# **Tittle: Network Traffic Analysis with Wireshark: Identifying TCP Handshakes and HTTP Requests**

## **Overview:**

As part of my cybersecurity training, I conducted hands-on network traffic analysis using **Wireshark** on a **Kali Linux** virtual machine.  
 The objective was to capture, analyze, and interpret **TCP 3-way handshakes** and **HTTP GET requests** to deepen my understanding of how fundamental internet communications operate.

## **Tools Used:**

* **Operating System:** Kali Linux (Virtual Machine)
* **Software:** Wireshark (Network Packet Analyzer)
* **Browser:** Firefox (to generate traffic)
* **Network Interface:** eth0 (Ethernet Network)

## **Process:**

### **1. Environment Setup:**

Launched Wireshark with root permissions on Kali Linux:  
sudo wireshark

* Selected the active network interface (**eth0**) to begin packet capture.

### **2. Traffic Generation:**

* Opened Firefox and navigated to:  
  + <http://example.com>
  + <http://neverssl.com>
* This generated both **HTTP** and **TCP** traffic for analysis.

### **3. Capturing TCP 3-Way Handshake:**

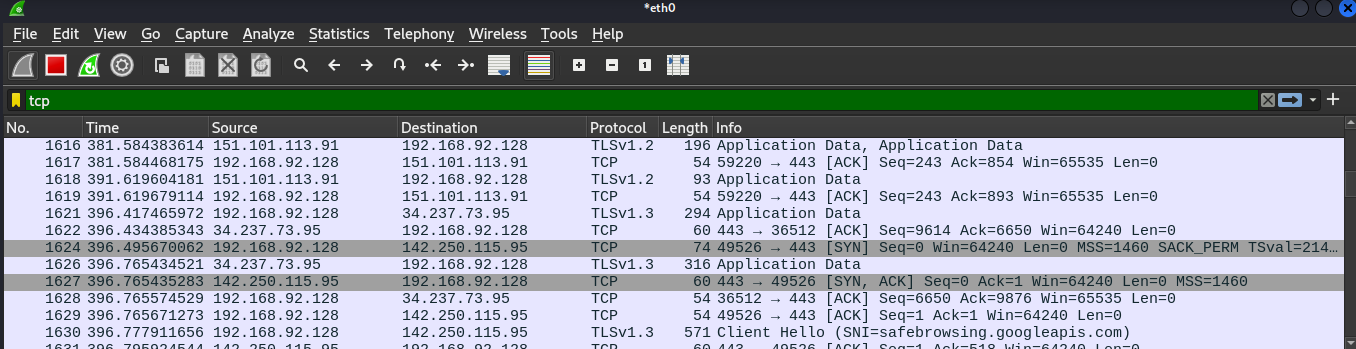
* Applied the filter tcp in Wireshark to narrow down TCP traffic.
* Identified the **three critical packets** between my IP and the destination server:  
  + **SYN** – Initiation of connection.
  + **SYN-ACK** – Acknowledgment and synchronization by the server.
  + **ACK** – Final acknowledgment by the client.
* **Packet Analysis Details:**
  + **Source Port:** Random high-numbered port (client)
  + **Destination Port:** 80 (HTTP) or 443 (HTTPS)
  + **Flags Observed:** SYN, SYN-ACK, ACK
  + Confirmed successful establishment of TCP connection.

### **4. Capturing HTTP GET Request:**

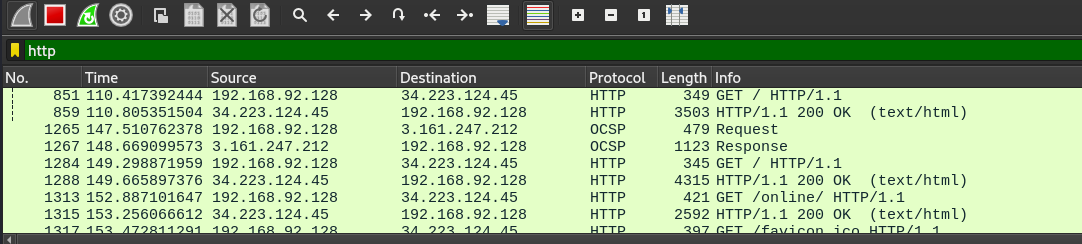
* Applied the filter http in Wireshark.
* Located an HTTP **GET** request sent from the browser to the server.
* **Key fields observed:**
  + **Host:** example.com / neverssl.com
  + **Request URI:** /
  + **User-Agent:** Mozilla/5.0 (Firefox on Linux)
* **Packet Analysis Details:**
  + The GET method requested the homepage of the site.
  + The request was sent over plain HTTP (unencrypted).

## **Screenshots:**

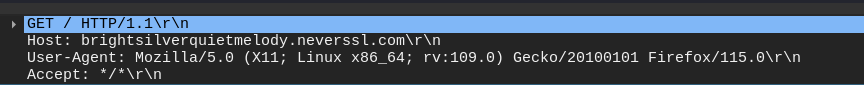
**TCP 3-way handshakes**

**

**HTTP GET requests**



**HOST NAME & User-Agent.**



## **Key Learnings:**

* Understood the detailed steps of how a TCP connection is initiated.
* Observed how web browsers request resources from servers via HTTP.
* Gained practical experience in using Wireshark to filter, capture, and analyze network communications.
* Recognized the importance of encryption (HTTPS) by observing how plain HTTP traffic can easily be inspected.

## **Next Steps:**

* Capture and analyze encrypted HTTPS traffic (understand SSL/TLS handshake basics).
* Perform deeper packet inspection to identify cookies, authentication tokens, and potential security vulnerabilities.

# **🚀 Skills Demonstrated:**

| **Skill** | **Description** |
| --- | --- |
| Network Traffic Capture | Used Wireshark to monitor live packets |
| Protocol Analysis | Interpreted TCP and HTTP traffic |
| Security Awareness | Identified unencrypted sensitive information |
| Linux Networking | Worked with Kali Linux network interfaces |