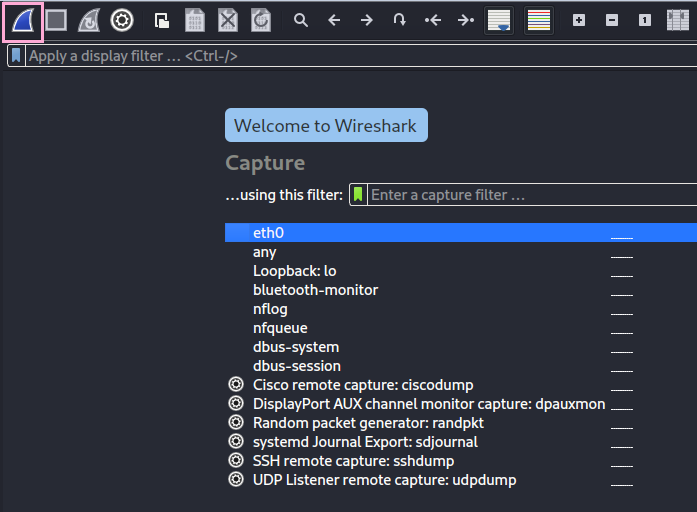
**🍓Wireshark Protocol Analyzer🍓**

Wireshark is a powerful Protocol Analyzer or a Sniffer, it can be used to analyze network traffic, identify the origin of attacks. Here, I’m going to show simple examples of network traffic analyzes.

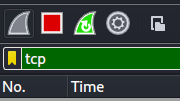
**TCP Three-way-handshake**

TCP is a connection-oriented protocol, which means it confirms if the connection is working before starting the transmission. To establish the connection, TCP uses Three-way-handshake.

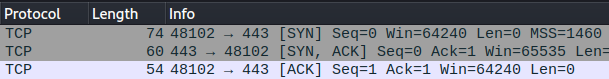
Start Wireshark and capture the traffic on your network interface:



Access any website, and then go back to Wireshark and filter for TCP:



You’ll be able to find the three-way-handshake:



The three-way-handshake consists of the three TCP Flags: [SYN] [SYN, ACK] [ACK].

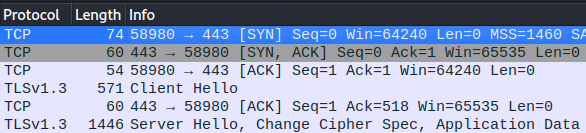
**SYN** for Synchronize, starts the connection, sent by the browser;

**SYN, ACK** for Synchronize and Acknowledgement, starts the connection and acknowledges the successful receipt of a package, answer sent by the web server;

**ACK** for Acknowledgement, answer given by the browser to confirm the receipt of a package.

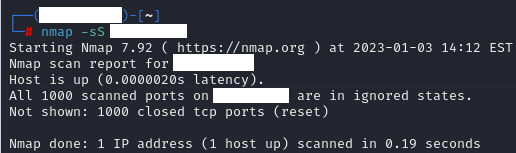
**TLS Handshake**

If the website being analyzed has SSL/TLS cryptography, you’ll be able to see the Client Hello and Server Hello packages, which indicates the TLS handshake connection being established.



**Detecting Attacks with Wireshark**

As an example, I started capturing with Wireshark and did an TCP SYN scan on my own machine using nmap:



* Observation: a TCP SYN scan is where nmap sends an SYN package and waits for the SYN ACK answer, without answering with ACK back. If the target doesn’t answer with SYN ACK, we can assume the port isn’t available or being filtered. That way, nmap discovers if the port is available without finalizing the connection.

Coming back to Wireshark, it’s possible to see the origin IP scanning my target machine, which means you can detect the IP from the machine performing network attacks/scans by analyzing the traffic:



By Clicking on the package, it’s possible to see other useful informations, like the source and destination ports:

