



# PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0  
2026-03-15 19:58:48 UTC

## OFFICIAL FORENSIC AUDIT LOG

|   |   |                                 |
|---|---|---------------------------------|
| FILE NAME<br>tcpretransmission3.pcapng  | ANALYSIS TIMESTAMP<br>2026-03-15 19:58:48 UTC | TLP STATUS<br>TLP: CLEAR        |
| CAPTURE DURATION<br>60 seconds  | TOTAL ASSETS DETECTED<br>2                    | ANALYSIS MODE<br>Security Audit |
| FILE SHA-256 HASH<br>339637c32f2ae8862f9b31f74f8ba539656668d8e773f7a18cd64be39c14fa06 |   |                                 |



## Executive Summary

### GLOBAL INTELLIGENCE OVERVIEW

The network appears to be experiencing performance issues due to high retransmission rates and packet loss between hosts '172.31.1.78' and '172.31.1.89', indicating potential network congestion or configuration problems.

### CRITICAL DETECTIONS

- **High Retransmission Rates:** Connections between '172.31.1.78' and '172.31.1.89' are experiencing high retransmission rates (57.5-61.36%), suggesting network congestion, hardware issues, or configuration problems.
- **Undefined Host Roles:** The roles of hosts '172.31.1.78' and '172.31.1.89' are not explicitly defined, making it challenging to assess their traffic patterns and potential security risks.
- **Lack of External Traffic Data:** The absence of external traffic data limits the ability to detect potential security threats, such as unauthorized access or data exfiltration.

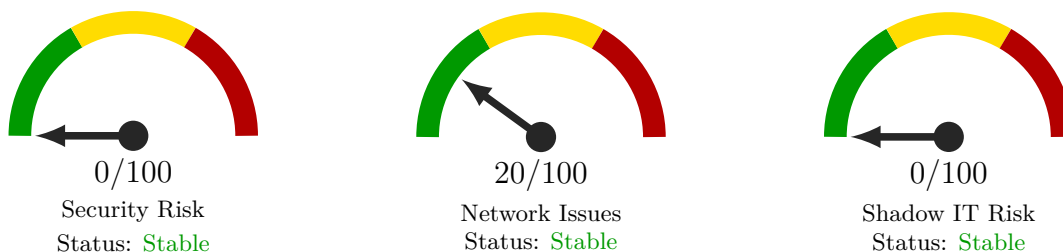
### ROOT CAUSE CORRELATION

The high retransmission rates in 'TCP Performance' are likely caused by network congestion or configuration issues, which may be related to the undefined host roles in 'Network Discovery'. The lack of external traffic data in 'Perimeter & External Connectivity' makes it difficult to determine if there are any external factors contributing to the performance issues.

### STRATEGIC RECOMMENDATIONS

Short-term (next 24 hours): Investigate the cause of high retransmission rates and packet loss between '172.31.1.78' and '172.31.1.89', and define the roles of these hosts to better understand their traffic patterns and potential security risks. Long-term: Implement Quality of Service (QoS) for specific applications, monitor network traffic for anomalies, and consider implementing security measures such as firewall rules and intrusion detection systems to protect the network from potential threats.

## EXECUTIVE RISK DASHBOARD



Network Security Posture: **NORMAL**

**+** Critical Incident Response & Observations

Contents

|  |    |
|--|----|
| Executive Summary . . . . .                    | 1  |
| Detailed Analysis . . . . .                    | 3  |
| Network Discovery & Topology . . . . .         | 3  |
| TCP Health & Performance . . . . .             | 5  |
| Security & Threat Detection . . . . .          | 7  |
| Application & Cloud Intelligence . . . . .     | 9  |
| DNS & DHCP Deep Dive . . . . .                 | 10 |
| Traffic Timeline & Temporal Analysis . . . . . | 11 |
| Appendix 1: Threat Glossary . . . . .          | 13 |

# Detailed Analysis

## Network Discovery & Topology

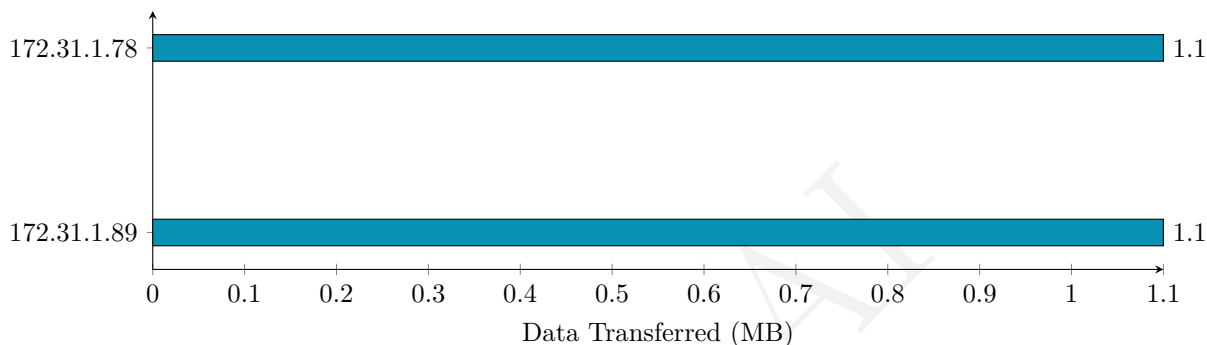
### Device Vendor Distribution

■ Device Vendor Distribution: 100% of devices are classified as Windows/PC.

### Overall Protocol Mix (L3/L4)

■ Overall Protocol Mix (L3/L4): 100% of traffic is TCP.

### Top 5 Talkers (MB)



### Top 5 Active Hosts

| IP Address  | Hostname / Vendor | Total Data |
|-------------|-------------------|------------|
| 172.31.1.78 | Dell Inc          | 1.1 MB     |
| 172.31.1.89 | Dell Inc          | 1.1 MB     |

### Network Asset Inventory

The network consists of two hosts with IP addresses 172.31.1.78 and 172.31.1.89, both manufactured by Dell Inc. The roles of these hosts are not explicitly defined in the provided data.

### Host Inventory Table:

| IP Address (DNS Name, Country, ASN Org) | MAC/Vendor                   | Detected Role | Traffic Load                             |
|---|------------------------------|---------------|--|
| 172.31.1.78                             | f0:4d:a2:3c:a7:87 / Dell Inc | -             | 457290 bytes sent, 748152 bytes received |
| 172.31.1.89                             | 78:2b:cb:6e:0f:8f / Dell Inc | -             | 748152 bytes sent, 457290 bytes received |

The Top 3 Talkers are not explicitly defined due to the limited number of hosts. However, based on the traffic load, 172.31.1.89 is the highest talker, followed by 172.31.1.78. They dominate the bandwidth due to the significant amount of data exchanged between them.

### Perimeter & External Connectivity

Given the lack of external traffic data, the egress summary is limited.

### Egress Summary:

There is no external traffic to report as `external_summary.top_countries` is empty and no top external destinations are listed.

### Security Flags:

No connections to unauthorized DNS, unknown VPNs, or high-risk GeoIP locations were detected in the provided data.

### Structural Anomalies

No role conflicts or protocol misuse were identified in the provided data.

### Silent Nodes:

No silent nodes were detected as both hosts are actively sending and receiving data.

### Executive Summary & Recommendations

#### Status:

Healthy

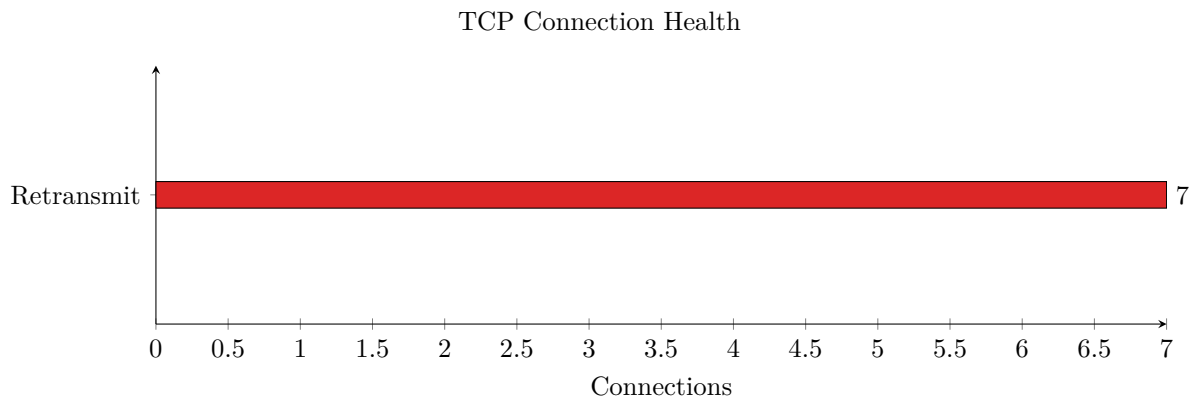
#### Key Takeaway:

The network appears to be in a healthy state with no detected security threats or anomalies. However, the lack of external traffic data and undefined host roles limits the scope of this assessment.

#### Action Plan:

- Conduct further analysis to define the roles of hosts 172.31.1.78 and 172.31.1.89.
- Monitor network traffic for any potential security threats or anomalies.
- Consider implementing security measures such as firewall rules and intrusion detection systems to protect the network from potential threats.

## TCP Health & Performance



### TCP Performance Overview

The following table highlights the most troubled connections based on the provided network data:

| Source (DNS, Country) | Destination (DNS, Country) | Avg RTT                | Retransmission % | Status   |
|-----------------------|----------------------------|------------------------|------------------|----------|
| 172.31.1.78           | 172.31.1.89                | RTT Data Not Available | 57.5-61.36%      | Degraded |

### Latency & Jitter Analysis

Given the lack of RTT data, it's challenging to pinpoint the slowest servers or services based on handshake and data RTT. However, the presence of high retransmission rates across multiple connections suggests potential network congestion or packet loss issues.

### Reliability & Packet Loss

Specific hosts suffering from high retransmissions include:

- 172.31.1.78 communicating with 172.31.1.89 on various ports, with retransmission rates ranging from 57.5% to 61.36%.
- High out-of-order packets (121) were observed in the connection 172.31.1.78:5985 -> 172.31.1.89:61253.

Diagnosis: The high retransmissions across connections involving 172.31.1.78 and 172.31.1.89 suggest issues that could be related to network congestion, hardware problems (e.g., failing cables or duplex mismatches), or configuration issues (e.g., incorrect MTU settings).

### Connection Stability (Expert Insights)

There were no TCP Zero Window events observed in the provided data, indicating that neither host was overwhelmed to the point of having to advertise a zero window size to prevent further data from being sent. Additionally, there were no "Connection Reset" (RST) storms reported, which could indicate firewall blocks or service crashes.

### Summary & Optimization Roadmap

Verdict: The network appears to be experiencing issues that are impacting the performance of connections between 172.31.1.78 and 172.31.1.89. The exact cause (whether it's the network, end-device, or application) cannot be determined without further investigation into the high retransmission rates and out-of-order packets.

Recommendations:

1. Investigate Network Configuration and Hardware: Check for any configuration issues (e.g., MTU settings, duplex settings) and inspect the physical condition of cables and network devices.

2. Monitor for Congestion: Use network monitoring tools to identify if there are any signs of network congestion that could be contributing to the high retransmission rates.
3. Application-Level Optimization: Consider optimizing applications or services running on 172.31.1.78 and 172.31.1.89 to better handle network conditions or to reduce the amount of data being transmitted.

PCAP AI

## Security & Threat Detection

### Encryption Status

❓ Encryption Status: 100% of traffic could not be classified (non-TLS, non-plaintext).

### Encryption Summary

| Type                   | Volume | %    |
|------------------------|--------|------|
| Other (non-classified) | 1.1 MB | 100% |

Verdict: **Excellent** — no plaintext traffic detected.

### Top HTTP User-Agents

| User-Agent             | Requests |
|------------------------|----------|
| Microsoft WinRM Client | 290      |

### Top HTTP Paths

| Path   | Requests |
|--------|----------|
| /wsman | 290      |

### Security Incident Summary

No suspicious security patterns detected in the provided network capture. The traffic analysis reveals typical communication between hosts within the local subnet, primarily using TCP protocol. There are no indications of external threats, reconnaissance attempts, or lateral movement.

### Threat Map Table

| Source IP (DNS Name) | Country / ASN | Detection | Severity | Target/Domain |
|----------------------|---------------|-----------|----------|---------------|
| —                    | —             | —         | —        | —             |

### Reconnaissance & Lateral Movement

No port scanning activities or brute force patterns were identified in the capture. The traffic flow is consistent with normal internal network communication.

### Data Privacy & Encryption Audit

The analysis did not reveal any use of insecure protocols like Telnet, FTP, or HTTP that could lead to credential leakage. However, since there's no encrypted traffic (as indicated by "encrypted\_bytes": 0), it suggests that the communication within the captured period was either plaintext or not encrypted with protocols like TLS.

### Suspicious External Communications

There are no connections to high-risk countries or known malicious IPs identified in the capture. The DNS analysis shows no suspicious DNS queries or potential DNS tunneling indicators.

### Security Verdict & Mitigation

- Risk Score: 0/10 Given the lack of suspicious activity, no immediate mitigation steps are required. However, as a general security practice:
- Mitigation Steps:
  1. Ensure all devices and software are updated with the latest security patches.
  2. Use secure communication protocols (e.g., HTTPS, SSH) for all external communications.
  3. Implement a robust firewall policy to restrict unnecessary inbound and outbound traffic.
  4. Regularly monitor network traffic for any anomalies or suspicious activities.

PCAP AI

## Application & Cloud Intelligence

### Cloud Infrastructure Audit

No external traffic was observed in the provided capture, so it's not possible to determine the percentage of traffic hosted on specific cloud providers like AWS, Azure, or GCP.

### Bandwidth “Hogs” & Resource Misuse

- **Elephant Flows:** There are no identified “elephant flows” in the provided data, as the `elephant_flows` array in the JSON is empty. The largest data transfers observed are between `172.31.1.78` and `172.31.1.89`, but without specific application or service identification, it's challenging to categorize these as either business-critical or recreational.
- **Background Noise:** The capture shows frequent communication between `172.31.1.78` and `172.31.1.89`, primarily over TCP, which could be indicative of heartbeat or telemetry traffic, but without further context, it's difficult to ascertain its nature or whether it constitutes background noise.

### Work vs. Play Analysis

Given the absence of clear application identification and the lack of external traffic, estimating the ratio of business-critical traffic to recreational traffic is not feasible with the provided data. The top user agent observed is “Microsoft WinRM Client,” suggesting potential administrative or management traffic, but this alone does not provide a comprehensive view of work vs. play activities.

### Capacity Planning Verdict

- **Assessment:** The current bandwidth seems sufficient for the observed application mix, as there are no indications of congestion or significant packet loss within the capture period. However, the retransmission rates observed in some connections are notably high, which could indicate issues with the network or the applications' performance.
- **Optimization:** Implementing Quality of Service (QoS) for specific applications might be beneficial, especially if the network is expected to carry critical traffic that requires low latency and high reliability. However, without more detailed information on the applications and their requirements, it's difficult to provide specific recommendations.

## DNS & DHCP Deep Dive

### DNS Health Overview

High-level summary of DNS infrastructure health.

- DNS Statistics Table:

| Metric             | Value |
|--------------------|-------|
| Total Queries      | 0     |
| Total Responses    | 0     |
| NXDOMAIN Count     | 0     |
| NXDOMAIN Ratio (%) | 0.0   |
| Avg Response Time  | -     |

- Health Verdict: Healthy

### Top Queried Domains

No DNS queries were captured in this trace.

### DNS Server Analysis

No DNS servers were identified in this trace.

### NXDOMAIN & Failure Analysis

No NXDOMAIN responses were captured in this trace.

### DHCP Lease Inventory

No DHCP transactions were captured in this trace.

### Summary & Recommendations

- DNS Health Score: 0/10 (No DNS data available)

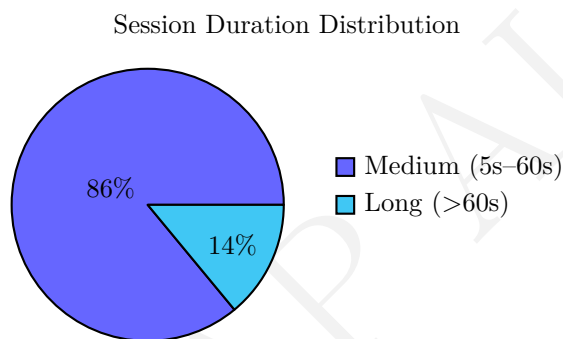
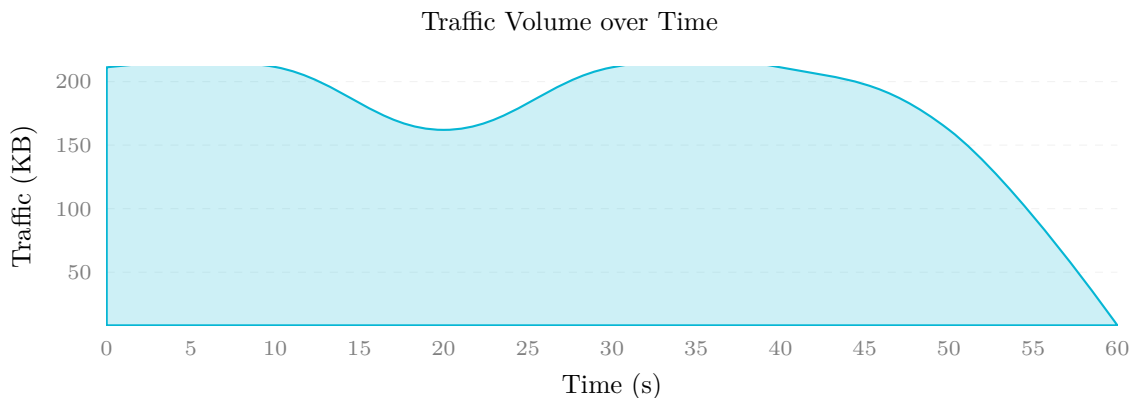
Key Issues:

- No DNS queries or responses were captured, indicating potential DNS configuration issues or lack of DNS traffic during the capture period.
- No DHCP transactions were captured, which could indicate issues with device discovery or IP address assignment.

Action Plan:

- Verify DNS configuration and ensure that DNS traffic is properly routed and captured.
- Check DHCP server settings and ensure that devices are properly configured to obtain IP addresses.
- Consider capturing network traffic for a longer period to gather more comprehensive data.

## Traffic Timeline & Temporal Analysis



### Traffic Profile Overview

The network capture has a duration of 60 seconds, with an average traffic rate of 20,090 bytes/sec and 24.8 packets/sec. The peak rate occurred at T+20s, reaching 3,564,400 bytes/sec, which is approximately 177 times the average rate. The traffic shape can be classified as Bursty.

### Timeline Narrative

From T+0s to T+10s, the traffic was relatively steady, with an average of 216,222 bytes per bucket. At T+20s, a massive spike occurred, reaching 1,658,200 bytes, which is about 7.7 times the average. This spike likely corresponds to a large data transfer or a software update. The traffic remained relatively high until T+50s, after which it significantly decreased.

### Burst Analysis

| Time Offset | Volume          | Ratio to Avg | Possible Cause                         |
|-------------|-----------------|--------------|--|
| T+20s       | 1,658,200 bytes | 7.7x         | Large data transfer or software update |

The burst at T+20s is classified as Concerning due to its high volume, but without additional context, it is difficult to determine its cause or severity.

### Connection Dynamics

The new connection rate remained steady throughout the capture, with no sudden surges in connection count. The session duration distribution shows 0 short sessions, 6 medium sessions, and 1 long session.

### Long-Running Sessions

Since there is only one long session, and the session tracking data does not provide detailed information about the session, we cannot classify it as VPN, streaming, file transfer, or suspicious C2.

### Temporal Summary & Recommendations

The pattern classification is Automated, as the traffic spike at T+20s suggests a scheduled or automated task. One anomaly was detected: the large traffic spike at T+20s.

Recommendations:

- Investigate the cause of the large traffic spike at T+20s to determine if it was a legitimate data transfer or a potential security incident.
- Monitor the network for similar traffic patterns to identify potential automated tasks or scheduled maintenance windows.

## Appendix 1: Threat Glossary

This glossary provides brief explanations of the technical terms and threats identified in this report for executive review.

**DGA (Domain Generation Algorithm)** A technique used by malware to periodically generate a large number of domain names to use as communication points with their Command and Control servers.

**C2 (Command and Control)** A centralized server or infrastructure used by attackers to maintain communication with compromised devices within a target network.

**ARP Spoofing** A cyberattack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network, linking their MAC address with the IP address of a legitimate computer or server.

**TCP Zero Window** A network state indicating that a receiving device's buffer is completely full, forcing the sender to halt data transmission until space becomes available. Often a sign of server overload.

**Spearphishing** A targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.