# EXPERIMENT 07

**Aim:** Study of packet sniffer tools wireshark

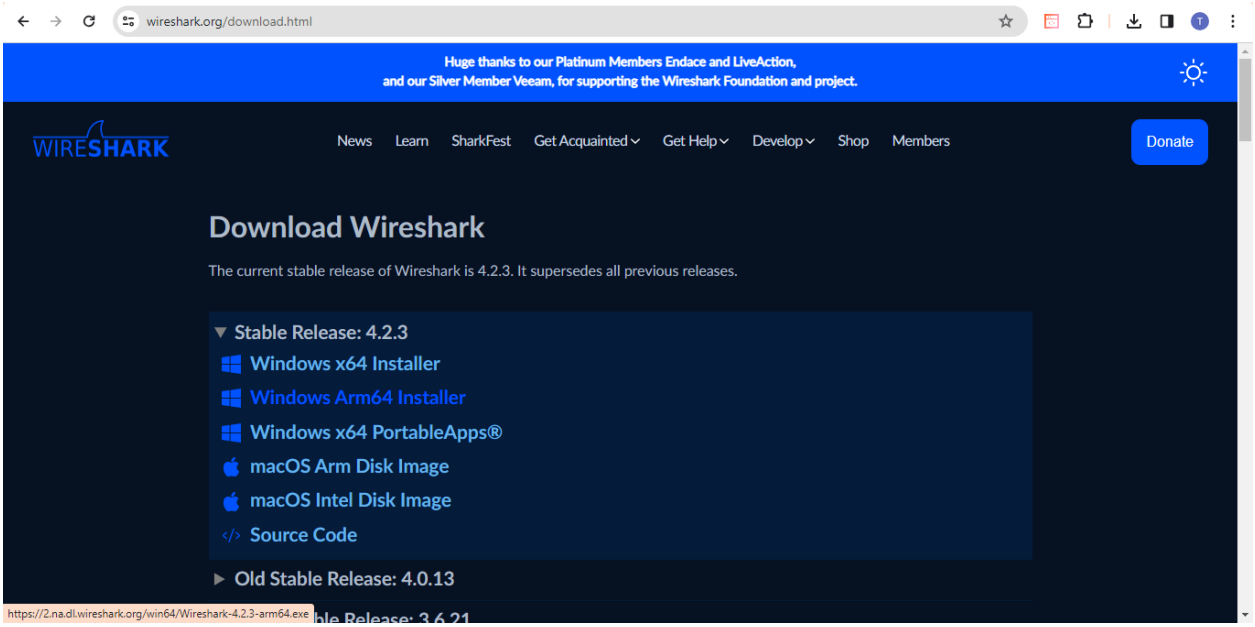
**1. Observer performance in promiscuous as well as non-promiscuous mode.**
**2. Show the packets can be traced based on different filters.**

**What Is Wireshark?**

Originally known as Ethereal, Wireshark displays data from hundreds of different protocols on all major network types. Data packets can be viewed in real-time or analyzed offline. Wireshark supports dozens of capture/trace file formats, including CAP and ERF. Integrated decryption tools display the encrypted packets for several common protocols, including WEP and WPA/WPA2.

**How to Download and Install Wireshark**

Wireshark can be downloaded at no cost from the Wireshark Foundation website for both macOS and




Windows. You'll see the latest stable release and the current developmental release. Unless you're an advanced user, download the stable version.

During the Windows setup process, choose to install WinPcap or Npcap if prompted as these include libraries required for live data capture.

You must be logged in to the device as an administrator to use Wireshark. In Windows 10, search for Wireshark and select Run as administrator. In macOS, right-click the app icon and select Get Info. In the Sharing & Permissions settings, give the admin Read & Write privileges.

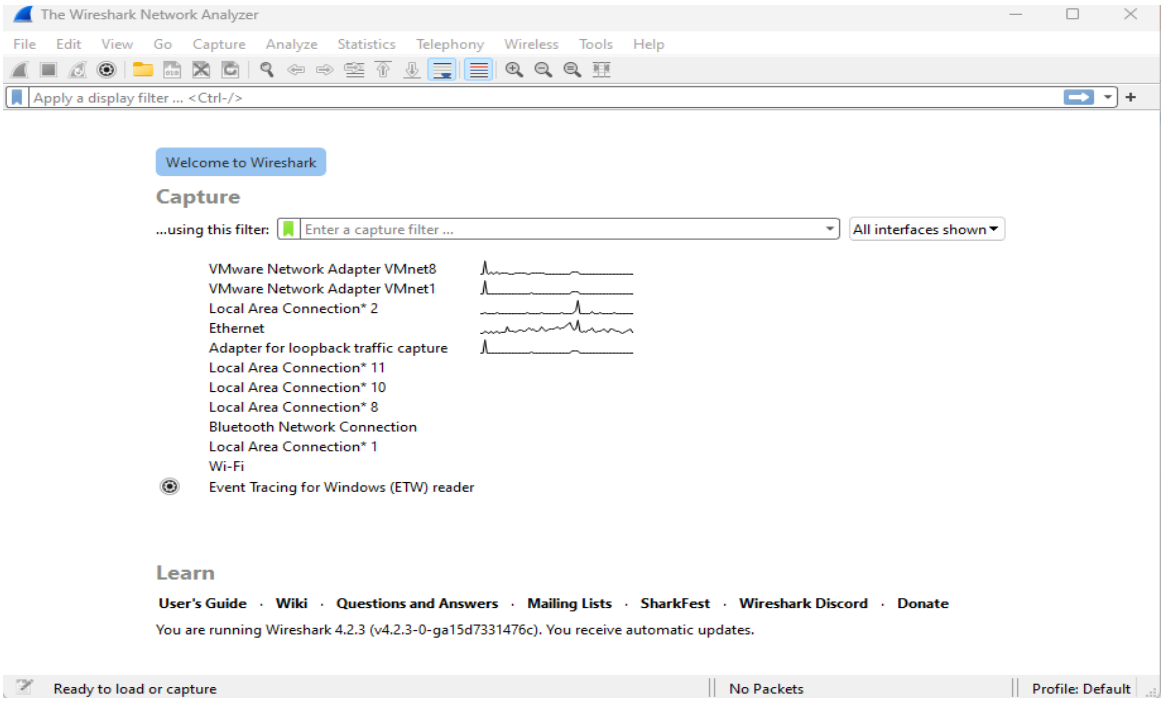
The application is also available for Linux and other UNIX-like platforms including Red Hat, Solaris, and FreeBSD. The binaries required for these operating systems can be found toward the bottom of the Wireshark download page under the Third-Party Packages section.

**How to Capture Data Packets With Wireshark**

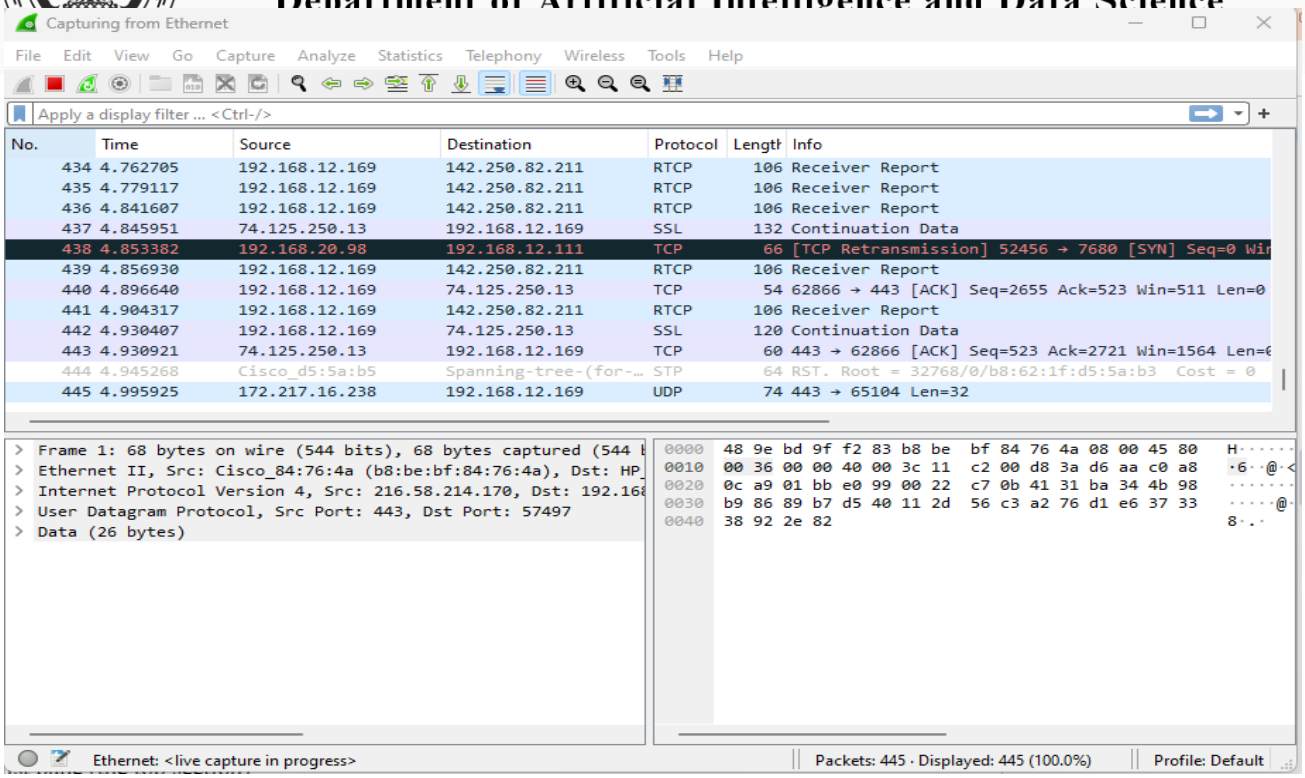
When you launch Wireshark, a welcome screen lists the available network connections on your current device. Displayed to the right of each is an EKG-style line graph that represents live traffic on that network.

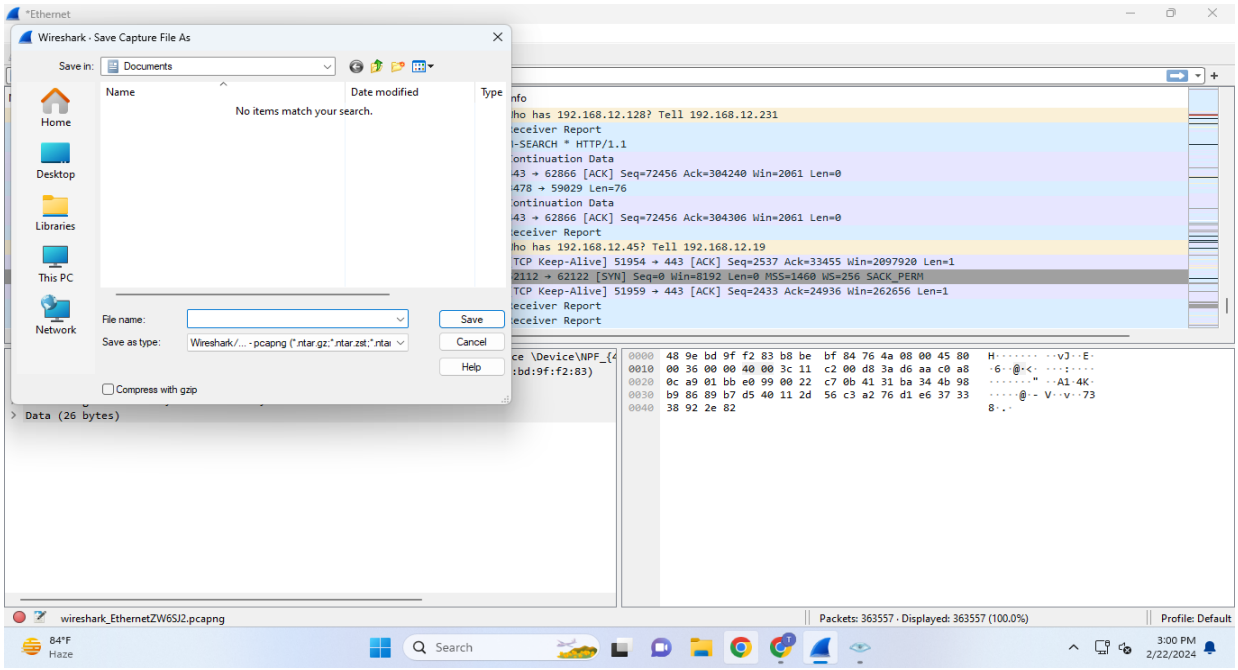
To begin capturing packets with Wireshark:

1. Select one or more of networks, go to the menu bar, then select Capture.




2. In the Wireshark Capture Interfaces window, select Start.




Select File > Save As or choose an Export option to record the capture.

capturing, press Ctrl+E. Or, go to the Wireshark toolbar and select the red Stop button that's located next to the shark fin.

**How to View and Analyze Packet Contents**

The captured data interface contains three main sections:
The packet list pane (the top section)
The packet details pane (the middle section)
The packet bytes pane (the bottom section)

1. **Packet List**

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points:

- No: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.
- Time: The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created.
- Source: This column contains the address (IP or other) where the packet originated.
- Destination: This column contains the address that the packet is being sent to.
  Protocol: The packet's protocol name, such as TCP, can be found in this column.
  Length: The packet length, in bytes, is displayed in this column.
  Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.
  When a packet is selected in the top pane, you may notice one or more symbols appear in the No. column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of the conversation.

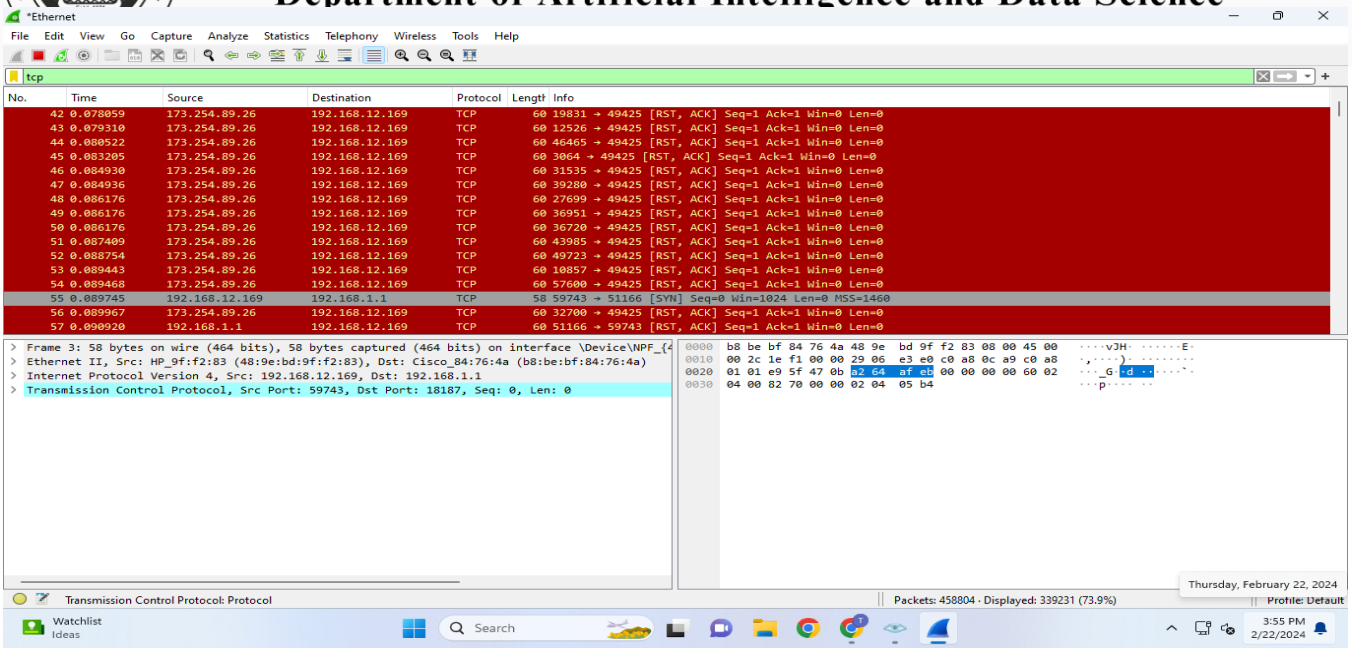
**2. Packet Details**

The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.

**3. Packet Bytes**

At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.
Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that cannot be printed are represented by a period.
To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.

**How to Use Wireshark Filters**




Capture filters instruct Wireshark to only record packets that meet specified criteria. Filters can also be applied to a capture file that has been created so that only certain packets are shown. These are referred to as display filters. Wireshark provides a large number of predefined filters by default. To use one of these existing filters, enter its name in the Apply a display filter entry field located below the Wireshark toolbar or in the Enter a capture filter field located in the center of the welcome screen.

For example, if you want to display TCP packets, type tcp. The Wireshark autocomplete feature shows suggested names as you begin typing, making it easier to find the correct moniker for the filter you're seeking.

Another way to choose a filter is to select the bookmark on the left side of the entry field. Choose Manage Filter Expressions or Manage Display Filters to add, remove, or edit filters.

You can also access previously used filters by selecting the down arrow on the right side of the entry field to display a history drop-down list.

Capture filters are applied as soon as you begin recording network traffic. To apply a display filter, select the right arrow on the right side of the entry field.

**Conclusion:**

In conclusion, Wireshark is a powerful and versatile network protocol analyzer that allows users to capture, analyze, and troubleshoot data packets in real-time or from offline captures. It supports various protocols and provides detailed information through its intuitive interface, featuring packet lists, details, and byte views. The application is available for multiple operating systems, making it widely accessible for network administrators and enthusiasts alike. Wireshark's ability to capture, filter, and interpret network traffic is essential for diagnosing issues, verifying configurations, and understanding the dynamics of data communication.