

CHALLENGE NAME: [Leaky Streams]   
DEV : [Bhakti,Dhanashri]

CATEGORY: [Digital Forensics]   
LEVEL: [Easy]

2025

CHALLENGE NAME: []

**Challenge Description**: In the middle of our conversation, some packets went amiss. We managed to resend a few but they were slightly altered.

Help me reconstruct the message and I'll reward you with something useful ;)

**Solution: Got it! Your Wireshark digital forensics challenge involves extracting a flag that is split into two parts:**

**1. Open the PCAP File in Wireshark**

**Load the .pcap file in Wireshark.**

**2. Finding Packet Retransmissions**

**Retransmissions occur when a sender resends a packet because it was not acknowledged.**

**Apply this filter to identify retransmitted packets:**

**tcp.analysis.retransmission**

**Alternatively, check for fast retransmissions:**

**tcp.analysis.fast\_retransmission**

**Go through the retransmitted packets to see if any contain readable text, a partial flag, or encoded data.**

**Follow TCP Stream (Right-click → Follow → TCP Stream) to reconstruct conversations and extract the first part of the flag.**

**3. Finding Unsent Data**

**Unsent data can exist in packets that were lost, not acknowledged, or never successfully transmitted.**

**Use this filter to locate unacknowledged segments:**

**tcp.analysis.lost\_segment**

**Another approach is to check TCP zero-window conditions, which indicate data might have been buffered but never sent:**

**tcp.analysis.zero\_window**

**Look for incomplete messages or fragments of text that might contain the second part of the flag.**

**4. Reconstruct the Flag**

**Combine both extracted parts from retransmissions and unsent data to get the full flag.**

**If parts are encoded (Base64, Hex, XOR), decode them.**

**The final flag might follow a standard format like CTF{...} or {flag\_part1\_flag\_part2}.**