NETWORK TRAFFIC ANALYSIS – SOC PERSPECTIVE

Objective of the Analysis

To perform real-time network traffic monitoring and analysis using live packet capture in order to identify, validate, and interpret encrypted communication behavior and potential security events from a Security Operations Center (SOC) perspective.

Analysis Aims To :

- Monitor live network traffic to observe real-time communication patterns
- Analyze encrypted traffic including HTTPS (TCP/443) and QUIC (UDP/443)
- Detect abnormal behaviors such as connection resets, timing anomalies, and high-frequency access attempts
- Validate the presence or absence of SSH-based attack activity on port 22
- Convert live packet observations into SOC-ready findings and risk assessments

Tools Used:
Wireshark

Dataset:
Live Wi-Fi Network Capture

Prasented by: Vinit Shankar Raparti

Filter: tcp

Observation:

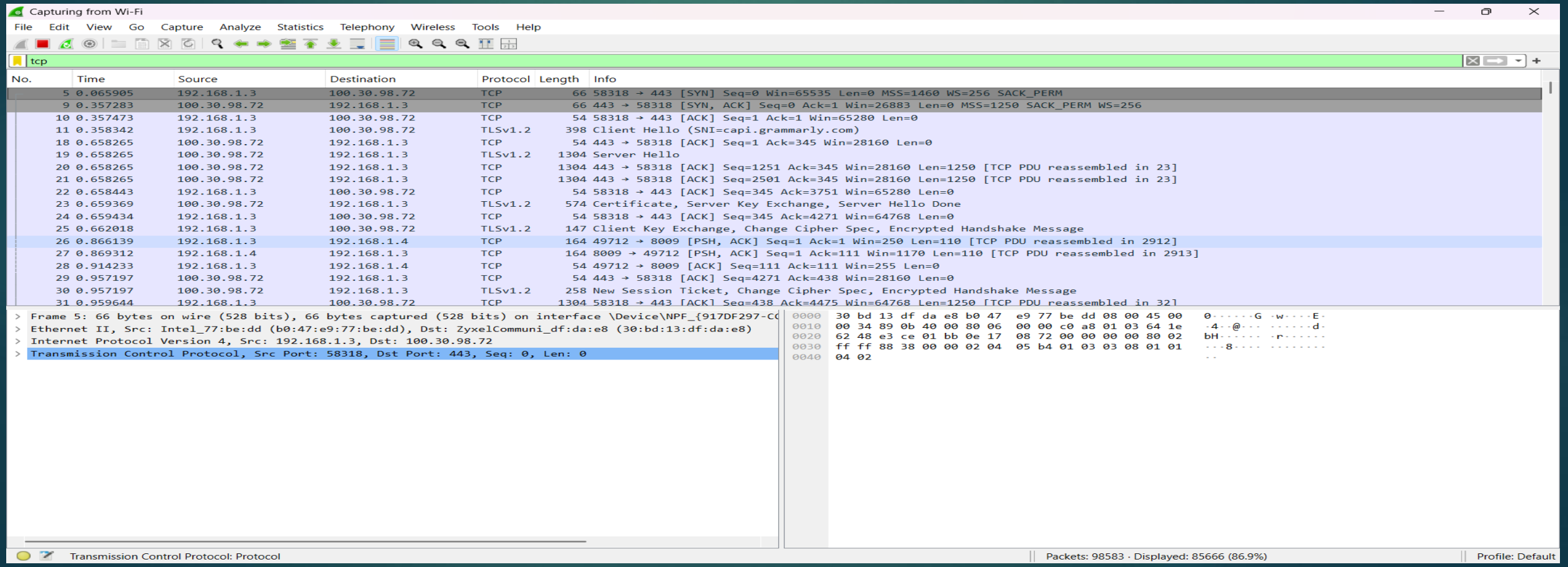
TCP traffic dominates the capture, mainly over destination port 443.

Reason:

Most web applications use TCP as the transport layer for HTTPS.

Conclusion:

The host is actively communicating with external web services using standard TCP-based HTTPS.



Filter: udp.port == 443

Observation:

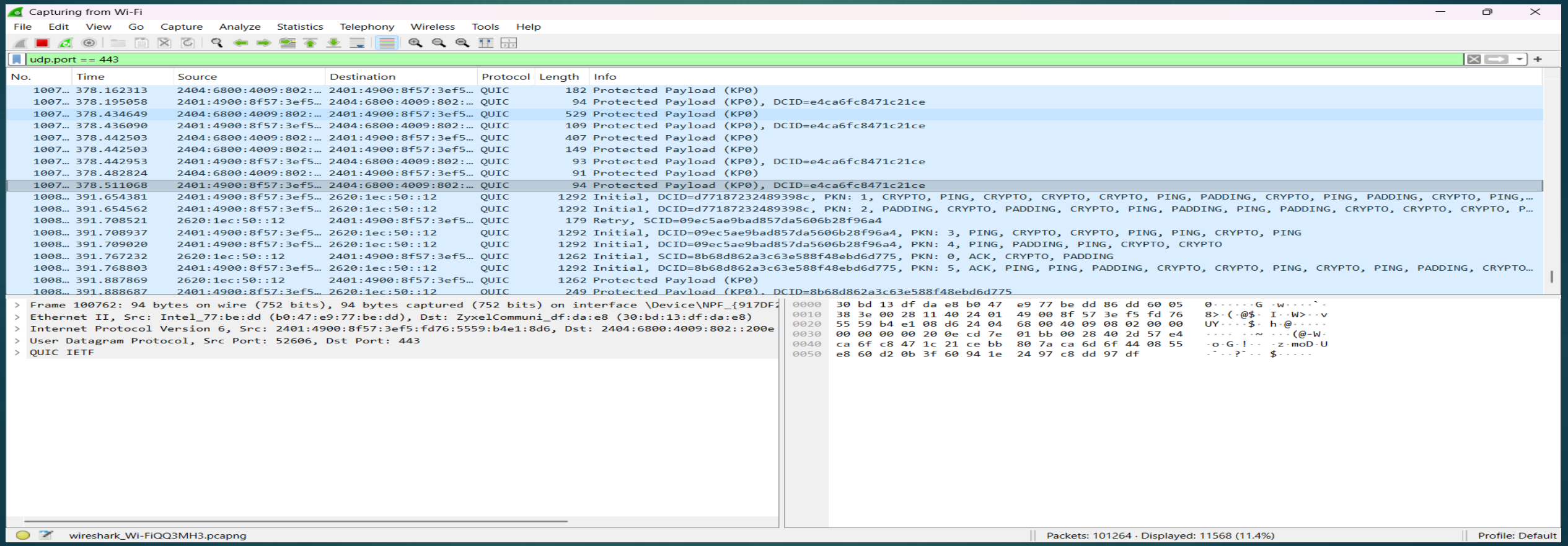
Significant UDP traffic observed on port 443 using the QUIC protocol.

Reason:

Modern applications use QUIC (HTTP/3) for faster encrypted communication.

Conclusion:

The host is communicating with services that support QUIC-based HTTPS.



Filter: ip.addr == 192.168.1.3

Observation:

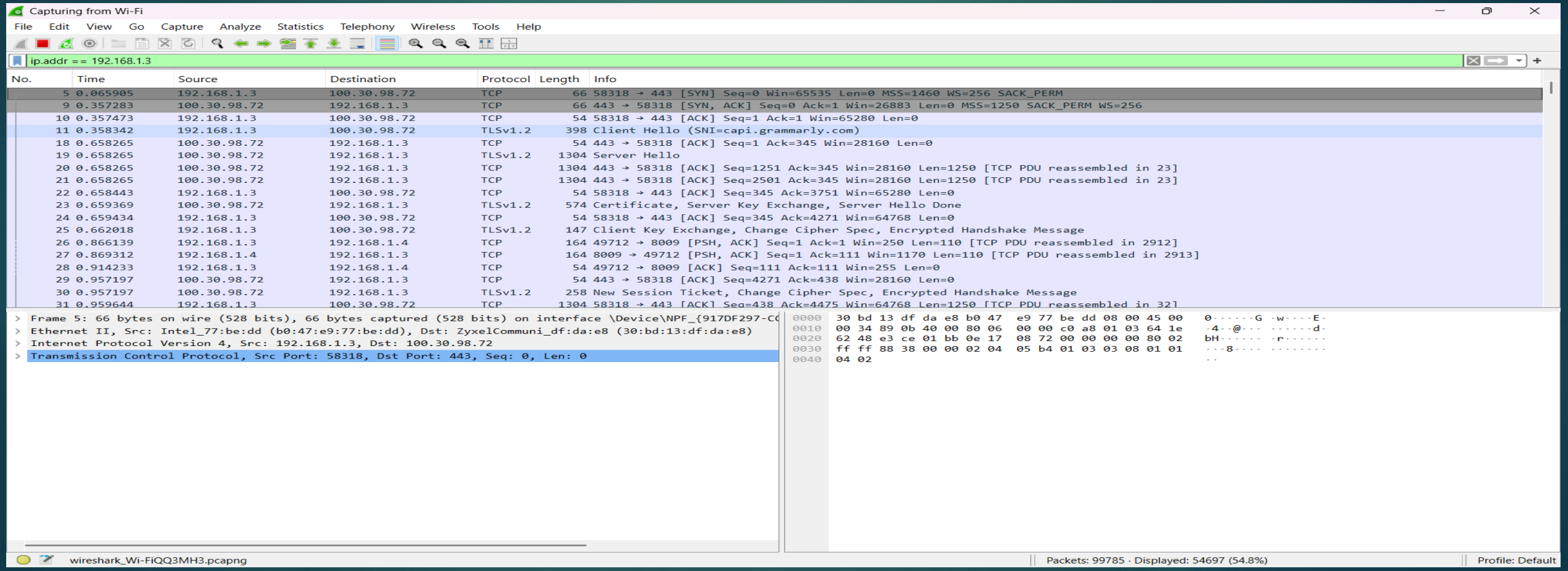
All displayed packets involve the internal host 192.168.1.3.

Reason:

This filter isolates traffic generated or received by the target endpoint.

Conclusion:

The analysis is focused on a single internal system's network behavior.



Filter: ip.addr == 192.168.1.3 and tcp.port == 443

Observation:

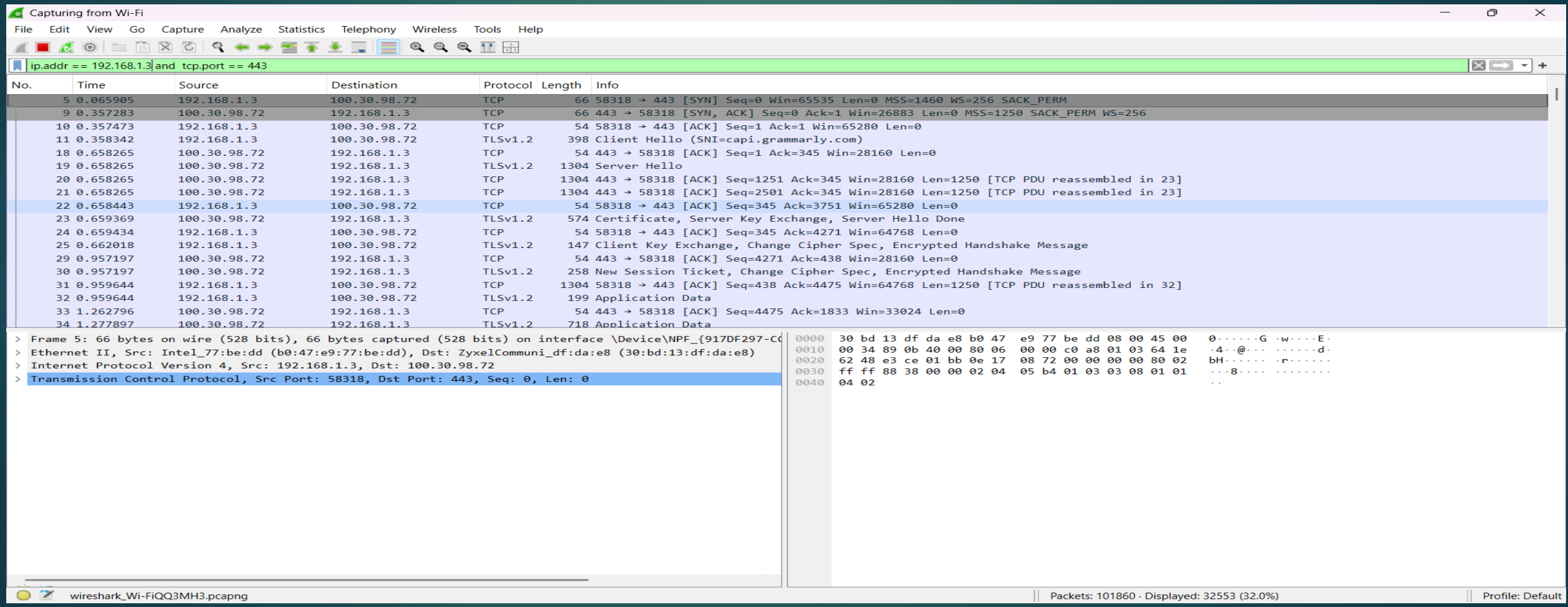
TLS 1.2 handshake packets (Client Hello, Server Hello, Certificate) are visible.

Reason:

TLS negotiation occurs before encrypted data transfer begins.

Conclusion:

Secure HTTPS sessions are being properly established by the internal host.



Filter: ip.dst != 192.168.0.0/16 and ip.dst != 10.0.0.0/8

Observation:

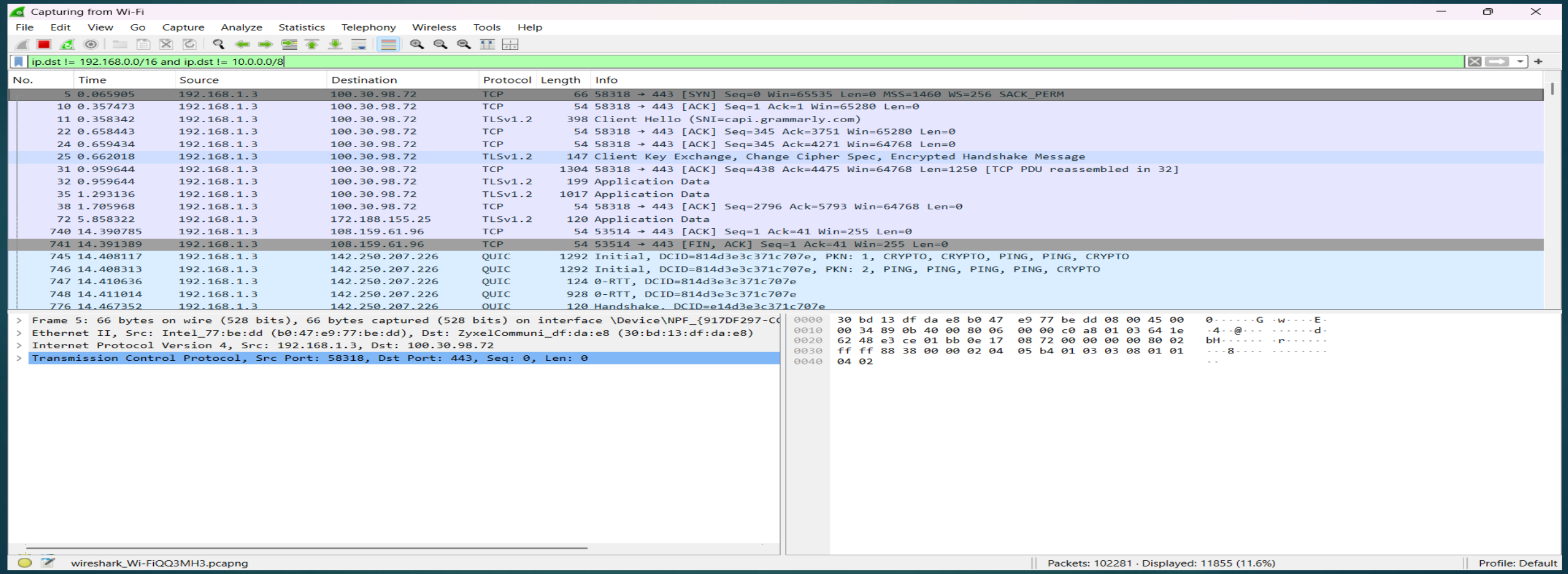
Traffic is directed to public IP addresses outside private network ranges.

Reason:

The host is communicating with external internet-based services.

Conclusion:

Outbound internet access is active and functioning as expected.



Filter: tcp.flags.reset == 1

Observation:

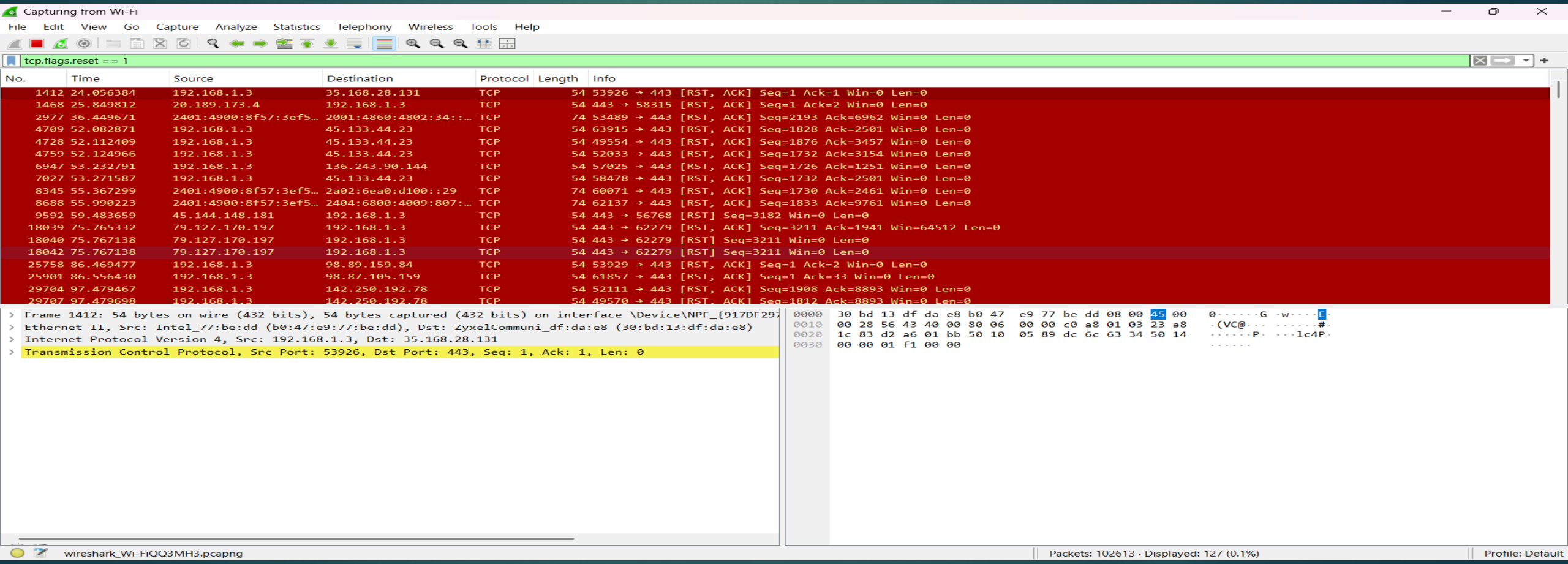
Multiple TCP RST packets observed, primarily on port 443 connections.

Reason:

Connections were abruptly terminated by either client or server.

Conclusion:

Session termination behavior is present and appears non-malicious.



Filter: tcp.port == 22 and frame.time_delta < 1

Observation:

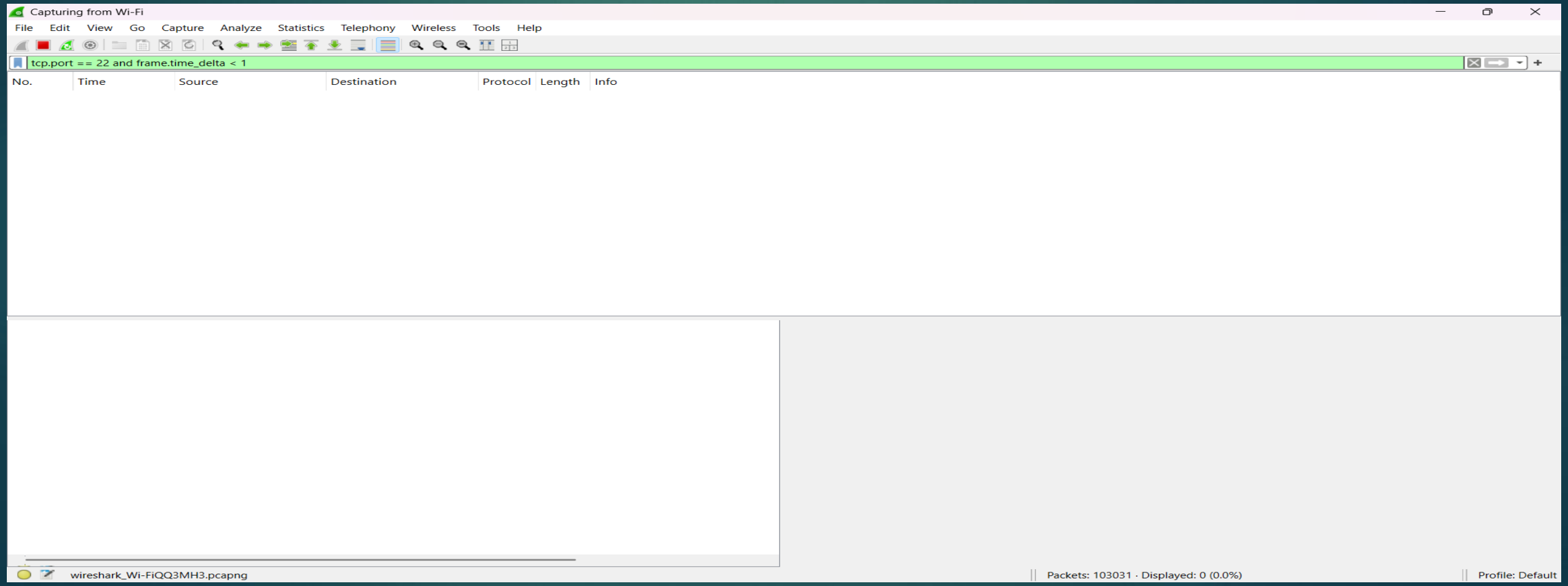
No packets were displayed for TCP port 22 within a time delta of less than 1 second.

Reason:

There is no evidence of rapid or repeated SSH connection attempts during the capture period.

Conclusion:

No SSH brute-force activity or automated attack behavior was detected.



Filter: quic

Observation:

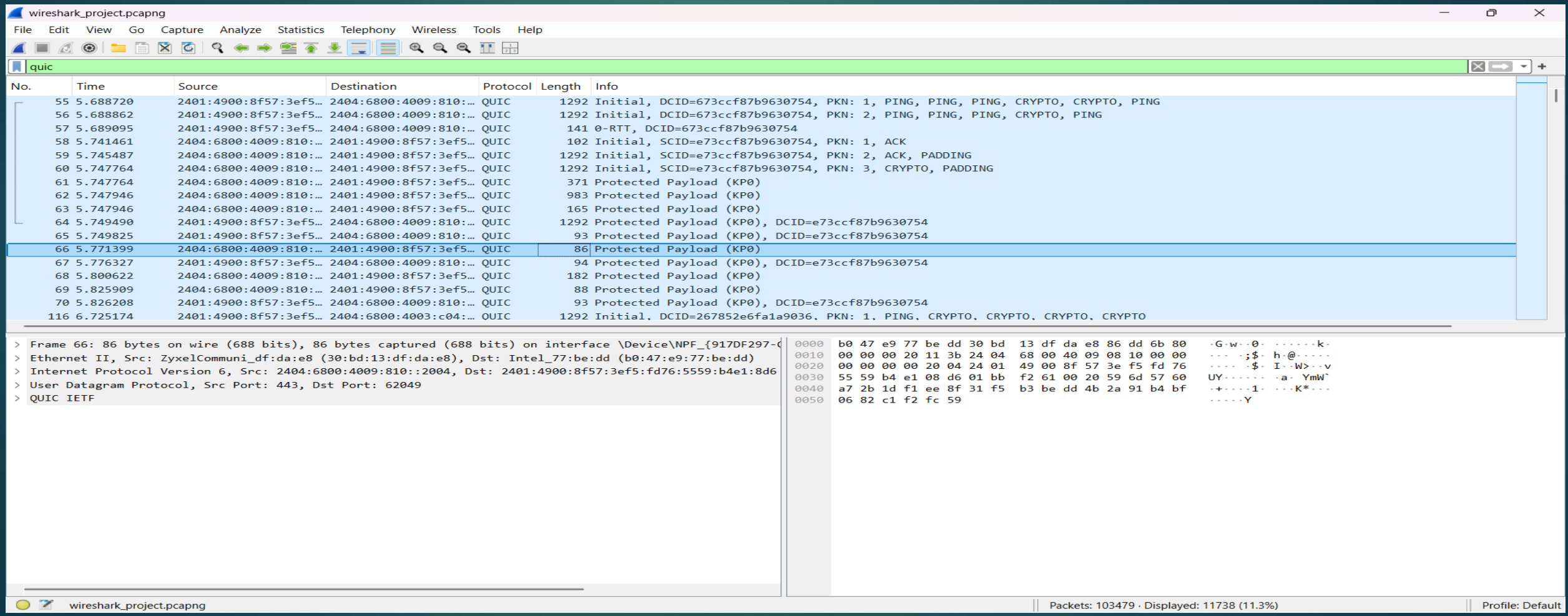
QUIC Initial, Handshake, and Protected Payload packets detected.

Reason:

QUIC is used by modern browsers and cloud services for performance improvements.

Conclusion:

The network supports modern encrypted transport protocols.



Filter: tls (TLS 1.2)

Observation:

TLS handshake and application data packets are present.

Reason:

TLS encrypts application-layer data to ensure confidentiality.

Conclusion:

Captured traffic is encrypted, limiting payload inspection but confirming secure communication.