

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

01 / Quick reference and concepts

Find the conversation, inspect handshake failures and use TCP analysis flags as leads rather than verdicts.

Wireshark display filters for captured traffic. Capture filters use a different language; field availability depends on installed Wireshark version.



A capture shows what reached the observation point. Missing packets may reflect capture loss, asymmetric paths or a filter, rather than network loss.

Task	Display filter	Interpretation
One IPv4 host	<code>ip.addr == 192.0.2.10</code>	Either direction
One IPv6 host	<code>ipv6.addr == 2001:db8::10</code>	Either direction
HTTPS TCP traffic	<code>tcp.port == 443</code>	Does not prove HTTP or decryption
Initial SYN	<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>	Connection attempts
Reset	<code>tcp.flags.reset == 1</code>	Inspect sender and timing
DNS query	<code>dns.flags.response == 0</code>	Only decoded DNS
DNS errors	<code>dns.flags.response == 1 && dns.flags.rcode != 0</code>	Error response; inspect code
Retransmission lead	<code>tcp.analysis.retransmission</code>	Analyzer heuristic
Single stream	<code>tcp.stream == 7</code>	Index belongs to this capture

What to understand first

- Display filters select packets already in the capture. They do not reduce the original capture file. Use a capture filter only when its narrower acquisition scope is deliberate.
- Boolean fields must be compared to their value when checking a flag. `tcp.flags.syn` tests field presence; `tcp.flags.syn == 1` checks whether SYN is set.
- TCP analysis marks are derived from observed sequence and timing. Missing capture packets, offload and out-of-order arrival can affect conclusions.
- DNS and HTTP filters only work when those protocols are decoded and visible. Encrypted DNS, TLS and QUIC cannot be interpreted as cleartext by merely choosing a port.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Wireshark display bar

Read-only analysis filters

```
ip.addr == 192.0.2.10 && tcp.port == 443
tcp.flags.syn == 1 && tcp.flags.ack == 0
tcp.analysis.retransmission || tcp.analysis.fast_retransmission
```

Inspect: Select the failing tuple first, then inspect sequence, acknowledgment and timing in the full stream.

Conversation triage

Read-only analysis filters

```
dns.flags.response == 1 && dns.flags.rcode != 0
tcp.flags.reset == 1
tcp.analysis.zero_window
```

Inspect: An error, reset or zero window needs source identity and surrounding packets to explain it.

Illustrative handshake timeline

Illustrative teaching example, not captured device output.

```
0.000s Client -> Server: SYN
1.000s Client -> Server: SYN retransmission
3.000s Client -> Server: SYN retransmission
No SYN-ACK observed at this capture point
```

- This shows no observed response here. Check capture completeness, server-side receipt and the return path.
- A second authorized capture near the server can distinguish a missing request from a missing reply.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

03 / Troubleshooting and acceptance

1. Record capture point, interfaces, clock accuracy, tuple and any acquisition filter.
2. Select the conversation and inspect SYN/SYN-ACK/ACK or the applicable UDP exchange.
3. Follow the stream and compare failures with a successful attempt under similar conditions.
4. Correlate retransmissions, resets, windows and response times with endpoint and network logs.
5. Preserve the original capture; share only the authorized minimum with a clear conclusion and its limits.

Common mistakes

- Pasting a display filter into a capture-filter field.
- Calling every retransmission flag proof of a bad network.
- Inferring no DNS activity from absent cleartext DNS while encrypted DNS is used.

Acceptance checks

- Capture includes the relevant directions and interval.
- Analysis identifies observations separately from hypotheses.
- A repeated application test confirms the corrected behavior.

Primary references

[Wireshark display-filter expressions](#)[Wireshark TCP field reference](#)[Wireshark documentation](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)