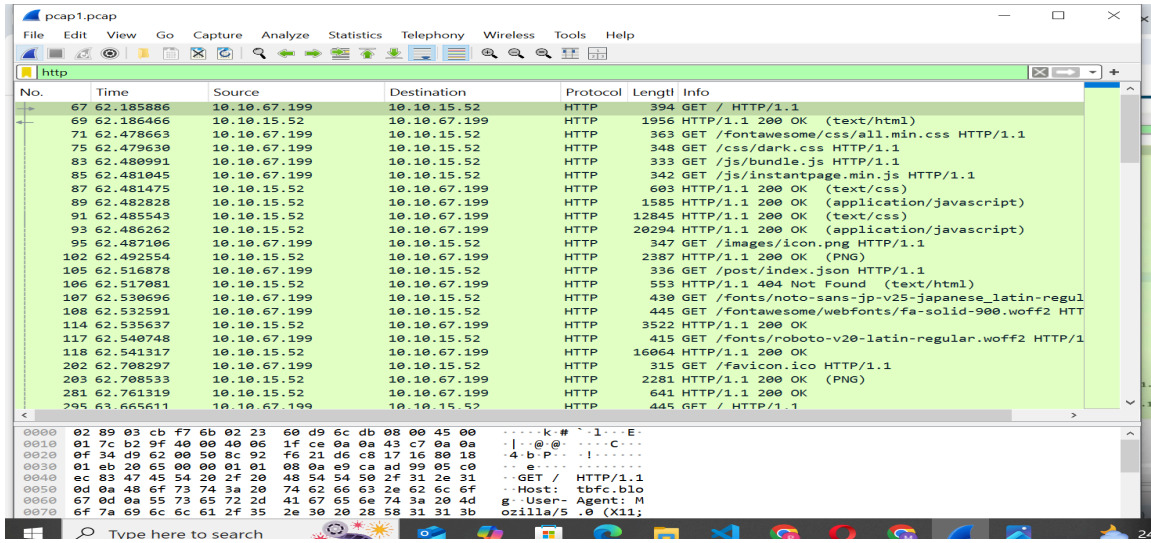


- udp for User Datagram Protocol.

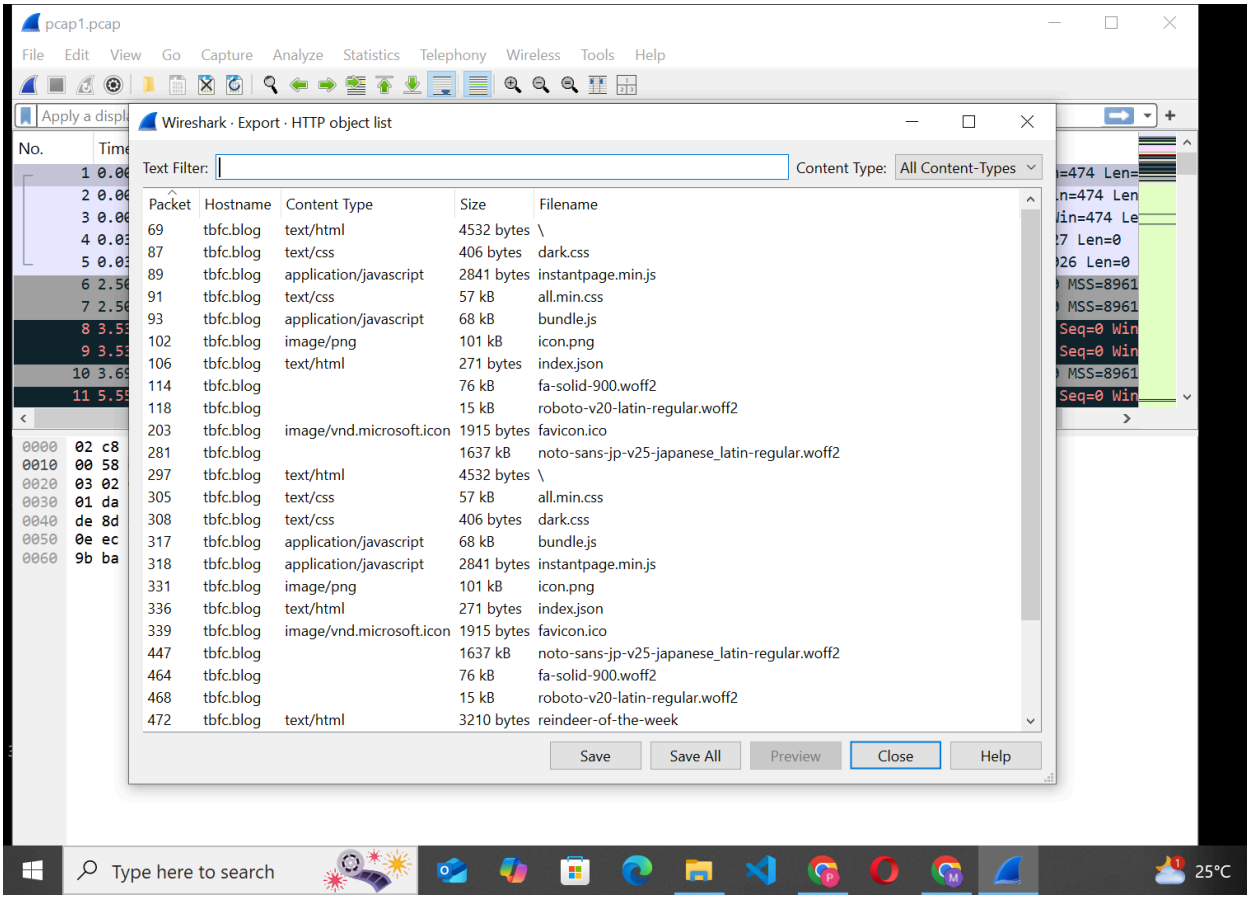


- dns for Domain Name System queries.

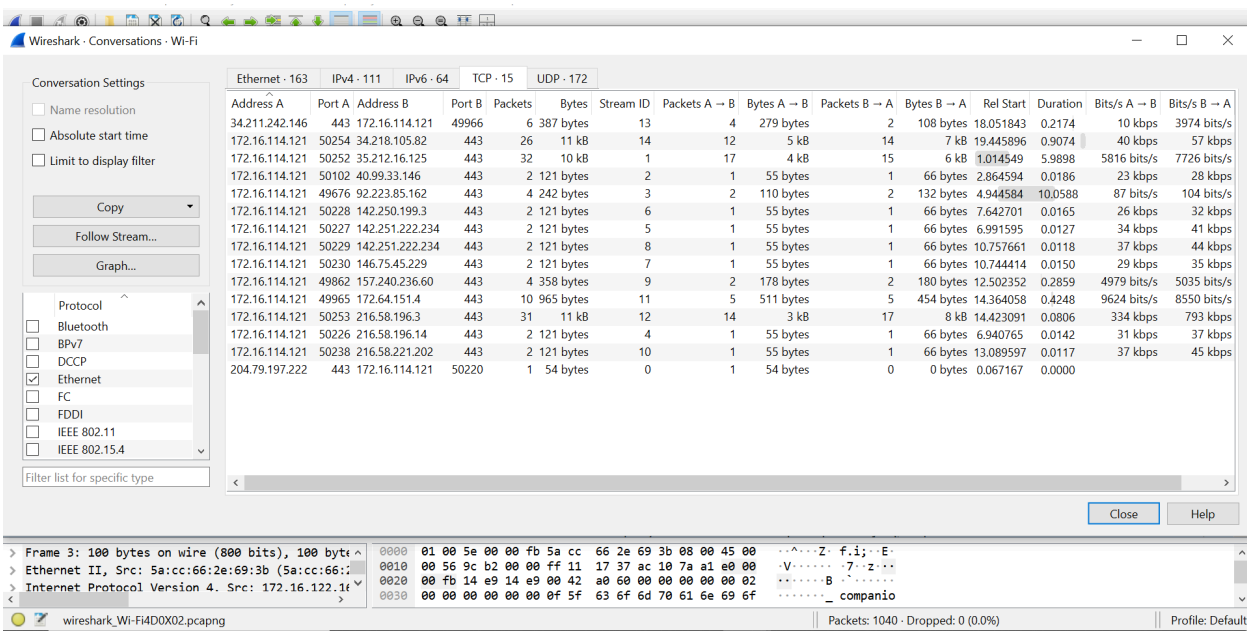
- 

- http and https for web traffic.
- 

3. **Analysis:**
   - Inspected the captured packets for headers, payloads, and communication patterns.
   -



   -



- Noted anomalies such as repeated failed connection attempts or irregular DNS queries.

3. Findings

3.1. Common Protocols Identified

1. **TCP (Transmission Control Protocol):**
   - Accounts for the majority of traffic.
   - Observed as the backbone for web browsing (HTTP/HTTPS), file transfers, and email communication.
   - Reliable, connection-oriented communication was evident through SYN, SYN-ACK, and ACK handshakes.
2. **UDP (User Datagram Protocol):**
   - Primarily associated with DNS and some streaming traffic.
   - Notable for its low latency but lack of reliability (e.g., no acknowledgment mechanisms).
3. **DNS (Domain Name System):**
   - Used for hostname-to-IP resolution.
   - Frequent DNS queries, including standard A (IPv4) and AAAA (IPv6) records.
4. **HTTP/HTTPS:**
   - Predominant for web browsing.
   - HTTPS traffic was encrypted, making payloads inaccessible, but metadata such as SNI (Server Name Indication) and server IPs were available.
5. **ICMP (Internet Control Message Protocol):**
   - Observed occasional pings for network diagnostics.

3.2. Traffic Patterns

1. **High Peak Traffic:**
   - During specific hours, there was a surge in HTTP/HTTPS traffic, likely due to employees accessing web-based applications.
2. **DNS Queries:**

    - Consistent DNS traffic with occasional spikes during browsing sessions or application launches.
3. **TCP Retransmissions and Latency:**
    - A small percentage of packets exhibited retransmissions, indicating potential congestion or packet loss.
4. **Unusual Activity:**
    - Repeated connection attempts to unresponsive servers were flagged for potential investigation.

---

4. Insights and Recommendations

4.1. Insights

1. HTTPS encryption ensures privacy for web traffic but limits visibility into payloads for analysis.
2. The network exhibited a mix of standard office traffic with no immediate signs of malicious activity.
3. DNS servers responded quickly, ensuring smooth hostname resolution.

4.2. Recommendations

1. **Optimize Network Performance:**
    - Identify and reduce retransmission occurrences by addressing congestion points.
    - Ensure adequate bandwidth for peak usage times.
2. **Enhance Security:**
    - Monitor for anomalies like excessive DNS queries or connection attempts to unknown servers.
    - Deploy intrusion detection systems (IDS) to complement packet analysis.
3. **Regular Monitoring:**
    - Schedule periodic network traffic analysis to identify evolving patterns or threats.
    - Analyze logs from multiple points in the network for comprehensive insights.

5. Conclusion

The analysis revealed a healthy mix of standard network traffic with no critical anomalies. Wireshark proved to be an invaluable tool for capturing and analyzing network packets, offering insights into protocol usage and traffic patterns. Continuous monitoring and proactive measures are recommended to maintain network performance and security.