Date: 9/3/2025

Lab Practical #09:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #09:

Explain usage of Wireshark tool.

Wireshark is one of the most popular open-source network protocol analyzers. It captures real-time network traffic and displays it in detail, allowing administrators, developers, and students to study how data flows across the network.

Primary Uses of Wireshark:

1. **Network Troubleshooting**
   - Helps diagnose common network issues such as high latency, dropped packets, or connectivity failures.
   - Can detect misconfigurations in routing or protocol setups.
2. **Protocol Analysis**
   - Provides detailed inspection of how various protocols (e.g., TCP, UDP, ICMP, HTTP, DNS) function.
   - Helps verify whether devices are communicating correctly according to standards.
3. **Security Monitoring**
   - Useful in spotting suspicious or malicious activities (e.g., packet sniffing, man-in-the-middle attacks).
   - Aids in detecting unauthorized access attempts and data leaks.
4. **Performance Measurement**
   - Monitors bandwidth usage and data flow patterns.
   - Identifies bottlenecks affecting network performance.
5. **Application Debugging**
   - Developers can analyze how their applications exchange data with servers.
   - Helps track down bugs in client-server communication.
6. **Educational Purposes**
   - A valuable tool for students and professionals to understand networking protocols and packet structures.

Date: 9/3/2025

Basic Steps to Use Wireshark:

1. **Install Wireshark**
   - Available on Windows, macOS, and Linux platforms.
   - Requires administrative rights for capturing live network data.
2. **Start Capturing Packets**
   - Select the correct interface (Ethernet, Wi-Fi, etc.).
   - Click the Start button to begin recording network traffic.
3. **Apply Filters**
   - Select the correct interface (Ethernet, Wi-Fi, etc.).
   - Click the Start button to begin recording network traffic.
4. **Analyze Packets**
   - Every packet can be viewed in three panes:
     1. Packet List (summary)
     2. Packet Details (protocol hierarchy)
     3. Packet Bytes (raw data view)
   - Information includes IP addresses, ports, flags, and payload.
5. **Save and Export Data**
   - Packet captures can be stored as .pcap files for further analysis or sharing.
6. **Use Built-in Tools**
   - View statistics like **Protocol Hierarchy**, **Conversations**, and **I/O Graphs**.
   - Use **Follow TCP Stream** to see the entire conversation between two endpoints.

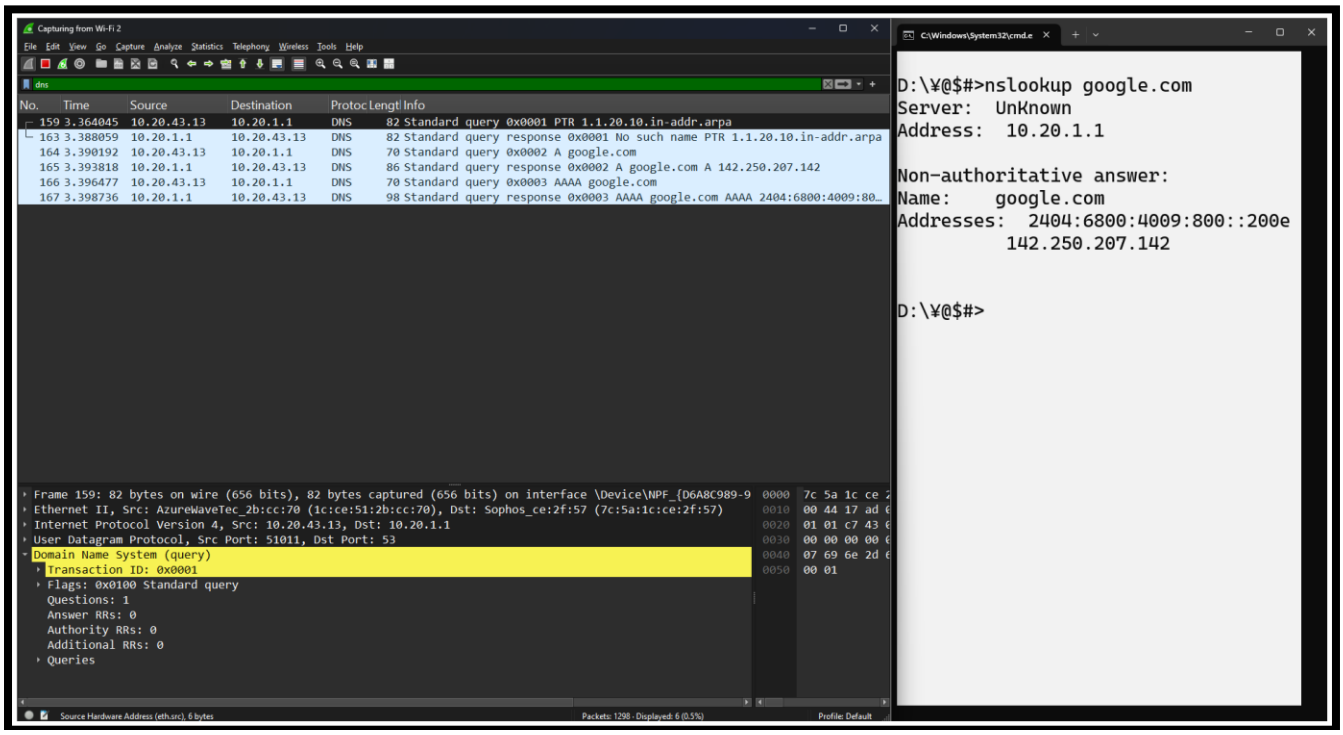
Example Use Case:
Suppose a website is loading unusually slowly:

1. Start capturing traffic while accessing the website.
2. Apply a filter such as http to focus on web requests.
3. Look for delays in TCP handshakes or slow response times from the server.
4. Examine headers and response codes to find possible misconfigurations.

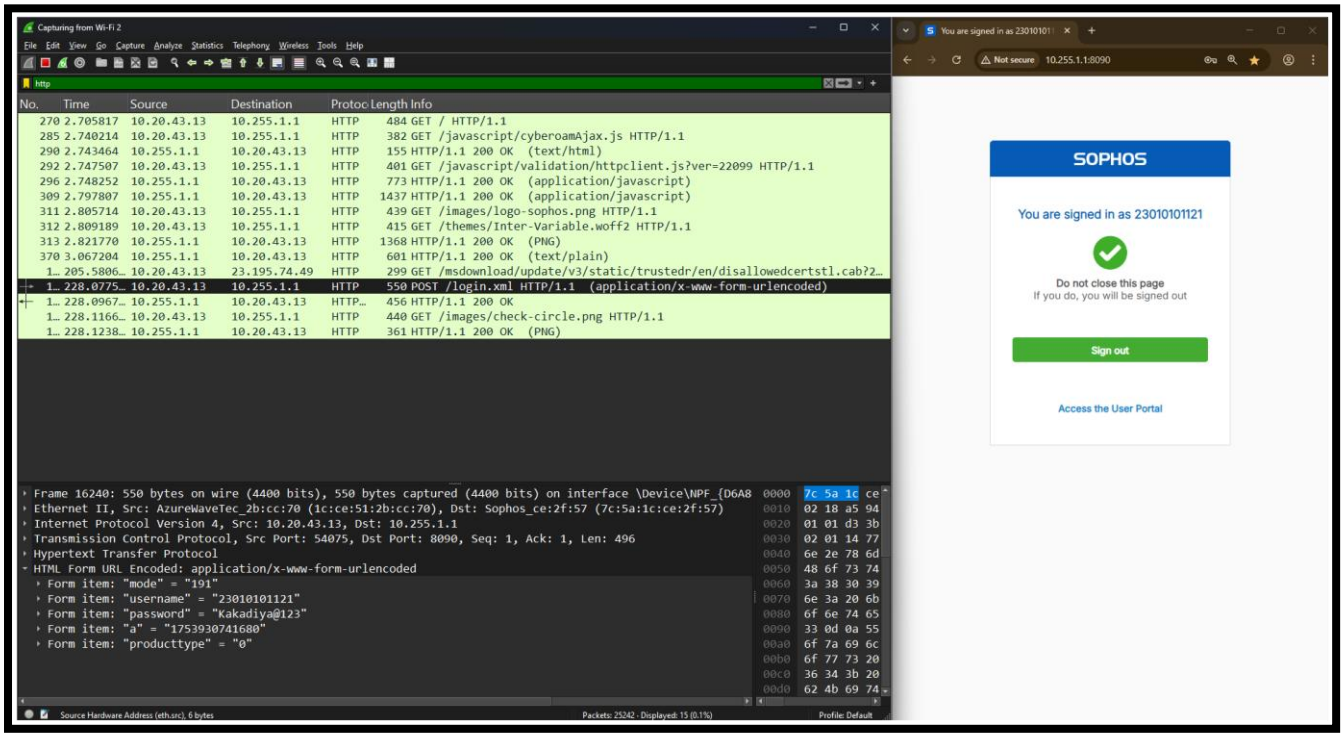
Date: 9/3/2025

Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

1. DNS :

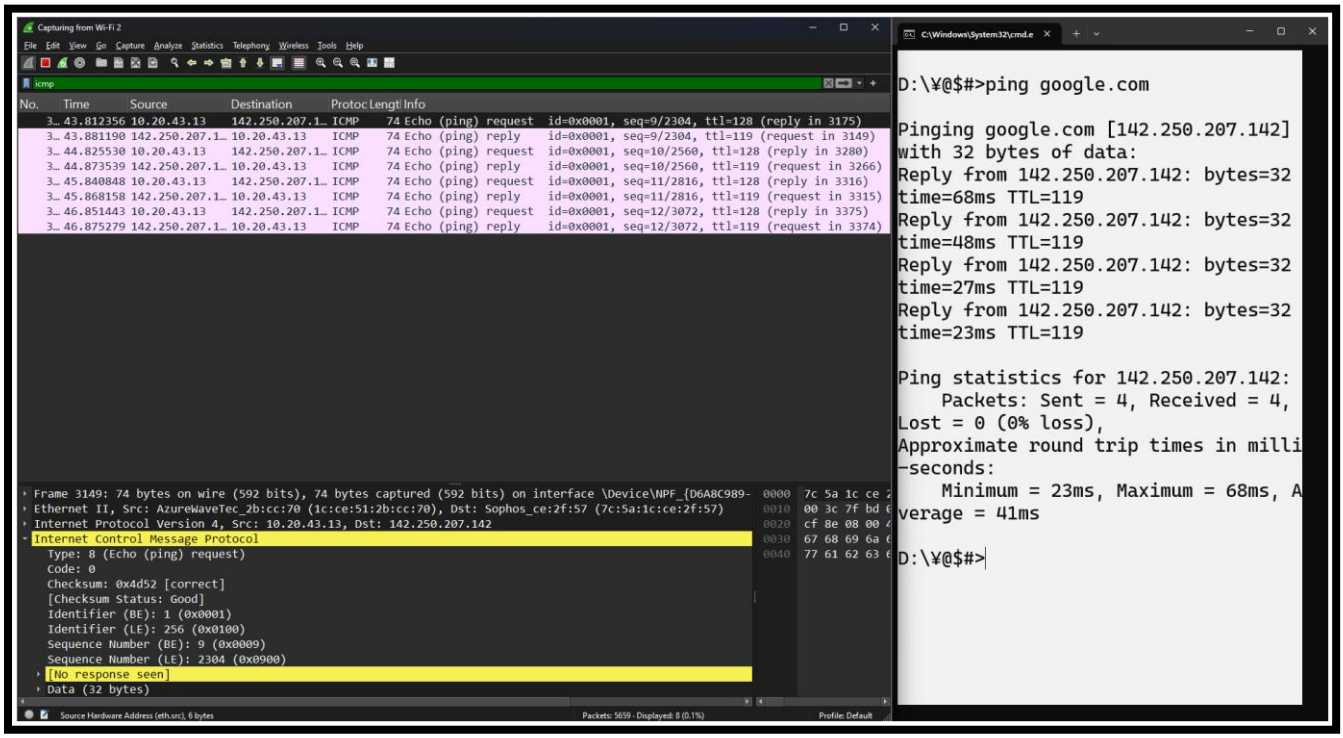


2. HTTP :

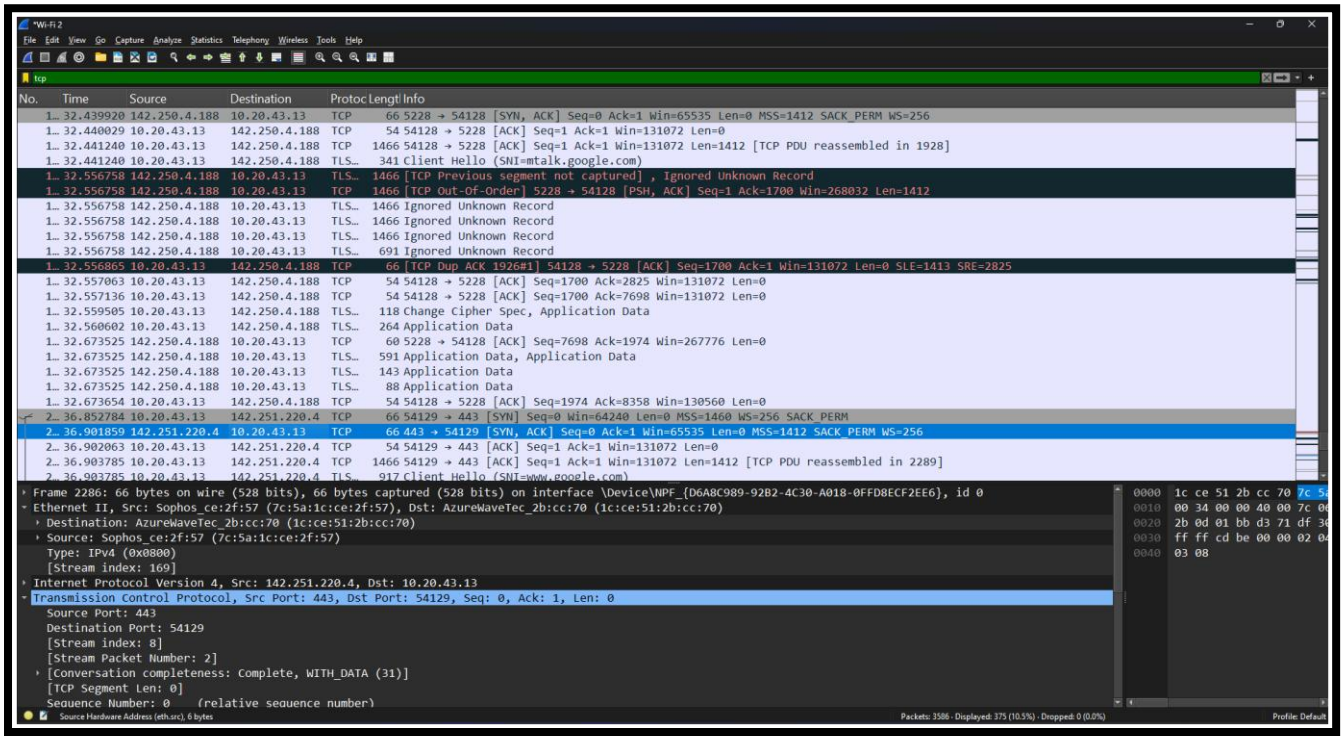


Date: 9/3/2025

3. ICMP :



4. TCP :



Date: 9/3/2025

5. UDP :