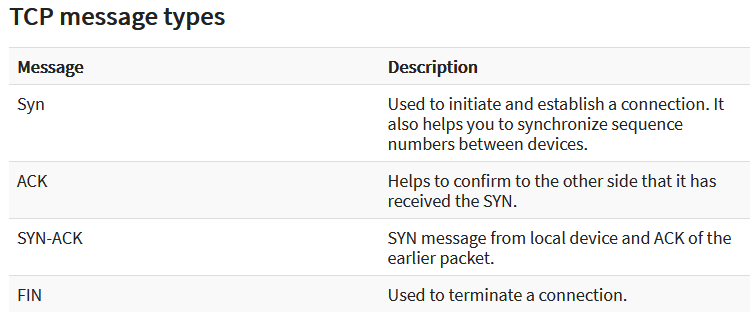
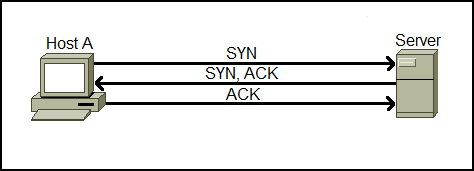
Lab - Capturing a 3-way TCP Handshake Using Wireshark

**Overview**

A Three-way handshake or a TCP 3-way handshake is a process that is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the actual communication process starts.





* Host A begins the connection by sending the TCP SYN packet to its host destination. The packets contain a random sequence number (For example, 4321) that indicates the beginning of the sequence numbers for data that the Host X should transmit.
* After that, the server will receive the packet, and it responds with its sequence number. The server’s response also includes the acknowledgment number, that is, Host A’s sequence number incremented with 1 (Here, it is 4322).
* Host A responds to the server by sending the acknowledgment number that is mostly the server’s sequence number that is incremented by 1.
* After the data transmission process is over, TCP automatically terminates the connection between two separate endpoints.

**Key Points**

Malicious network traffic begins the same way as legitimate traffic, using a TCP 3-way handshake. If a client or server has been taken over and is now part of a botnet, the traffic coming and going must still adhere to the rules of how devices communicate. The difference would be a large amount of network traffic the zombie machine would be generating as part of the botnet.

**Lab Requirements**

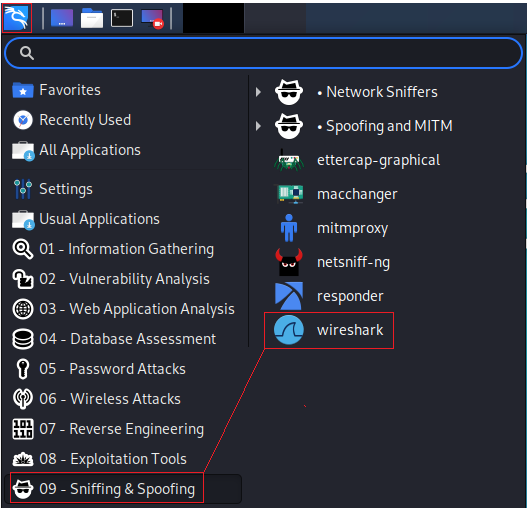
* One virtual install of Kali Linux
* Wireshark
* Internet connection

**Lab Scenario**

In this lab, we will look at a normal 3-way handshake using Wireshark. We will also learn how to filter just the information we wish to see.

**Begin the lab**

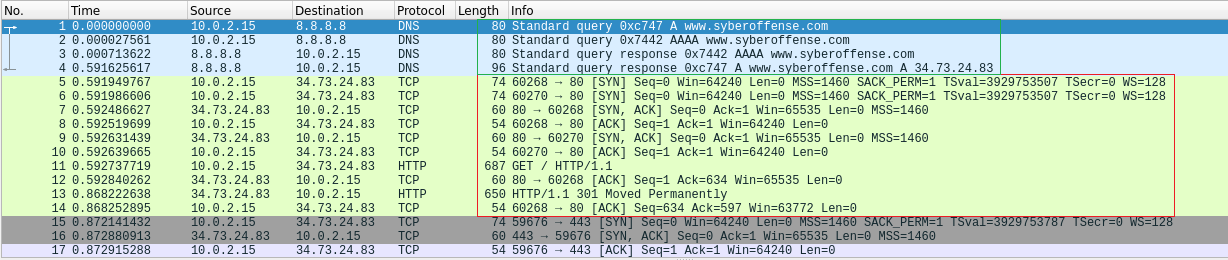
Using the Kali Quick Launch toolbar, under Sniffing and Spoofing, find and launch Wireshark.



For this lab, I will be using my wired adapter, but you are free to use a wireless or wired adapter. Ensure that your Kali machine has Internet access.

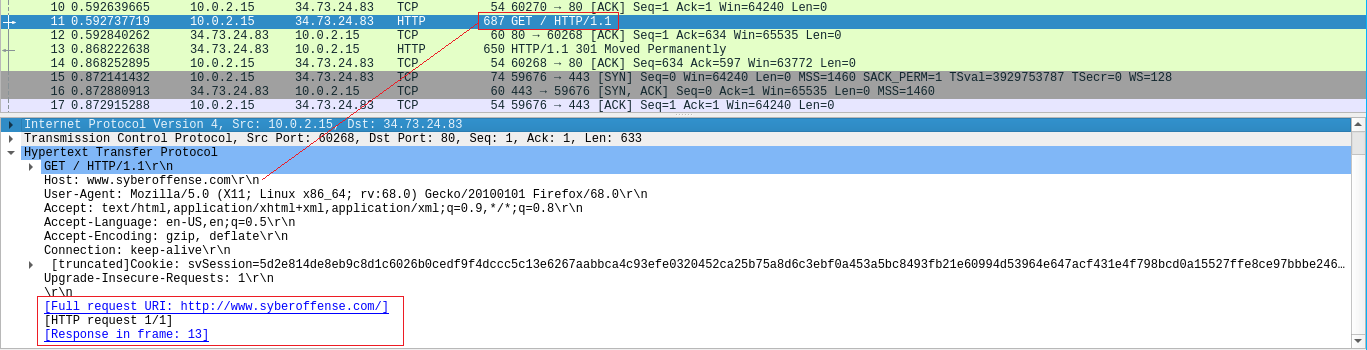
* Start a packet capture with Wireshark.
* Next, open a browser and navigate to [www.syberoffense.com](http://www.syberoffense.com)
* Once the website has loaded, stop the Wireshark capture.

We can now examine the Wireshark capture and see the TCP 3 Way Handshake as it happened.



The first three lines show that my website request for [www.sybersoffence.com](http://www.sybersoffence.com) was converted to an IP address or machine language (Line 5). On the same line, you can see the beginning of the 3-way handshake. The three-way is concluded by line 10, and on line 11, we see the GET / HTTP:1.1 request, which is a direct request for a web page from the source IP address.

If we examine the contents of the GET / HTTP:1.1 packet by double-clicking it, in the second windows pane, we can see what web page we were requesting.



**Summary –**

As a network administrator, pentester, or digital forensic investigator, it is important to discern malicious traffic from legitimate traffic. This begins with being able to look at and analyze a three-way handshake.