**Experiment-2**

**Name:** Dhrish S Kumar

**Unique ID:** E0320008

**Problem Statement:**

Analysis of network traffic using packet capturing tools.

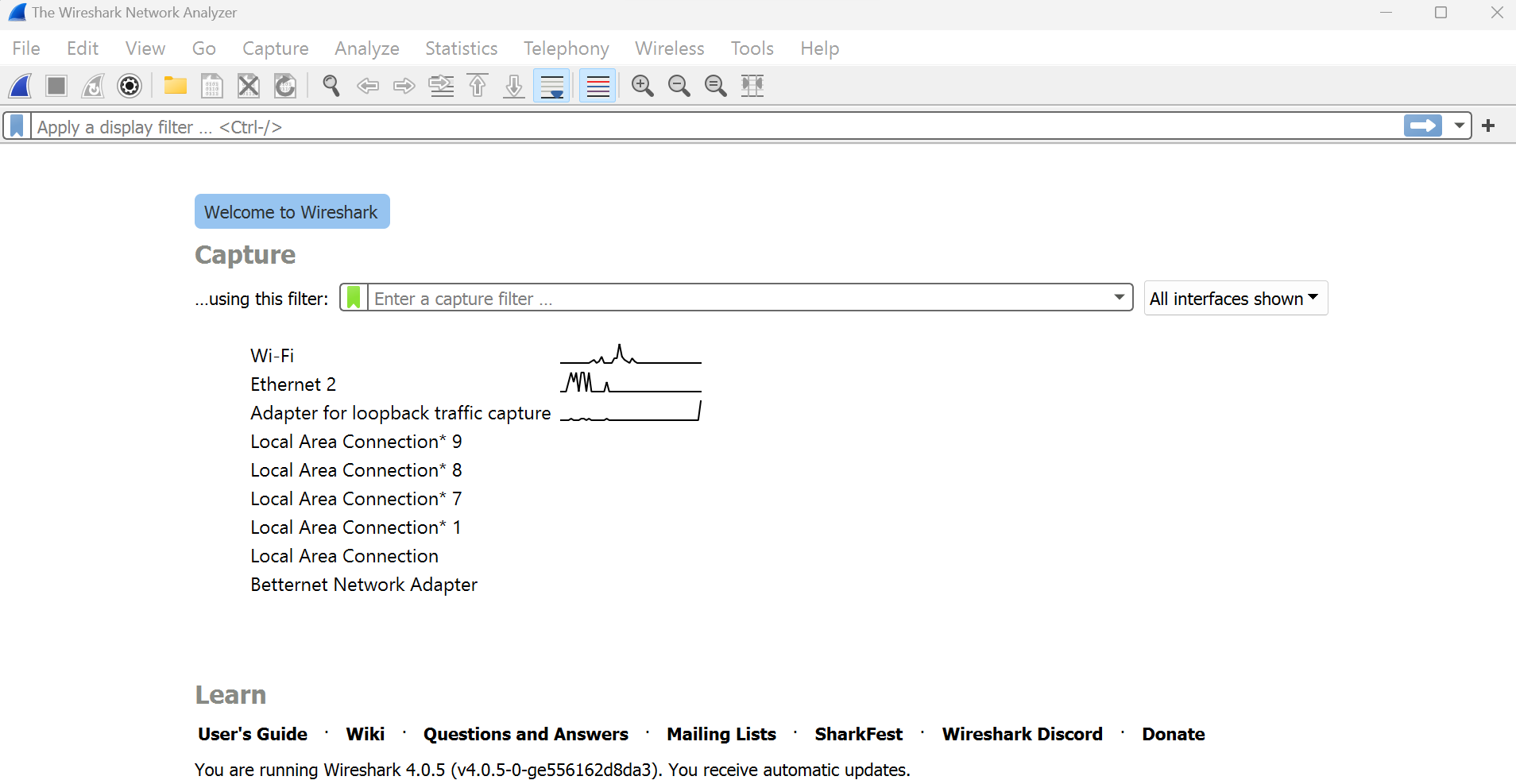
**Tools used:**

**WireShark:**

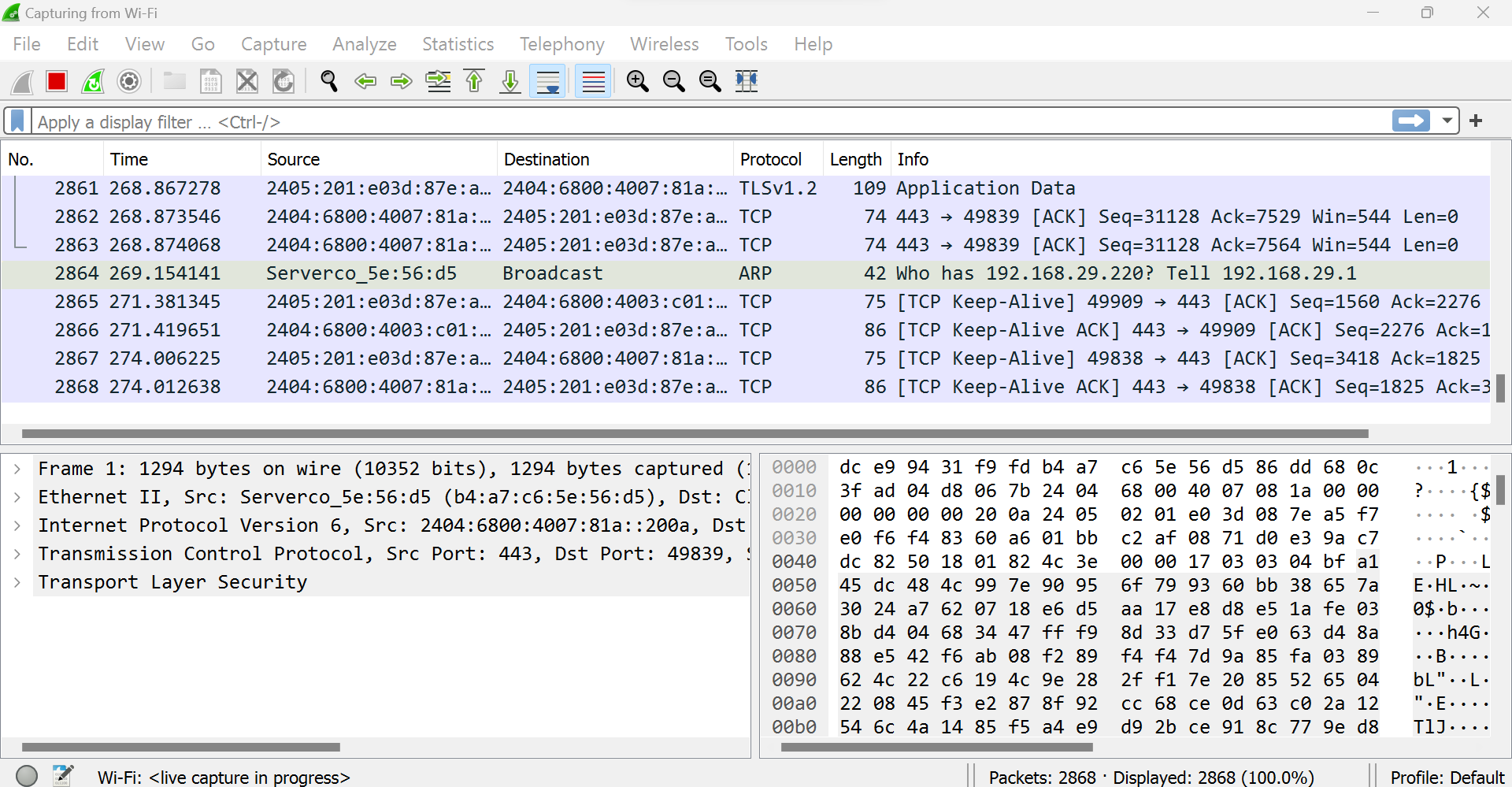
Wireshark is a free and open-source network protocol analyzer. It is widely used by network administrators, security professionals, and developers to capture, analyze, and troubleshoot network traffic in real-time. With Wireshark, you can inspect and analyze the packets flowing over a network, helping you understand network behavior, diagnose network issues, and investigate security incidents.

**Procedure:**

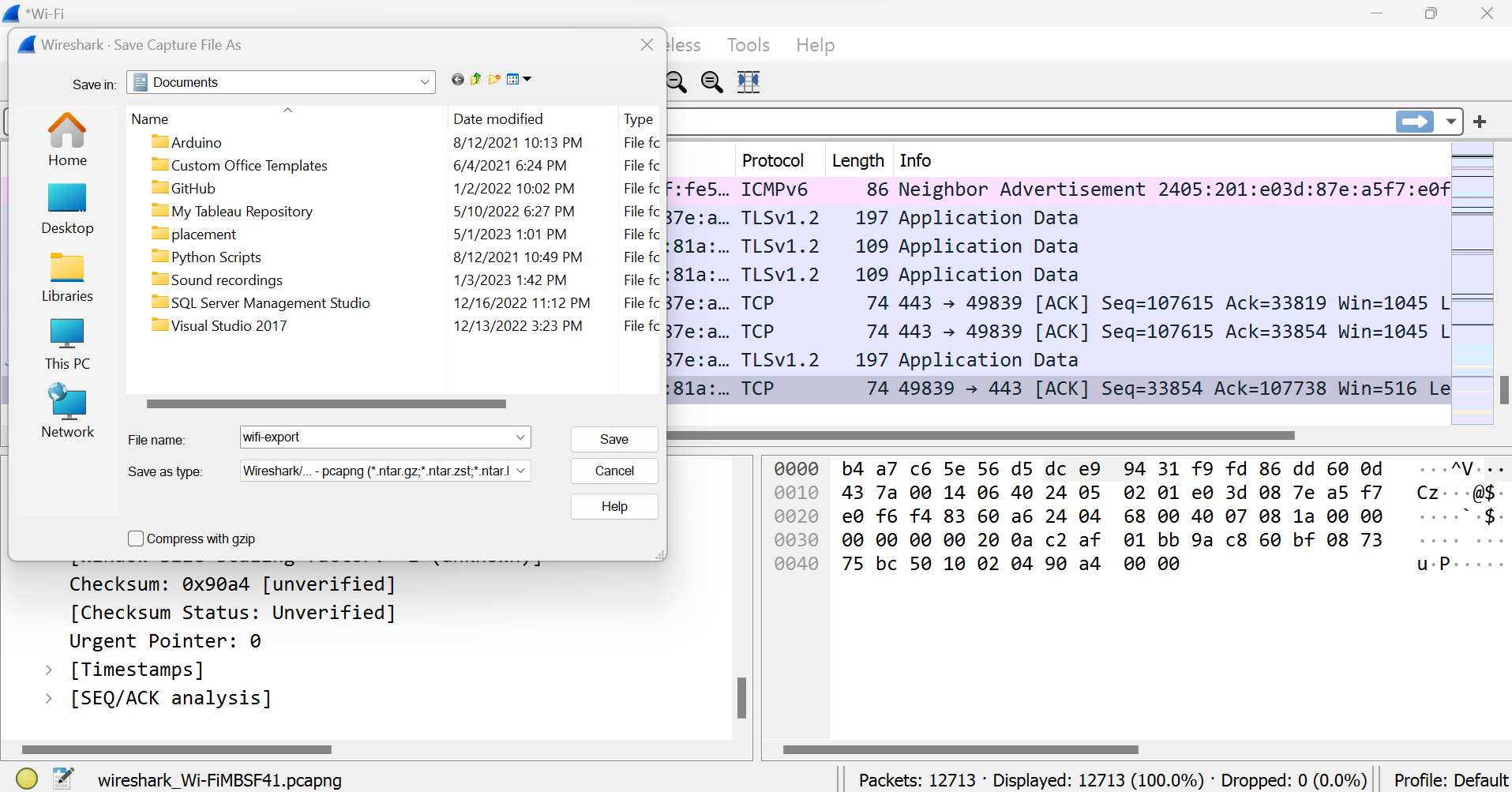
1. Select one or more of networks, go to the menu bar, then select Capture.



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

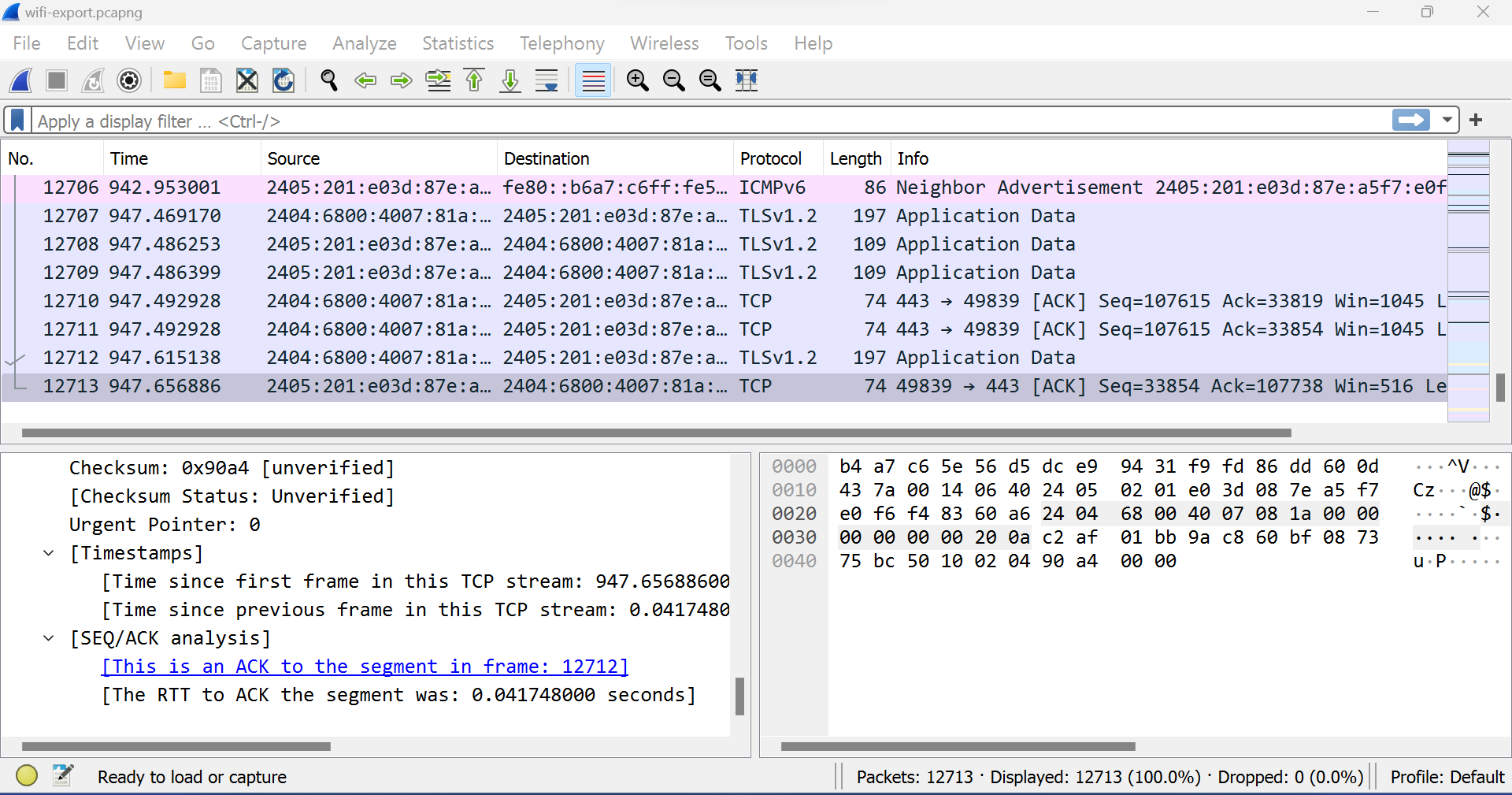


1. Select File > Save As or choose an Export option to record the capture.



To stop capturing, press Ctrl+E. Or, go to the Wireshark toolbar and select the

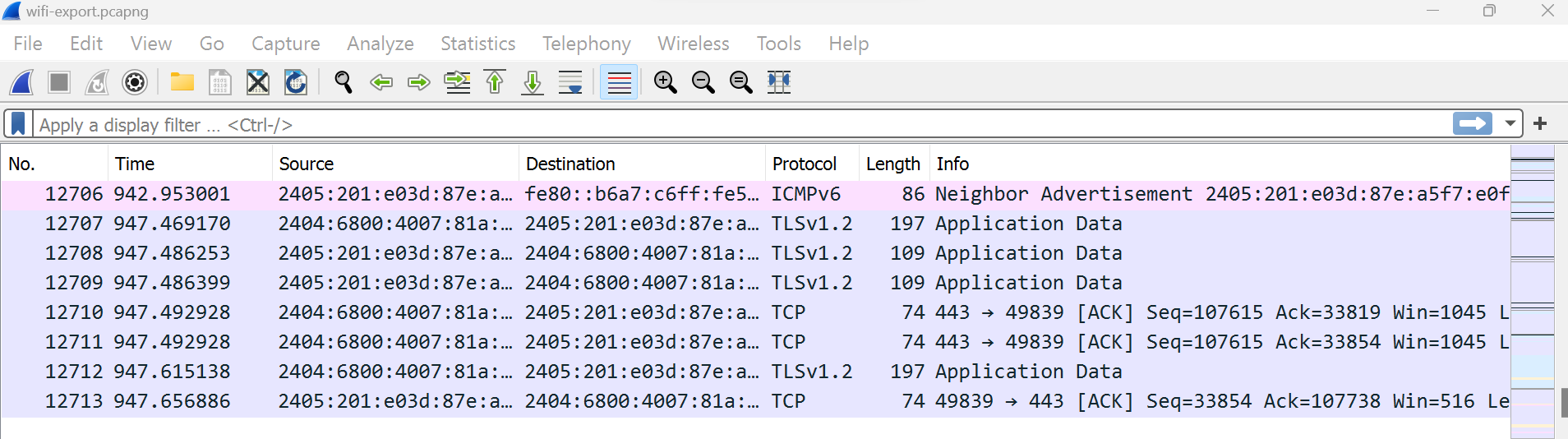
red Stop button that's located next to the shark fin.



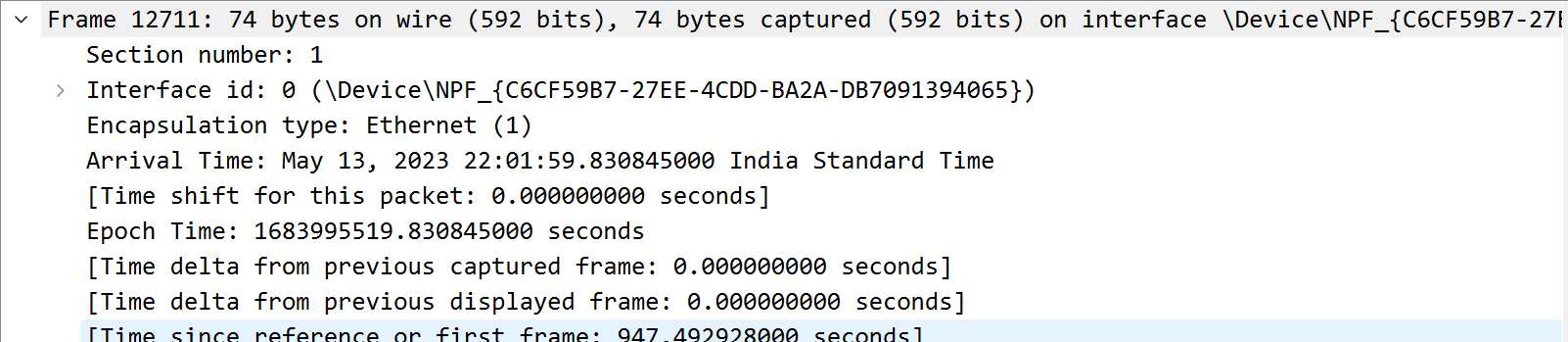
1. View and Analyze Packet Contents

The captured data interface contains three main sections:

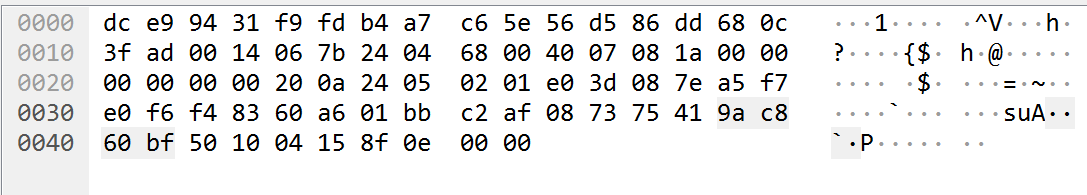
● The packet list pane (the top section)



● 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.

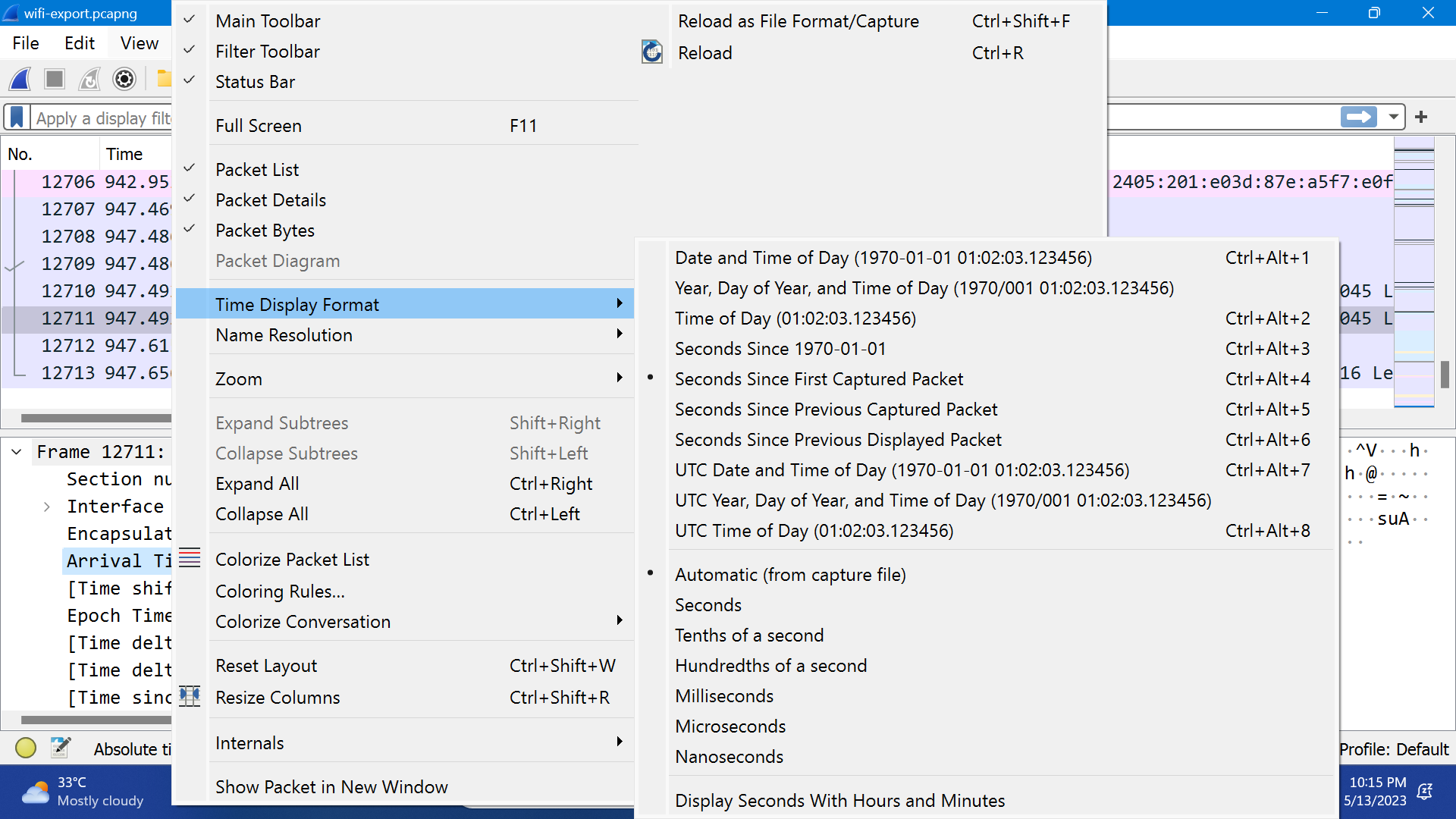
● Length: The packet length, in bytes, is displayed in this column.

● Info: Additional details about the packet are presented here. The contents of this

column can vary greatly depending on packet contents.

To change the time format to something more useful (such as the actual time of day),

select View > Time Display Format.



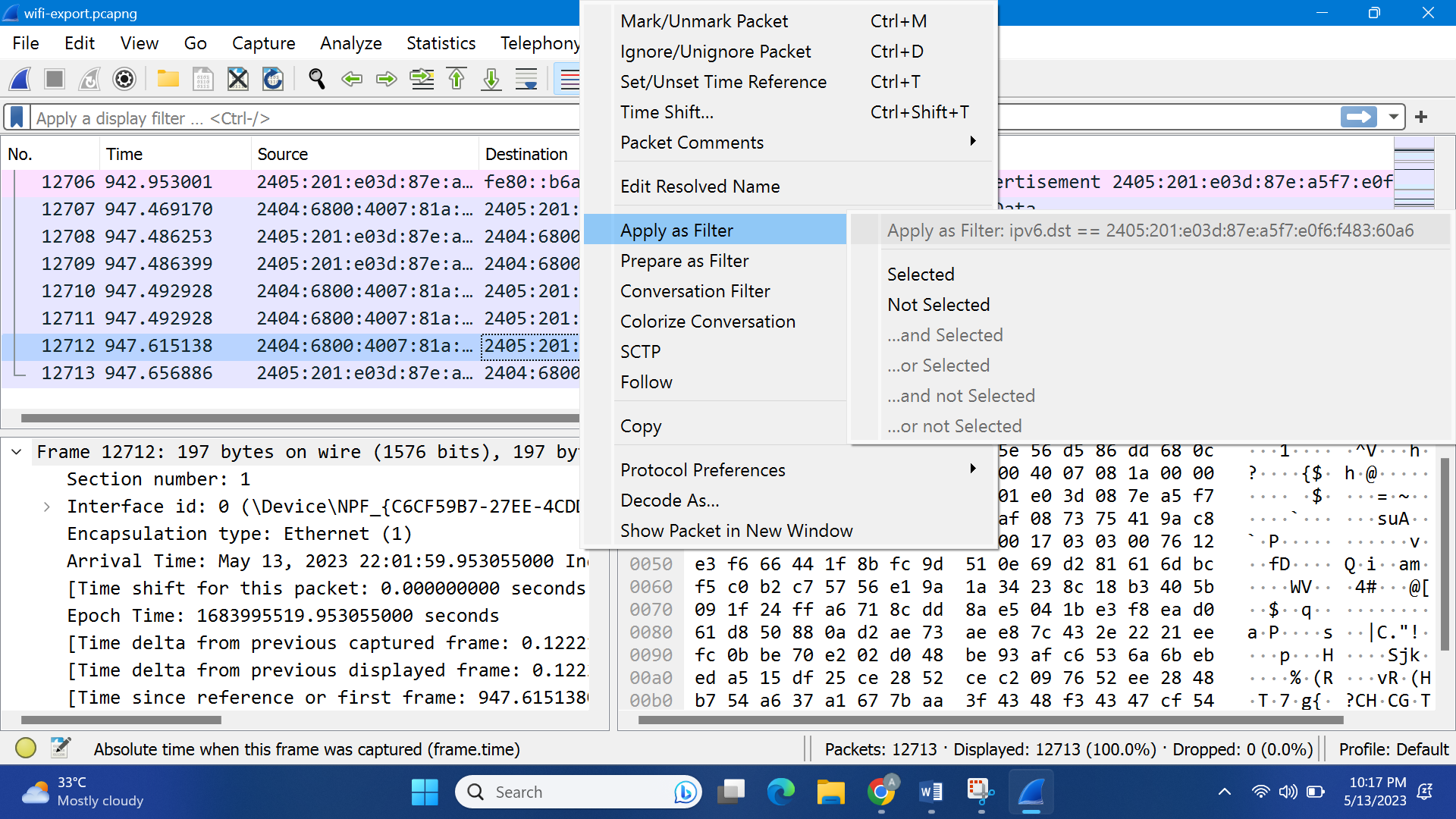
1. PACKET DETAILS

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



1. PACKET BYTES

At the bottom is the packet bytes pane, which displays the raw data of the selected packet in

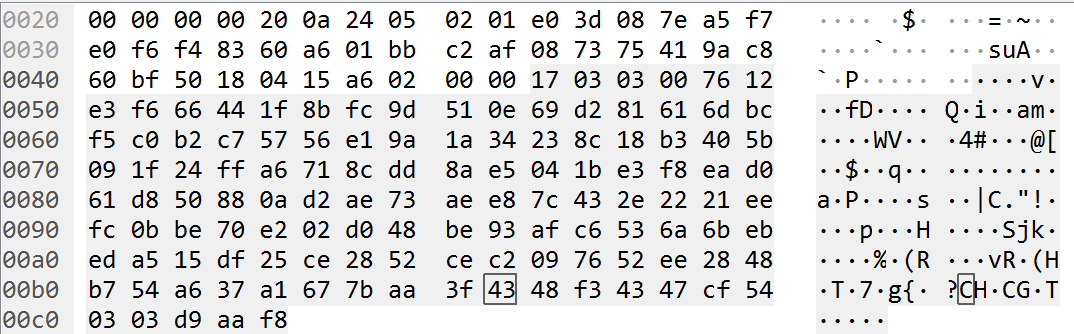
a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes

alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in

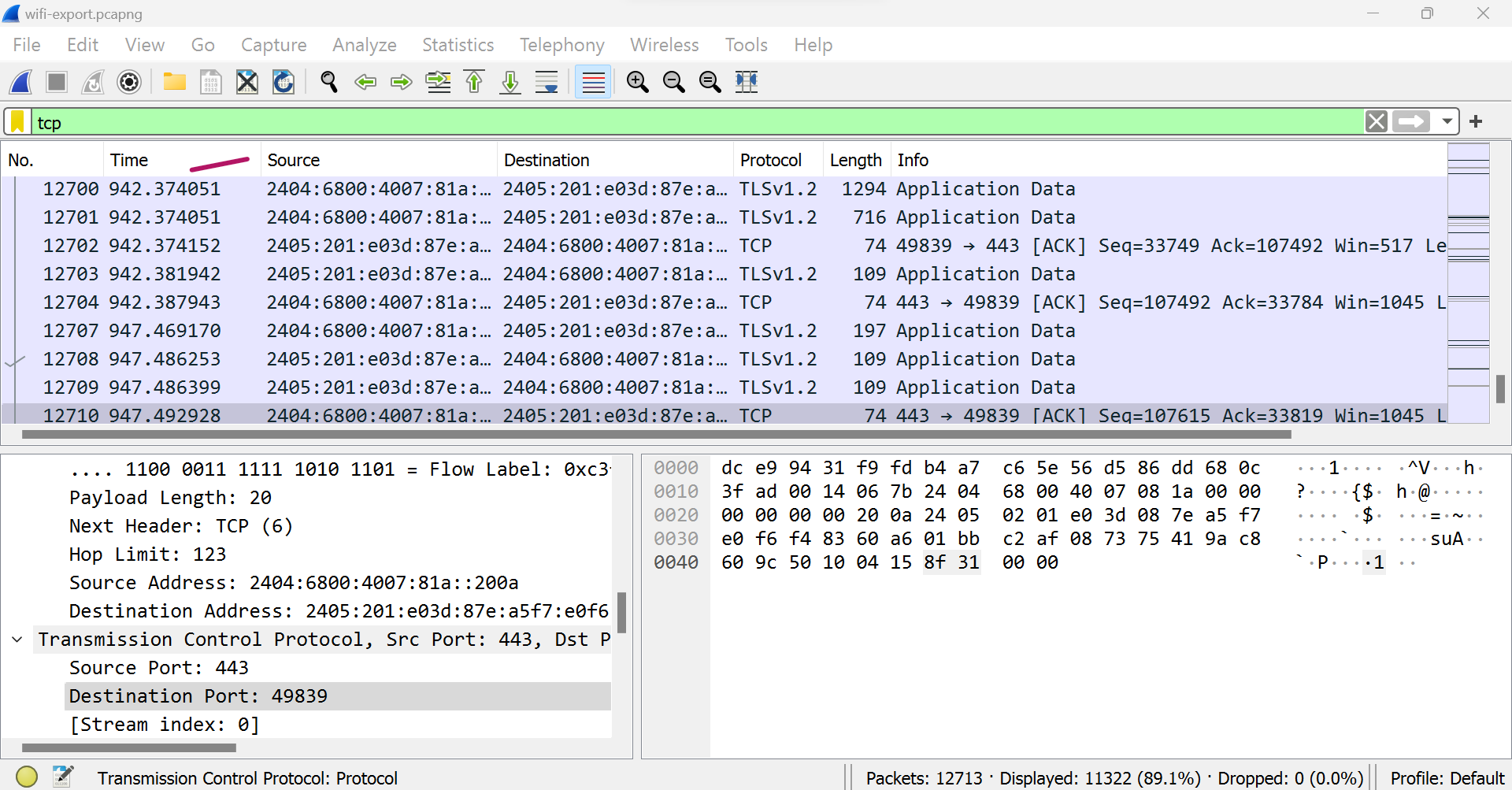
the packet details pane and vice versa. Any bytes that cannot be printed are represented by

a period.



To display this data in bit format as opposed to hexadecimal, right-click anywhere within the

pane and select as bits.



1. Using 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

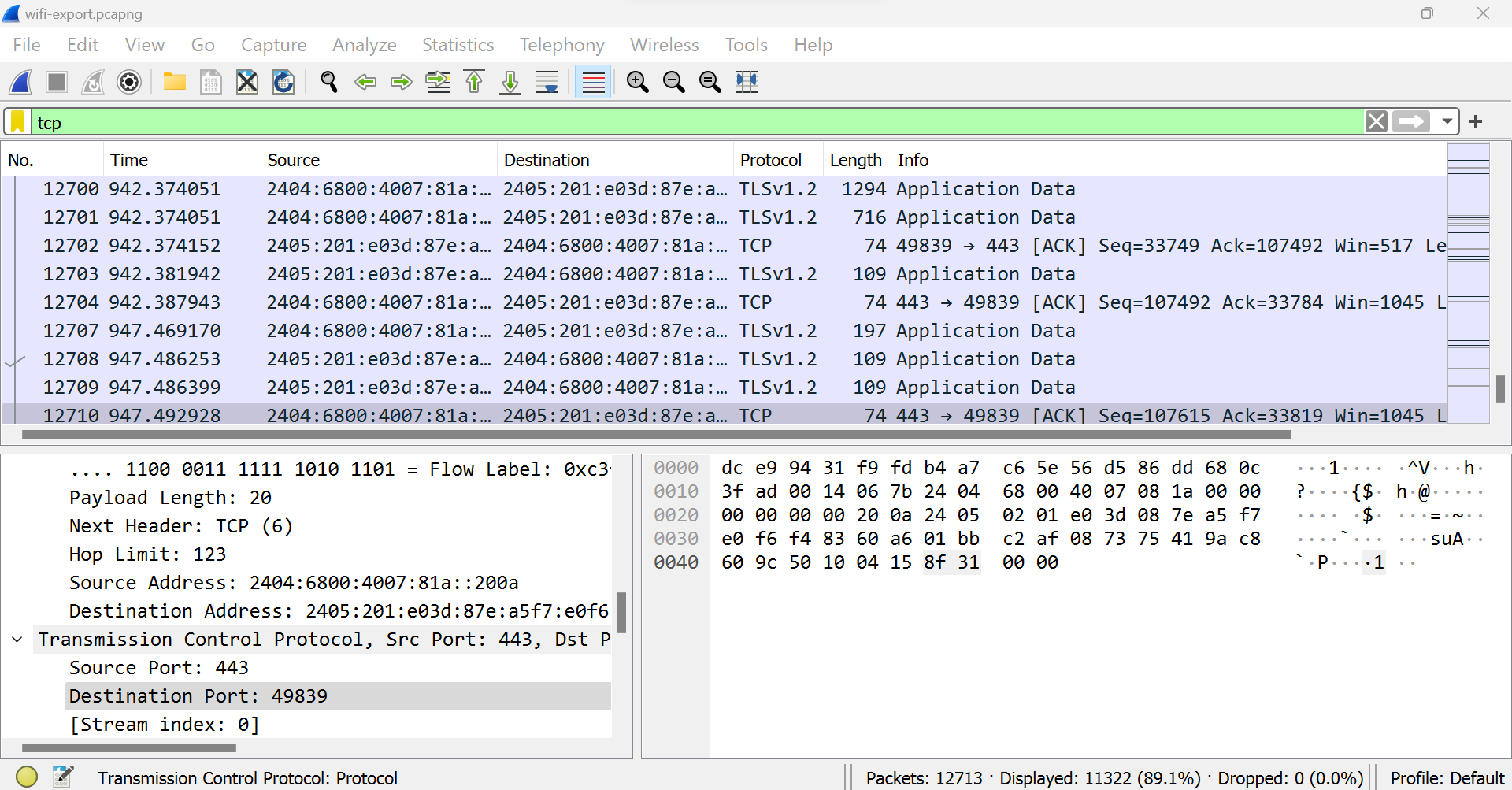
Wireshark toolbar or in the Enter a capture filter field located in the center of the welcome

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

moniter for the filter you're seeking.



Wireshark Color Rules:

While Wireshark's capture and display filters limit which packets are recorded or shown on

the screen, its colorization function takes things a step further: It can distinguish between

different packet types based on their individual hue. This quickly locates certain packets

within a saved set by their row color in the packet list pane.

