

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 image shows a Wireshark capture of DNS traffic. The top pane displays a list of packets, with the selected packet (295) highlighted. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Source	Destination	Protocol	Port	Length	Information
2603:7001:fa40::...	2603:7001:fa40::...	DNS	64...	92	Standard query 0x3bd1 A www.bing.com
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	374	Standard query response 0x7b79 AAAA assets.msn.com CNAME assets-msn-com-world-a
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	295	Standard query response 0x8eaf HTTPS assets.msn.com CNAME assets-msn-com-world-a
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	266	Standard query response 0x9ad2 A assets.msn.com CNAME assets-msn-com-world-atm-
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	357	Standard query response 0x3bd1 A www.bing.com CNAME www-www.bing.com.trafficman
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	274	Standard query response 0xbc65 HTTPS www.bing.com CNAME www-www.bing.com.traffic
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	353	Standard query response 0xb76a AAAA www.bing.com CNAME www-www.bing.com.traffic
2603:7001:fa40::...	2603:7001:fa40::...	DNS	61...	107	Standard query 0xbd00 HTTPS img-s-msn-com.akamaized.net
2603:7001:fa40::...	2603:7001:fa40::...	DNS	52...	107	Standard query 0xb470 AAAA img-s-msn-com.akamaized.net
2603:7001:fa40::...	2603:7001:fa40::...	DNS	52...	107	Standard query 0xd255 A img-s-msn-com.akamaized.net
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	205	Standard query response 0xbd00 HTTPS img-s-msn-com.akamaized.net CNAME a1834.ds
2603:7001:fa40::...	2603:7001:fa40::...	DNS	53	280	Standard query response 0xb470 AAAA img-s-msn-com.akamaized.net CNAME a1834.dsc

Name: assets.msn.com
[Name Length: 14]
[Label Count: 3]
Type: HTTPS (65) (HTTPS Specific Service Endpoints)
Class: IN (0x0001)

Answers
assets.msn.com: type CNAME, class IN, cname assets-msn-com-world-atm-default.trafficmanager.net
Name: assets.msn.com
Type: CNAME (5) (Canonical NAME for an alias)
Class: IN (0x0001)
Time to live: 21033 (5 hours, 50 minutes, 33 seconds)
Data length: 53
CNAME: assets-msn-com-world-atm-default.trafficmanager.net

0050 73 03 6d 73 6e 03 63 6f 6d 00 00 41 00 01 c0 0c s·msn·co
0060 00 05 00 01 00 00 52 29 00 35 20 61 73 73 65 74R
0070 73 2d 6d 73 6e 2d 63 6f 6d 2d 77 6f 72 6c 64 2d s·msn·co
0080 61 74 6d 2d 64 65 66 61 75 6c 74 0e 74 72 61 66 atm·defa
0090 66 69 63 6d 61 6e 61 67 65 72 03 6e 65 74 00 c0 ficmanag
00a0 2c 00 05 00 01 00 00 00 16 00 1f 06 61 73 73 65 ,.....
00b0 74 73 03 6d 73 6e 07 63 6f 6d 2d 69 6f 6e 09 65 ts·msn·c
00c0 64 67 65 73 75 69 74 65 c0 5c c0 6d 00 05 00 01 dgesuite
00d0 00 00 00 bd 00 14 05 61 31 36 36 36 04 64 73 63a
00e0 72 06 61 6b 61 6d 61 69 c0 5c c0 9e 00 06 00 01 r·akamai
00f0 00 00 00 14 00 31 06 6e 30 64 73 63 72 c0 a3 0a1.n
0100 68 6f 73 74 6d 61 73 74 65 72 06 61 6b 61 6d 61 hostmast
0110 69 c0 17 69 81 32 a7 00 00 03 e8 00 00 03 e8 00 i·i·2·
0120 00 03 e8 00 00 07 08
Activar Windows
Ve a Configuración para activar Windows

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.

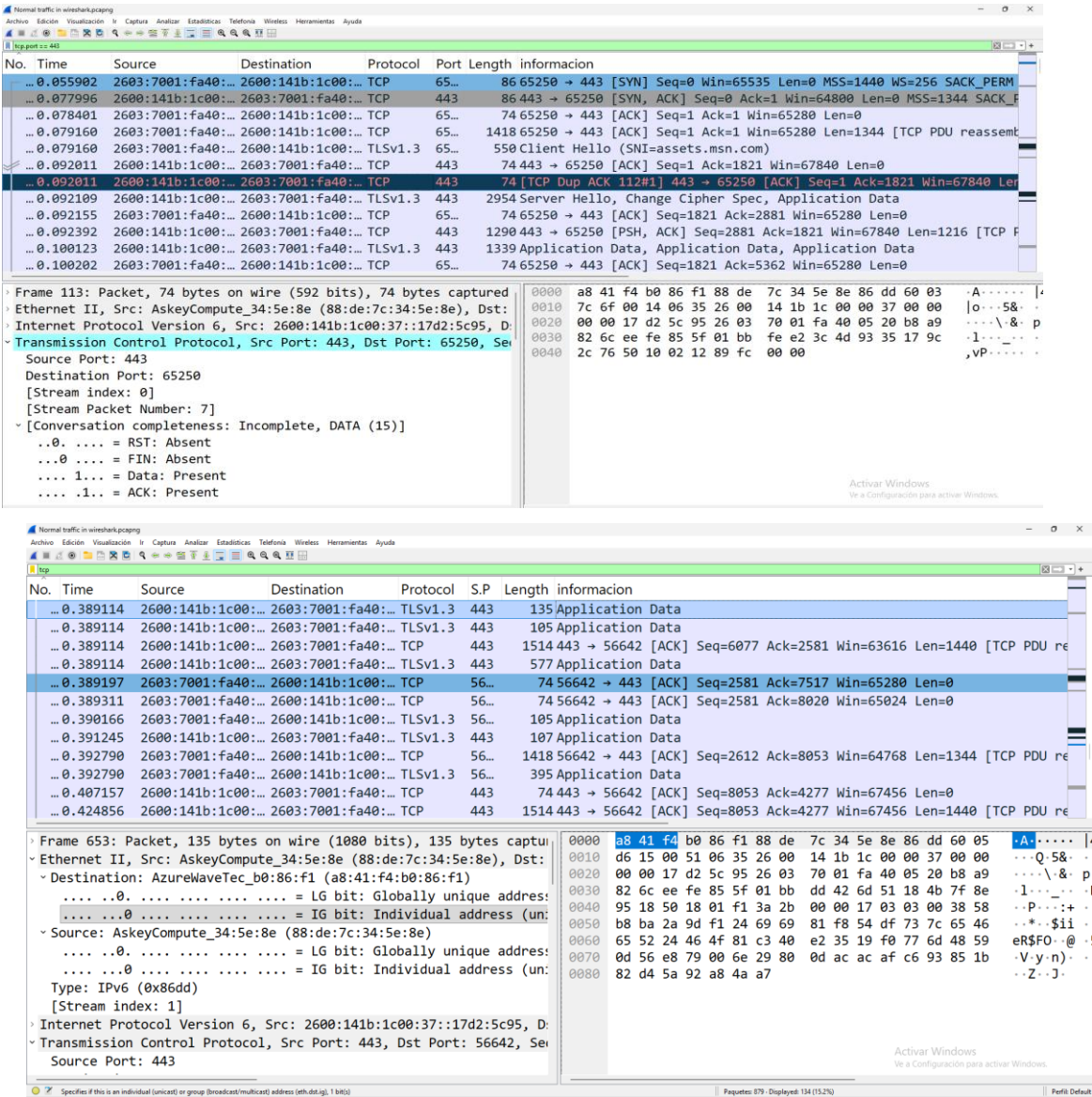
The DNS responses include A, AAAA, and HTTPS record types, as well as CNAME redirections to content delivery network (CDN) domains. This behavior is consistent with normal name resolution processes used by modern web applications and content providers. No abnormal query patterns or unusually long domain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