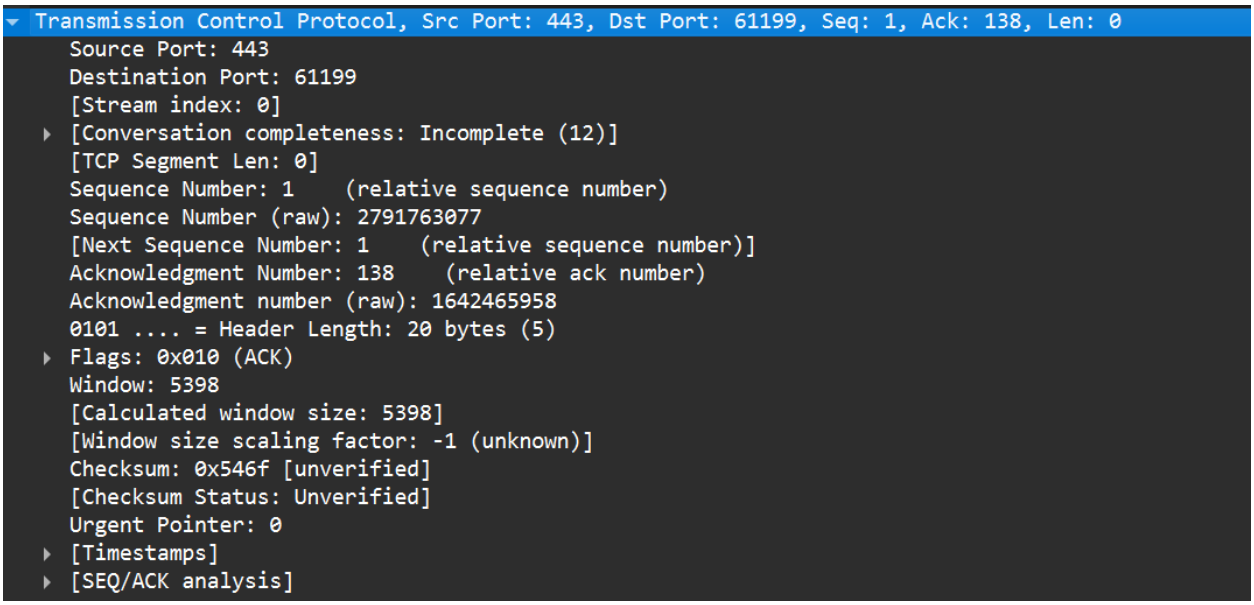
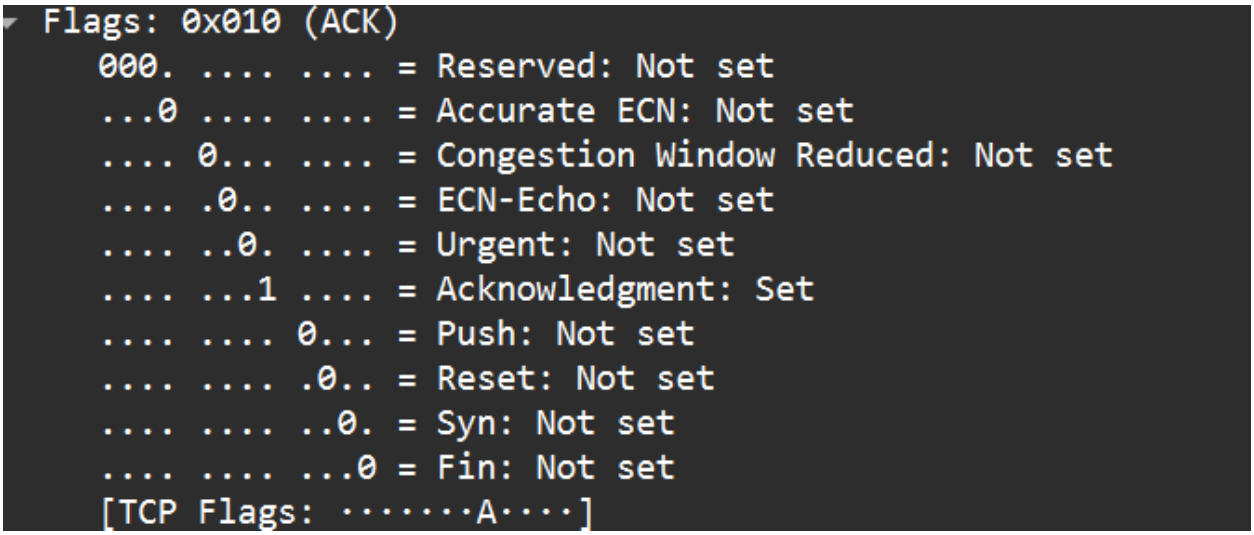
# Transmission control protocol packets in wireshark




Wireshark is a powerful network protocol analyzer that allows you to capture and examine the details of TCP packets, among other types of network traffic. When

analyzing TCP packets in Wireshark, you will encounter several key fields and features. Here's a guide on what to look for and how to interpret the information:

## Capturing TCP Packets

1. **Open Wireshark**: Start Wireshark and select the network interface you want to capture traffic on.
2. **Start Capture**: Click the "Start Capturing Packets" button (the shark fin icon).
3. **Apply Filter**: Use a filter to capture only TCP packets. The filter expression is `tcp`.

## Analyzing TCP Packets

When you capture TCP packets, you can see detailed information about each packet. Here are the main components of a TCP packet in Wireshark:

## Packet Details Pane

- **Frame**: Information about the captured frame, including the frame number and length.
- **Ethernet II**: Ethernet header information, including source and destination MAC addresses.
- **Internet Protocol Version 4 (IPv4)**: IP header information, including source and destination IP addresses.
- **Transmission Control Protocol (TCP)**: Detailed TCP header information:
  - **Source Port**: The port number on the source device.
  - **Destination Port**: The port number on the destination device.
  - **Sequence Number**: The sequence number of the first byte in the segment.
  - **Acknowledgment Number**: If the ACK flag is set, this field contains the value of the next sequence number that the sender of the segment is expecting to receive.
  - **Header Length**: The length of the TCP header.

- **Flags**: Control flags such as SYN, ACK, FIN, RST, PSH, URG, and ECE. Common combinations:
  - **SYN**: Synchronize sequence numbers (initiating a connection).
  - **ACK**: Acknowledgment field significant (acknowledging received data).
  - **FIN**: Finish flag (indicating the sender has finished sending data).
  - **RST**: Reset the connection.
  - **PSH**: Push function (data should be passed to the application as soon as possible).
  - **URG**: Urgent pointer field significant.
  - **ECE**: Explicit Congestion Notification Echo.
- **Window Size**: The size of the sender's receive window (buffer space available).
- **Checksum**: Used for error-checking the TCP header and data.
- **Urgent Pointer**: If the URG flag is set, this field is significant.
- **Options**: Various TCP options, such as Maximum Segment Size (MSS), Window Scale, and Timestamps.

## Common TCP Packet Types

- **SYN**: The initial packet sent to establish a TCP connection.
- **SYN-ACK**: The packet sent in response to a SYN, indicating readiness to establish a connection.
- **ACK**: Acknowledgment packet, often sent in response to receiving data.
- **FIN**: Packet indicating the sender wants to close the connection.
- **RST**: Packet indicating that the connection should be reset.

## Interpreting TCP Streams

Wireshark allows you to follow and analyze entire TCP streams:

1. **Select a Packet**: Right-click on a TCP packet and select "Follow" > "TCP Stream".
2. **View the Stream**: Wireshark will display the conversation between the two endpoints in a separate window.