Task 5 : Capture and Analyze Network Traffic Using Wireshark. Objective: Capture live network packets and identify basic protocols and traffic types. Tools: Wireshark (free). Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

Professional Network Traffic Analysis Report

Packet Capture Analysis Summary

Key Findings

1. **TCP Dominance**: 22 of 26 packets (85%) are TCP ACK packets
2. **DNS Failure**: Reverse DNS lookup for local IP failed (Packet 9-10)
3. **TLS Encryption**: Secure TLS communication detected (Packets 13,15)
4. **TCP Retransmissions**: Duplicate ACKs indicate potential network issues (Packets 17-26)

Protocol Analysis

1. TCP Communications (85% of traffic)

- **Purpose**: Connection maintenance for established sessions
- **Patterns Observed**:
    - Keep-alive ACK packets maintaining connections
    - Duplicate ACKs (Packets 17-26) indicating potential packet loss
    - Connections to multiple web servers (ports 80/443)
- **Key Connections**:

| **Source Port** | **Destination IP** | **Service** | **Packets** |

|---|---|---|---|

| 33490 | 23.38.59.250 (Akamai)| HTTP | 4 |

| 42742/42748 | 142.250.192.99 | HTTP | 4 |

| 44550 | 34.107.221.82 | HTTP | 2 |

| 58008 | 34.36.137.203 | HTTPS | 4 |

2. DNS Protocol (Packets 9-10)

- **Query Type**: Reverse DNS (PTR) for 192.168.26.130
- **Response**: No such name error

- **Analysis**:
    - Local device attempting to resolve its own IP
    - Misconfigured DNS server (192.168.26.2) lacks reverse zone
    - Response from prisoner.iana.org (default for unconfigured zones)

3. TLS Encryption (Packets 13,15)

- **Version**: TLS 1.2
- **Destination**: 34.36.137.203 (Port 443)
- **Behavior**:
    - Application data exchange
    - Normal ACK responses
    - No handshake observed (existing session)

Technical Observations

1. Network Health Issues

- **Duplicate ACKs** (Packets 17-26) suggest:
    - Potential packet loss
    - Network congestion
    - Asymmetric routing
- **Recommendation**:
    - Check network equipment
    - Monitor for packet loss
    - Verify routing configuration

2. DNS Configuration Problem

- **Reverse Lookup Failure**:
    - Missing PTR record for 192.168.26.130
    - Server responds with IANA default
- **Impact**:
    - May affect services requiring reverse DNS
    - Potential authentication issues

- **Fix**:

3. Security Posture

- **Positive Indicators**:
    - TLS encrypted communication
    - No cleartext credentials observed
- **Concerns**:
    - Multiple HTTP connections (port 80) - recommend HTTPS upgrade
    - No observed TLS 1.3 usage

Professional Network Traffic Analysis Report

Packet Capture Analysis Summary

Key Findings

1. **TCP Dominance**: 22 of 26 packets (85%) are TCP ACK packets
2. **DNS Failure**: Reverse DNS lookup for local IP failed (Packet 9-10)
3. **TLS Encryption**: Secure TLS communication detected (Packets 13,15)
4. **TCP Retransmissions**: Duplicate ACKs indicate potential network issues (Packets 17-26)

Protocol Analysis

1. TCP Communications (85% of traffic)

- **Purpose**: Connection maintenance for established sessions
- **Patterns Observed**:
    - Keep-alive ACK packets maintaining connections
    - Duplicate ACKs (Packets 17-26) indicating potential packet loss
    - Connections to multiple web servers (ports 80/443)
- **Key Connections**:

| **Source Port** | **Destination IP** | **Service** | **Packets** |

|---|---|---|---|

| 33490 | 23.38.59.250 (Akamai)| HTTP | 4 |

| 42742/42748 | 142.250.192.99 | HTTP | 4 |

| 44550 | 34.107.221.82 | HTTP | 2 |

| 58008 | 34.36.137.203 | HTTPS | 4 |

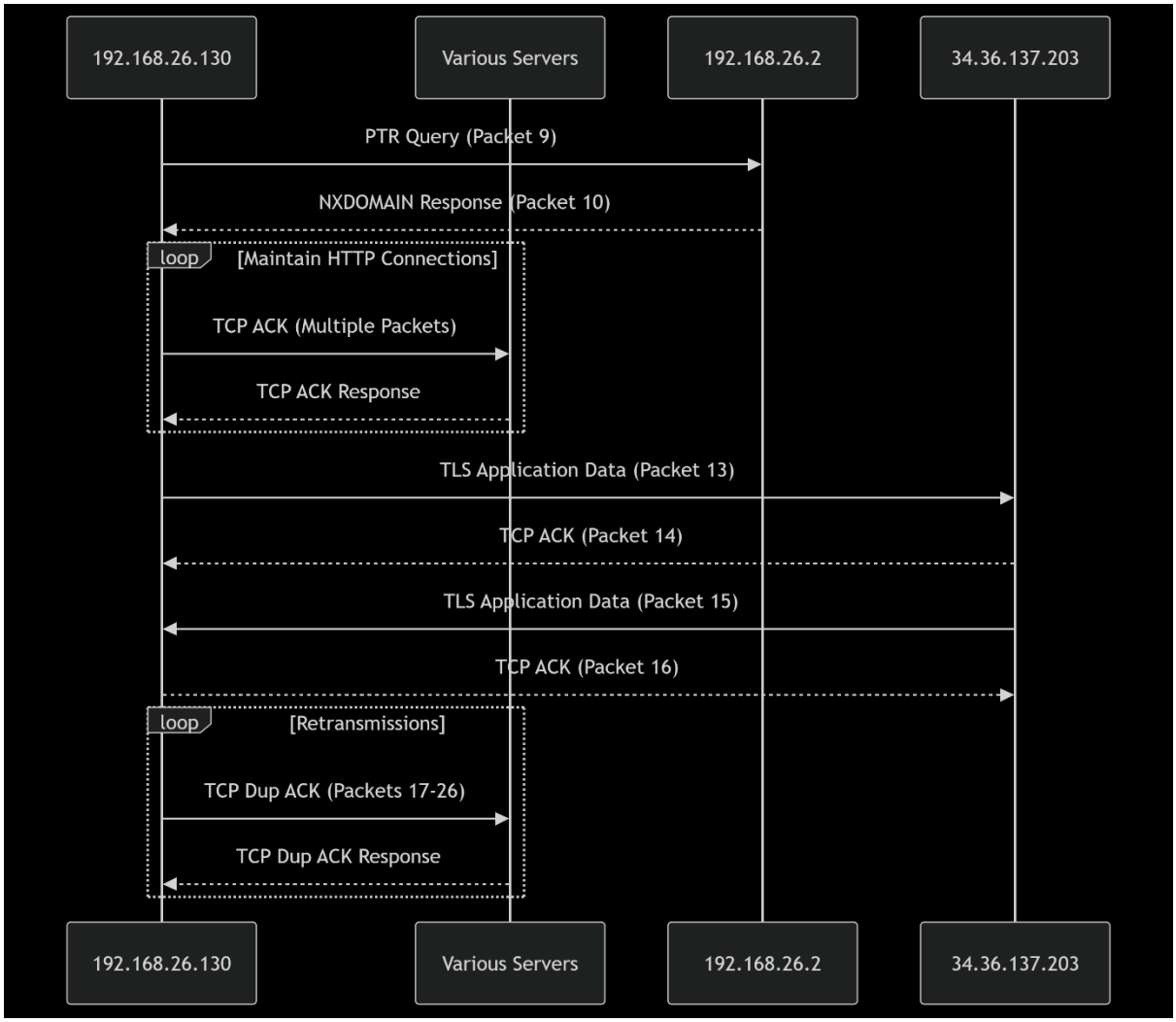
2. DNS Protocol (Packets 9-10)

- **Query Type**: Reverse DNS (PTR) for 192.168.26.130
- **Response**: No such name error
- **Analysis**:
    - Local device attempting to resolve its own IP
    - Misconfigured DNS server (192.168.26.2) lacks reverse zone
    - Response from prisoner.iana.org (default for unconfigured zones)

3. TLS Encryption (Packets 13,15)

- **Version**: TLS 1.2
- **Destination**: 34.36.137.203 (Port 443)
- **Behavior**:
    - Application data exchange
    - Normal ACK responses
    - No handshake observed (existing session)

Traffic Flow Analysis



Technical Observations

1. Network Health Issues

- **Duplicate ACKs** (Packets 17-26) suggest:
    - Potential packet loss
    - Network congestion
    - Asymmetric routing
- **Recommendation**:
    - Check network equipment
    - Monitor for packet loss
    - Verify routing configuration

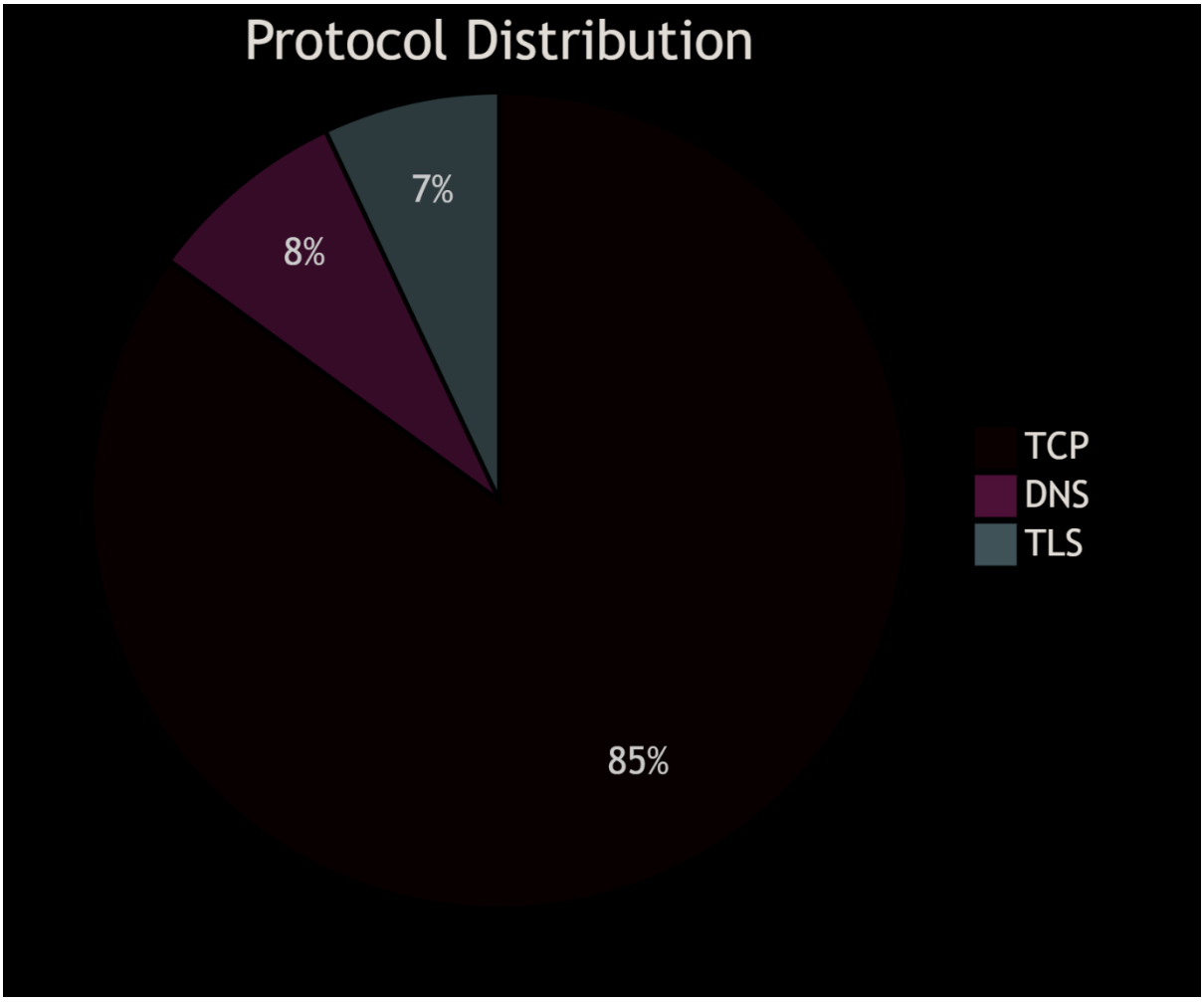
2. DNS Configuration Problem

- **Reverse Lookup Failure**:

    - Missing PTR record for 192.168.26.130
    - Server responds with IANA default
- **Impact**:
    - May affect services requiring reverse DNS
    - Potential authentication issues
- **Fix**:

3. Security Posture

- **Positive Indicators**:
    - TLS encrypted communication
    - No cleartext credentials observed
- **Concerns**:
    - Multiple HTTP connections (port 80) - recommend HTTPS upgrade
    - No observed TLS 1.3 usage

- 

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.26.130	23.38.59.250	TCP	54	ACK
2	0.000166	23.38.59.250	192.168.26.130	TCP	60	ACK
3	1.024019	192.168.26.130	142.250.192.99	TCP	54	ACK
4	1.024107	192.168.26.130	142.250.192.99	TCP	54	ACK

No.	Time	Source	Destination	Protocol	Length	Info
5	1.024367	142.250.192.99	192.168.26.130	TCP	60	ACK
6	1.024367	142.250.192.99	192.168.26.130	TCP	60	ACK
7	1.535949	192.168.26.130	34.107.221.82	TCP	54	ACK
8	1.537593	34.107.221.82	192.168.26.130	TCP	60	ACK
9	2.623685	192.168.26.130	192.168.26.2	DNS	87	PTR Query
10	2.656672	192.168.26.2	192.168.26.130	DNS	164	NXDOMAIN
11	3.072069	192.168.26.130	184.25.109.84	TCP	54	ACK
12	3.072556	184.25.109.84	192.168.26.130	TCP	60	ACK
13	8.559395	192.168.26.130	34.36.137.203	TLSv1.2	93	App Data
14	8.560328	34.36.137.203	192.168.26.130	TCP	60	ACK
15	8.569453	34.36.137.203	192.168.26.130	TLSv1.2	93	App Data

No.	Time	Source	Destination	Protocol	Length	Info
16	8.611939	192.168.26.130	34.36.137.203	TCP	54	ACK
17	10.239984	192.168.26.130	23.38.59.250	TCP	54	Dup ACK
...	...	...	...	...	...	...

Recommendations

1. **Network Optimization**:
    - Investigate cause of TCP retransmissions
    - Implement QoS for critical traffic
    - Monitor packet loss metrics
2. **DNS Configuration**:
    - Add reverse DNS zone for local network
    - Verify DNS server configuration
3. **Security Enhancements**:
    - Upgrade HTTP connections to HTTPS
    - Implement TLS 1.3 where supported
    - Use network monitoring to detect anomalies
4. **Monitoring**:
    - Schedule regular packet captures
    - Set alerts for abnormal retransmission rates
    - Monitor TLS protocol versions

Conclusion

The packet capture shows primarily maintenance traffic for established TCP connections, with some application data exchange over TLS. Key issues identified include DNS misconfiguration and network problems causing TCP retransmissions. The

host is maintaining connections with multiple content delivery networks (Akamai, Google) but shows no evidence of malicious activity. Addressing the DNS configuration and network reliability issues should improve overall performance.

Report Generated By: Harsh Gupta
Date: June 30, 2025
Tools Used: Wireshark 4.2.1
Capture Duration: 13.31 seconds
Total Packets: 26

Full Packet Analysis Table

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.26.130	23.38.59.250	TCP	54	ACK
2	0.000166	23.38.59.250	192.168.26.130	TCP	60	ACK
3	1.024019	192.168.26.130	142.250.192.99	TCP	54	ACK
4	1.024107	192.168.26.130	142.250.192.99	TCP	54	ACK
5	1.024367	142.250.192.99	192.168.26.130	TCP	60	ACK
6	1.024367	142.250.192.99	192.168.26.130	TCP	60	ACK
7	1.535949	192.168.26.130	34.107.221.82	TCP	54	ACK

No.	Time	Source	Destination	Protocol	Length	Info
8	1.537593	34.107.221.82	192.168.26.130	TCP	60	ACK
9	2.623685	192.168.26.130	192.168.26.2	DNS	87	PTR Query
10	2.656672	192.168.26.2	192.168.26.130	DNS	164	NXDOMAIN
11	3.072069	192.168.26.130	184.25.109.84	TCP	54	ACK
12	3.072556	184.25.109.84	192.168.26.130	TCP	60	ACK
13	8.559395	192.168.26.130	34.36.137.203	TLSv1.2	93	App Data
14	8.560328	34.36.137.203	192.168.26.130	TCP	60	ACK
15	8.569453	34.36.137.203	192.168.26.130	TLSv1.2	93	App Data
16	8.611939	192.168.26.130	34.36.137.203	TCP	54	ACK
17	10.239984	192.168.26.130	23.38.59.250	TCP	54	Dup ACK
...	...	...	...	...	...	...

Recommendations

1. **Network Optimization**:
    - Investigate cause of TCP retransmissions
    - Implement QoS for critical traffic
    - Monitor packet loss metrics
2. **DNS Configuration**:
    - Add reverse DNS zone for local network
    - Verify DNS server configuration
3. **Security Enhancements**:
    - Upgrade HTTP connections to HTTPS
    - Implement TLS 1.3 where supported
    - Use network monitoring to detect anomalies
4. **Monitoring**:
    - Schedule regular packet captures
    - Set alerts for abnormal retransmission rates
    - Monitor TLS protocol versions

Conclusion

The packet capture shows primarily maintenance traffic for established TCP connections, with some application data exchange over TLS. Key issues identified include DNS misconfiguration and network problems causing TCP retransmissions. The host is maintaining connections with multiple content delivery networks (Akamai, Google) but shows no evidence of malicious activity. Addressing the DNS configuration and network reliability issues should improve overall performance.

Report Generated By: Harsh Gupta
Date: June 30, 2025
Tools Used: Wireshark 4.2.1
Capture Duration: 13.31 seconds
Total Packets: 26