# Experiment No.:10

Batch: C1 Roll No.: 16010122221

Experiment / assignment / tutorial No. 10 Grade: AA / AB / BB / BC / CC / CD /DD

**Signature of the Staff In-charge with date**

**TITLE: Study of Packet Analyzer tool: Wireshark**



**AIM:** To study and analyse various Protocols using Packet Analyzer tool: Wireshark



**Books/ Journals/ Websites referred:**

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition



# Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands



# New Concepts to be learned: Packet Analyzer tool: Wireshark.



**THEORY:**

Wireshark is a widely used open-source network protocol analyzer and packet capture tool. It allows users to capture, view, and analyze data packets traveling across a computer network. Here are some key points about Wireshark:

Packet Capture: Wireshark captures data packets as they move across a network. This can include packets from various network protocols, such as Ethernet, Wi-Fi, TCP/IP, and more.

Network Analysis: Users can analyze the captured packets to understand network traffic, troubleshoot network issues, and diagnose problems. It's a valuable tool for network administrators, security professionals, and developers.

Real-Time Monitoring: Wireshark can capture packets in real-time, making it useful for monitoring ongoing network activity and diagnosing issues as they occur.

Protocol Support: Wireshark supports a vast number of network protocols, ranging from common ones like HTTP, DNS, and FTP to more specialized and less-known protocols.

Filtering and Search: Wireshark offers powerful filtering and search capabilities, allowing users to focus on specific packets or types of traffic.

Packet Decoding: Wireshark decodes packet data, presenting it in a human-readable format. Users can inspect packet headers, payloads, and other details.

Graphical User Interface (GUI): Wireshark provides a user-friendly graphical interface that makes it accessible to a wide range of users, including those who may not have a deep understanding of network protocols.

Cross-Platform: Wireshark is available for multiple operating systems, including Windows, macOS, and various Linux distributions.

Community and Development: It is an open-source project with an active community of developers and users who contribute to its development and maintenance.

Security Analysis: Wireshark can be used to analyze network security by identifying suspicious or malicious activity, such as unusual traffic patterns or unauthorized access attempts.

Education and Training: Wireshark is commonly used in educational institutions and training programs to teach networking concepts and network analysis techniques.

Packet Export: Users can export captured packets and analysis results in various formats, making it easier to share findings or integrate data with other tools.

It's important to note that Wireshark is a powerful tool that can capture sensitive information, so its use should be conducted responsibly and in accordance with applicable laws and regulations. Additionally, users should have the necessary permissions to capture network traffic on the networks they are monitoring.

# IMPLEMENTATION:

**Apparatus / Software tools used:**

Desktop pc, Wireshark software

Wireshark follow link

https://www.wireshark.org/download.html

https://www.youtube.com/watch?v=TkCSr30UojM

https://www.youtube.com/watch?v=jvuiI1Leg6w

Wireshark is network protocol analyser for Unix and Windows. It is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communication protocol development. Wireshark is cross-platform. Using the Qt widget toolkit in current releses to implement its user interface, and using pcap to capture packets, it runs on Linux, macOS, Solaris.some other Unix-like operating systems, and Microsoft Windows,

**Capturing Packets**:

After downloading and installing Wireshark, launch it and click the name of an interface under Interface List to start capturing packets n that interface. For example, to capture traffic on the wireless network, click wireless interface. Configure advanced features by clicking Capture Options

After clicking interface name. the packets start to appear in real time. Wireshark captures each packet sent to or from the system

Click the stop capture button near the top left corner of the window to stop capturing traffic.

**Color Coding**:

Wireshark uses color to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems – for example, they could have been delivered out of order.



**Functionality**

Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture the packets on the types of networks that pcap supports.

Data can be captured "from the wire" from a live network connection or read from a file that recorded already-captured packets. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback. Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program. Data display can be refined using a display filter. Plug-ins can be created for dissecting new protocols.



**To install wireshark**

Sudo install wireshark

**To run wireshark**

Wireshark

**Select the interface**

Default interface is eth0 for this network.

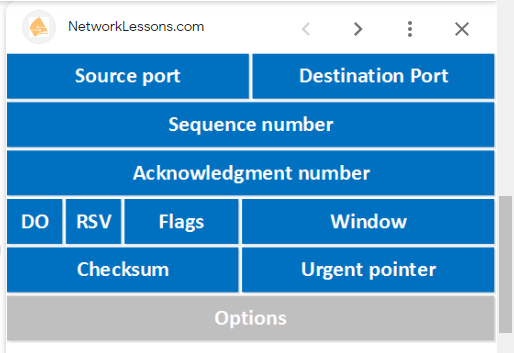
**Grab the packets**

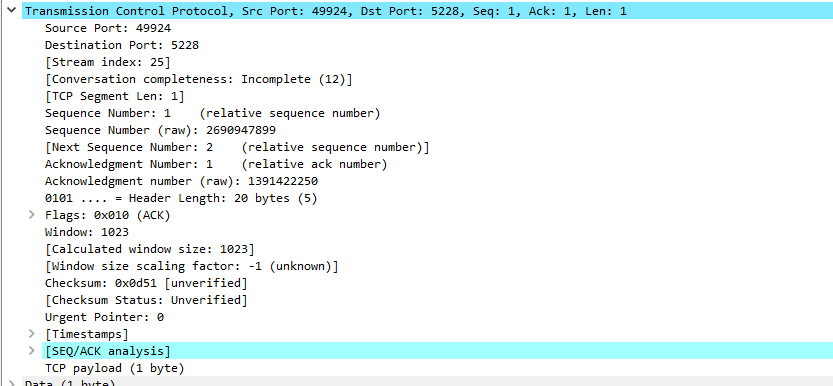
**See different options available.**

**Packet Header Format**

**Transport Layer Protocol**

TCP header Format





Source port:49924

Destination:5228

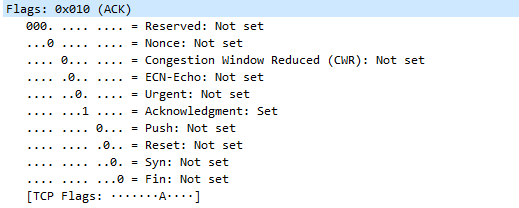
Sequence no



Acknowledgement:



Flags:



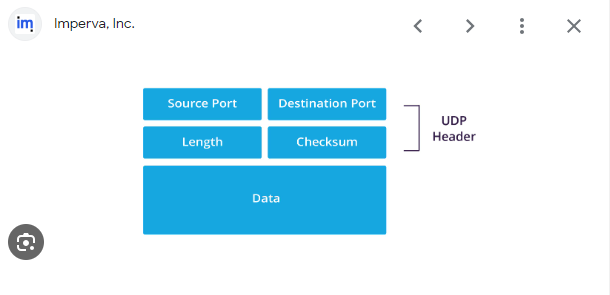
Window:1023

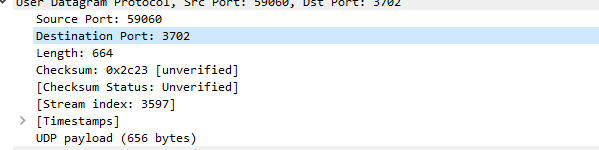
Checksum:



Urgent pointer :0

UDP Header Format





**Post Lab Subjective/Objective type Questions:**

1.Different types of analysis options provided by wireshark?

**Different types of analysis options provided by Wireshark**:

* Wireshark offers several analysis options, including packet capture, protocol analysis, and real-time network monitoring. It supports various protocols such as TCP, UDP, HTTP, DNS, and many others. Users can filter and search for specific packets, decode packet data, view packet headers and payloads, and inspect details of each packet in a human-readable format. Additionally, it provides color-coded packet types for easier identification and allows users to export packet data for further analysis or sharing.

2.Types of packets analyzed in experiment?

**Types of packets analyzed in the experiment**:

* In this experiment, various packet types were analyzed, including TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) packets, as well as others depending on the network traffic. The analysis covered packet headers and payloads, focusing on details such as source and destination ports, sequence numbers, and flags within these packet types.

**CONCLUSION:**

In this experiment we learnt study and analyze various Protocols using Packet Analyzer tool: Wireshark

**Date: Signature of faculty in-charge**