# TCP Completeness Cheatsheet By Betty DuBois of Packet Detectives

| Wireshark Column Description | Wireshark Assigned Value | Description |
|---|---|---|
| Incomplete, SYN_Sent | 1 | SYN only. If it happens once in a stream it could be just packet loss. If it happens multiple times, it was likely dropped by the firewall. |
| SYN/ACK | 2 | You would not see only a 2, that would just be weird. You'll see it in combination with other values. |
| ACK | 4 | If there are only ACKs in a stream, are they Keep-Alives or are they recon scans hoping for RSTs? |
| DATA | 8 | The reason we use TCP, all conversations should have some unless a handshake is the last few packets in the pcap. |
| FIN | 16 | Graceful tear down. |
| RST | 32 | Talk to the hand. |
| Those are the only possibilities, but when you combine them..... | | |
| Complete, no Data | 23, 39, 55 | 23 Handshake + Fin, but no Data. Weird. 1+2+4+16=23<br>39 Handshake + RST, but no Data. Weird. 1+2+4+32=39<br>55 Handshake + Fin + RST, but no Data. Weird. 1+2+4+16+32=55 |
| Complete, with Data | 31, 47, 63 | 31 Handshake, Data, FIN. 1+2+4+8+16=31<br>47 Handshake, Data, but a RST vs FIN. 1+2+4+8+32=47<br>63 Everything, both FIN and RST 1+2+4+8+16+32=63 |
| Incomplete | 3, 4, 12, 20, 22, 28, 33, 35, 36, 37, 44, 52, 60 | 3 SYN + SYN/ACK, missing ACK<br>4 ACK only, missing handshake, data and tear down, weird or just keep-alives check for pattern in timing<br>12 ACK+DATA, missing handshake and tear down<br>20 ACK+FIN, missing handshake and data<br>22 SYN/ACK+ ACK+FIN, missing SYN and data<br>28 ACK+DATA+FIN, missing handshake<br>33 SYN+RST, the port is closed and the RST came from either the actual server, or an IDS on the server's behalf<br>35 SYN+SYN/ACK+RST, missing data, and FIN<br>36 ACK+RST, no handshake, data or tear down<br>37 SYN+ACK+RST, no SYN/ACK<br>44 ACK+DATA+RST, no SYN or SYN/ACK. The closer they are to the beginning of the pcap, the more normal they are. The conversations had already been happening **before** you started capturing.<br>52 ACK+FIN+RST, no handshake or data. Same note as 44 but no data.<br>60 ACK+DATA+FIN+RST, same as 52 but with data. |
| Incomplete, with Data | 15 | SYN+SYN/ACK+ACK+DATA, is this at the end of the pcap? Or is it just that the socket is still open, but the capture stopped? 1+2+4+8=15 |
| Incomplete, Established | 7 | SYN+SYN/ACK+ACK, handshake, but nothing else. 1+2+4=7 |