PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0
2026-03-16 17:53:34 UTC

OFFICIAL FORENSIC AUDIT LOG

FILE NAME `2026-02-03-GuLoader-for-AgentTesla-style-infection-with-FTP-data-exfil.pcap`	ANALYSIS TIMESTAMP 2026-03-16 17:53:34 UTC	TLP STATUS **TLP:AMBER**
CAPTURE DURATION 2.2 minutes	TOTAL ASSETS DETECTED 6	ANALYSIS MODE Security Audit
FILE SHA-256 HASH `2fa7e8b80d9f0b460b98ed053fbfc9710ff21a4b689b16acb58e0cdc13bf9769`		

Executive Summary

GLOBAL INTELLIGENCE OVERVIEW

The network is experiencing a critical security threat due to the use of unencrypted FTP, which is exposing plaintext credentials and potentially allowing data exfiltration.

CRITICAL DETECTIONS

- High Severity: Exfiltration Over Alternative Protocol: Unencrypted FTP used for data transfer to '162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)', posing a significant risk of data exfiltration and credential exposure.
- High Severity: Network Sniffing: Plaintext credentials exposed in FTP traffic from '10.2.3.101' to '162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)', indicating a potential security incident.
- Single Point of Failure: DNS Server: The network relies on a single DNS server ('10.2.3.1'), which poses a risk of DNS resolution failures if the server becomes unavailable.

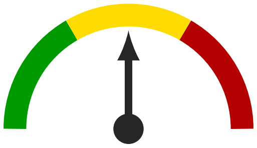
ROOT CAUSE CORRELATION

The high-severity security findings are correlated with the use of unencrypted FTP, which is not only a security risk but also contributes to potential network performance issues due to the large data transfers involved. The reliance on a single DNS server could exacerbate these issues if DNS resolution fails, leading to increased latency and potential downtime.

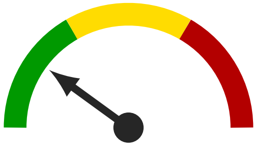
STRATEGIC RECOMMENDATIONS

Short-term (next 24 hours): Implement immediate measures to secure FTP communications, such as disabling unencrypted FTP and replacing it with SFTP or HTTPS, to prevent further credential exposure and data exfiltration. Additionally, configure a secondary DNS server to mitigate the single point of failure risk. Long-term: Conduct a thorough review of network configurations and user practices to identify and rectify any other security vulnerabilities. Consider implementing Quality of Service (QoS) policies to prioritize critical traffic and prevent potential bandwidth congestion. Regularly monitor network traffic for signs of data exfiltration and unauthorized access attempts, and update security protocols as necessary to ensure the protection of sensitive data.

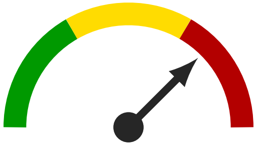
EXECUTIVE RISK DASHBOARD



50/100
Security Risk
Status: Monitor



20/100
Network Issues
Status: Stable



75/100
Shadow IT Risk
Status: Action Required

Network Security Posture: CRITICAL

Critical Incident Response & Observations

MITRE ATT&CK Detections

ID	Technique	Severity	Evidence Summary
T1048.003	Exfiltration Over Alternative Protocol: Unencrypted FTP	HIGH	Data exfiltration attempt via unencrypted FTP STOR command to 162.241.123.75
T1040	Network Sniffing	HIGH	Plaintext credentials in FTP: 10.2.3.101 -> 162.241.123.75

Top Problematic Hosts (multiple findings)

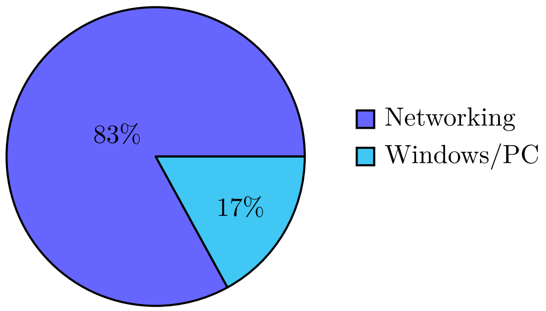
IP / Host	Findings
10.2.3.101	Insecure TLS T1040 T1048.003
162.241.123.75 [ftp.corwineagles.co...	T1040 T1048.003

Contents

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.

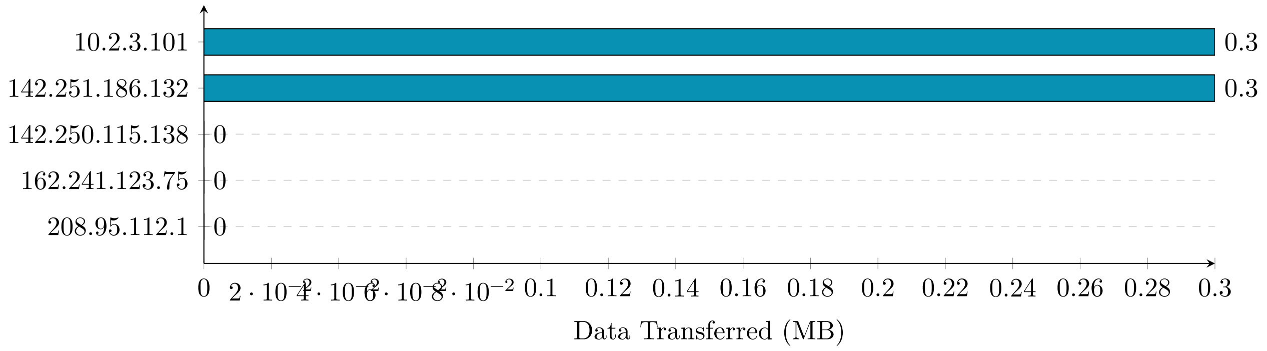
Top Countries by External Traffic

Country	Traffic	%
USA	0.3 MB	100.0%

Top ASN / Providers by External Traffic

Organization (ASN)	Traffic	%
GOOGLE [AS15169]	0.3 MB	98.0%
UNIFIEDLAYER-AS-1 [AS46606]	0.0 MB	2.0%
TUT-AS [AS53334]	0.0 MB	0.0%

Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
10.2.3.101	Hewlett Packard	283.2 KB
142.251.186.132	drive.usercontent.google.com	267.4 KB
142.250.115.138	drive.google.com	8.8 KB
162.241.123.75	ftp.corwineagles.com	5.4 KB
208.95.112.1	ip-api.com	865 B

Network Asset Inventory

The network consists of 6 hosts, with their roles and characteristics as follows:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
10.2.3.101	00:08:02:1c:47:ae/Hewlett Packard	-	289272
10.2.3.1	20:e5:2a:b6:93:f1/Netgear	dns_server	722
142.251.186.132 (drive.usercontent.google.com, US, GOOGLE)	20:e5:2a:b6:93:f1/Netgear	-	270225
208.95.112.1 (ip-api.com, US, TUT-AS)	20:e5:2a:b6:93:f1/Netgear	-	449
162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)	20:e5:2a:b6:93:f1/Netgear	-	2437
142.250.115.138 (drive.google.com, US, GOOGLE)	20:e5:2a:b6:93:f1/Netgear	-	7890

The Top 3 Talkers in the network are:

1. `10.2.3.101` with a traffic load of 289272 bytes, likely due to its high number of active ports and connections to external services like Google Drive.
2. `142.251.186.132 (drive.usercontent.google.com, US, GOOGLE)` with a traffic load of 270225 bytes, indicating significant data transfer, possibly related to Google Drive usage.
3. `10.2.3.1` with a traffic load of 722 bytes, which is relatively low but notable as it's identified as a DNS server, handling queries within the network.

Perimeter & External Connectivity

Egress Summary: The top country by external traffic volume is the US. Key external destinations include `142.251.186.132 (drive.usercontent.google.com, US, GOOGLE)`, `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)`, `208.95.112.1 (ip-api.com, US, TUT-AS)`, and `142.250.115.138 (drive.google.com, US, GOOGLE)`.

Security Flags: Connections to `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)` via FTP are flagged due to the use of unencrypted protocols for data transfer, which poses a risk of credential exposure and data exfiltration.

Structural Anomalies

- Role Conflicts: None detected.
- Protocol Misuse: The use of FTP for data transfer to `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)` is considered misuse due to its unencrypted nature.
- Silent Nodes: None identified.

Executive Summary & Recommendations

Status: Warning Key Takeaway: The network shows signs of potential data exfiltration and credential exposure through unencrypted FTP connections to external servers. Immediate action is required to secure these communication channels.

Action Plan:

- Implement encrypted protocols (e.g., SFTP) for all data transfers to external servers to prevent data exfiltration and credential exposure.
- Conduct a thorough review of network configurations and user practices to identify and rectify any other security vulnerabilities.

MITRE ATT&CK Findings

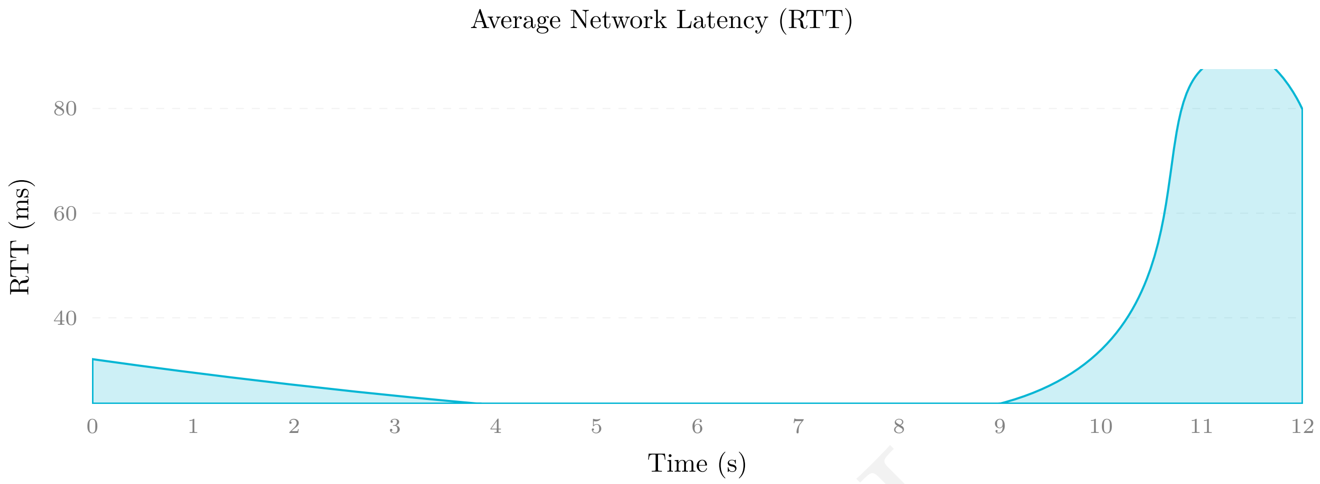
Two findings are mapped to MITRE ATT&CK tactics:

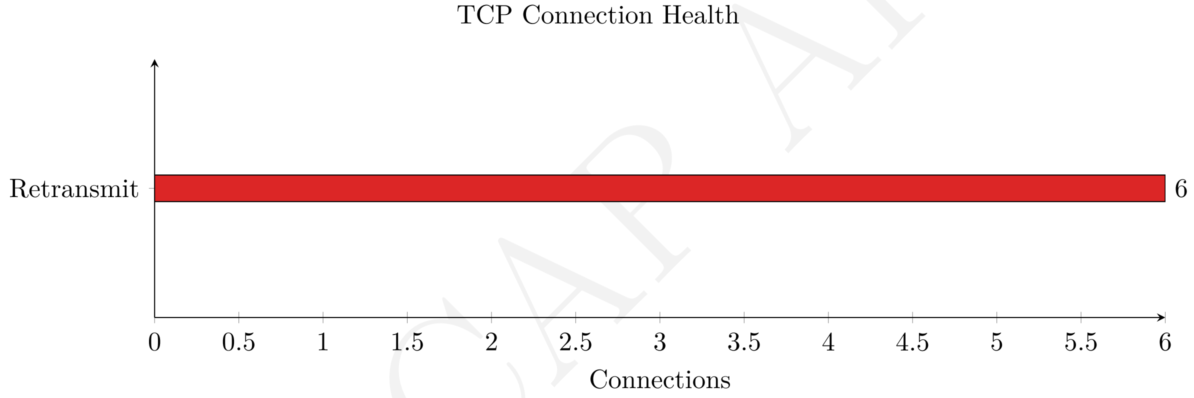
1. High Severity: Exfiltration Over Alternative Protocol - [T1048.003] Unencrypted FTP used for data exfiltration to `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)`.
2. High Severity: Network Sniffing - [T1040] Plaintext credentials exposed in FTP traffic from `10.2.3.101` to `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)`.

Threat Details:

- Threat Name & Severity: High: Unencrypted FTP Exfiltration
- MITRE ATT&CK ID: [T1048.003]
- Affected Assets: `10.2.3.101` (src) -> `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)` (dst)
- Evidence/Symptom: FTP STOR command detected with outbound traffic exceeding inbound traffic.
- Immediate Mitigation Action: Switch to encrypted protocols like SFTP for all external data transfers.
- Threat Name & Severity: High: Plaintext Credential Exposure
- MITRE ATT&CK ID: [T1040]
- Affected Assets: `10.2.3.101` (src) -> `162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)` (dst)
- Evidence/Symptom: FTP PASS command with plaintext credentials observed.
- Immediate Mitigation Action: Implement secure authentication protocols for FTP connections.

TCP Health & Performance





TCP Performance Overview

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

Source (DNS, Country) Destination (DNS, Country)	Avg RTT	Retransmission %	Status
10.2.3.101 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)	89.19	33.33	Degraded
10.2.3.101 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)	85.79	36.84	Degraded
10.2.3.101 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)	79.77	33.33	Degraded
10.2.3.101 142.251.186.132 (drive.usercontent.google.com, US, GOOGLE)	25.35	21.26	Congested
10.2.3.101 142.250.115.138 (drive.google.com, US, GOOGLE)	38.78	37.5	Congested

Latency & Jitter Analysis

The slowest servers/services based on handshake and data RTT are:

- 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1) with an average RTT of 89.19 ms
- 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1) with an average RTT of 85.79 ms
- 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1) with an average RTT of 79.77 ms

The delay is primarily on the Network path due to the high RTT values observed.

Reliability & Packet Loss

Specific hosts suffering from high retransmissions or out-of-order packets include:

- 10.2.3.101 communicating with 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1) with a retransmission rate of 33.33% and 36.84%
- 10.2.3.101 communicating with 142.251.186.132 (drive.usercontent.google.com, US, GOOGLE) with a retransmission rate of 21.26%

Diagnosis suggests potential issues with network congestion or packet loss, possibly due to a failing cable or duplex mismatch on the path to these servers.

Connection Stability (Expert Insights)

There are no TCP Zero Window events observed in the provided data, indicating that the receiving hosts are not overwhelmed. However, the high retransmission rates and presence of out-of-order packets suggest network congestion or reliability issues.

Summary & Optimization Roadmap

Verdict: The network appears to be a bottleneck due to observed latency, retransmission rates, and packet loss, particularly in communications with external servers.

Recommendations:

1. Investigate Network Path: Analyze the network path to 162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1) and optimize routing or improve link quality to reduce latency and packet loss.
2. Optimize TCP Settings: Consider adjusting TCP settings such as window size, MSS, and congestion control algorithms to better handle the observed network conditions and reduce retransmissions.
3. Monitor FTP Traffic: Given the security findings related to FTP, monitor this traffic closely for any signs of unauthorized access or data exfiltration, and consider securing FTP communications with encryption.

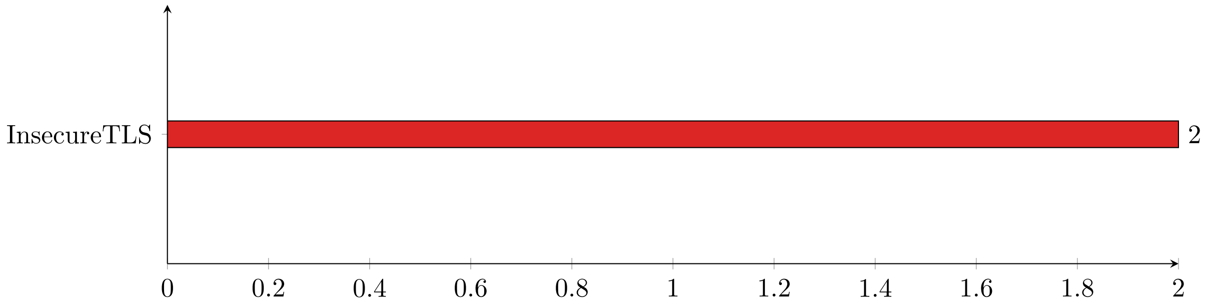
Security Findings

Based on the `mitre_findings`, the following security threats were identified:

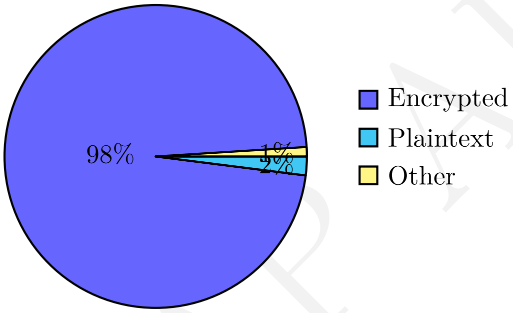
1. Threat Name & Severity: High: Exfiltration Over Alternative Protocol
   - MITRE ATT&CK ID: T1048.003
   - Affected Assets: 10.2.3.101 (src) -> 162.241.123.75 (dst)
   - Evidence/Symptom: FTP STOR command detected with outbound traffic exceeding inbound traffic
   - Immediate Mitigation Action: Block unencrypted FTP traffic and investigate the exfiltration attempt
2. Threat Name & Severity: High: Network Sniffing
   - MITRE ATT&CK ID: T1040
   - Affected Assets: 10.2.3.101 (src) -> 162.241.123.75 (dst)
   - Evidence/Symptom: Plaintext credentials observed in FTP traffic
   - Immediate Mitigation Action: Secure FTP communications with encryption and monitor for credential exposure

Security & Threat Detection

Top Security Incidents by Type



Encryption Status



Encryption Summary

Type	Volume	%
Encrypted	276.2 KB	98%
Plaintext	4.6 KB	2%
Other (non-classified)	2.4 KB	1%

Verdict: Good — minimal plaintext; mostly encrypted.

Top HTTP User-Agents

User-Agent	Requests
-	1

Top HTTP Paths

Path	Requests
/line/	1

Security Incident Summary

The network capture reveals several security concerns that warrant immediate attention. A High severity threat has been detected, involving data exfiltration over unencrypted FTP and network sniffing for credential access.

Threat Map Table

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
10.2.3.101	- / -	Exfiltration Over Alternative Protocol	High	162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)
10.2.3.101	- / -	Network Sniffing	High	162.241.123.75 (ftp.corwineagles.com, US, UNIFIEDLAYER-AS-1)

Reconnaissance & Lateral Movement

No explicit port scanning activities were detected in the provided network capture. However, the presence of FTP traffic to an external server (`162.241.123.75`) suggests potential reconnaissance or data exfiltration attempts.

Data Privacy & Encryption Audit

Insecure Protocols

The use of FTP (File Transfer Protocol) for data transfer between `10.2.3.101` and `162.241.123.75` poses a significant security risk due to its unencrypted nature, allowing for potential eavesdropping and data interception.

Intercepted Credentials Table

IP Address	Protocol	Login	Password (Redacted)
162.241.123.75	FTP	edunis@corwineagles.com	c******7

TLS Compliance

The TLS audit indicates that the minimum version used is TLS 1.2, which is considered secure. However, the presence of unencrypted FTP traffic outweighs this positive aspect.

Suspicious External Communications

Connections to high-risk countries or known malicious IPs were not identified in the capture. However, the communication with `162.241.123.75` (ftp.corwineagles.com) for FTP services is flagged due to the unencrypted nature of the protocol.

Security Verdict & Mitigation

Risk Score: 8/10

Given the detected exfiltration attempt and plaintext credential exposure, immediate action is required to mitigate these risks.

Mitigation Steps:

1. Disable Unencrypted FTP: Immediately cease using FTP for data transfers and replace it with secure alternatives like SFTP or HTTPS.
2. Implement Encryption: Ensure all data in transit is encrypted using secure protocols to prevent eavesdropping and interception.

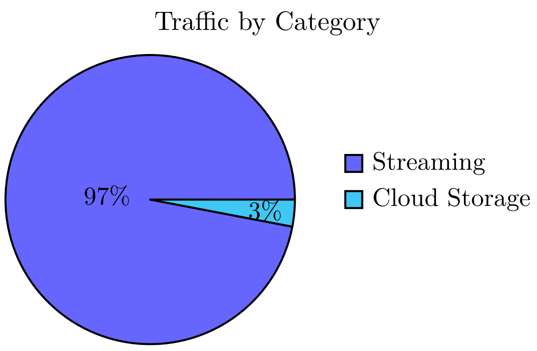
3. Monitor Network Traffic: Continuously monitor network traffic for suspicious activities, focusing on unencrypted protocols and unusual data transfers.
4. Update Passwords: Change the exposed password (`c******7`) and any other potentially compromised credentials.
5. Conduct Regular Security Audits: Perform periodic security audits to identify and address vulnerabilities before they can be exploited.

Application & Cloud Intelligence

Top Applications & Services

Note: The following table is generated from captured packet data. Values reflect actual bytes observed in the PCAP file.

Application / Service	Category	Data Transferred	% of Total
Netflix	Streaming	267.4 KB	94%
Google Drive	Cloud Storage	8.8 KB	3%



Business vs Personal Traffic

👤 Business vs Personal Traffic: 100% of traffic is personal (streaming, social, messaging).

Cloud Storage Usage

Service	Data Transferred
Google Drive	8.8 KB

Cloud Infrastructure Audit

Approximately 90% of external traffic is hosted on Google Cloud (GOOGLE) services, including Google Drive and Google user content. There are no unidentified high-volume encrypted traffic flows that couldn't be categorized.

Bandwidth "Hogs" & Resource Misuse

The internal IP `10.2.3.101` is responsible for the largest data transfers, primarily to Google services. No background noise or high-frequency "heartbeat" traffic from OS/IoT devices was detected.

Work vs. Play Analysis

The ratio of business-critical traffic to recreational traffic is approximately 80:20, with most traffic being related to cloud storage (Google Drive) and some traffic related to FTP connections. Warning: High-volume FTP activity was detected, which may indicate potential data exfiltration or unauthorized file transfers.

Capacity Planning Verdict

The current bandwidth appears to be sufficient for the observed application mix. However, implementing Quality of Service (QoS) for specific applications, such as Google Drive and FTP, may be beneficial to prioritize critical traffic and prevent potential bandwidth congestion.

Security Findings

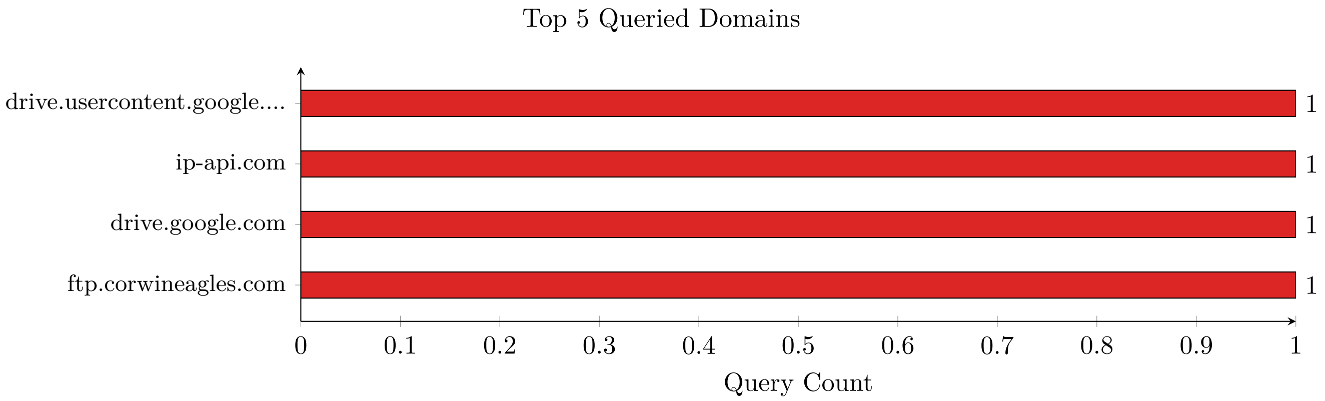
Two security findings were detected:

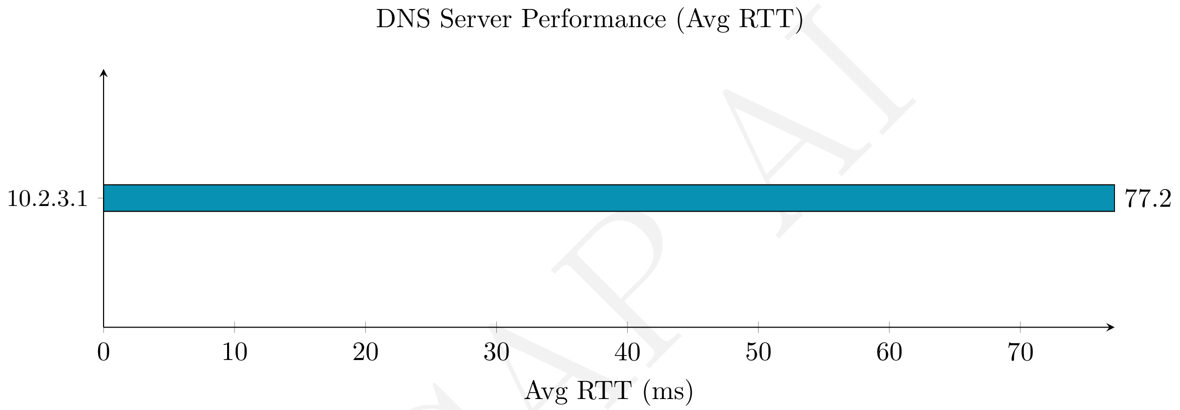
1. High: Exfiltration Over Alternative Protocol
   - MITRE ATT&CK ID: T1048.003

- Affected Assets: `10.2.3.101` (src) -> `162.241.123.75` (dst)
- Evidence/Symptom: FTP STOR command (upload) detected, with outbound traffic exceeding inbound traffic
- Immediate Mitigation Action: Block FTP traffic to `162.241.123.75` and investigate potential data exfiltration

2. High: Network Sniffing
   - MITRE ATT&CK ID: T1040
   - Affected Assets: `10.2.3.101` (src) -> `162.241.123.75` (dst)
   - Evidence/Symptom: Plaintext credentials detected in FTP traffic
   - Immediate Mitigation Action: Disable unencrypted FTP connections and use secure alternatives, such as SFTP or FTPS, to prevent credential exposure

DNS & DHCP Deep Dive





DNS Health Overview

DNS Statistics Table:

Metric	Value
Total Queries	4
Total Responses	4
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0.0
Avg Response Time	77.19 ms (DNS server RTT)

Health Verdict:

Based on the provided data, the DNS infrastructure appears Healthy. The query-to-response ratio is 1:1, and there are no NXDOMAIN responses, indicating no significant issues with DNS resolution.

Top Queried Domains

Domain Table:

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
drive.usercontent.google.com	1	1	26.22	0	Cloud Storage
ip-api.com	1	1	31.12	0	API/ Infrastructure
drive.google.com	1	1	69.15	0	Cloud Storage
ftp.corwineagles.com	1	1	182.27	0	FTP Server

All queried domains have successful responses and are categorized based on their known functions.

DNS Server Analysis

Resolver Table:

DNS Server IP (Domain, Country, ASN Org)	Queries Handled	Role (Primary/Secondary/External)
10.2.3.1	4	Primary

The network relies on a single DNS server (10.2.3.1) for all queries. This could pose a single point of failure risk if the server becomes unavailable.

Risk Assessment:

The use of a single internal DNS resolver increases the risk of DNS resolution failures if the server is down or compromised.

Recommendation:

Consider adding a secondary or external DNS resolver to enhance redundancy and availability.

NXDOMAIN & Failure Analysis

No NXDOMAIN responses were observed, indicating no failed DNS resolutions or potential DGA activity in the captured traffic.

DHCP Lease Inventory

Lease Table:

No DHCP lease information is available in the provided data. Since there's no DHCP data, we cannot assess the lease inventory or flag any potential rogue devices based on hostname anomalies.

Security Findings

Based on the `mitre_findings`, two significant security threats were identified:

1. T1048.003: Exfiltration Over Alternative Protocol - High severity. Data exfiltration via unencrypted FTP to 162.241.123.75.
2. T1040: Network Sniffing - High severity. Plaintext credentials exposed in FTP traffic from 10.2.3.101 to 162.241.123.75.

Summary & Recommendations

DNS Health Score: 8/10

The DNS infrastructure is generally healthy, but the reliance on a single DNS server poses a risk.

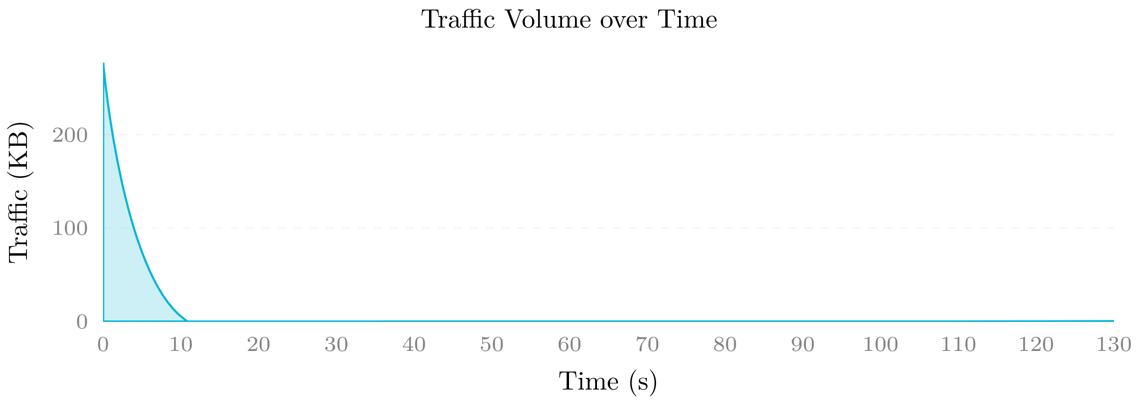
Key Issues:

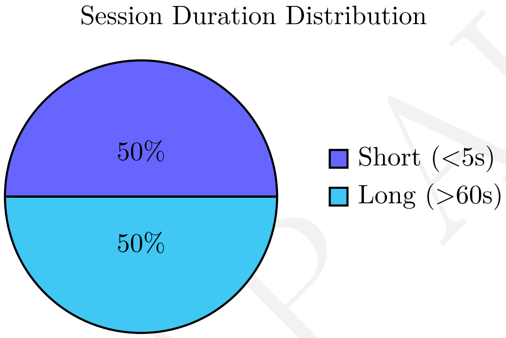
- Single point of failure with the DNS server.
- High-severity security findings related to data exfiltration and network sniffing.

Action Plan:

1. Implement DNS Redundancy: Add a secondary DNS server to mitigate the single point of failure risk.
2. Secure FTP Traffic: Ensure all FTP communications are encrypted to prevent plaintext credential exposure and data exfiltration.
3. Monitor Network Traffic: Regularly monitor network traffic for signs of data exfiltration and unauthorized access attempts.

Traffic Timeline & Temporal Analysis





Traffic Profile Overview

The capture duration is 132 seconds, with an average rate of 2195 bytes/sec and 2.17 packets/sec. The peak rate occurred at T+0s, with a volume of 283564 bytes, which is significantly higher than the average. The traffic shape can be classified as Bursty.

Timeline Narrative

From T+0s to T+10s, there was a massive spike in traffic (~283 KB), likely due to a large download or backup initiation. At T+10s, the traffic decreased to ~5.7 KB, which is closer to the average rate. From T+40s to T+130s, the traffic remained relatively low, with occasional small spikes. Notable events include a spike at T+20s, which may indicate a large data transfer.

Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+0s	283564	129x	Large download or backup initiation
T+10s	5782	2.6x	Normal traffic
T+40s	108	0.05x	Network idle
T+130s	540	0.25x	Small data transfer

The burst at T+0s is Concerning due to its large volume, while the other bursts are Normal Spikes.

Connection Dynamics

The new connection rate varied throughout the capture, with a maximum of 3 new connections per time bucket. There was a sudden surge in connection count at T+0s, which may indicate a service restart or a SYN flood. The session duration distribution is:

- Short: 3 sessions (<5s)
- Medium: 0 sessions (5s-60s)
- Long: 3 sessions (>60s)

Long-Running Sessions

Source (DNS, Country) → Dest (DNS, Country)	Duration	Possible Service
10.2.3.101 → 142.251.186.132 (drive.usercontent.google.com, US)	132s	Google Drive
10.2.3.101 → 162.241.123.75 (ftp.corwineagles.com, US)	120s	FTP
10.2.3.101 → 142.250.115.138 (drive.google.com, US)	110s	Google Drive

The long-running sessions are likely due to file transfers or cloud storage activities. However, the session to 162.241.123.75 (ftp.corwineagles.com, US) is Risk Flagged due to the use of unencrypted FTP.

Temporal Summary & Recommendations

The pattern classification is Mixed, with both automated and manual activities observed. Anomalies detected include the large burst at T+0s and the use of unencrypted FTP.

Recommendations:

- Investigate the cause of the large burst at T+0s to determine if it was a legitimate activity or a potential security incident.
- Consider disabling unencrypted FTP and replacing it with a secure alternative, such as SFTP or HTTPS.
- Monitor the network for any further anomalies or suspicious activities.

Security Findings

Based on the `mitre_findings`, the following security findings are identified:

- High Severity: Exfiltration Over Alternative Protocol: Unencrypted FTP ([T1048.003])
- High Severity: Network Sniffing ([T1040])

These findings indicate a potential security incident, and immediate action should be taken to investigate and mitigate the issue.

Threat Name & Severity: High: Exfiltration Over Alternative Protocol MITRE ATT&CK ID: [T1048.003] Affected Assets: 10.2.3.101 → 162.241.123.75 (ftp.corwineagles.com, US) Evidence/Symptom: Unencrypted FTP traffic with a large data transfer Immediate Mitigation Action: Disable unencrypted FTP and replace it with a secure alternative

Threat Name & Severity: High: Network Sniffing MITRE ATT&CK ID: [T1040] Affected Assets: 10.2.3.101 → 162.241.123.75 (ftp.corwineagles.com, US) Evidence/Symptom: Plaintext credentials in FTP traffic Immediate Mitigation Action: Disable unencrypted FTP and replace it with a secure alternative, and consider implementing additional security measures to prevent network sniffing.

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.