LAB NO: 2 **Date:**

WIRESHARK

Objectives:

In this lab, student will be able to:

- Identify the details about data communication, working of the protocols involved in communication using Wireshark.
- Analyze the working of network protocols and identify the vulnerabilities in the communication system related to confidentiality using Wireshark.
- Viewing the input/output traffic graph using Wireshark.
- View and Analyze Packet Contents of real network.

Description:

Wireshark is a network protocol analyser, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

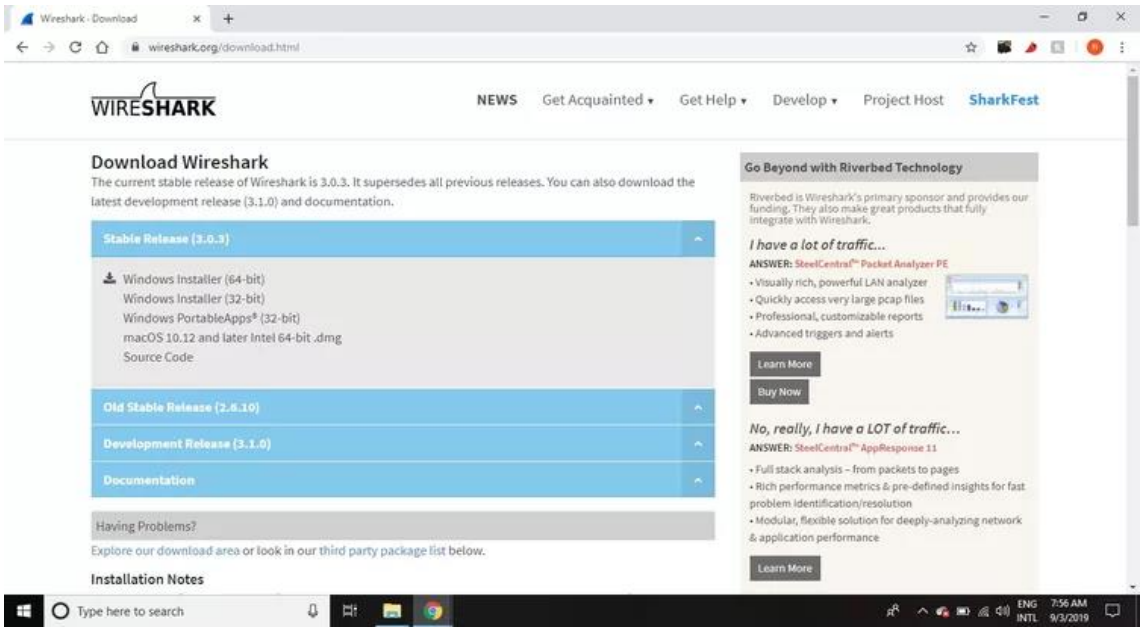
The use of Wireshark:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals.

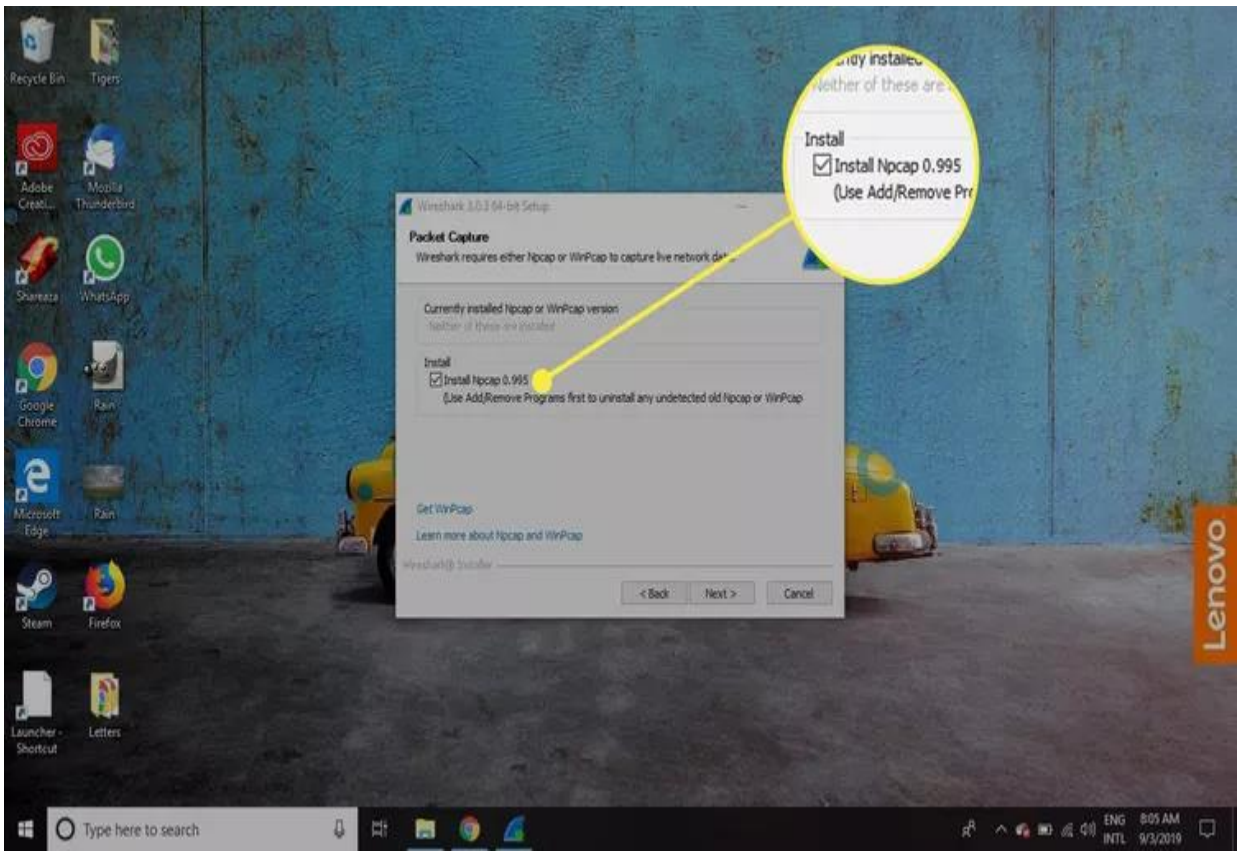
I. SOLVED EXERCISE:

1) Install, Capture and Analyze Data Packet Contents using Wireshark

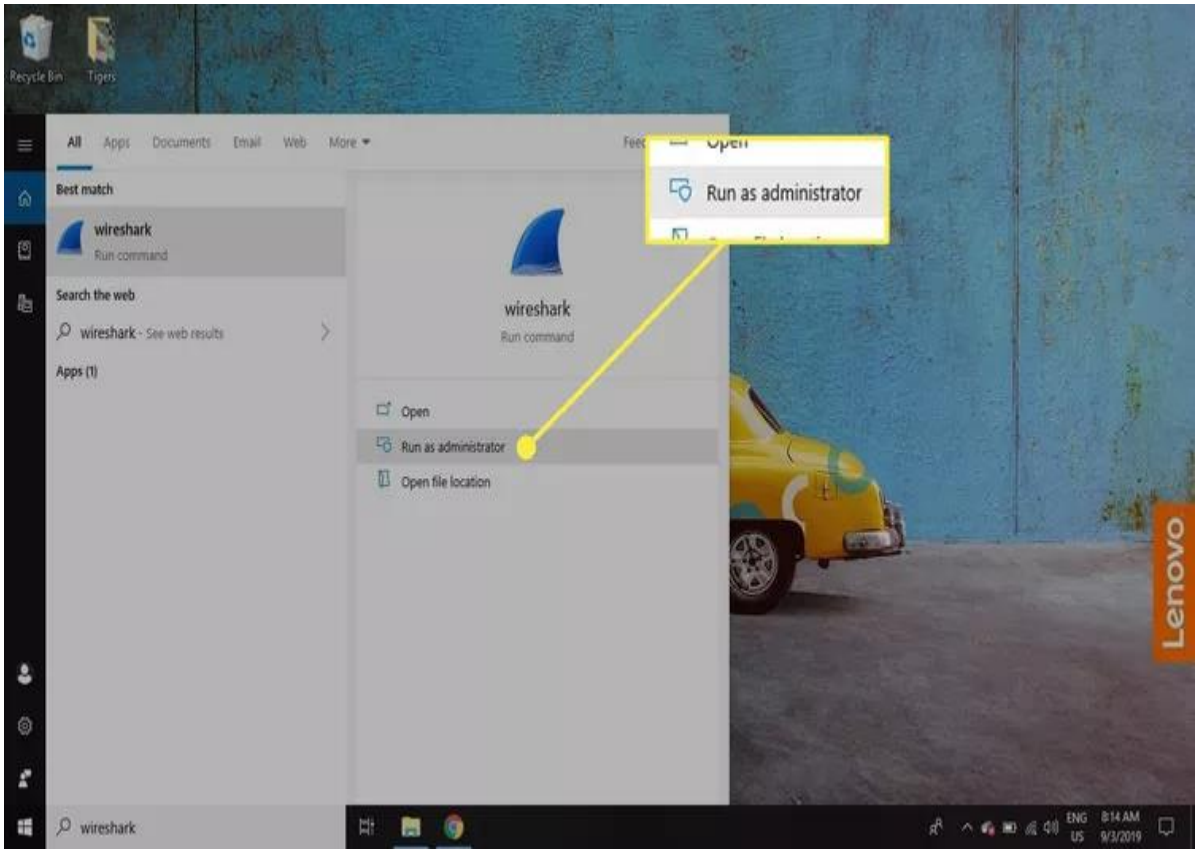
Wireshark can be downloaded at from the Wireshark Foundation website for both macOS and Windows.



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. You can also download Wireshark's source code from this page.

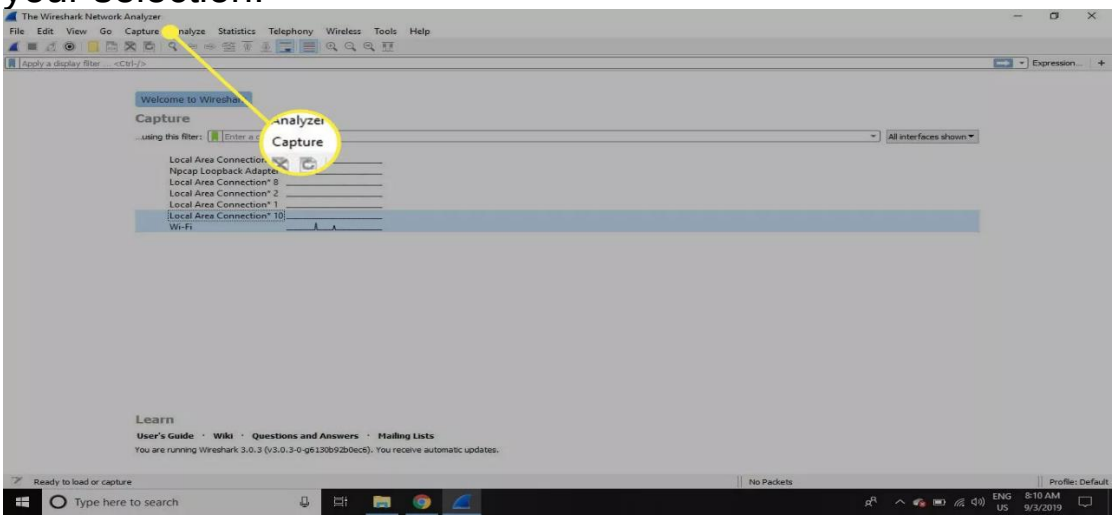
How to Capture Data Packets With Wireshark

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:

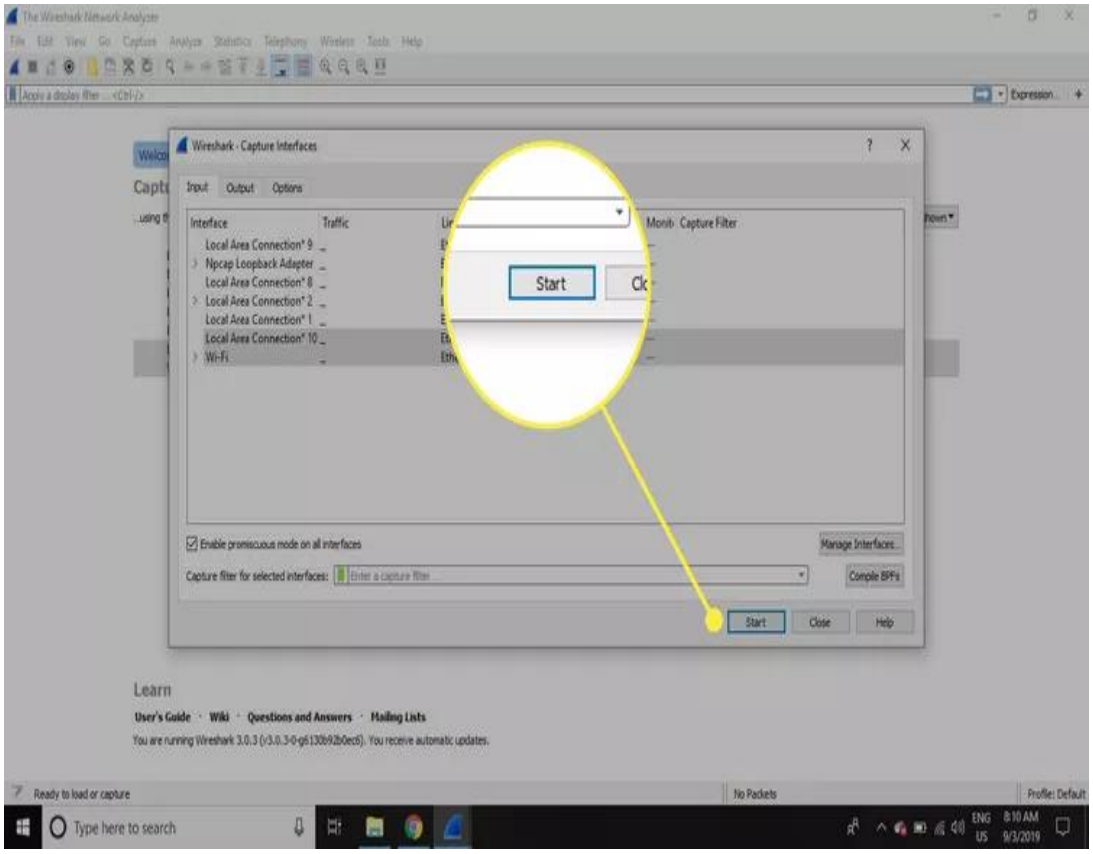
1. Select one or more of networks, go to the menu bar, then select **Capture**.

   To select multiple networks, hold the **Shift** key as you make your selection.

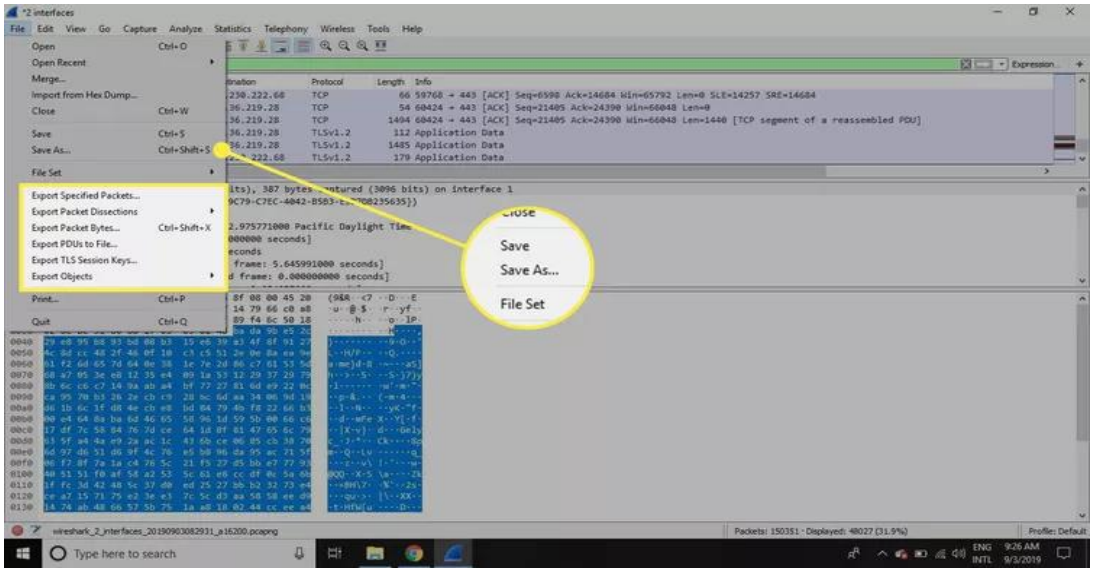


2. In the **Wireshark Capture Interfaces** window, select **Start**.

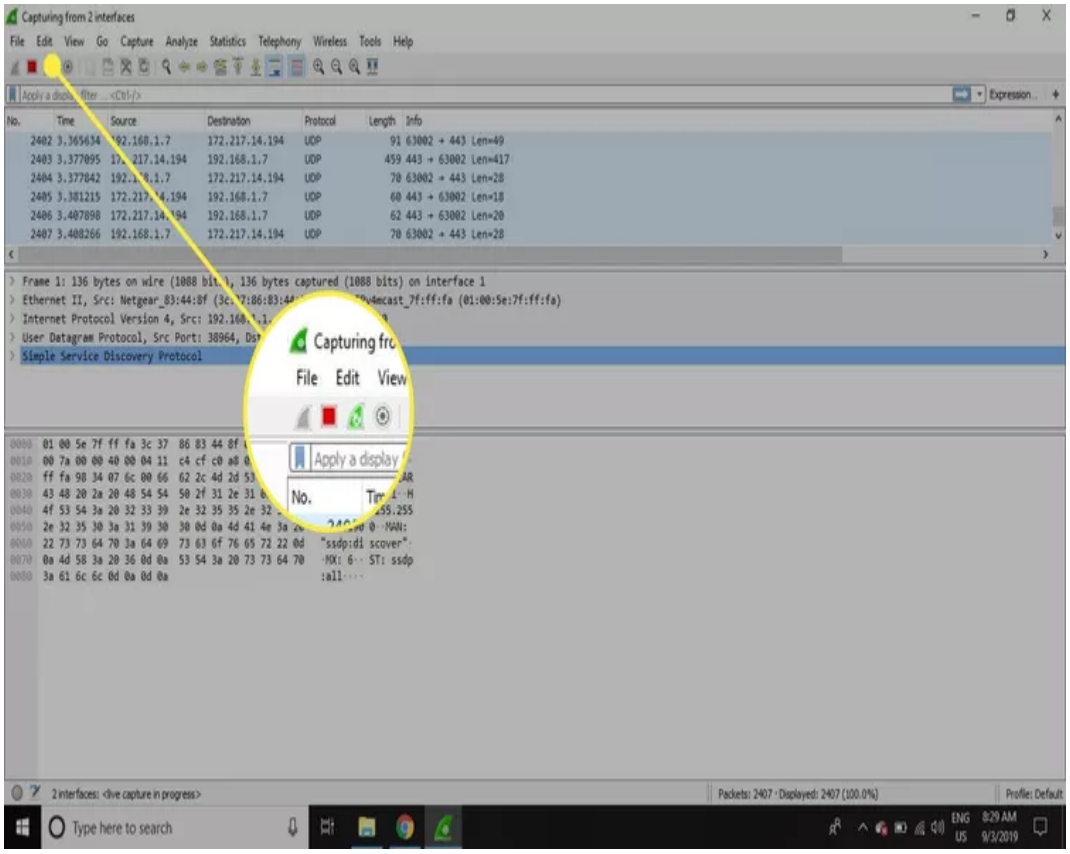
   There are other ways to initiate packet capturing. Select the **shark fin** on the left side of the Wireshark toolbar, press **Ctrl+E**, or double-click the network.



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



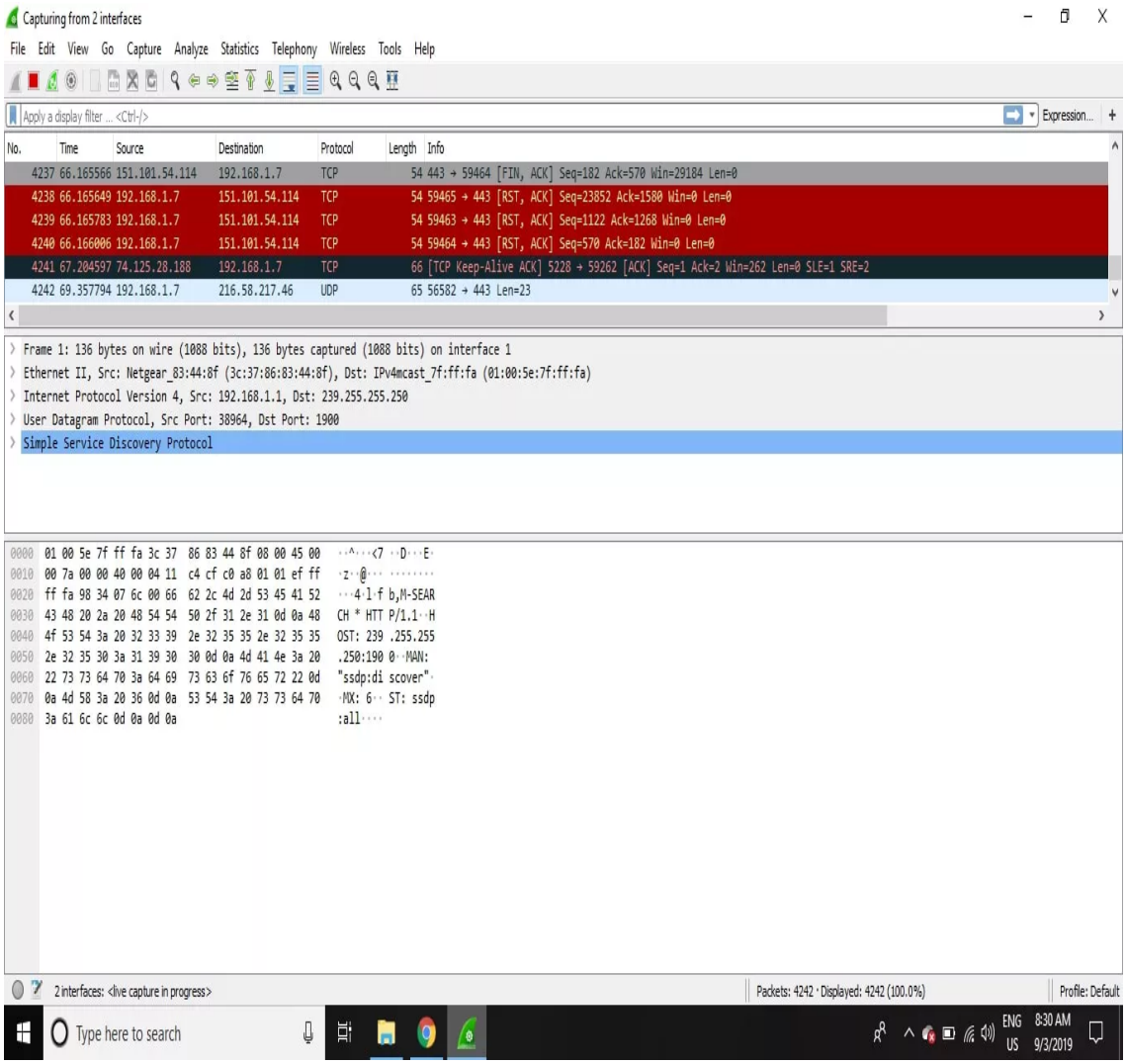
4. To stop capturing, press **Ctrl+E**. Or, go to the Wireshark toolbar and select the red **Stop** button that's located next to the shark fin.



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)



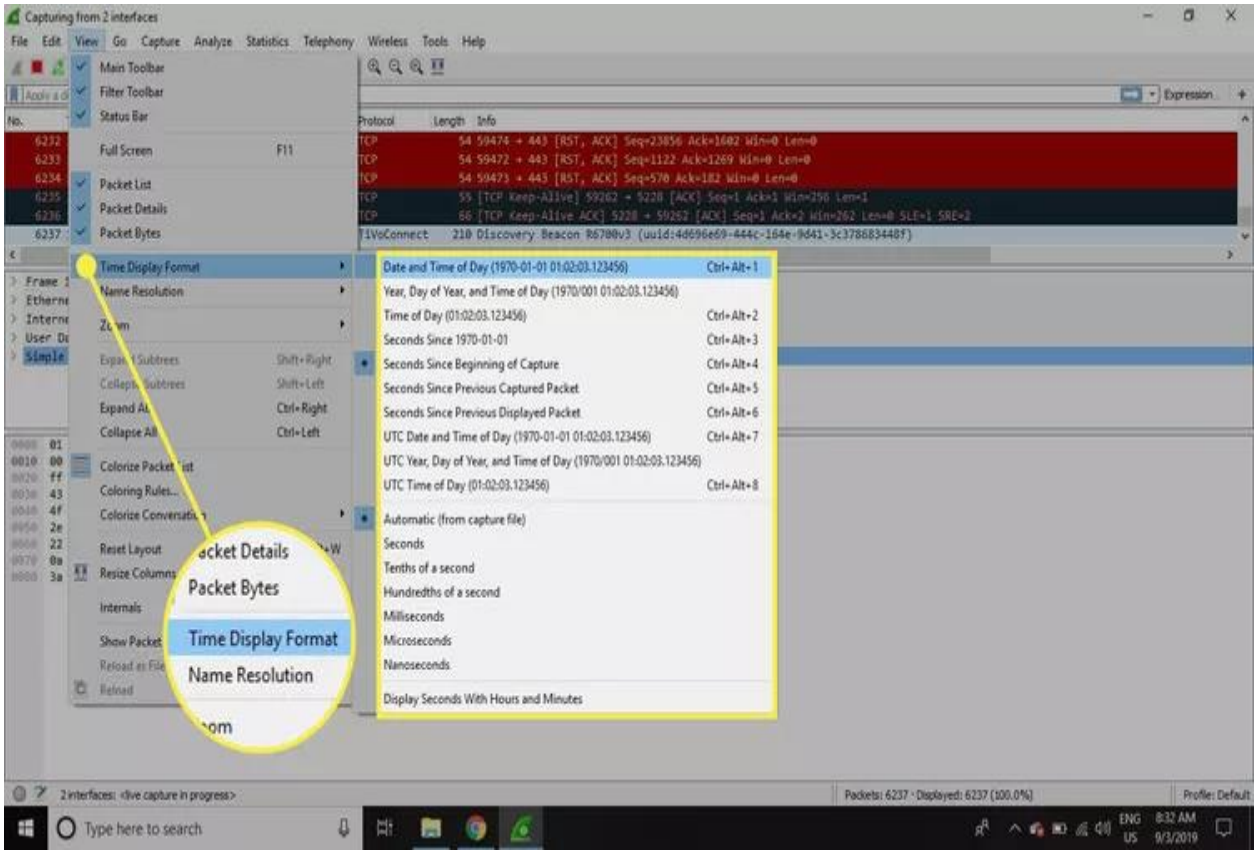
Packet List

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:

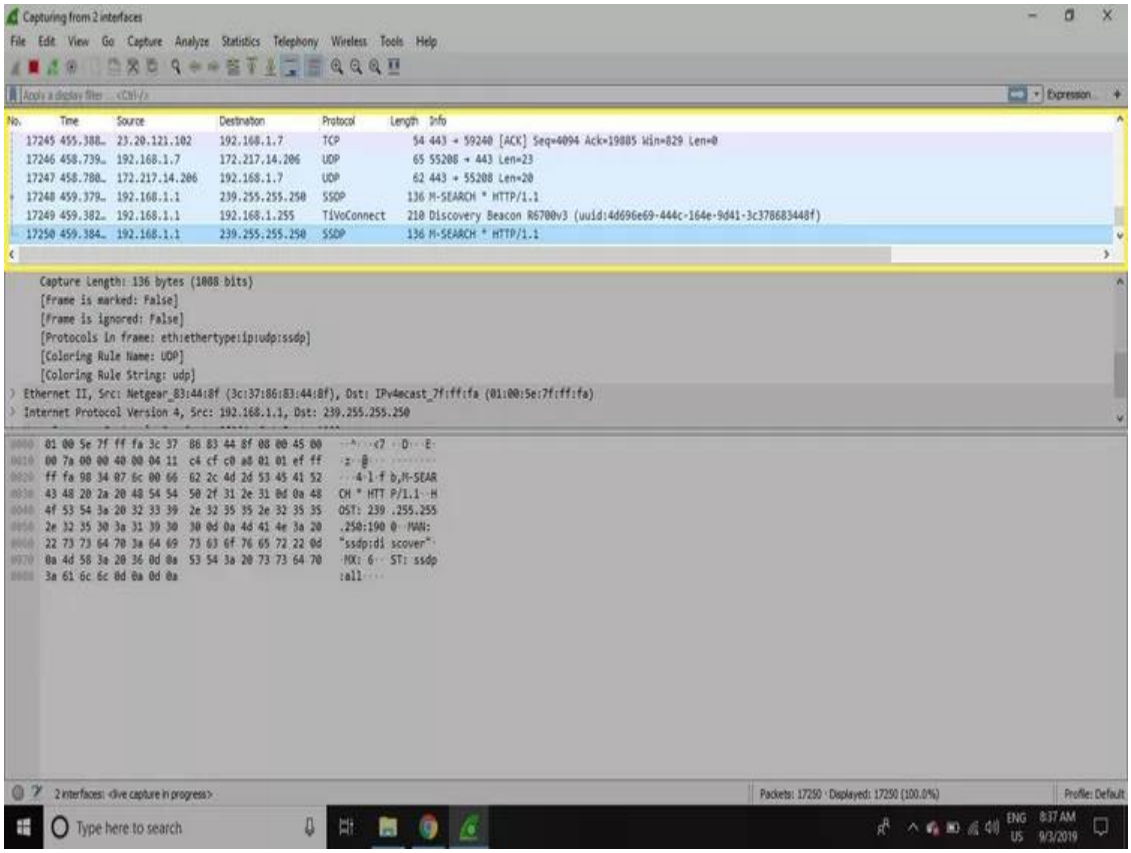
- **No**: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.
- **Time:** The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture 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.

To change the time format to something more useful (such as the actual time of day), select **View** > **Time Display Format**.

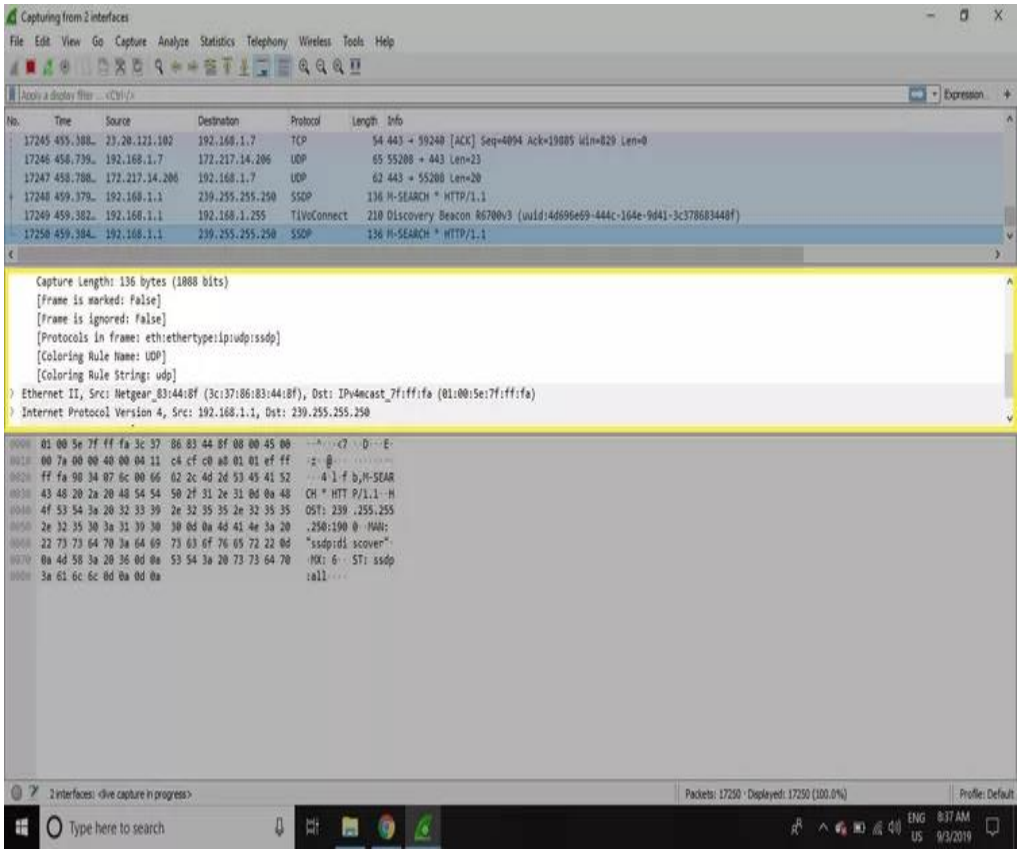


When a packet is selected in the top pane, you may notice one or more symbols appear in the **No.** column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of the conversation.



Packet Details

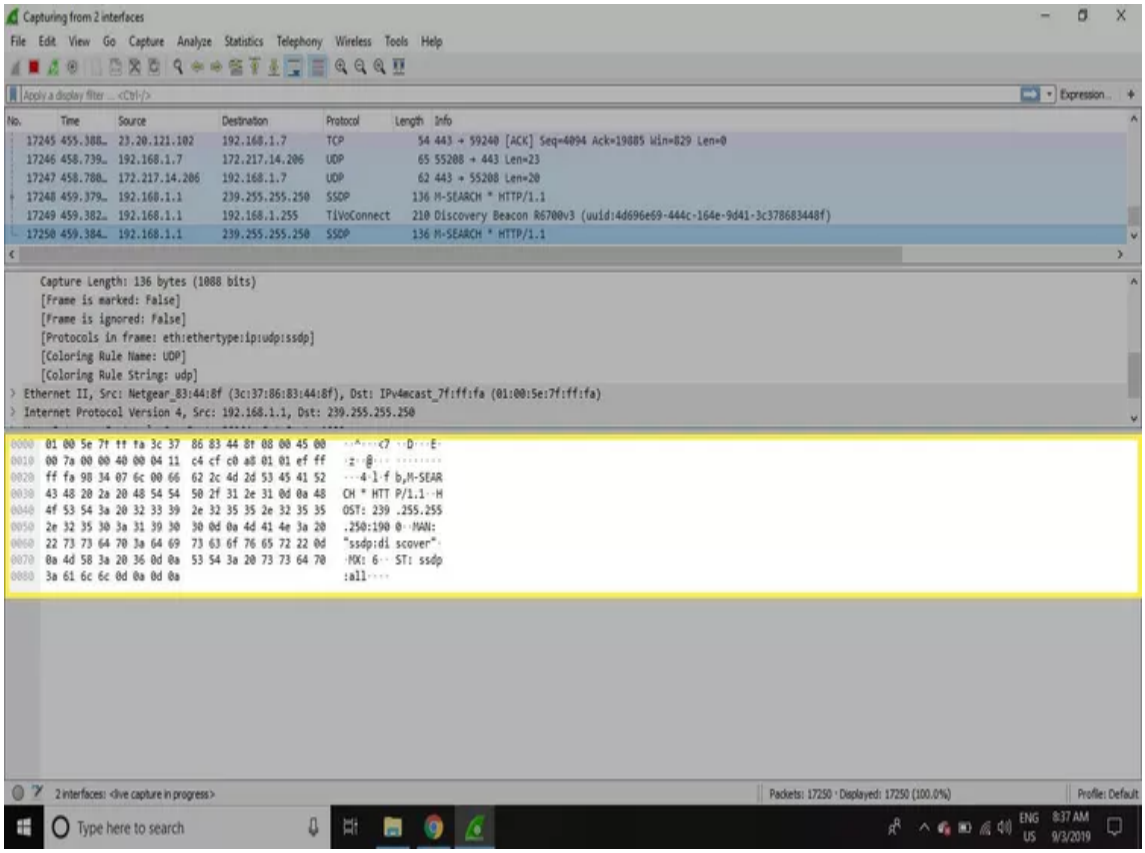
The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking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



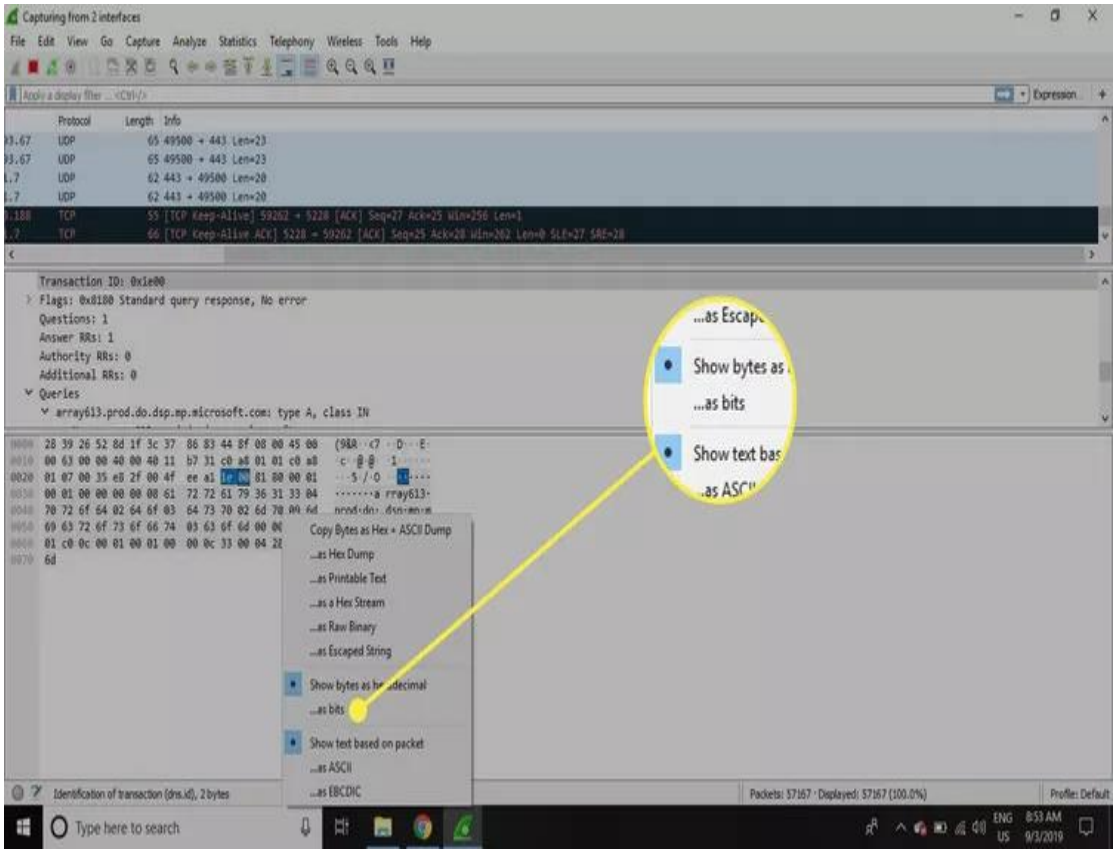
Packet Bytes

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**.



LAB EXERCISES

1.Identify specific type of packets as mentioned by the instructor using the Wireshark Filters further use the options under statistics tab (Use all possible interface with promiscuous mode)

2.Identify and obtain the input/output traffic graph using Wireshark.

3.Identify any website and demonstrate how confidential data is compromised (example: password or any other data).

4.Demonstrate major functionalities of the Wireshark tool.