Network Traffic Analysis – Phase 1 (Baseline)

Author: Oscar Santos
Role: Junior SOC Analyst
Tool Wireshark
Date: 2/2/2026

This document presents the analysis of legitimate network traffic captured in a controlled environment. The purpose of this phase is to establish a baseline of normal network behavior, which will be used as a reference to identify anomalous or potentially traffic in later phases of the project.

Phase 1

The aim of Phase 1 is to identify and document normal network traffic patterns, including DNS, TLS TCP, and HTTP activity, to understand typical user behavior and establish a baseline.

Environment

- Operating System: Windows
- Tool: Wireshark
- Traffic Type: Normal web browsing
- Capture Duration: 3–5 minutes
- Main Protocols Observed: TCP, DNS, TLS

Limitations:

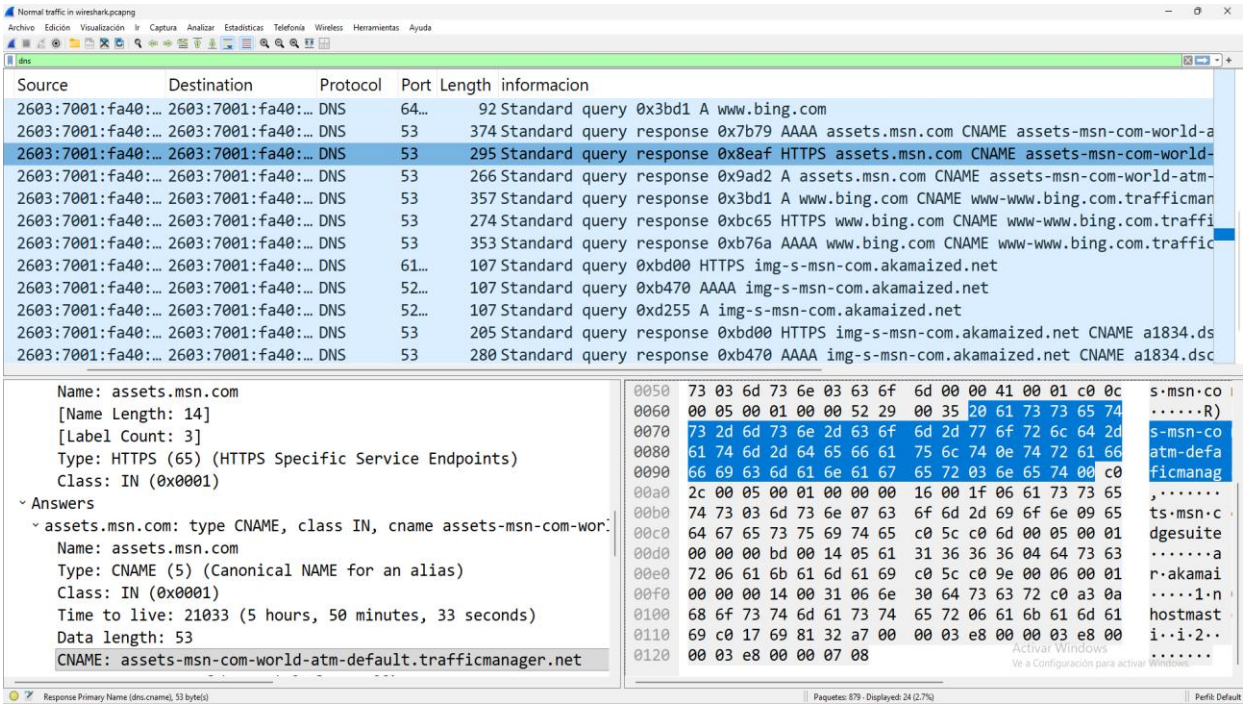
This phase focuses exclusively on baseline traffic and does not include malicious activity simulation or deep packet inspection due to encryption. The established baseline will be used as a reference to identify deviations and suspicious network behavior in Phase 2.

Methodology

Network traffic was captured using Wireshark while performing common user activities such as web browsing and connectivity tests. The captured traffic was then analyzed using protocol-specific filters to identify normal communication patterns. The traffic represents a single endpoint performing standard user web browsing behavior.

Findings – Normal Traffic:

DNS



The screenshot displays normal DNS traffic captured in Wireshark using the DNS filter. The queries and responses are related to legitimate domains such as www.bing.com and assets.msn.com, which are commonly accessed during standard web browsing.

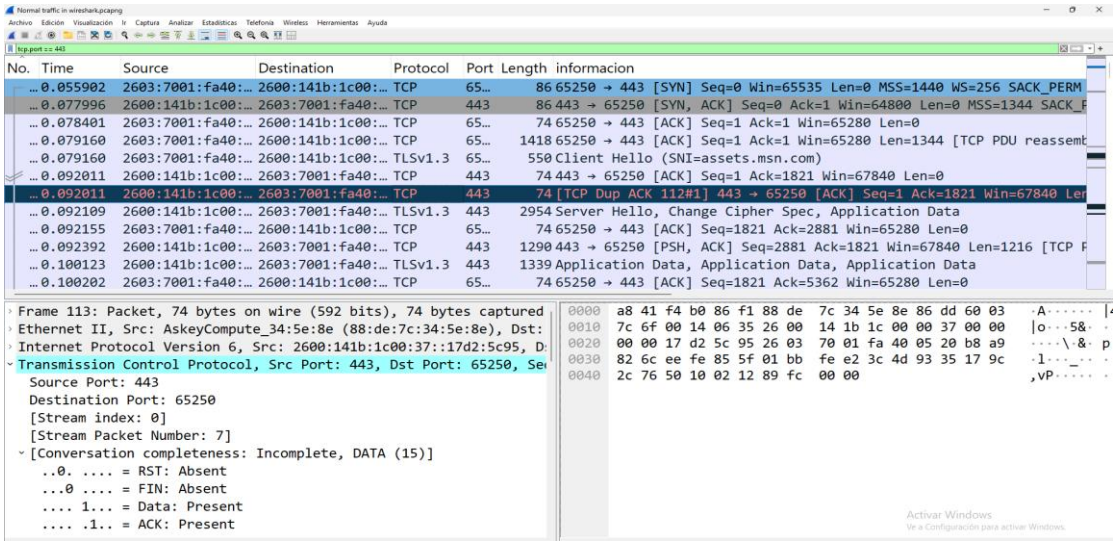
The DNS responses include A, AAAA, and HTTPS record types, as well as CNAME redirections to content delivery network (CDN) domains. This behavior is consistent with normal name resolution processes used by modern web applications and content providers. No abnormal query patterns or unusually long domain names were observed.

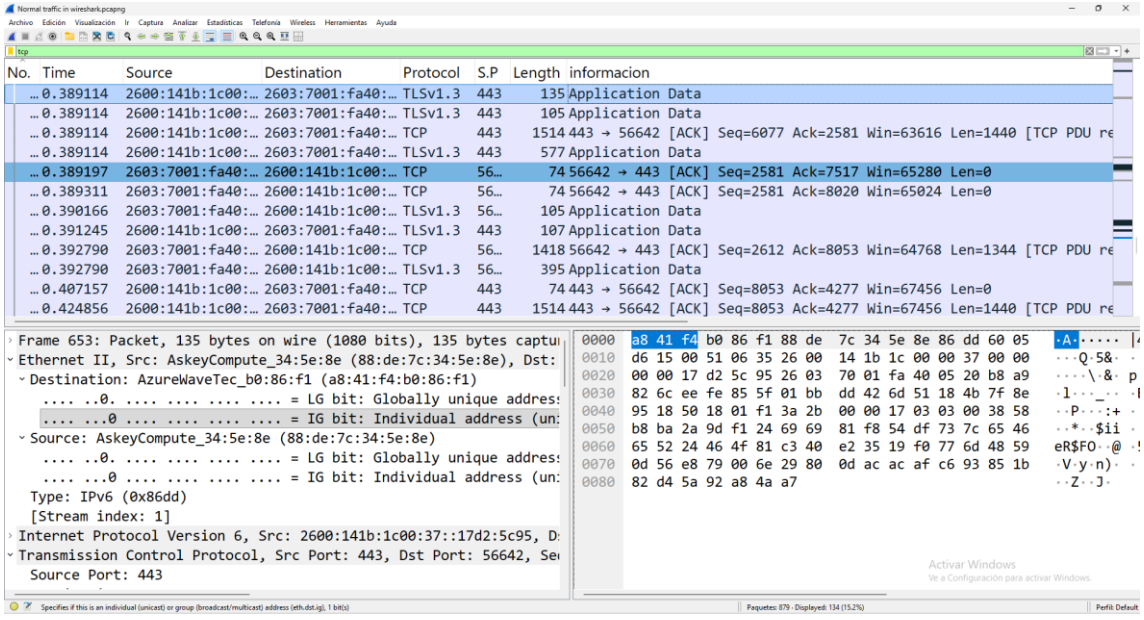
Encrypted HTTPS Communication Over TCP Port 443

Description:

The screenshot shows encrypted HTTPS traffic identified through TCP sessions over port 443. The capture includes a complete TCP connection setup followed by a TLSv1.3 handshake, with Client Hello and Server Hello messages successfully observed.

Later packets are labeled as TLS application data, which indicates encrypted payload transmission typical of secure web browsing. The presence of acknowledgment (ACK) packets and a stable packet flow confirm a legitimate and healthy encrypted client-server communication.





Conclusion

Phase 1 established the baseline of normal network traffic by analyzing DNS, TCP, and HTTPS activity generated by typical user behavior. The observed traffic demonstrated legitimate name resolution processes, encrypted communications, and stable TCP sessions, with no indicators of abnormal or suspicious behavior.

Establishing this baseline is essential in a SOC environment, as it provides a reliable reference point for identifying deviations, reducing false positives, and supporting accurate incident analysis.