Wireshark Troubleshooting Guide

Capture workflow, switched-network reality, encrypted traffic limits, and practical filters.

A packet capture proves what crossed one capture point. It does not automatically prove what happened everywhere else.

Capture Placement

- Client capture shows what the client sent and received.
- Server capture shows what reached the server.
- SPAN/TAP shows what the network point observed.
- Firewall capture shows pre-NAT or post-NAT depending on platform and stage.

Promiscuous Mode

Promiscuous mode lets the adapter accept frames not addressed to it, but on a switched network you still usually see your own traffic, broadcasts, multicasts, and traffic mirrored to you. It does not magically show every host.

CAPTURE VS DISPLAY FILTERS

TYPE	EXAMPLE	USE
Capture	`host 10.1.1.10 and port 443`	Limit what is written to disk.
Display	`ip.addr == 10.1.1.10 && tcp.port == 443`	Search within packets already captured.
Display	`dns || dhcp || arp`	See supporting services around a failure.

USEFUL DISPLAY FILTERS

NEED	FILTER
TCP resets	`tcp.flags.reset == 1`
Retransmissions	`tcp.analysis.retransmission`
Handshake	`tcp.flags.syn == 1 || tcp.flags.fin == 1 || tcp.flags.reset == 1`
DNS	`dns`
DHCP	`bootp`
ARP	`arp`
TLS handshake	`tls.handshake`
QUIC	`quic || udp.port == 443`

Encrypted Traffic

For HTTPS and HTTP/2, you often see DNS, TCP, TLS handshake, SNI where available, certificate details, IPs, ports, timing, and resets. You usually do not see URLs or payload without keys or endpoint instrumentation.

HTTP/3 And QUIC

Modern web traffic may use QUIC over UDP/443. If you only filter for TCP/443, you can miss the conversation.

DIAGNOSIS PATTERNS

SYMPTOM	LIKELY EVIDENCE
DNS failure	Query with no response, SERVFAIL, NXDOMAIN, wrong resolver, long response time.
Firewall block	SYN retries with no SYN/ACK, ICMP unreachable, reset from middlebox, deny log.
MTU issue	Large packets fail, fragmentation needed, PMTUD black hole, TLS stalls.
App reset	Handshake succeeds, server responds with RST or HTTP error.
Loss	Retransmissions, duplicate ACKs, gaps, high delta times.

Workflow

1. Write the failing flow: source, destination, protocol, port.
2. Capture near the source.
3. Capture near the destination if disputed.
4. Filter after capture.
5. Compare timestamps and sequence.
6. Save the pcap and the conclusion.

Fast Reference

Use the HTML Wireshark Display Filters sheet for quick filter lookup. Use this guide for capture process and interpretation.