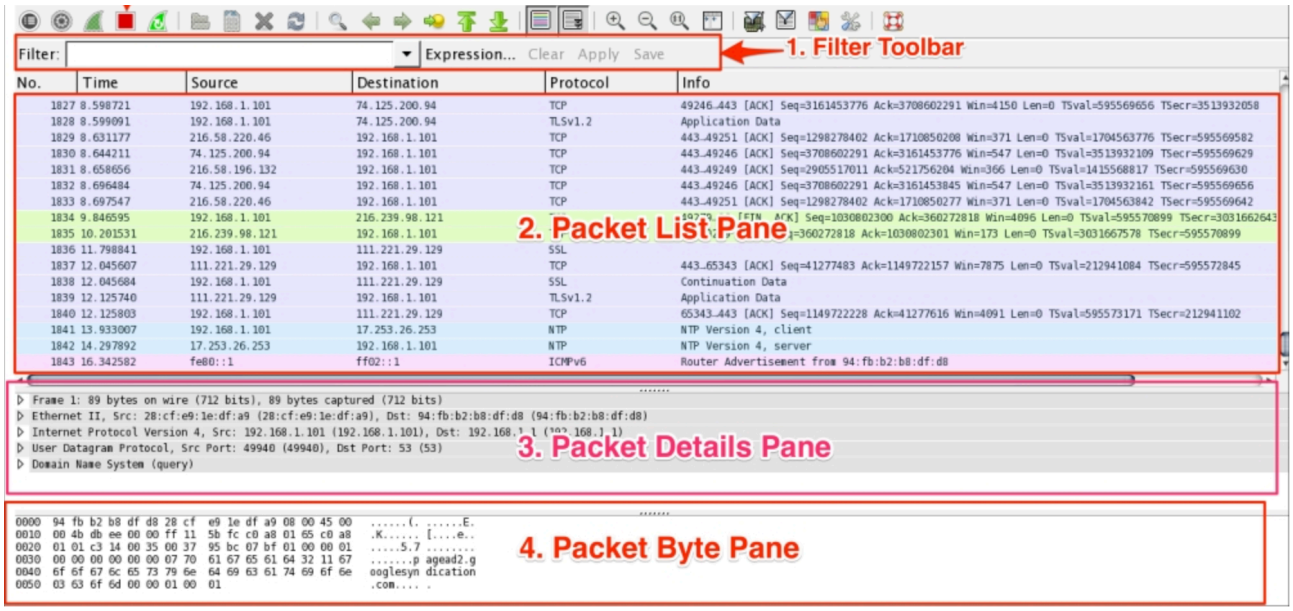
Wireshark Analysis Instructions

1. **Opening the Capture File:**
    - Launch Wireshark and open the provided .pcap file.
    - Familiarize yourself with the Wireshark interface: the filter toolbar at the top, the packet list pane below the filter toolbar, the details pane in the middle, and the packet bytes pane at the bottom.



2. **Applying Display Filters:**
    - Use display filters to narrow down the traffic. For example, if you know the communication involves a specific IP address or port, enter a filter like:
        - `ip.addr == x.x.x.x` (replace `x.x.x.x` with an IP address of interest)
        - `tcp.port == 5000` or `udp.port == 5000`
    - Or you can use TCP to display packets only for the TCP protocol when you have different protocols in the traffic.
3. **Following Streams:**
    - Right-click on a packet that appears to contain relevant data and select “Follow TCP Stream” (or UDP Stream if applicable). This feature allows you to see the entire conversation in one window.
    - Analyze the stream to observe if and when the data changes or if there is any evidence of interference.
5. **Comparing Packets:**
    - Identify and compare packets that are supposed to be similar. Look for any discrepancies in the payloads, such as differences in coordinate values.
    - Note the timestamps and sequence numbers to understand the order of packets and pinpoint when changes occur.
6. **Noting Anomalies:**

- Document any anomalies you find. For instance, if the same communication shows different coordinate values in different packets, this might indicate data manipulation.
- Pay attention to the source IP addresses—if you see unexpected or repeated IPs, that could be a sign of an attacker's involvement.

7. **Utilizing Wireshark Tools:**

   - **Statistics:** Use Wireshark's statistics features (e.g., "Protocol Hierarchy" or "Endpoints") to get an overview of the traffic and identify unusual patterns.
   - **Exporting Data:** If needed, export specific packets or streams to review in more detail or to include as part of your report.

8. **General Approach:**

   - Start by getting an overview of the traffic.
   - Narrow down to the segments relevant to GPS data.
   - Compare "before" and "after" states of the data.
   - Focus on identifying the attacker's IP and any manipulation in the payload.