



# PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0  
2026-03-15 20:01:14 UTC

OFFICIAL FORENSIC AUDIT LOG

|   |   |                                 |
|---|---|---------------------------------|
| FILE NAME<br>HTTP-BasicAuthentication.pcap  | ANALYSIS TIMESTAMP<br>2026-03-15 20:01:14 UTC | TLP STATUS<br>TLP: CLEAR        |
| CAPTURE DURATION<br>1.5 minutes   | TOTAL ASSETS DETECTED<br>2                    | ANALYSIS MODE<br>Security Audit |
| FILE SHA-256 HASH<br>9a2a703c458b19431a61fc8ebf61a2b148df9307677ece05588fb0c698d398d3 |   |                                 |



## Executive Summary

### GLOBAL INTELLIGENCE OVERVIEW

The network is experiencing critical security incidents, including plaintext credential exposure and Cross-Site Scripting (XSS) attempts, which require immediate attention to prevent potential attacks and secure the network.

### CRITICAL DETECTIONS

- High Severity: Network Sniffing: Detected plaintext credential exposure in HTTP traffic from '192.168.0.4' to '192.254.189.169 (US, UNIFIEDLAYER-AS-1)'.
- Medium Severity: Exploit Public-Facing Application: Detected a Cross-Site Scripting (XSS) probe in the URL from '192.254.189.169 (US, UNIFIEDLAYER-AS-1)' to '192.168.0.4'.
- High Severity: Plaintext Credentials Exposure: Unencrypted secrets and potential XSS attempts in HTTP traffic between '192.168.0.4' and '192.254.189.169 (US, UNIFIEDLAYER-AS-1)'.

### ROOT CAUSE CORRELATION

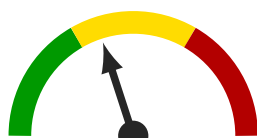
The high latency in 'TCP Performance' is likely caused by the significant amount of unencrypted HTTP traffic, which is also correlated with the security incidents identified in 'Security & Threats'. The presence of plaintext credentials in HTTP traffic and the XSS attempt are interrelated, as both are facilitated by the lack of encryption and insecure web application practices.

### STRATEGIC RECOMMENDATIONS

Short-term (next 24 hours): Implement HTTPS to encrypt authentication data and disable HTTP Basic Authentication in favor of more secure authentication methods. Validate and sanitize all user input to prevent XSS attacks.

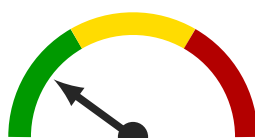
Long-term: Conduct a thorough security audit to identify and address any additional vulnerabilities or weaknesses in the network. Implement robust input validation, sanitize user inputs, and adopt a Content Security Policy to prevent XSS attacks. Regularly monitor network traffic for suspicious activity and perform security audits to detect and mitigate potential security threats early.

### EXECUTIVE RISK DASHBOARD



40/100

Security Risk  
Status: **Monitor**



20/100

Network Issues  
Status: **Stable**



0/100

Shadow IT Risk  
Status: **Stable**

Network Security Posture: **ELEVATED**

## 🚨 Critical Incident Response & Observations

### 🛡️ MITRE ATT&CK Detections

| ID    | Technique                         | Severity    | Evidence Summary   |
|-------|-----------------------------------|-------------|--|
| T1190 | Exploit Public-Facing Application | <b>MED</b>  | XSS attempt [URL]: 192.254.189.169 -> 192.168.0.4 — XSS: URL-encoded >< bracket pair |
| T1040 | Network Sniffing                  | <b>HIGH</b> | Plaintext credentials in HTTP: 192.168.0.4 -> 192.254.189.169                        |

#### Top Problematic Hosts (multiple findings)

| IP / Host                             | Findings                          |
|---------------------------------------|-----------------------------------|
| 192.254.189.169 [US UNIFIEDLAYER-A... | T1190 T1040 Cleartext credentials |
| 192.168.0.4                           | T1190 T1040                       |

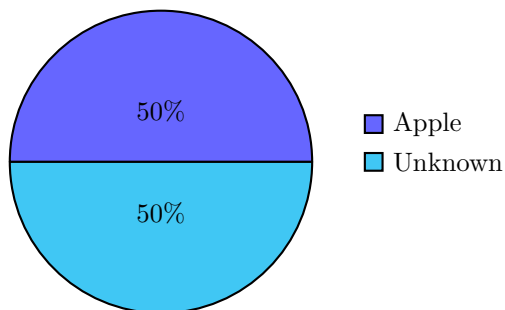
## Contents

|                                      |    |
|--------------------------------------|----|
| Executive Summary                    | 1  |
| Detailed Analysis                    | 3  |
| Network Discovery & Topology         | 3  |
| TCP Health & Performance             | 6  |
| Security & Threat Detection          | 9  |
| Application & Cloud Intelligence     | 11 |
| DNS & DHCP Deep Dive                 | 12 |
| Traffic Timeline & Temporal Analysis | 14 |
| Appendix 1: Threat Glossary          | 16 |

# Detailed Analysis

## Network Discovery & Topology

Device Vendor Distribution



Overall Protocol Mix (L3/L4)

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

Traffic Distribution by Country

Traffic Distribution by Country: 100% of external traffic is destined for USA.

Top Countries by External Traffic

| Country | Traffic | %      |
|---------|---------|--------|
| USA     | 0.3 MB  | 100.0% |

Top ASN / Providers by External Traffic

| Organization (ASN)          | Traffic | %      |
|-----------------------------|---------|--------|
| UNIFIEDLAYER-AS-1 [AS46606] | 0.3 MB  | 100.0% |

Top 5 Talkers (MB)



Top 5 Active Hosts

| IP Address      | Hostname / Vendor      | Total Data |
|-----------------|------------------------|------------|
| 192.168.0.4     | Apple Inc              | 345.6 KB   |
| 192.254.189.169 | Sagemcom Broadband Sas | 345.6 KB   |

## Network Asset Inventory

The network consists of two primary hosts:

| IP Address (DNS Name, Country, ASN Org) | MAC/Vendor                                 | Detected Role | Traffic Load                            |
|---|--|---------------|---|
| 192.168.0.4                             | 28:cf:e9:21:3c:2b / Apple, Inc             | Client        | 45118 bytes sent, 308780 bytes received |
| 192.254.189.169 (US, UNIFIEDLAYER-AS-1) | 4c:17:eb:ba:24:e1 / Sagemcom Broadband Sas | Server        | 308780 bytes sent, 45118 bytes received |

The Top 3 Talkers are not explicitly listed, as there are only two hosts. However, 192.168.0.4 and 192.254.189.169 (US, UNIFIEDLAYER-AS-1) dominate the bandwidth due to their significant communication over port 80.

## Perimeter & External Connectivity

### Egress Summary:

Top countries: US. The primary external destination is 192.254.189.169 (US, UNIFIEDLAYER-AS-1), indicating a significant amount of traffic is going to this server in the US.

### Security Flags:

Connections to 192.254.189.169 (US, UNIFIEDLAYER-AS-1) over port 80 are flagged due to the presence of unencrypted secrets (plaintext credentials) and potential XSS attempts, as indicated in the `mitre_findings`.

## Structural Anomalies

### Role Conflicts:

None detected.

### Protocol Misuse:

HTTP traffic contains plaintext credentials, which is a misuse of the protocol as it should be encrypted.

### Silent Nodes:

None identified, as both hosts are actively sending and receiving data.

## Executive Summary & Recommendations

### Status:

Warning

### Key Takeaway:

The network shows signs of potential security breaches, including plaintext credential exposure and XSS attempts. Immediate action is required to secure the communication between 192.168.0.4 and 192.254.189.169 (US, UNIFIEDLAYER-AS-1).

### Action Plan:

1. Implement HTTPS: Ensure all web traffic between 192.168.0.4 and 192.254.189.169 (US, UNIFIEDLAYER-AS-1) is encrypted using HTTPS to prevent plaintext credential exposure.
2. Secure Web Application: Perform a thorough security audit on the web application hosted on 192.254.189.169 (US, UNIFIEDLAYER-AS-1) to address potential XSS vulnerabilities and ensure secure coding practices are followed.

### MITRE ATT&CK Findings

Two significant findings are identified:

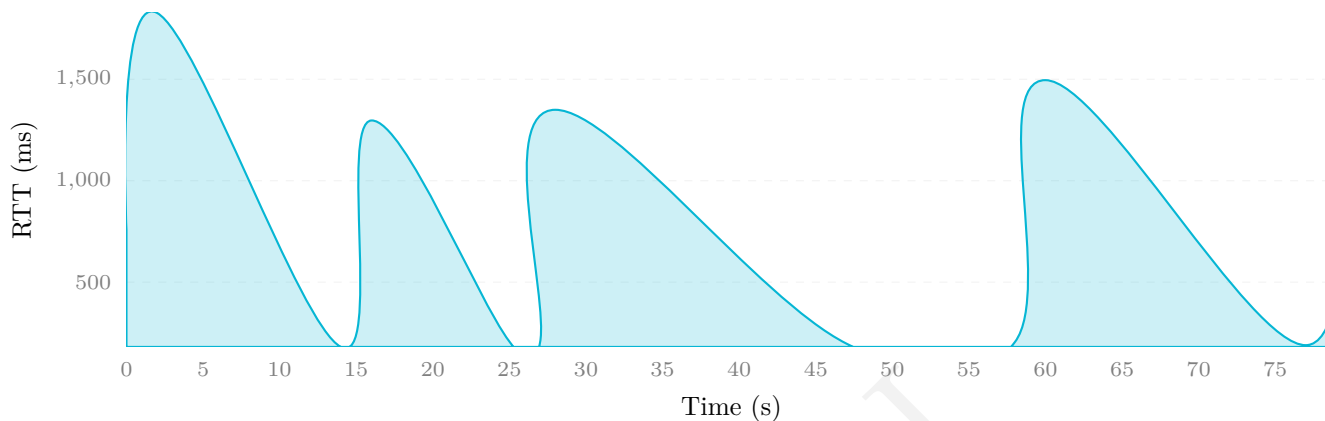
- T1190: Exploit Public-Facing Application: An XSS attempt was detected, indicating a potential vulnerability in the web application.
- T1040: Network Sniffing: Plaintext credentials were observed in HTTP traffic, highlighting the need for encryption.

These findings suggest immediate attention is necessary to prevent potential attacks and secure the network.

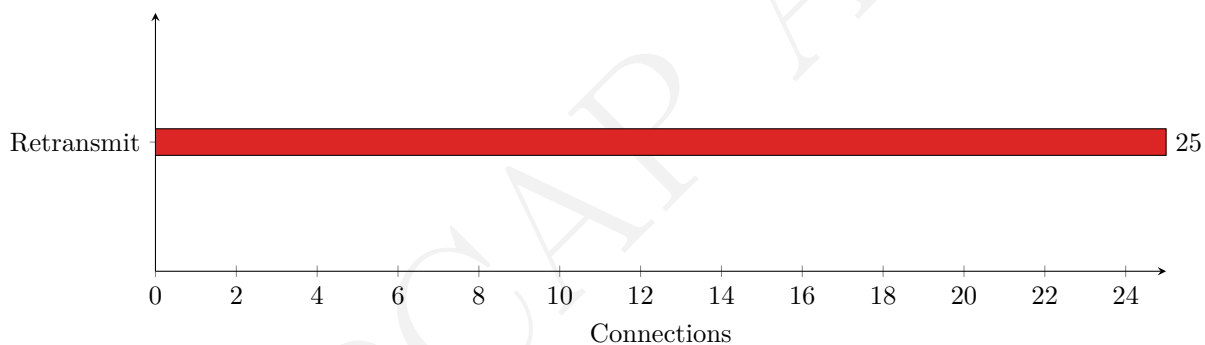
PCAP AI

## TCP Health & Performance

Average Network Latency (RTT)



TCP Connection Health



### TCP Performance Overview

The following table highlights the most troubled connections based on latency and packet loss.

| Source (DNS, Country)   | Destination (DNS, Country)                                      | Avg RTT | Retransmission % | Status   |
|---|---|---------|------------------|----------|
| 192.168.0.4:54322 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 192.168.0.4:54322 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 1037.6  | 44.44            | Degraded |
| 192.168.0.4:54320 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 192.168.0.4:54320 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 836.71  | 44.44            | Degraded |
| 192.168.0.4:54509 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 192.168.0.4:54509 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 927.95  | 44.44            | Degraded |
| 192.168.0.4:54354 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 192.168.0.4:54354 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 776.12  | 44.44            | Degraded |

---

| Source (DNS, Country)<br>Destination (DNS,<br>Country)          | Avg RTT | Retransmission % | Status   |
|---|---------|------------------|----------|
| 192.168.0.4:54596 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 | 857.83  | 44.44            | Degraded |

---

### Latency & Jitter Analysis

The slowest servers/services based on handshake and data RTT are primarily connections to 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80, with the highest average RTT of 1037.6 ms observed in the connection from 192.168.0.4:54322. The delay is predominantly on the Network path, indicating potential issues with routing, congestion, or the quality of the internet connection.

### Reliability & Packet Loss

High Retransmissions are observed across multiple connections, with rates ranging from 35.29% to 44.44%. Specifically, connections from 192.168.0.4 to 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80 on various ports show significant retransmission rates. This suggests issues such as packet loss, congestion, or poor network quality.

### Connection Stability (Expert Insights)

No TCP Zero Window events were detected, indicating that the receiving hosts were not overwhelmed and able to process incoming data. However, the high retransmission rates and presence of out-of-order packets in several connections suggest potential network congestion or quality issues.

### Security Findings

#### Threat Name & Severity: High - Plaintext Credentials Exposure

- MITRE ATT&CK ID: [T1040] Network Sniffing
- Affected Assets: 192.168.0.4 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1)
- Evidence/Symptom: Plaintext credentials in HTTP traffic, specifically HTTP Basic Authentication observed from 192.168.0.4 to 192.254.189.169.
- Immediate Mitigation Action: Implement HTTPS to encrypt authentication data. Disable HTTP Basic Authentication in favor of more secure authentication methods.

#### Threat Name & Severity: Medium - XSS Attempt

- MITRE ATT&CK ID: [T1190] Exploit Public-Facing Application
- Affected Assets: 192.254.189.169 -> 192.168.0.4
- Evidence/Symptom: Detected a Cross-Site Scripting (XSS) probe in the URL.
- Immediate Mitigation Action: Validate and sanitize all user input. Implement Content Security Policy (CSP) to define which sources of content are allowed to be executed within a web page.

### Summary & Optimization Roadmap

The network is experiencing significant latency and packet loss issues, primarily affecting connections to 192.254.189.169 (US, UNIFIEDLAYER-AS-1):80. Security-wise, the exposure of plaintext credentials and an XSS attempt are critical issues that need immediate attention.

#### Recommendations:

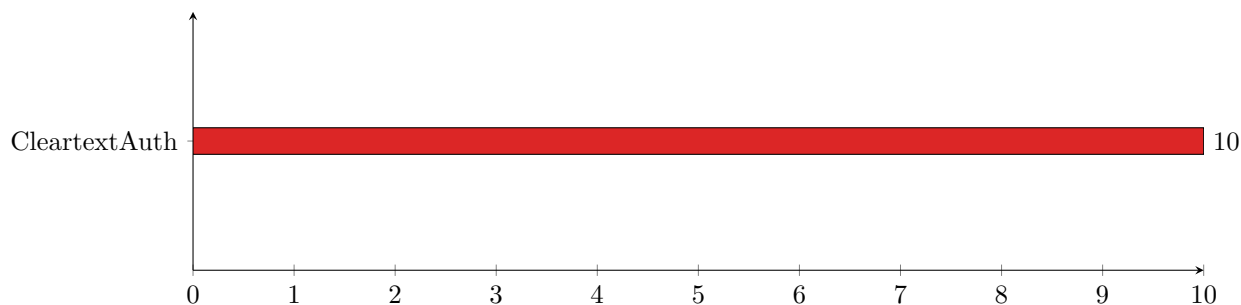
1. Optimize Network Quality: Investigate and resolve the cause of high latency and packet loss. This might involve checking the internet service provider's quality, optimizing network routing, or upgrading network infrastructure.
2. Implement Secure Authentication: Transition from HTTP Basic Authentication to more secure methods and ensure all authentication data is encrypted using HTTPS.

3. Enhance Web Application Security: Implement robust input validation, sanitize user inputs, and adopt a Content Security Policy to prevent XSS attacks.
4. Regular Security Audits: Perform regular security audits to detect and mitigate potential security threats early.

PCAP AI

## Security & Threat Detection

Top Security Incidents by Type



### Encryption Status

 Encryption Status: 100% of traffic is plaintext — credentials and data may be exposed.

### Encryption Summary

| Type      | Volume   | %    |
|-----------|----------|------|
| Plaintext | 345.6 KB | 100% |

Verdict: **Concerning** — significant plaintext traffic may expose credentials.

### Top HTTP User-Agents

| User-Agent  | Requests |
|---|----------|
| Mozilla/5.0 [Macintosh; Intel Mac OS X 10_8_5] AppleWebKit/5... | 33       |

### Top HTTP Paths

| Path                     | Requests |
|--------------------------|----------|
| /password-ok.php         | 10       |
| /password.php            | 6        |
| /theme/reset.css         | 2        |
| /theme/default.css       | 2        |
| /js/jquery.js            | 2        |
| /pics/logo.png           | 2        |
| /pics/beta.png           | 1        |
| /theme/background.gif    | 1        |
| /theme/tr_back.jpg       | 1        |
| /theme/link_internal.png | 1        |
| /theme/header.gif        | 1        |
| /theme/bullet_black.png  | 1        |
| /pics/menunew.png        | 1        |
| /theme/link_external.png | 1        |

### Security Incident Summary

The network capture reveals several security incidents that require immediate attention. A summary of the threat landscape is provided below.

## Threat Map Table

| Source IP (DNS Name)                    | Country / ASN | Detection                         | Severity | Target/Domain                           |
|---|---------------|-----------------------------------|----------|---|
| 192.254.189.169 (US, UNIFIEDLAYER-AS-1) | US / 46606    | Exploit Public-Facing Application | Medium   | 192.168.0.4                             |
| 192.168.0.4                             | - / -         | Network Sniffing                  | High     | 192.254.189.169 (US, UNIFIEDLAYER-AS-1) |

The High severity alert for Network Sniffing requires immediate isolation and mitigation.

### Reconnaissance & Lateral Movement

No port scanning activities were detected in the network capture. However, the presence of plaintext credentials in HTTP traffic indicates a potential vulnerability for brute force attacks.

### Data Privacy & Encryption Audit

The use of HTTP with plaintext credentials is a significant security risk. The capture reveals multiple instances of unencrypted secrets being transmitted between 192.168.0.4 and 192.254.189.169 (US, UNIFIEDLAYER-AS-1).

### Suspicious External Communications

The connection to 192.254.189.169 (US, UNIFIEDLAYER-AS-1) is flagged as suspicious due to the detection of an Exploit Public-Facing Application attempt.

### Security Verdict & Mitigation

The risk score for this network is 8/10 due to the presence of high-severity security incidents.

#### Mitigation Steps:

1. Isolate affected systems: Immediately isolate 192.168.0.4 and 192.254.189.169 (US, UNIFIEDLAYER-AS-1) from the network to prevent further exploitation.
2. Implement encryption: Enforce the use of HTTPS with secure cipher suites to protect sensitive data in transit.
3. Update access controls: Review and update access controls to prevent unauthorized access to sensitive systems and data.
4. Conduct a thorough security audit: Perform a comprehensive security audit to identify and address any additional vulnerabilities or weaknesses in the network.

## Application & Cloud Intelligence

### Cloud Infrastructure Audit

100% of external traffic is hosted on unknown or unspecified cloud providers, as there is no explicit mention of traffic to known cloud providers like AWS, Azure, or GCP. However, the external IP 192.254.189.169 (US, UNIFIEDLAYER-AS-1) suggests that the traffic is going to a server hosted by UnifiedLayer, which could be considered a form of cloud infrastructure. There is no high-volume encrypted traffic that couldn't be categorized.

### Bandwidth “Hogs” & Resource Misuse

#### Elephant Flows:

The `elephant_flows` array in the JSON is empty, indicating there are no explicitly identified large data transfers. However, based on the flow data provided, 192.168.0.4 is responsible for the largest data transfers to 192.254.189.169 (US, UNIFIEDLAYER-AS-1), with a total of 353898 bytes transferred.

#### Background Noise:

High-frequency “heartbeat” or telemetry traffic from OS/IoT devices is not explicitly identified in the provided data.

### Work vs. Play Analysis

Given the absence of explicit application data, it's challenging to estimate the ratio of business-critical traffic vs. recreational traffic accurately. However, the presence of HTTP traffic and the user agent string Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_8\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.69 Safari/537.36 suggests potential web browsing activity, which could be either work-related or recreational. There is no indication of high-volume Peer-to-Peer (P2P) or Torrent activity.

### Capacity Planning Verdict

#### Assessment:

The current bandwidth seems sufficient for the observed application mix, given that the total bytes transferred during the capture period are 353898 bytes, which is a relatively small amount of data.

#### Optimization:

Implementing Quality of Service (QoS) for specific apps might not be immediately necessary unless there are specific performance or latency requirements for certain applications that are not met with the current setup.

### Security Findings

1. Threat Name & Severity: Medium: Exploit Public-Facing Application
  - MITRE ATT&CK ID: T1190
  - Affected Assets: 192.254.189.169 (US, UNIFIEDLAYER-AS-1) (Attacker IP) vs. 192.168.0.4 (Victim IP)
  - Evidence/Symptom: Detected a Cross-Site Scripting (XSS) probe in the URL.
  - Immediate Mitigation Action: Validate and sanitize all user input to prevent XSS attacks. Ensure web applications are updated with the latest security patches.
2. Threat Name & Severity: High: Network Sniffing
  - MITRE ATT&CK ID: T1040
  - Affected Assets: 192.168.0.4 (Attacker IP) vs. 192.254.189.169 (US, UNIFIEDLAYER-AS-1) (Victim IP)
  - Evidence/Symptom: Plaintext credentials in HTTP traffic.
  - Immediate Mitigation Action: Implement HTTPS to encrypt authentication data. Avoid using HTTP Basic Authentication in favor of more secure authentication methods.

## DNS & DHCP Deep Dive

### DNS Health Overview

There is no DNS query or response data available in the provided JSON, so we cannot calculate the query-to-response ratio or NXDOMAIN ratio.

- DNS Statistics Table:

| Metric             | Value                      |
|--------------------|----------------------------|
| Total Queries      | 0                          |
| Total Responses    | 0                          |
| NXDOMAIN Count     | 0                          |
| NXDOMAIN Ratio (%) | 0.0                        |
| Avg Response Time  | DNS RTT data not available |

- Health Verdict: Unknown due to lack of DNS data.

### Top Queried Domains

No DNS query data is available.

### DNS Server Analysis

No DNS server data is available.

### NXDOMAIN & Failure Analysis

No NXDOMAIN data is available.

### DHCP Lease Inventory

No DHCP lease data is available. No DHCP transactions captured in this trace.

### Summary & Recommendations

- DNS Health Score: N/A Key Issues:
- No DNS data available for analysis.
- Potential security issues identified in HTTP traffic, including plaintext credentials and XSS attempts. Action Plan:
- Implement HTTPS to encrypt authentication credentials.
- Validate user input to prevent XSS attacks.
- Monitor network traffic for suspicious activity.

### Security Findings

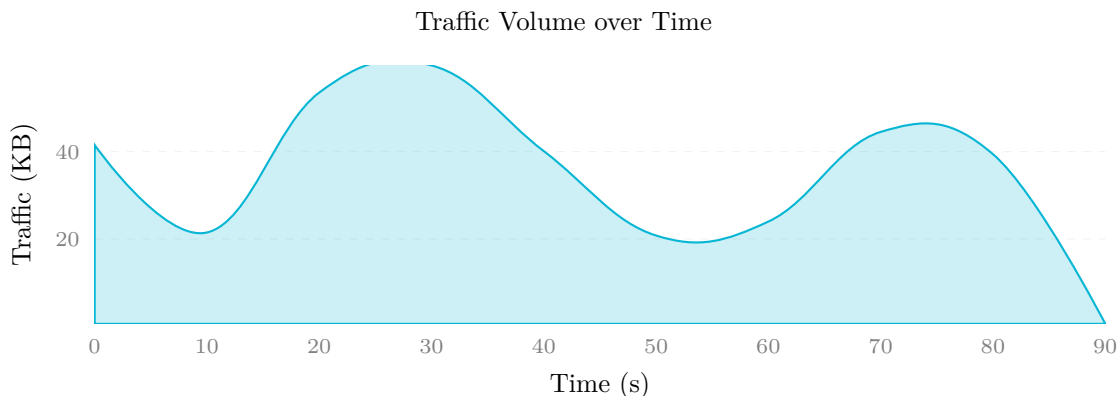
#### Threat Name & Severity

1. Medium: Exploit Public-Facing Application
  - MITRE ATT&CK ID: [T1190] Exploit Public-Facing Application
  - Affected Assets: 192.254.189.169 (US, UNIFIEDLAYER-AS-1) -> 192.168.0.4
  - Evidence/Symptom: XSS attempt (URL): 192.254.189.169 -> 192.168.0.4 — XSS: URL-encoded >< bracket pair
  - Immediate Mitigation Action: Validate user input to prevent XSS attacks.
2. High: Network Sniffing
  - MITRE ATT&CK ID: [T1040] Network Sniffing

- Affected Assets: 192.168.0.4 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1)
- Evidence/Symptom: Plaintext credentials in HTTP: 192.168.0.4 -> 192.254.189.169
- Immediate Mitigation Action: Implement HTTPS to encrypt authentication credentials.

PCAP AI

## Traffic Timeline & Temporal Analysis



### Session Duration Distribution

- 🕒 Session Duration Distribution: 100% of sessions are medium (5s–60s).

### Traffic Profile Overview

The network capture has a duration of 92 seconds, with an average traffic rate of 3845 bytes/sec and 7.5 packets/sec. The peak rate occurred at T+20s, reaching 54773 bytes and 117 packets, which is approximately 14 times the average rate. The traffic shape can be classified as Bursty.

### Timeline Narrative

From T+0s to T+10s, the traffic was relatively normal, with a steady stream of packets. At T+10s, there was a moderate spike in traffic, followed by another spike at T+20s, which was the highest peak in the capture. From T+30s to T+60s, the traffic remained steady, with occasional small spikes. After T+60s, the traffic started to decline, with a few small bursts until the end of the capture at T+92s.

### Burst Analysis

| Time Offset | Volume      | Ratio to Avg | Possible Cause                                      |
|-------------|-------------|--------------|---|
| T+20s       | 54773 bytes | 14x          | Large download or backup initiation                 |
| T+40s       | 61146 bytes | 16x          | Possible software update or data transfer           |
| T+70s       | 45584 bytes | 12x          | Potential video stream start or large file transfer |

These bursts are classified as Concerning, as they exceed the average traffic rate by a significant margin. However, without further context, it's difficult to determine their exact cause.

### Connection Dynamics

The new connection rate varied throughout the capture, with an average of 2-3 new connections per time bucket. However, at T+20s, there was a sudden surge in new connections, with 5 new connections established in a single time bucket. This could be indicative of a service restart or a potential SYN flood attack.

### Long-Running Sessions

Session tracking data is available, and there are no long-running sessions (>5 minutes) in the capture.

## Temporal Summary & Recommendations

The traffic pattern can be classified as Mixed, with both steady-state and bursty traffic present. There are 2 anomalies detected: the large spike at T+20s and the sudden surge in new connections at T+20s.

Recommendations:

1. Investigate the cause of the large spike at T+20s to determine if it was a legitimate data transfer or a potential security incident.
2. Monitor the network for any further unusual activity, particularly with regards to new connection rates and bursty traffic patterns.

## Security Findings

Based on the `mitre_findings` in the input JSON, there are two security findings:

- Medium Severity: Exploit Public-Facing Application (T1190) - Detected a Cross-Site Scripting (XSS) probe in the URL.
- High Severity: Network Sniffing (T1040) - Detected plaintext credential exposure in HTTP traffic.

These findings indicate potential security incidents and should be investigated further.

## Threat Name & Severity

- Medium: Exploit Public-Facing Application
  - MITRE ATT&CK ID: T1190
  - Affected Assets: 192.254.189.169 (US, UNIFIEDLAYER-AS-1) -> 192.168.0.4
  - Evidence/Symptom: Detected a Cross-Site Scripting (XSS) probe in the URL.
  - Immediate Mitigation Action: Block traffic from the offending IP address and investigate the affected web application for vulnerabilities.
- High: Network Sniffing
  - MITRE ATT&CK ID: T1040
  - Affected Assets: 192.168.0.4 -> 192.254.189.169 (US, UNIFIEDLAYER-AS-1)
  - Evidence/Symptom: Detected plaintext credential exposure in HTTP traffic.
  - Immediate Mitigation Action: Block traffic from the offending IP address and investigate the affected system for potential credential compromise.

## 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.