26/02/2019

Julio Alejandro Tejada Nava ITIW41

Profesor Neri Hernández Ricardo Ezequiel

ANáLISIS DE TRAFICO tcp

Seguridad de la Información

Contenido

[Introducción 2](#_Toc2003245)

[1.- Inicio de transmisión TCP SYN-ACK. 3](#_Toc2003246)

[2.- Intercambio SYN-ACK con el servidor web 5](#_Toc2003247)

[Conclusión 8](#_Toc2003248)

[Referencias 9](#_Toc2003249)

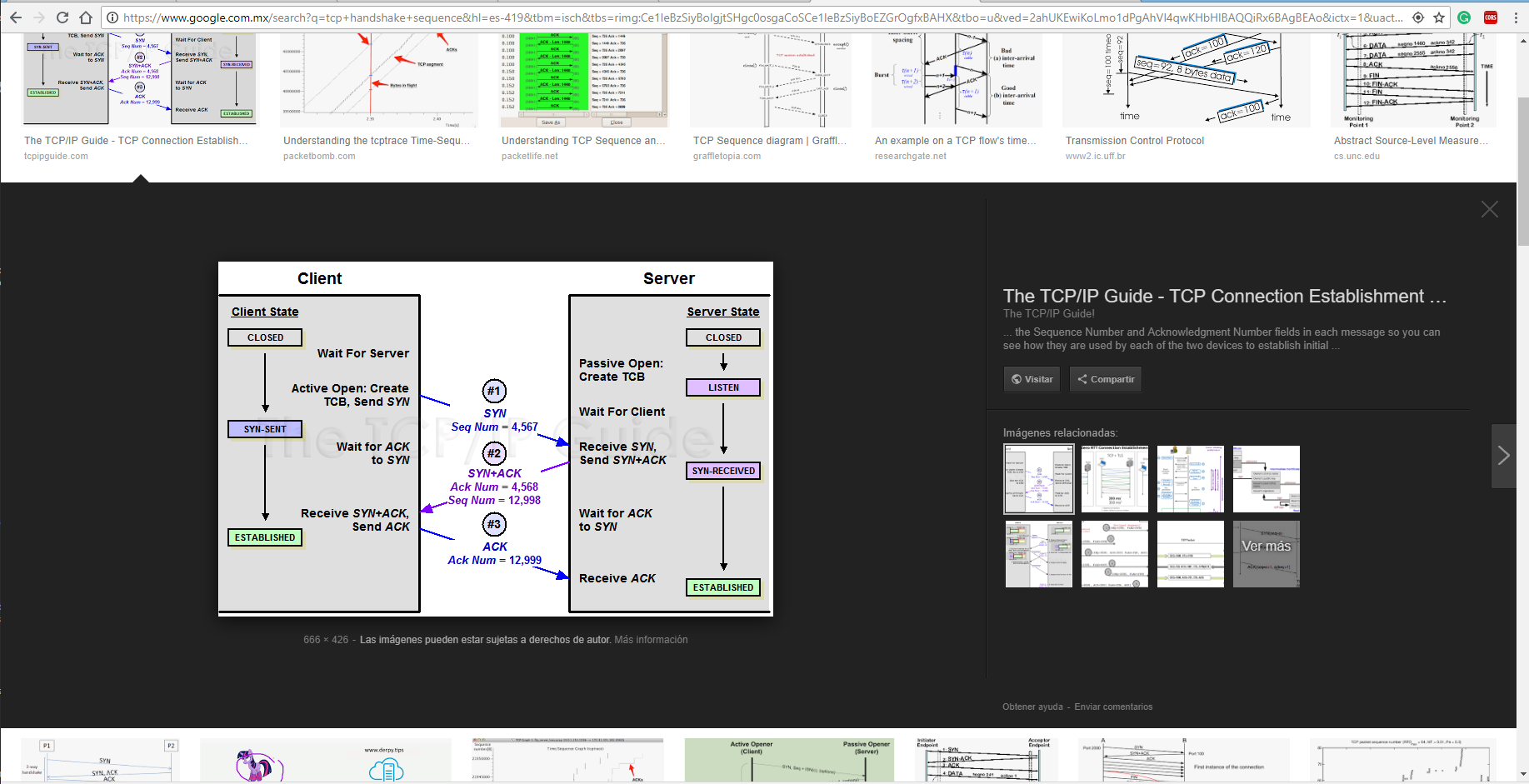
# Introducción

En este documento se realizó el análisis de transmisión de paquetes a un servidor por medio del protocolo TCP. El protocolo de enlace de tres vías TCP en el Protocolo de Control de Transmisión es la conexión TCP / IP a través de una red basada en el Protocolo de Internet. El mecanismo de protocolo de enlace TCP está diseñado para que dos computadoras que intentan comunicarse puedan negociar los parámetros de la conexión de socket de la red TCP antes de transmitir datos como SSH y solicitudes de navegador web HTTP.

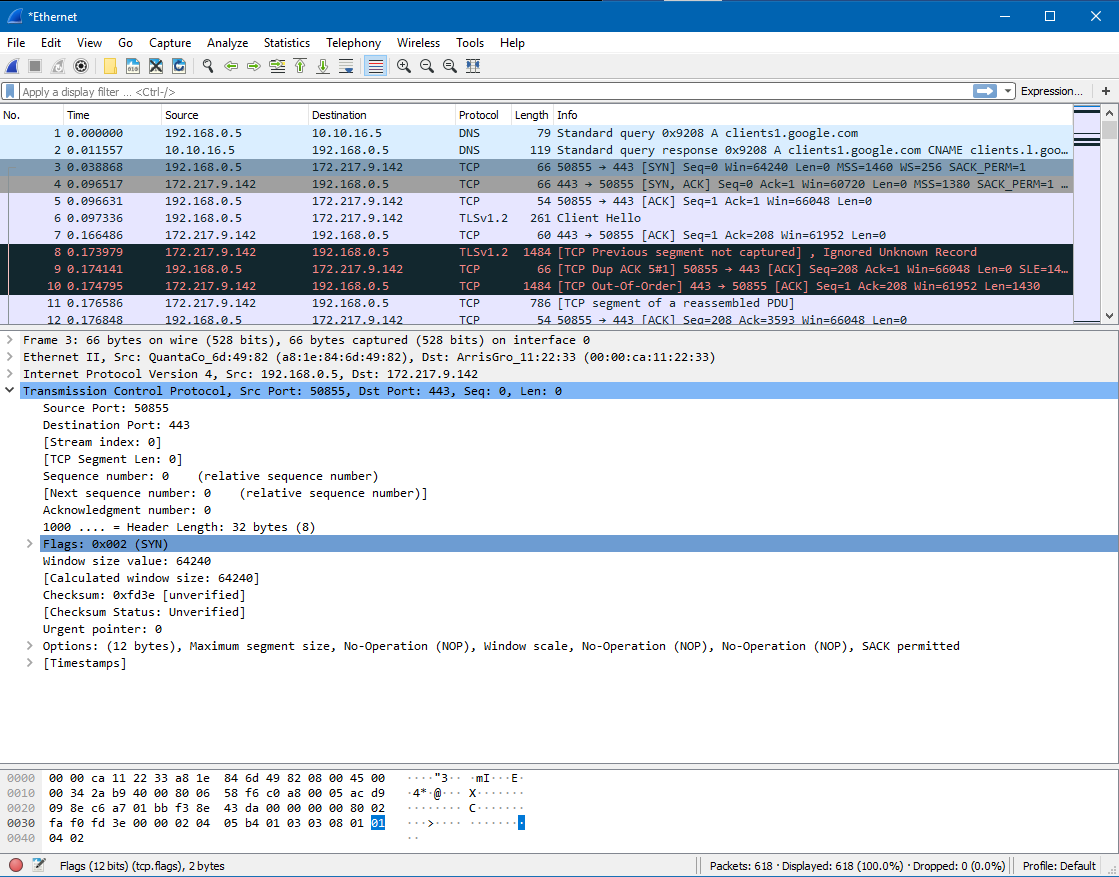
Las solicitudes se realizarán a un dominio propiedad de Google. La dirección IP pública será de un servidor establecido para el acceso a páginas web, en este caso Google Imágenes.

# 1.- Inicio de transmisión TCP SYN-ACK.

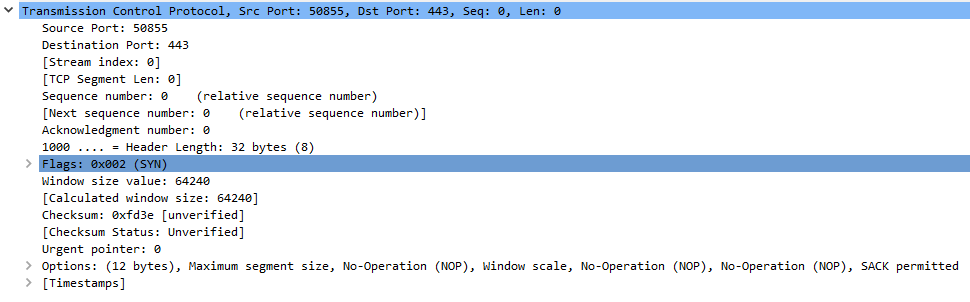
Recargando página web. Al recargar la página, se enviará una solicitud TCP al servidor Google. El análisis de paquetes se realizará través de la interfaz Ethernet.



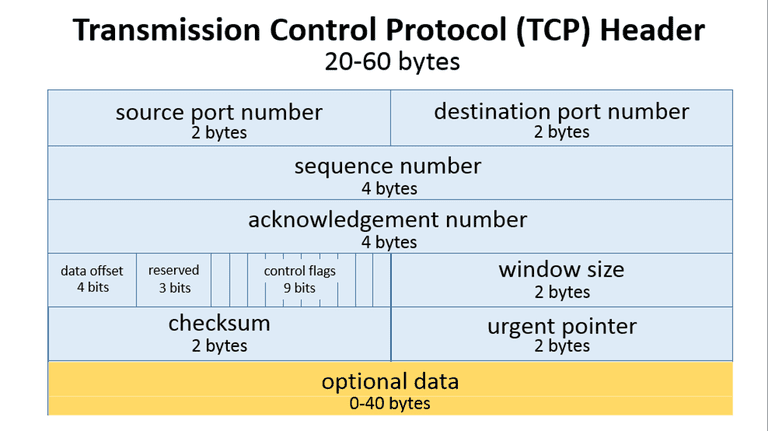
Analizando los paquetes en Wireshark se encontró el paquete con la bandera [SYN], es decir, la solicitud al servidor Google con la dirección IP [172.217.9.142]. La dirección fuente, en este caso la portadora del navegador web es: [192.168.0.5]. Se aplico un filtro para obtener solo los mensajes enviados y recibidos por parte de la dirección IP del servidor, en este caso la dirección IP [172.217.9.142].



El paquete [SYN] inicial contiene los siguientes datos de transmisión:

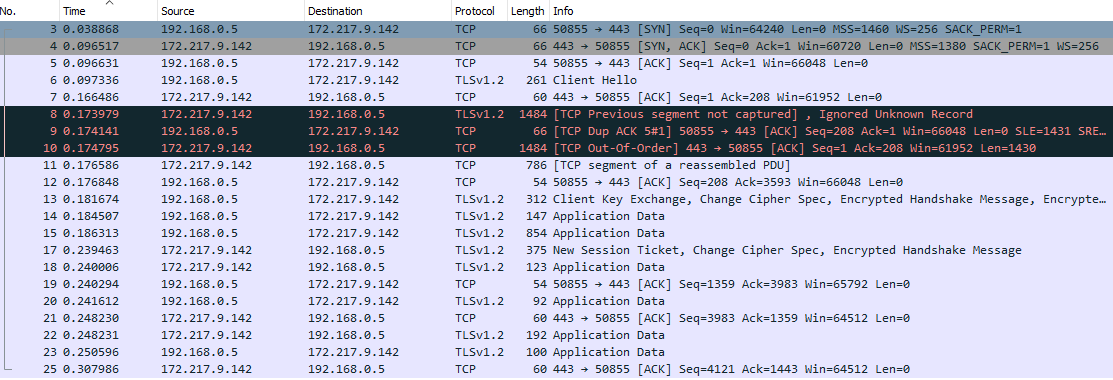


El cual contiene la siguiente estructura en el encabezado para paquetes TCP

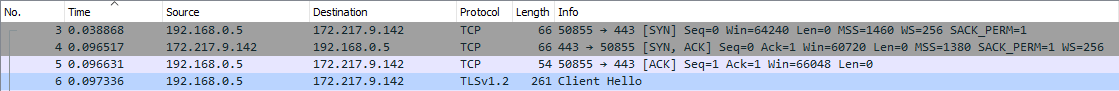


# 2.- Intercambio SYN-ACK con el servidor web

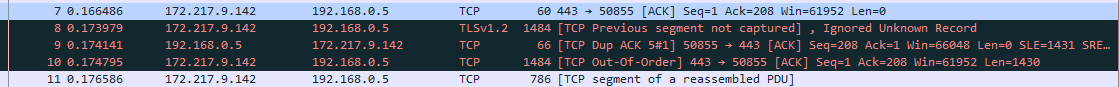
El intercambio con la dirección IP de destino [172.217.9.142] obtuvo los siguientes paquetes:



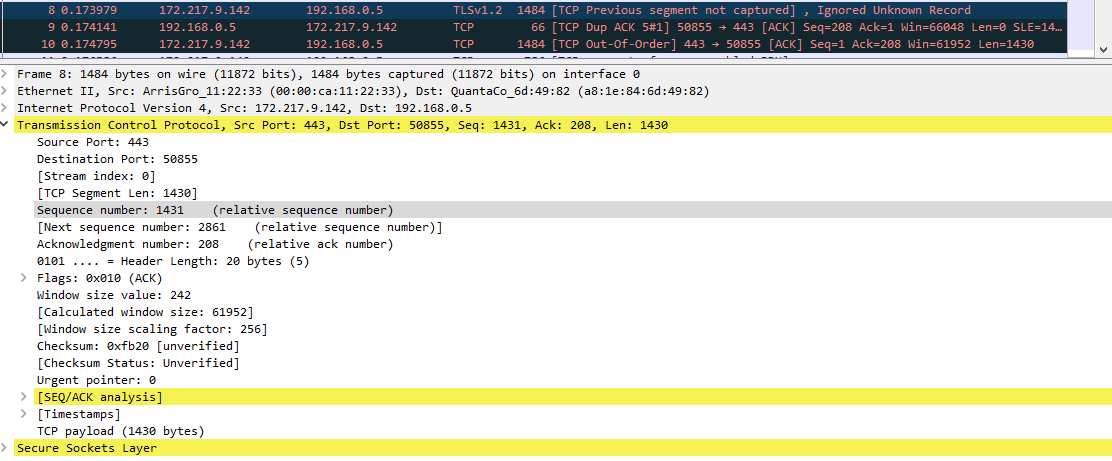
El primer intercambio de paquetes para establecer la conexión entre el cliente y el servidor se puede determinar en el intercambio de paquetes [SYN], [SYN, ACK], [ACK] y finalmente la respuesta [Client Hello].



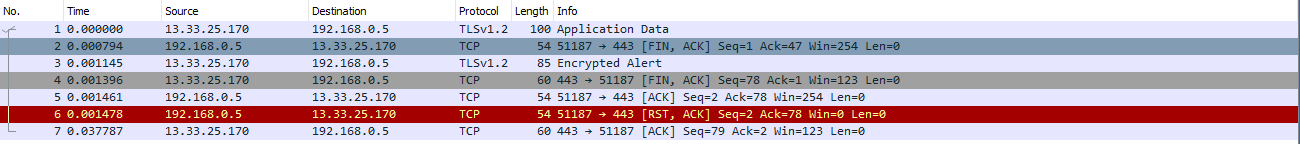
El primer envío de paquetes se dará después de llegado el mensaje [Client Hello]



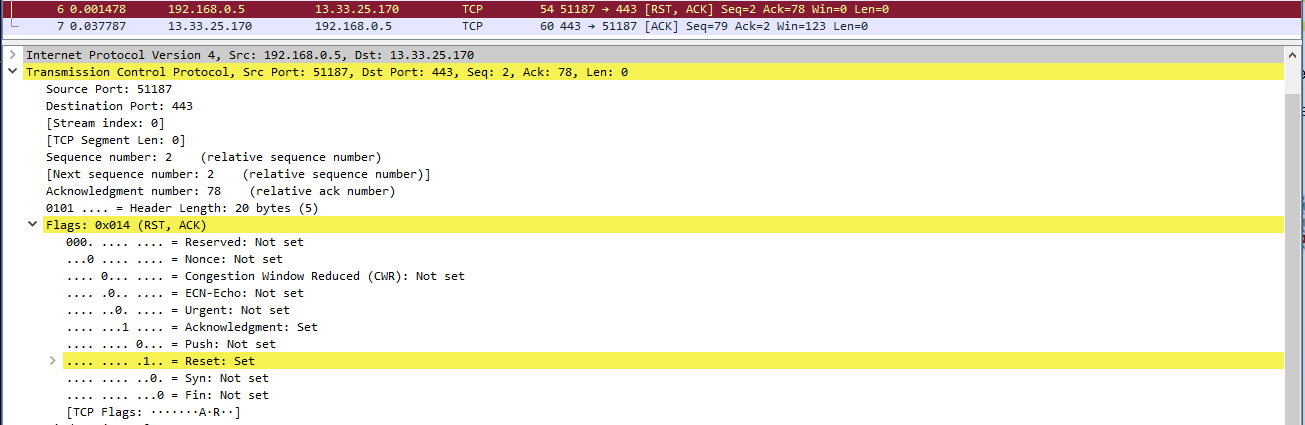
El primer paquete con la bandera [ACK] del servidor hacia el cliente estará avisando del inicio de transmisión de datagramas con un ancho mayor. Llegado el primer paquete del servidor, indica que tiene un ancho de 1430 bytes.



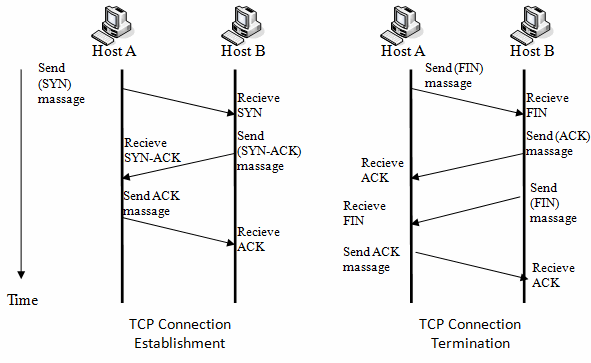
En este caso la conexión no había sido cerrada, por ende, no había paquetes con la bandera [FIN]. Se envió una nueva solicitud esta vez a la pagina de inicio de Google para obtener el paquete [FIN]. Se obtuvo el siguiente análisis de datos



Analizando un poco más de cerca el paquete enmarcado en rojo se puede obtener que tanto la bandera [ACK] como [FIN] están asignadas, con lo cual el servidor esta al tanto de que la conexión puede ser cerrada y el cliente esta enterado de la misma.



Estructura de handshake TCP



Los mensajes SYNchronize y ACKnowledge se indican mediante un bit SYN o un bit ACK dentro del encabezado TCP, y el mensaje SYN-ACK tiene los bits SYN y ACK activados (establecidos en 1) en el encabezado TCP.

TCP sabe si la conexión de socket TCP de la red se está abriendo, sincronizando, establecida mediante el uso de los mensajes SYNchronize y ACKnowledge al establecer una conexión de socket TCP de red.

Cuando finaliza la comunicación entre dos computadoras, se realiza otra comunicación de 3 vías para cortar la conexión de socket TCP. Esta configuración y eliminación de una conexión de socket TCP es parte de lo que califica a TCP de un protocolo confiable. TCP también reconoce que los datos se reciben con éxito y garantiza que los datos se vuelvan a agrupar en el orden correcto

# Conclusión

El protocolo TCP ha sido utilizado para acceder y comunicar datos del cliente con el servidor, los datos han sido solicitados y transmitidos satisfactoriamente. Gracias a este mecanismo es posible transmitir datos de forma segura y verificable de un lado a otro, a diferencia del protocolo UDP en donde estos paquetes viajan al cliente, y el servidor podría no estar verificando a su arribo.

Las imágenes presentadas han sido gracias al software para monitoreo de paquetes Wireshark, analizando la interfaz Ethernet a través de una solicitud al servidor web en el navegador Google Chrome.

# Referencias

Greer, C. (2017). *How TCP Works - The Handshake*. Obtenido de youtube.com: https://www.youtube.com/watch?v=HCHFX5O1IaQ

Inetdaemon. (2012). *TCP 3-WAY HANDSHAKE*. Obtenido de inetdaemon.com: https://www.inetdaemon.com/tutorials/internet/tcp/3-way\_handshake.shtml