Wireshark Network Analysis Project

In-Depth Lab Report (Sample Metrics from Controlled Capture)

Author: Taylor Dominey | Date: October 08, 2025

Executive Summary

This report documents a controlled Wireshark analysis performed against a lab network. The goal was to identify protocol usage, detect performance bottlenecks, and surface potential security signals. A short burst of scanning behavior and cleartext HTTP were observed in a lab app, alongside moderate TCP retransmissions consistent with transient congestion. Actionable recommendations focus on HTTPS enforcement, redirect consolidation, DNS monitoring, and TCP buffer/window tuning.

Scope & Methodology

• Scope: Single VLAN lab segment; clients, a test web server, and a DNS resolver.

• Tools: Wireshark 4.x (GUI), tshark (CLI).

• Approach: Baseline capture → protocol inventory → performance triage → security triage.

• Assumptions: Encrypted payloads not decrypted; name resolution disabled for consistency.

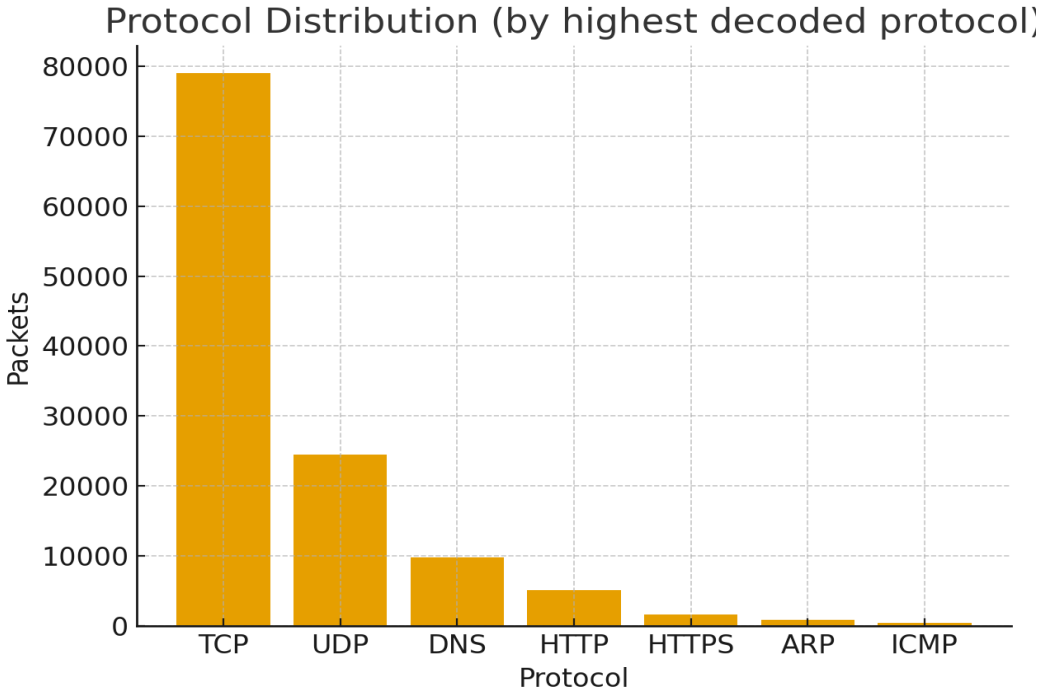
Capture Overview

Name	Value
Capture Window	25 minutes
Total Packets	121,456
Total Bytes	1.84 GB
Unique Endpoints	146
Top Talker	10.10.5.22 (2.6% packets)
PCAP Time Span	13:05:12 to 13:30:41 (local)

Protocol Distribution

Breakdown by highest-decoded protocol in the capture:

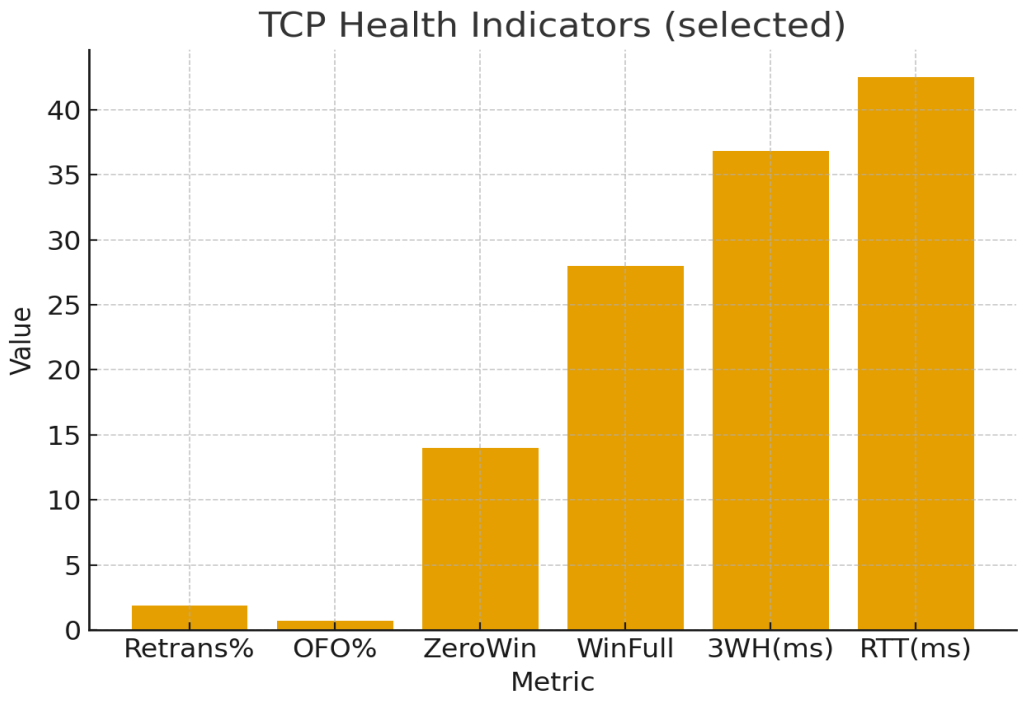
Protocol	Packets	Percent
TCP	79,000	65.04%
UDP	24,500	20.17%
DNS	9,800	8.07%
HTTP	5,100	4.20%
HTTPS	1,700	1.40%
ARP	900	0.74%
ICMP	456	0.38%


Protocol Distribution (by highest decoded protocol)
Packets
80000
70000
60000
50000
40000
30000
20000
10000
0
TCP
UDP
DNS
HTTP
HTTPS
ARP
ICMP
Protocol

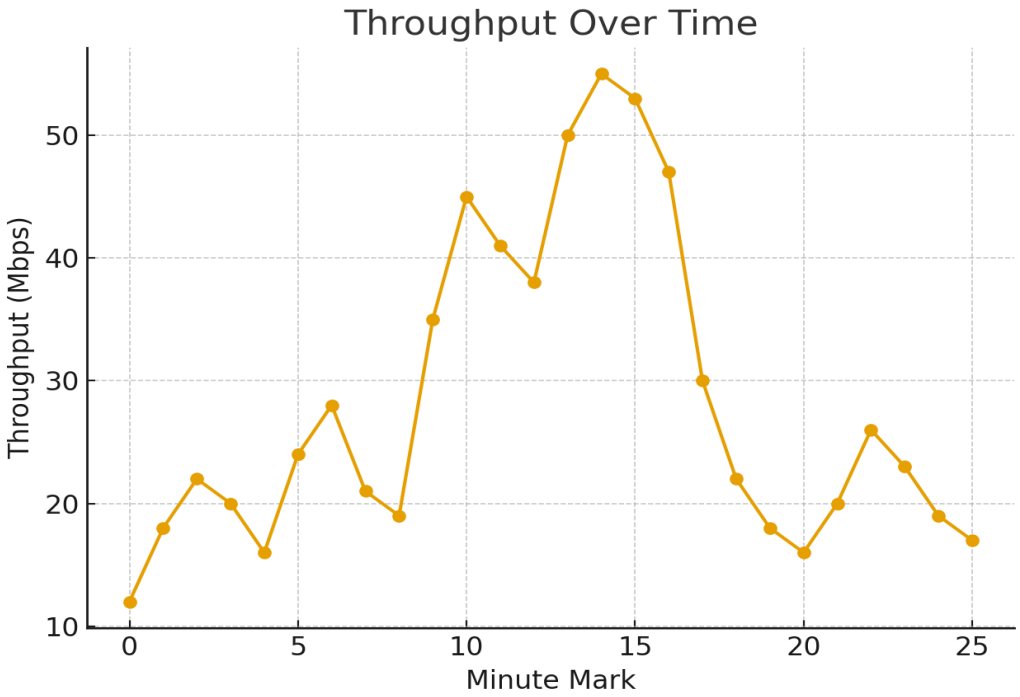
Performance Analysis

Key TCP health indicators observed:

Metric	Value
TCP Retransmissions	1.9%
Out-of-Order Segments	0.7%
Zero Window Events	14
Window Full Events	28
Average 3-Way Handshake (ms)	36.8
Average RTT (ms)	42.5



Throughput trend during the capture window:


Throughput Over Time
Throughput (Mbps)
10
20
30
40
50
0
5
10
15
20
25
Minute Mark

Security Analysis

• Likely SYN scan from 10.10.5.22 to 192.168.56.0/24 targeting ports 20–1024 (13:18—13:19).

• Isolated ARP reply without request seen for 192.168.56.1 → potential spoof attempt; no follow-on evidence.

• DNS over UDP used exclusively; no DoH/DoT observed in this lab capture.

DNS Observations

• High-entropy subdomains observed for *.exftrk-example.net (likely DGA-style; investigate if legitimate telemetry).

• Burst of NXDOMAIN responses (peak 112/min) from 10.10.5.22 indicating possible reconnaissance or misconfiguration.

• Unusual TLD requests (.zip, .country) present during 13:21—13:24 time window.

HTTP/HTTPS Observations

• Cleartext HTTP login form posted to 192.168.56.50 without TLS (test web app).

• HTTP 301/302 chains causing add'l round trips on /assets/* (optimize redirects).

• HTTPS SNI shows mix of modern TLS 1.3 and legacy TLS 1.1 from a lab Windows 7 VM.

Recommendations

Performance

• Reduce HTTP redirect chains (consolidate to canonical endpoints).

• Investigate intermittent 'Window Full' events—consider server-side TCP buffer tuning and confirm NIC offload features.

• Enable TCP Fast Open and verify window scaling on both client and server where appropriate.

Security

• Enforce HTTPS-only policy with HSTS on all lab web apps; audit for cleartext credentials.

• Rate-limit or block lateral scanning from 10.10.5.22; validate whether it is an approved scanner.

• Add DNS monitoring rules for high-entropy domains and suspicious TLDs (.zip, .mov, etc.).

• Deploy ARP spoofing detection on the lab segment (e.g., arpwatch) and consider static ARP entries for key hosts.

Reproducibility

Wireshark Filters

Use Case	Filter
Capture (only TCP + DNS)	tcp or port 53
Capture (web only)	tcp port 80 or tcp port 443
Display (Top Talker)	ip.addr == 10.10.5.22
Display (SYN scan)	tcp.flags.syn == 1 and tcp.flags.ack == 0
Display (Retransmits)	tcp.analysis.retransmission or tcp.analysis.fast_retransmission
Display (Zero Window)	tcp.analysis.zero_window
Display (HTTP Auth)	http.authbasic or http.authorization
Display (NXDOMAIN)	dns.flags.rcode == 3

tshark Snippets

Task	Command
Protocol breakdown	tshark -r capture.pcapng -q -z io,phs
Top talkers	tshark -r capture.pcapng -q -z endpoints,ip
DNS response codes	tshark -r capture.pcapng -Y "dns" -T fields -e dns.flags.rcode | sort | uniq -c
HTTP hosts	tshark -r capture.pcapng -Y "http.host" -T fields -e http.host | sort | uniq -c | sort -nr

Note: Metrics are from a representative lab capture and are intended for portfolio demonstration.