NETWORK TRAFFIC ANALYSIS OF DNS RESOLUTION AND TLS HANDSHAKE

Understanding Secure Web Communication using Wireshark

Self-Learning Cybersecurity Project
Alizha Syafahira | 2026

Project Overview

This project focuses on analyzing real network traffic to understand how web communication is established securely. The analysis covers the process starting from DNS resolution to encrypted HTTPS communication using the TLS protocol.

Objective

To analyze DNS resolution and TLS handshake in HTTPS communication

Scope

- DNS query and response
- TLS handshake process
- Encrypted application data
- TCP and UDP protocol usage

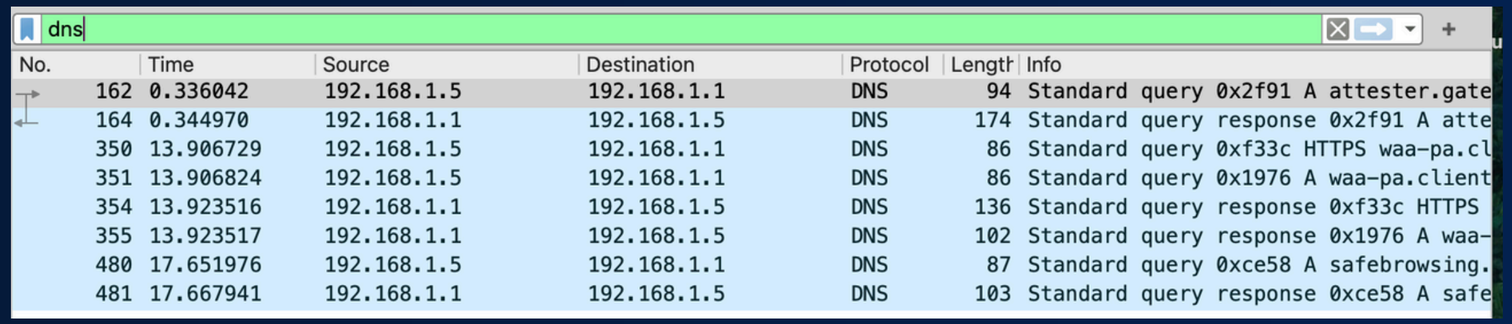
Tools Used

Wireshark

Environment

- Local Wi-Fi network
- Controlled and ethical traffic capture

DNS Resolution Process

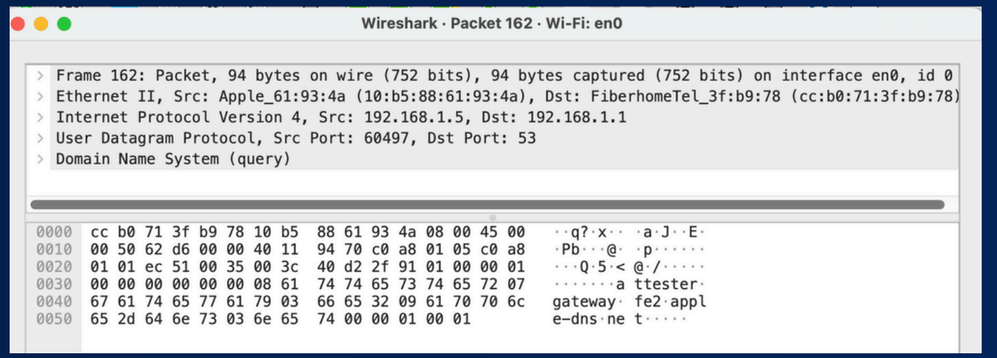


dns

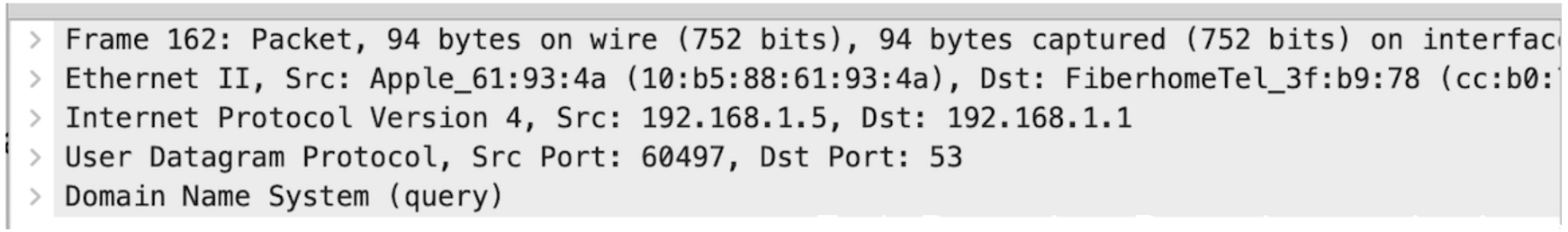
No.	Time	Source	Destination	Protocol	Length	Info
162	0.336042	192.168.1.5	192.168.1.1	DNS	94	Standard query 0x2f91 A attester.gate
164	0.344970	192.168.1.1	192.168.1.5	DNS	174	Standard query response 0x2f91 A atte
350	13.906729	192.168.1.5	192.168.1.1	DNS	86	Standard query 0xf33c HTTPS waa-pa.cl
351	13.906824	192.168.1.5	192.168.1.1	DNS	86	Standard query 0x1976 A waa-pa.client
354	13.923516	192.168.1.1	192.168.1.5	DNS	136	Standard query response 0xf33c HTTPS
355	13.923517	192.168.1.1	192.168.1.5	DNS	102	Standard query response 0x1976 A waa-
480	17.651976	192.168.1.5	192.168.1.1	DNS	87	Standard query 0xce58 A safebrowsing.
481	17.667941	192.168.1.1	192.168.1.5	DNS	103	Standard query response 0xce58 A safe

This slide shows the DNS resolution process captured during live network traffic. DNS communication occurs before secure HTTPS communication can be established.

1. DNS queries were captured using the dns display filter
2. The client sends a DNS request to resolve a domain name
3. The DNS server responds with the corresponding IP address



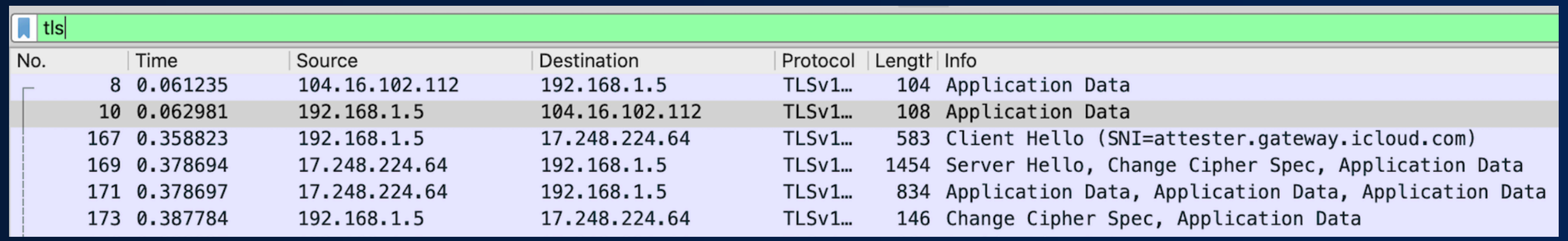
DNS Packet Details



The captured DNS packet was analyzed at the protocol level to identify how the client communicates with the DNS server. The analysis focuses on addressing information, transport protocol, and query content.

- Source and destination IP addresses were identified
- UDP protocol was used on port 53
- The queried domain name is visible in plain text

TLS Handshake Process



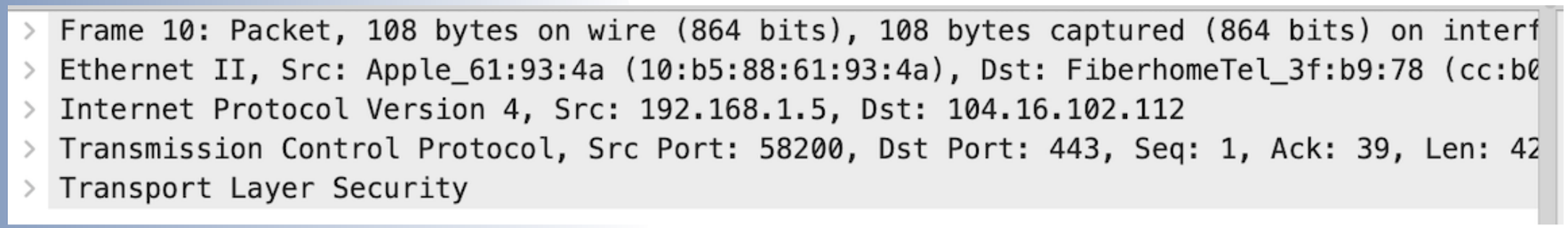
tls

No.	Time	Source	Destination	Protocol	Length	Info
8	0.061235	104.16.102.112	192.168.1.5	TLSv1…	104	Application Data
10	0.062981	192.168.1.5	104.16.102.112	TLSv1…	108	Application Data
167	0.358823	192.168.1.5	17.248.224.64	TLSv1…	583	Client Hello (SNI=attester.gateway.icloud.com)
169	0.378694	17.248.224.64	192.168.1.5	TLSv1…	1454	Server Hello, Change Cipher Spec, Application Data
171	0.378697	17.248.224.64	192.168.1.5	TLSv1…	834	Application Data, Application Data, Application Data
173	0.387784	192.168.1.5	17.248.224.64	TLSv1…	146	Change Cipher Spec, Application Data

1. Client Hello initiates secure communication
2. Server Hello responds with encryption parameters
3. Change Cipher Spec indicates encrypted communication begins

This slide shows the DNS resolution process captured during live network traffic. DNS communication occurs before secure HTTPS communication can be established.dbcajbe

Encrypted Application Data



After the TLS handshake process (Client Hello and Server Hello), the communication continues with Application Data packets. As shown in the capture, the payload appears unreadable, indicating that the data is encrypted using TLS. This demonstrates how HTTPS protects data confidentiality during transmission.

Key Findings

- DNS resolution occurs before secure communication begins
- TLS handshake establishes encryption before data exchange
- HTTPS traffic is encrypted and unreadable at packet level
- Secure communication protects user data from interception

Conclusion and Ethics

This project demonstrates how secure web communication is established through DNS resolution and TLS encryption. All traffic analyzed was generated from the author's own device in a controlled and ethical environment.

THANK YOU
FOR REVIEWING THIS PROJECT