Practical No: 10

Date Of Performance: 12/02/2025

Aim: Study & Install Wireshark N/W Protocol Analyzer Tool & Analyse the Traffic.

Lab Objectives:

The objective of this lab is to familiarize students with Wireshark, a powerful network protocol analyser, and its role in network monitoring and analysis. Students will learn to install and configure Wireshark, capture live network traffic, and analyse data packets to understand various network protocols such as TCP, UDP, ICMP, HTTP, and DNS. The lab also focuses on applying filters to isolate specific traffic, examining packet headers and payloads, and recognizing protocol interactions. Additionally, students will develop the skills to identify network issues, detect security threats, and analyse abnormal traffic patterns.

Lab Outcomes:

By the end of this lab, students will be able to successfully install and operate Wireshark for capturing and analysing network traffic. They will gain the ability to interpret real-time data packets, apply filters to focus on specific protocols, and analyse packet details such as source and destination IP addresses, ports, and protocol- specific information. Students will also develop skills in identifying network vulnerabilities, detecting unusual traffic behaviour, and using Wireshark as a tool for network troubleshooting, security analysis, and performance optimization.

Theory:

Wireshark is a popular open-source network protocol analyser that allows you to

capture and analyse the data traveling back and forth on a network in real-time. It

provides a detailed view of network traffic, helping network administrators, security

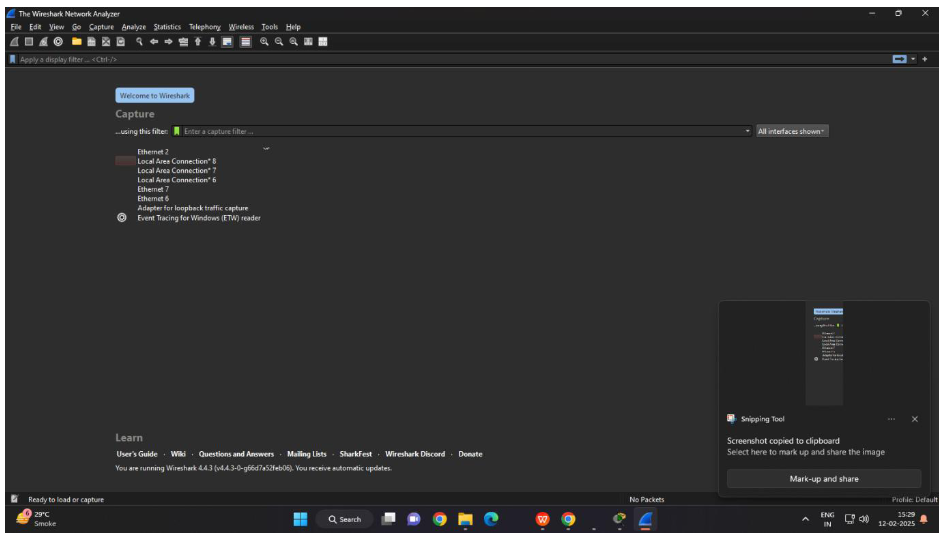
professionals, and developers troubleshoot network issues, detect security threats, and optimize performance.

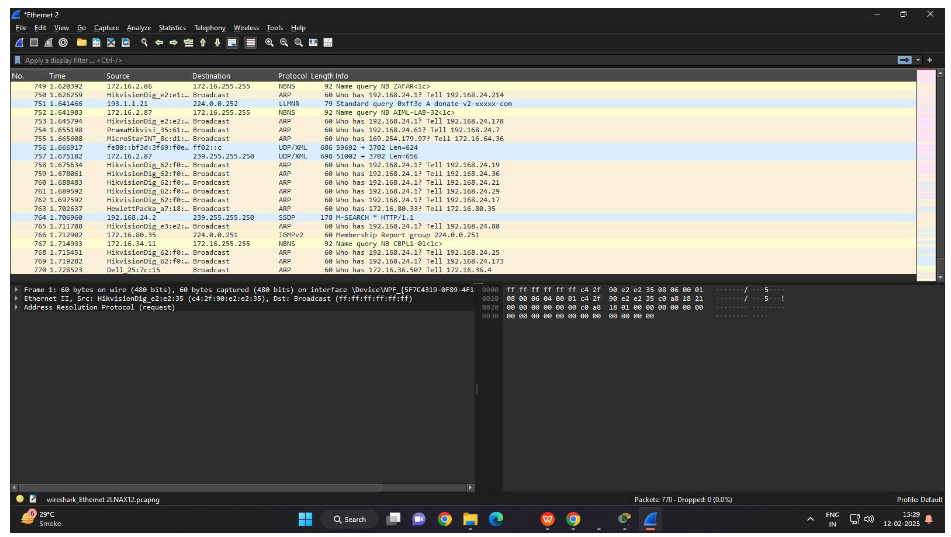
Key Features:

* Records data packets in real-time or from pre-existing files.
* Supports various protocols for analysing different OSI model layers.
* Allows the isolation of specific packets based on criteria like IP address or protocol type.
* Organizes packets for easier analysis of communication between hosts.
* Interprets and displays protocol content, with the option to create custom dissectors.
* Provides insights into network performance through various statistics and graphs.
* Useful for detecting and analysing network attacks and anomalies.
* Aids network administrators in identifying and resolving
* connectivity and performance issues.
* Reconstructs and displays entire data streams of TCP
* connections for application-layer protocol analysis.
* Highlights potential issues or anomalies in the captured traffic.

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analysers available today.

Wireshark requires a good understanding of networking protocols, and privacy and legal considerations should be taken into account when working with live networks or sensitive data.





Conclusion:

The Wireshark experiment helped analyse network traffic, inspect packet structures, measure performance, and identify security risks. It demonstrated effective troubleshooting, protocol analysis, and the importance of secure communication in network monitoring.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Performance  (7M) | Journal  (3M) | Lab Ethics  (2M) | Attendance  (3M) | Total  (15M) | Faculty Signature |
|  |  |  |  |  |  |