**Assignment No :- 5**

**Aim :-** Demonstrate the Wire shark tool, tcp dump and observe data transferred in client server communication.

**Introduction:-**

****

Wireshark is a powerful and widely-used open-source network packet analyzer. It is a critical tool for network administrators, security professionals, developers, and anyone interested in understanding the traffic on their network.Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

The extent of its popularity is such that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related profession.It has a great GUI as well as a conventional CLI(T Shark).

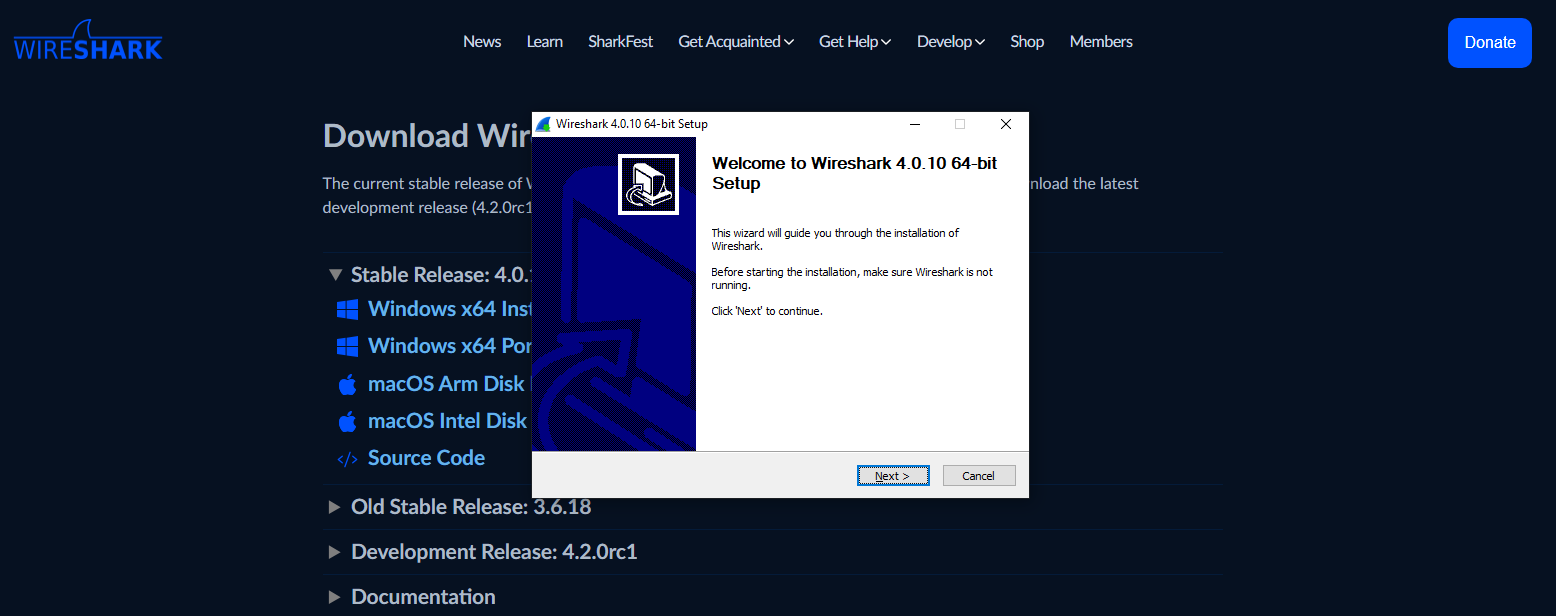
It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)

It is open-source with a large community of backers and developers.

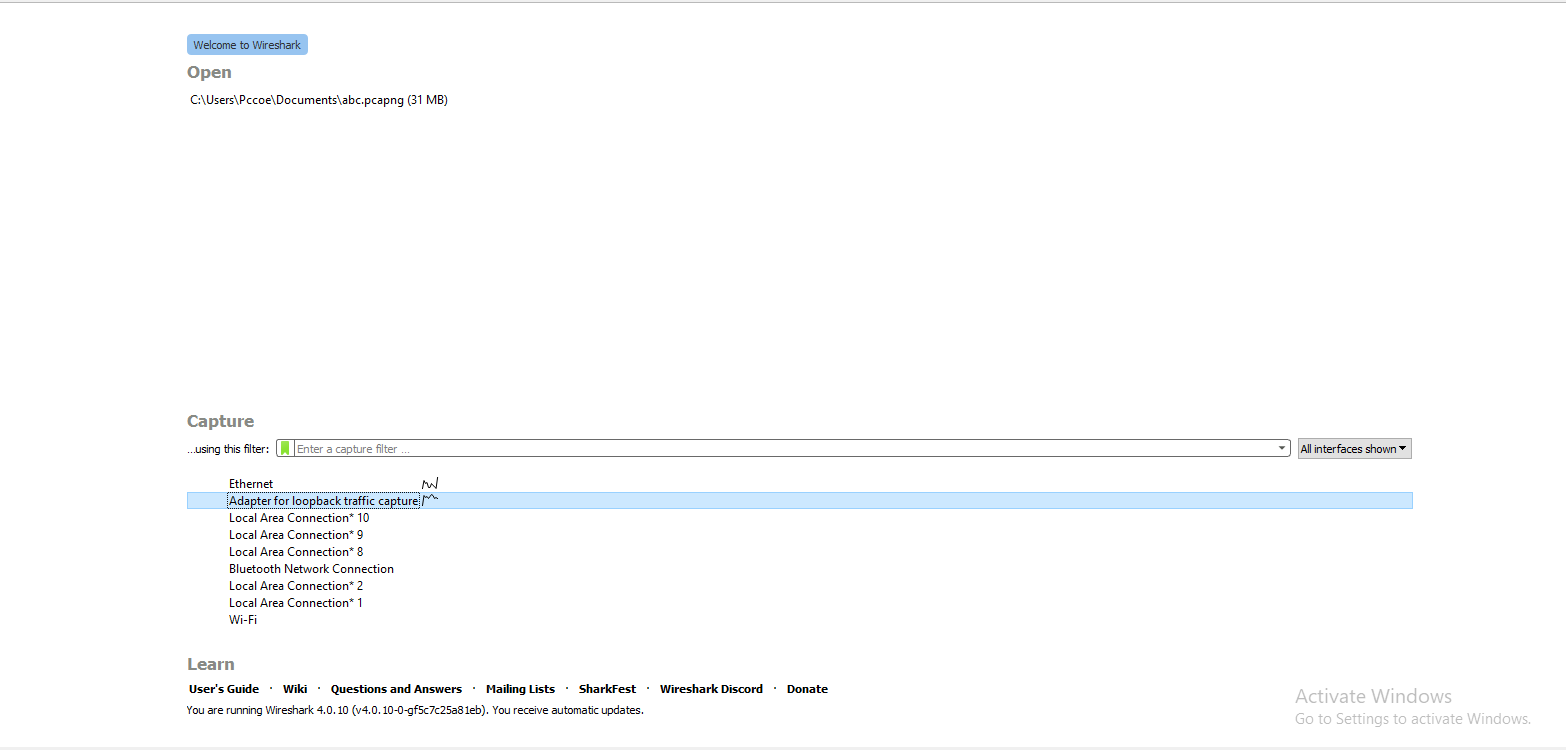
All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

**Steps to install and run the WireShark :**

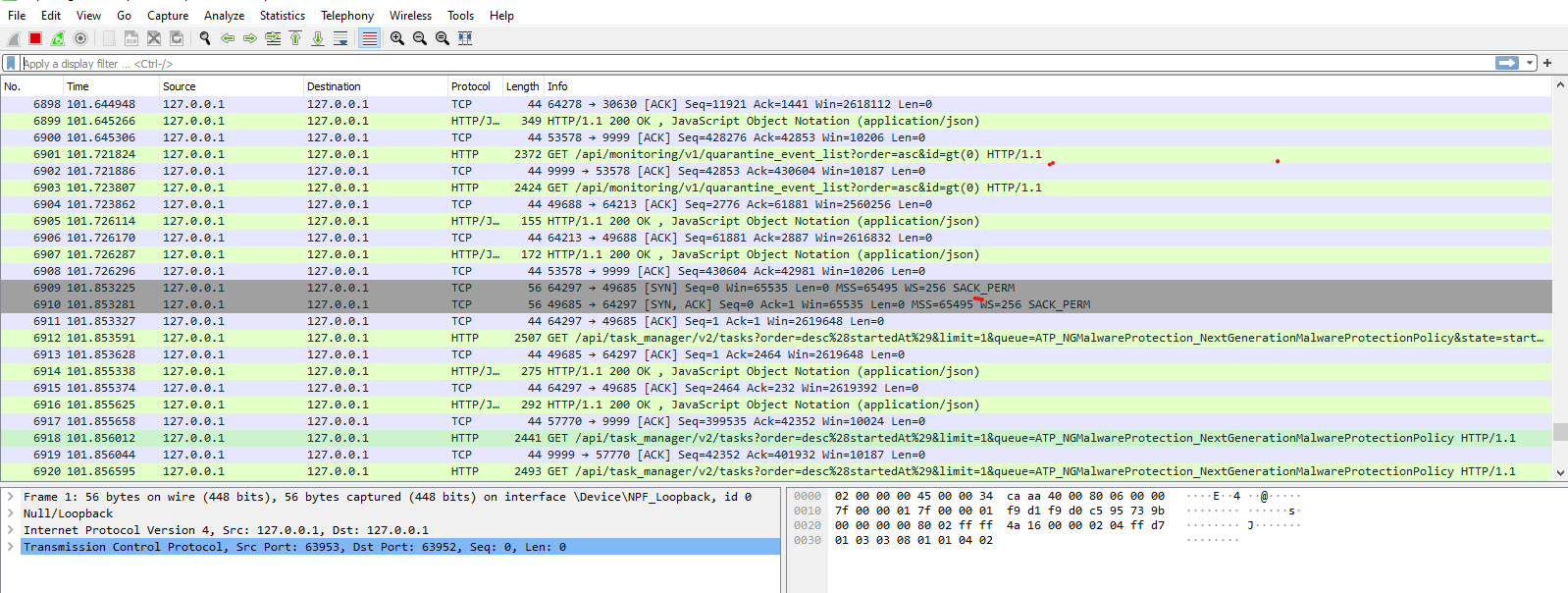
**Step 1 :-** Go to the official website of Wireshark and Click on download WireShark.



**Step 2 :-**  Start the WireShark and apply the filters

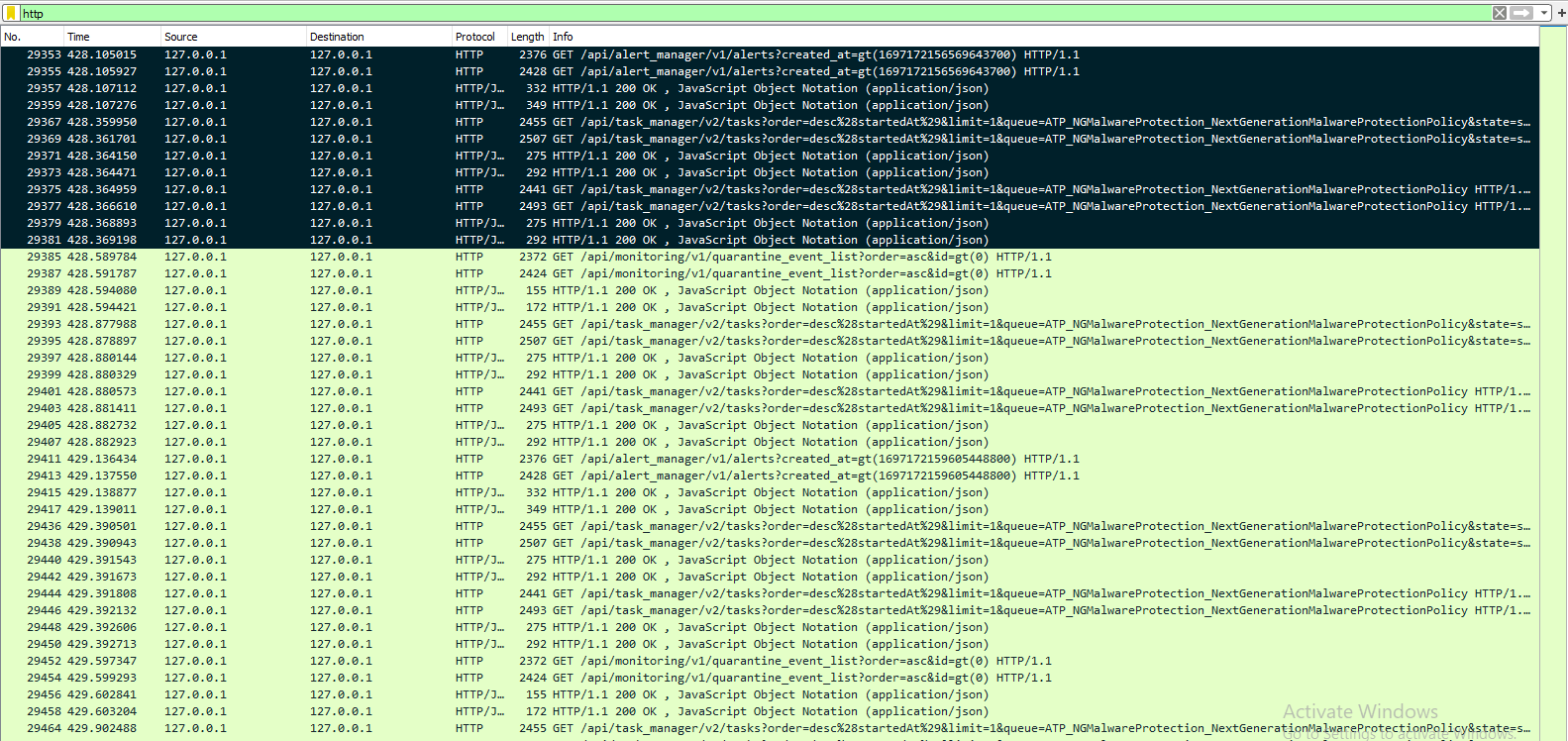


**Step 4:**-Analysis the transmission in the TCP and HTTP protocols



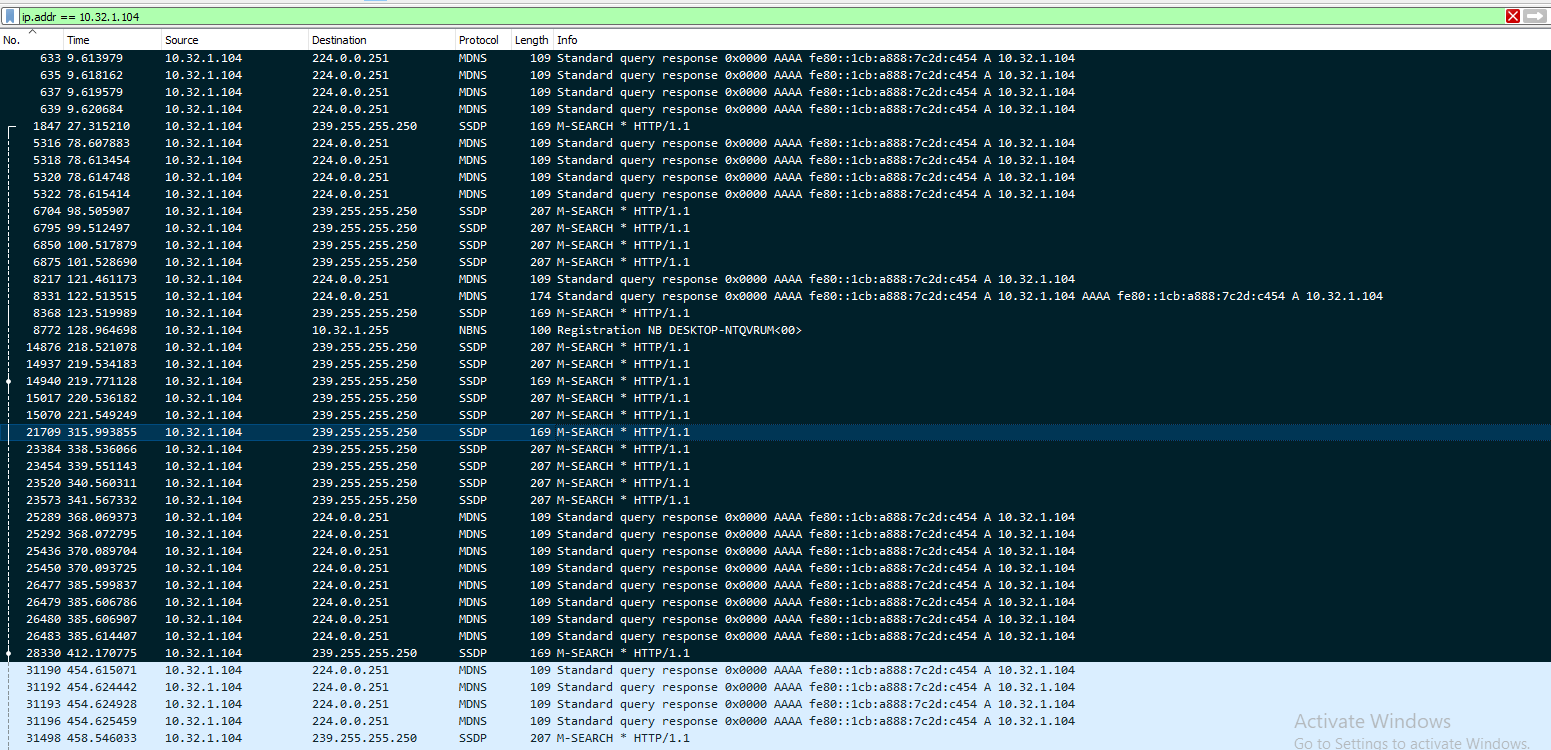
**Step 5:-** Explore various features of the WireShark

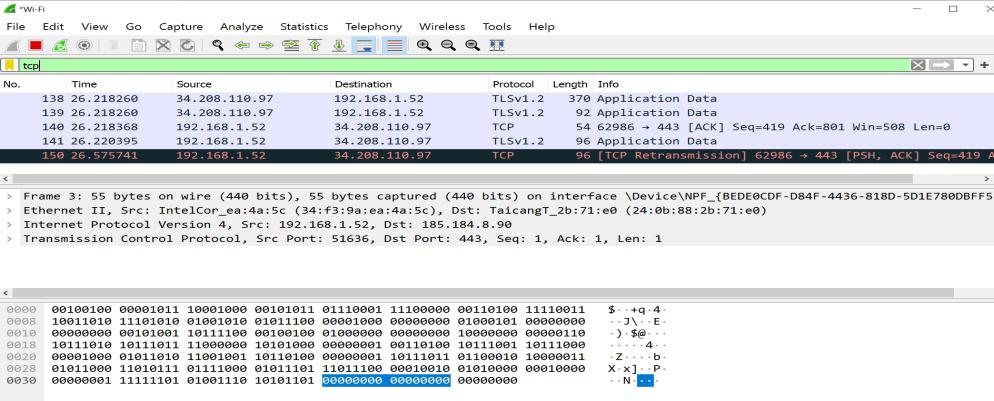
**1) http request send by the source**

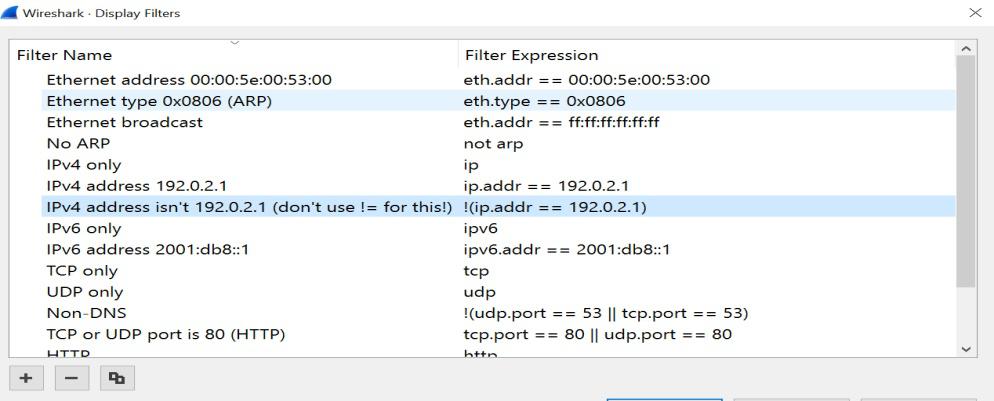
Wireshark is an indispensable network packet analyzer renowned for its extensive capabilities in dissecting and analyzing network traffic. Its versatility lies in the comprehensive support for numerous network protocols, from common ones like HTTP and TCP/IP to specialized ones used in diverse environments.

**2)Traffic on the Source system**

Monitoring traffic on the source system is essential for maintaining network performance and security. This involves analyzing the data flow originating from a particular device or network entity. By observing traffic patterns, network administrators can identify and address potential bottlenecks, optimize bandwidth allocation, and troubleshoot network issues.



**3.Analysis of TCP/IP Protocols using the Wireshark:-**To analyze TCP/IP protocol traffic in Wireshark, you can utilize display filters that focus on packets utilizing either the TCP or UDP protocol. By applying the filter expression.****



**Features :-**

1. **Packet Capture:**

Wireshark can capture live data from a network interface or read from saved capture files. This allows for real-time analysis of network traffic.

Multi-platform Support:

Wireshark is available for Windows, macOS, and various Linux distributions, making it accessible to a wide range of users.

1. **Rich Protocol Support**

It supports a vast array of network protocols, ranging from common ones like HTTP, TCP/IP, and UDP, to more specialized protocols used in industrial control systems, IoT devices, and more.

1. **Powerful Filters:**

Wireshark provides a flexible filtering system that allows users to focus on specific types of traffic based on various parameters such as source/destination IP, port numbers, protocols, and more.

1. **Packet Decoding:**

It can decode and display the contents of each packet, showing the information at different layers of the OSI model (Ethernet, IP, TCP/UDP, etc.).

1. **Statistical Analysis:**

Wireshark offers various statistical tools to help identify trends, patterns, and anomalies in network traffic.

**Advantages of Wireshark:**

1. **Comprehensive Packet Analysis:**

Wireshark provides a detailed view of network traffic, allowing users to analyze packets at various levels, including Ethernet, IP, TCP/UDP, and application layers.

1. **Multi-Platform Support:**

It is available for Windows, macOS, and various Linux distributions, making it accessible to a wide range of users.

1. **Rich Protocol Support:**

Wireshark supports a wide range of network protocols, both common and specialized. This makes it suitable for analyzing a diverse set of network environments.

1. **Real-Time Capture:**

It can capture live data from network interfaces, enabling real-time analysis of network traffic.

1. **Powerful Filters:**

Wireshark offers a flexible filtering system, allowing users to focus on specific types of traffic based on various parameters.

1. **Statistical Analysis:**

The tool provides statistical tools to help identify trends, patterns, and anomalies in network traffic.

**Disadvantages :-**

1. **Steep Learning Curve:**

Wireshark can be complex, especially for beginners. Understanding the nuances of network protocols and how to effectively use the tool requires time and practice.

1. **Resource Intensive:**

Capturing and analyzing a large amount of network traffic can be resource-intensive and may slow down the system.

1. **Privacy and Legal Considerations:**

Capturing and analyzing network traffic may raise privacy and legal concerns, especially in shared or public networks. Unauthorized monitoring of traffic can be illegal and unethical.

1. **Limited Performance on High-Speed Networks:**

Wireshark may struggle to keep up with extremely high-speed networks, potentially missing packets in such scenarios.

1. **Dependence on Hardware and Drivers:**

Compatibility and performance of Wireshark may be affected by the quality of network interfaces and drivers.

**Applications :-**

**Web Browsers:**

Examples: Chrome, Firefox, Safari, Edge

Purpose: Used to access and interact with websites and web-based applications.

**Office Productivity Suites:**

Examples: Microsoft Office, Google Workspace, LibreOffice

Purpose: Provides tools for creating, editing, and managing documents, spreadsheets, presentations, etc.

**Communication and Collaboration:**

Examples: Slack, Microsoft Teams, Zoom, Skype

Purpose: Facilitates communication and collaboration among teams through messaging, video conferencing, and file sharing.

**Social Media:**

Examples: Facebook, Twitter, Instagram, LinkedIn

Purpose: Platforms for social interaction, networking, and content sharing.

**Entertainment:**

Examples: Netflix, Spotify, YouTube, Steam

Purpose: Offers a wide range of entertainment content such as movies, music, videos, and games.

**Gaming:**

Examples: Fortnite, League of Legends, Minecraft

Purpose: Provides interactive gaming experiences for players.

**Conclusion :-**

In conclusion, the use of network analysis tools like Wireshark, tcpdump, and others plays a pivotal role in gaining insights into the intricacies of client-server communication. Wireshark, in particular, stands out as a versatile and powerful packet analyzer, catering to a broad spectrum of users from network administrators to security professionals. Its rich feature set, encompassing packet capture, extensive protocol support, powerful filtering capabilities, and statistical analysis tools, empowers users to dissect network traffic comprehensively.While Wireshark offers invaluable advantages such as real-time capture, wireless network analysis, and specialized VoIP analysis, it is important to acknowledge its challenges. Its complexity may pose a learning curve, and resource-intensive operations could impact system performance. Additionally, privacy and legal considerations, especially in shared or public networks, should be taken into account.