Tecnológico de Estudios Superiores de Jocotitlan

Carrera: Ingeniería en Sistemas Computacionales

Materia: Administración de Redes

Docente: Ing. Marcial Jesús Martínez Blas

Alumno: Luis Antonio Sánchez Fabián

Grupo: IC-801

**Actividad. Análisis de trafico**

**Índice**

**Introducción…………………………………. Pag. (3)**

**Marco teórico………………………………… Pag. (3)**

**Desarrollo…………………………………….. Pag. (4)**

**Análisis de resultados………………………… Pag. (11)**

**Conclusiones………………………………….. Pag. (12)**

**Referencias…………………………………… Pag. (12)**

**Introducción.**

El análisis de tráfico se llama así por el proceso de inferir información a partir de las características del tráfico de comunicación sin analizar la información que se intercambian lo comunicantes. Para obtener información podemos basarnos en el origen y el destino de las comunicaciones, su tamaño, se frecuencia, la temporización, patrones de comunicación, etc.

El análisis de tráfico está muy relacionado con el análisis de paquetes y se suelen usar de forma conjunta. En el análisis de paquetes se estudia la información contenida en los paquetes que circulan en la red y a partir de eso se trata de inferir información.

En el contexto de las redes de comunicaciones, el análisis de tráfico infiere información a partir de las características observables de los datos que circulan por la red. Por ejemplo, puede ser interesante el tamaño de los paquetes o la temporización de los mensajes. Aunque este tipo de técnicas suelen ser utilizadas por atacantes para deducir tamaños de claves durante sesiones interactivas o para deducir el origen y destino de una comunicación y también es utilizada por administradores de redes para descubrir actividades potencialmente maliciosas.

Por tanto, la [seguridad informática](https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica) se ocupa del estudio de las técnicas de análisis de tráfico y de contramedidas para protegernos de dicho tipo de técnicas. ​La elección de la característica del tráfico que es usada en el análisis de tráfico depende fuertemente del tipo de información que queremos inferir y de los protocolos subyacentes involucrados. Por ejemplo:

* Para detectar una comunicación de IP nos podemos basar en las temporizaciones de los mensajes. En efecto los protocolos de voz sobre IP envían paquetes a intervalos fijos de tiempo para asegurarse una calidad de llamada.
* ​Para deducir que información está accediéndose vía [SSL](https://es.wikipedia.org/wiki/Transport_Layer_Security) podemos usar el tamaño de los paquetes. Esto es debido a que el tamaño de los paquetes SSL frecuentemente es similar a el tamaño de los contenidos en texto plano.

**Marco teórico.**

El software de análisis de trafico que usaremos para esta práctica será Wireshark, pero, ¿Por qué utilizar Wireshark?

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark “entiende” la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico.

De forma similar a Tcpdump, Wireshark incluye una versión en línea de comandos, denominada Tshark, aunque el presente documento se centrará únicamente en su versión gráfica. Es importante indicar también que las funcionalidades utilizadas en el presente informe solo representan una pequeña parte de todo el potencial que puede ofrecernos Wireshark, y cuyo objetivo principal es servir de guía orientativa para cualquier administrador que necesite detectar, analizar o solucionar anomalías de red.

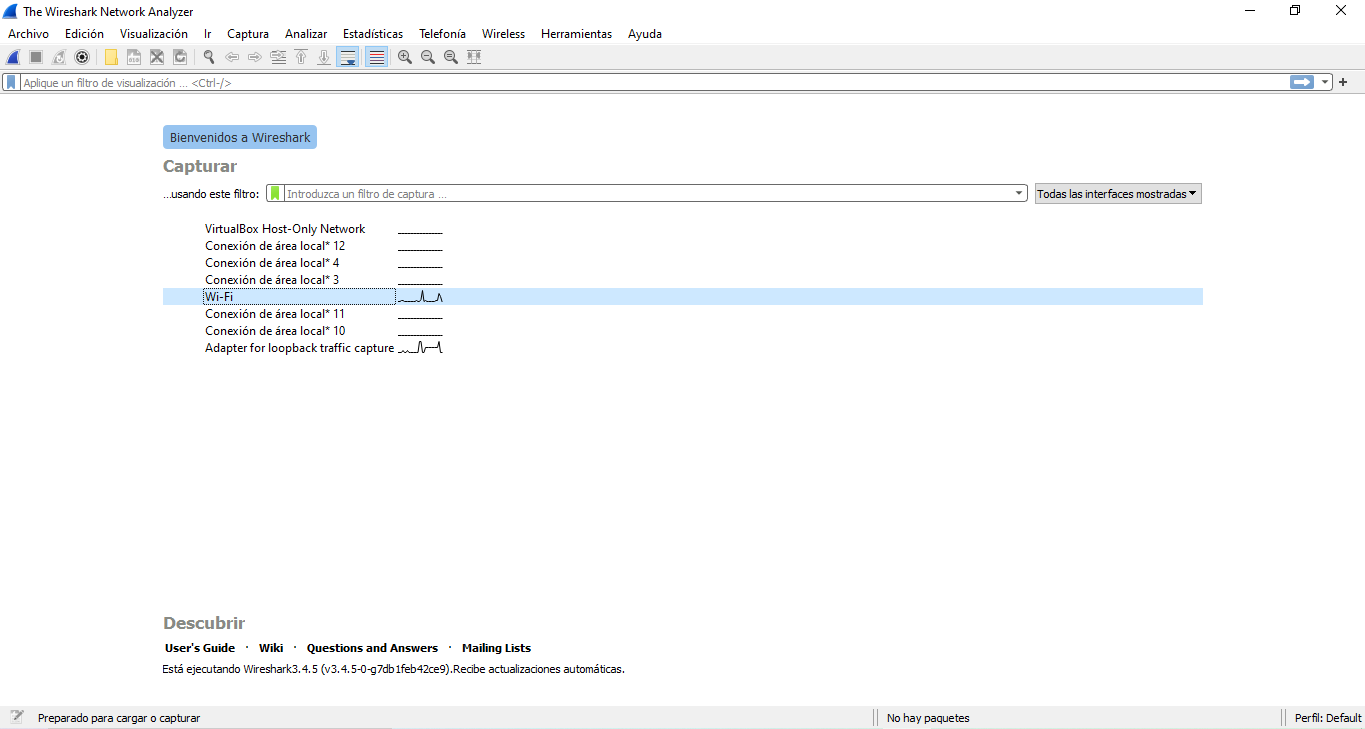
De esta manera usando Wireshark se utilizará para analizar el tráfico de red de nuestro hogar y detectar los paquetes y protocolos que se manejan, además de hacer pruebas del funcionamiento de este software para detectar e tráfico de red.

**Desarrollo. (Implementación del análisis de tráfico)**

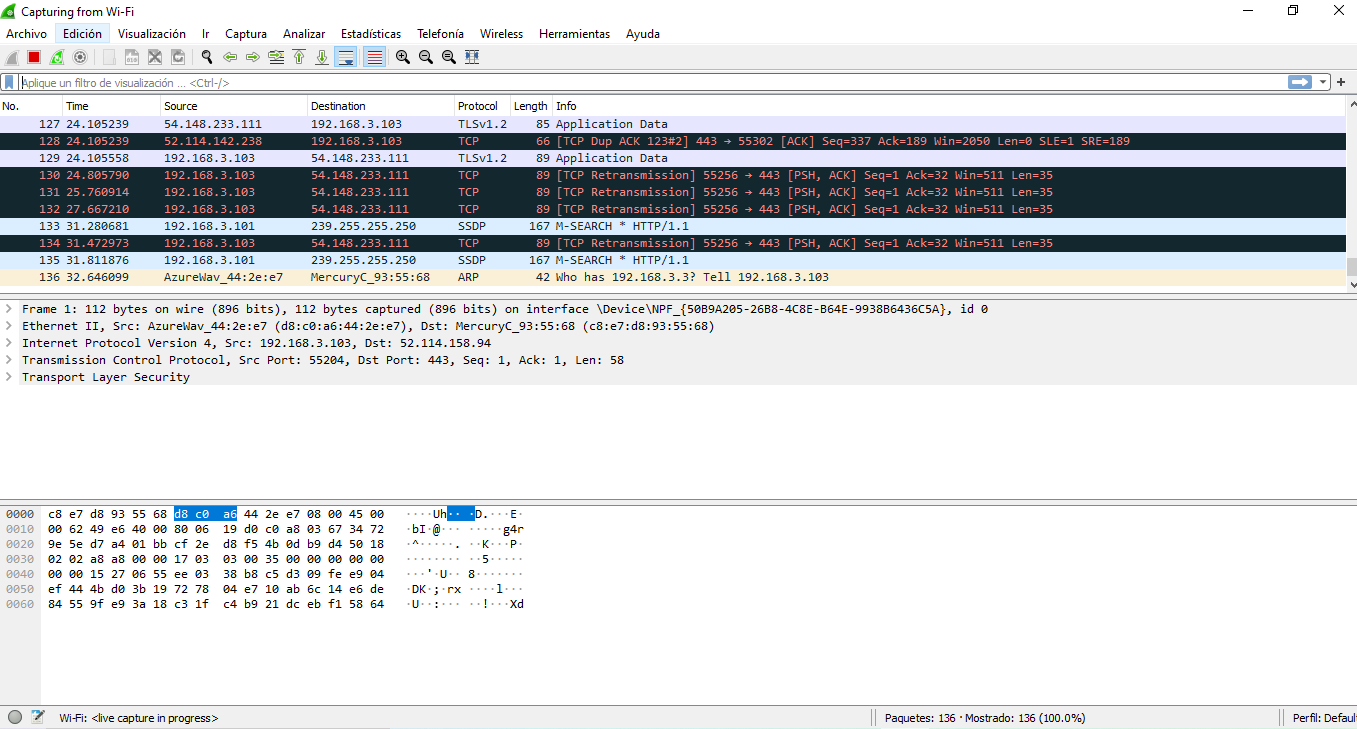
**Texto

Descripción generada automáticamente**

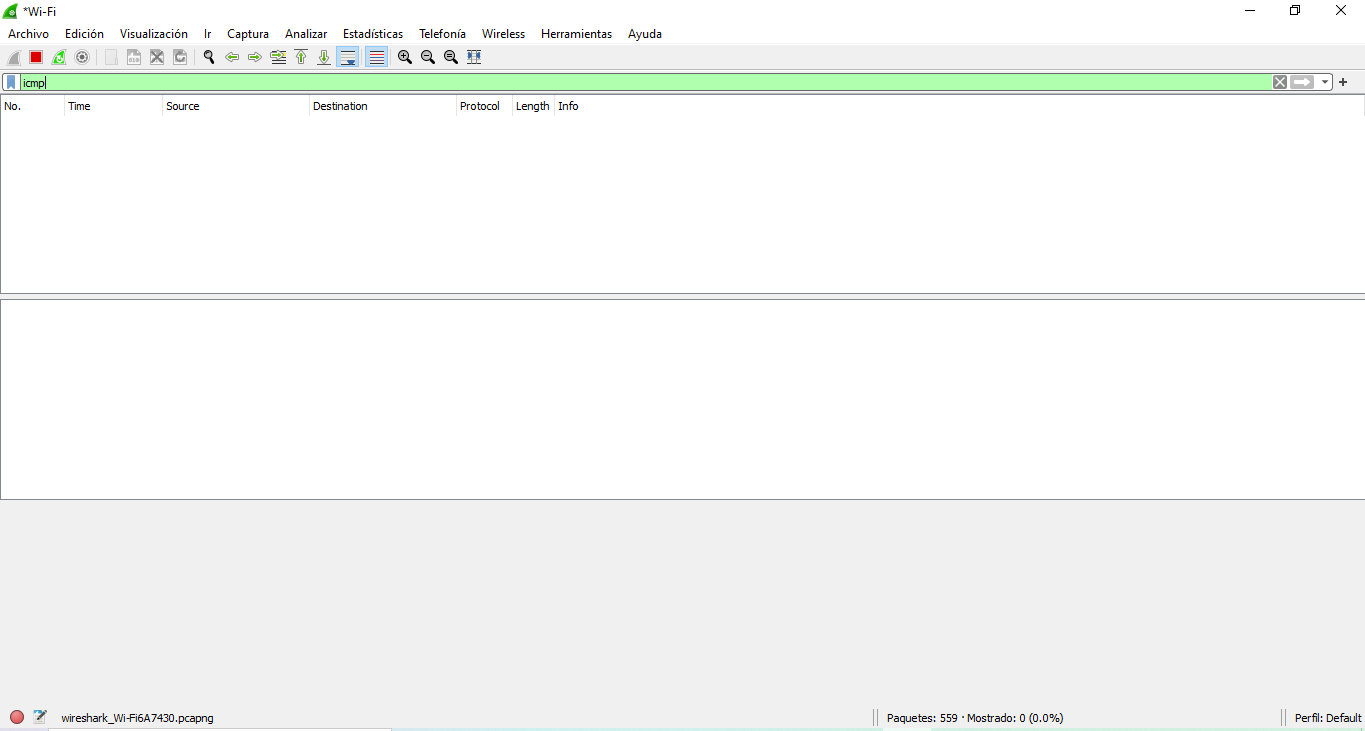
*Fig. 1 se realiza una solicitud para comprobar la dirección IP y la dirección MAC (dirección física) del equipo en que se realizara el análisis de trafico*

****

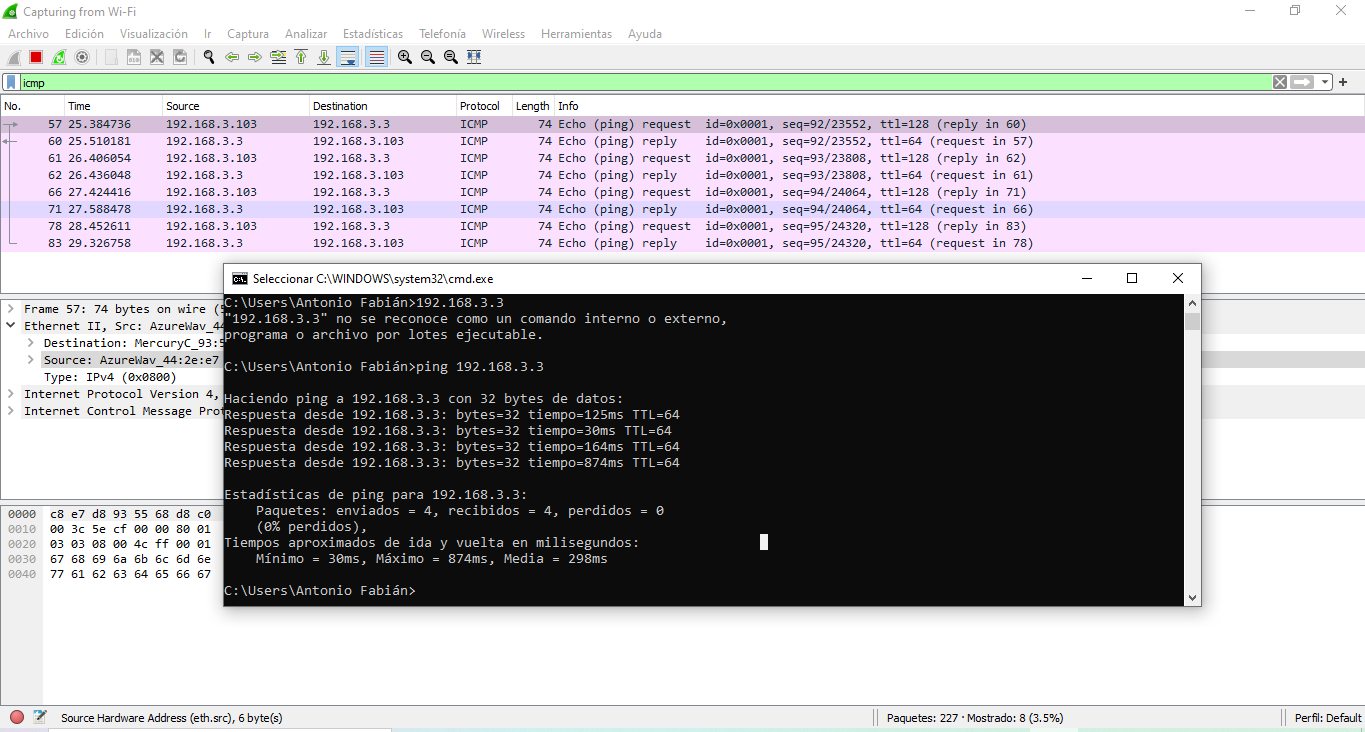
*Fig. 2 al abrir Wireshark muestra una lista de las interfaces o red para comenzar a capturar el tráfico, en este caso se analizará el de Wi-Fi y muestra a su vez que esta recibiendo trafico*

****

*Fig. 3 al dar clic a la interfaz para capturar datos empieza a desplegar los paquetes que se están capturando y mostrando información como la IP de origen y destino, el protocolo, etc.*

****

*Fig. 4 hacemos un filtro para solamente ver los paquetes ICMP que se van a capturar, aun así se siguen capturando los demás paquetes como los mostrados en la imagen anterior*

****

*Fig. 5 se realiza un ping con miembro del equipo desde la línea de comandos y como se ve Wireshark captura los paquetes ICMP del pingeo*

*Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente*

*Fig. 6 Una vez terminado la solicitud del ping con el miembro del equipo, observamos que la información que muestra en la parte media y baja de la interfaz de Wireshark corresponde a la dirección MAC de origen y destino que se realizo la solicitud.*

**Texto

Descripción generada automáticamente**

*Fig. 7 hacemos una solicitud con* ***arp*** *para mostrar que en efecto la dirección MAC (dirección física) del miembro del equipo la muestra tal cual en la interfaz de Wireshark*

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

*Fig. 8 ahora procedemos a analizar datos ICMP remotos, ya no desde el propio equipo y cerramos el análisis anterior que hicimos*

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

*Fig. 9 realizamos un ping a la dirección URL de Yahoo!, como muestra la imagen muestra los paquetes ICMP capturados y en la terminal de comandos transforma la dirección URL a la dirección IP que está asociada*

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

*Fig. 9 realizamos otro ping ahora a la dirección URL de Google, como muestra la imagen muestra los paquetes ICMP capturados y en la terminal de comandos transforma la dirección URL a la dirección IP que está asociada*

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

*Fig. 9 hacemos un último ping a la dirección URL de Cisco, como muestra la imagen muestra los paquetes ICMP capturados y en la terminal de comandos transforma la dirección URL a la dirección IP que está asociada*

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

*Fig. 10 se realiza el análisis que muestra la IP del sitio Yahoo a la que se hizo el ping, y también observamos la dirección MAC de destino del sitio*

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

*Fig. 11 se realiza el análisis que muestra la IP del sitio de Google a la que se hizo el ping, y también observamos la dirección MAC de destino del sitio*

**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**

*Fig. 10 se realiza el análisis que muestra la IP del sitio de Cisco a la que se hizo el ping, y también observamos la dirección MAC de destino del sitio*

**Análisis de resultados.**

Como vemos en la práctica, se pudo observar y realizar el análisis y monitoreo del trafico de red que ocurre dentro de nuestro hogar. En especifico nos enfocamos a analizar y capturar los paquetes ICMP, siendo que este es el protocolo que se encarga de manejar los mensajes que se envían a través de Internet, e hicimos pruebas primeramente con un equipo miembro del equipo y observamos que los paquetes ICMP se transmitían entre el equipo miembro la dirección IP asignada del equipo físico, mostrándonos el origen y destino, también el protocolo que en este caso ICMP se estaba ocupando y de la misma manera la dirección MAC (dirección física) de los equipos. De manera similar también observamos estos paquetes a sitios remotos con un ping desde la terminal de comandos, observando también la misma información que en la primera parte.

Esto nos ayuda a identificar la manera en que se manejan estos paquetes, de donde salen y a donde llegan y en un futuro caso también analizar de mejor manera estos paquetes para evitar posibles intrusiones a nuestro sistema y que nuestra información personal se vea comprometida.

**Conclusiones.**

Bueno de esta manera como observamos en la práctica, utilizando Wireshark podemos hacer uso de varias funcionalidades para identificar y analizar los paquetes que se manejan en nuestra red, ver de donde proviene la información de un sitio a la cual se lo solicitamos o del uso frecuente que le damos a una aplicación conectada a Internet, pero también lo podemos usar para detectar fallas en nuestra red que puedan causar la lentitud de esta misma que pueda ser causado por algún defecto en la red o de malas configuraciones hechas por otras persona. Además, también es una gran herramienta que nos puede ayudar a monitorear o prevenir de ataques internos o externos que puede suceder de diversas formas.

**Referencias.**

* https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\_inf\_seguridad\_analisis\_trafico\_wireshark.pdf