Instituto Politécnico Nacional

ESCOM

Investigación de Wireshark

Redes

Ortiz Meraz Isaac Baruch

2014081135

06/06/20

06/06/20

Wireshark

Es una herramienta de código abierto que se utiliza para el analisis de paquetes, ya sea paquetes que manda la computadora para poder comunicarse o paquetes que llegan al momento de conectarse con la internet.

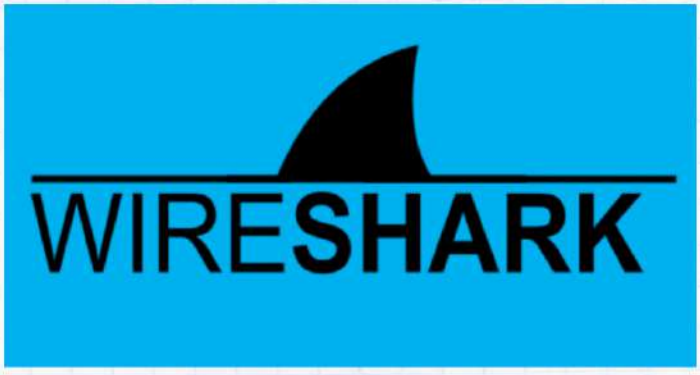
Originalmente se le conocia como Ethereal, en el 2006 creado originalmente por Gerald Combs.

Tiene una manera muy grafica de mostrar los resultados que el usuario este pidiendo, dependiendo de que herramientas este aplicando de la amplia cantidad de herramientas que pose Wireshark. Con el tiempo esta herramienta se a mantenido como el analizador de paquetes mas confiable en nuestra epoca.

Funciones Esenciales

- Capturar paquetes en directo
- Importar paquetes en archivos de texto
- Analisis de paquetes y información de protocolos
- Salvar paquetes capturados
- Desplegar paquetes
- Filtrar paquetes
- Buscar paquetes
- Marcar paquetes
- Generación de estadisticas

*La mayoria de usuarios lo utilizan para detectar problemas en sus conexiones de red y sus sistemas que mantengan comunicación con internet.

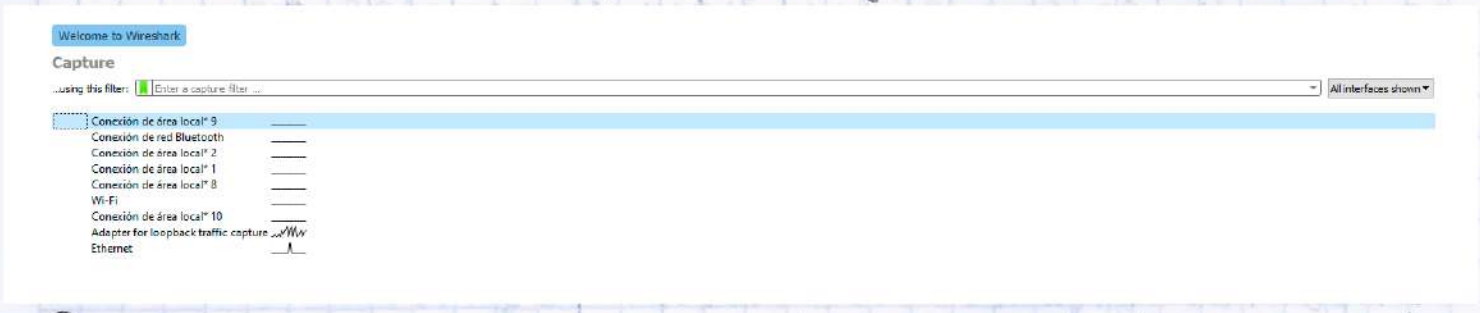


Capturar paquetes

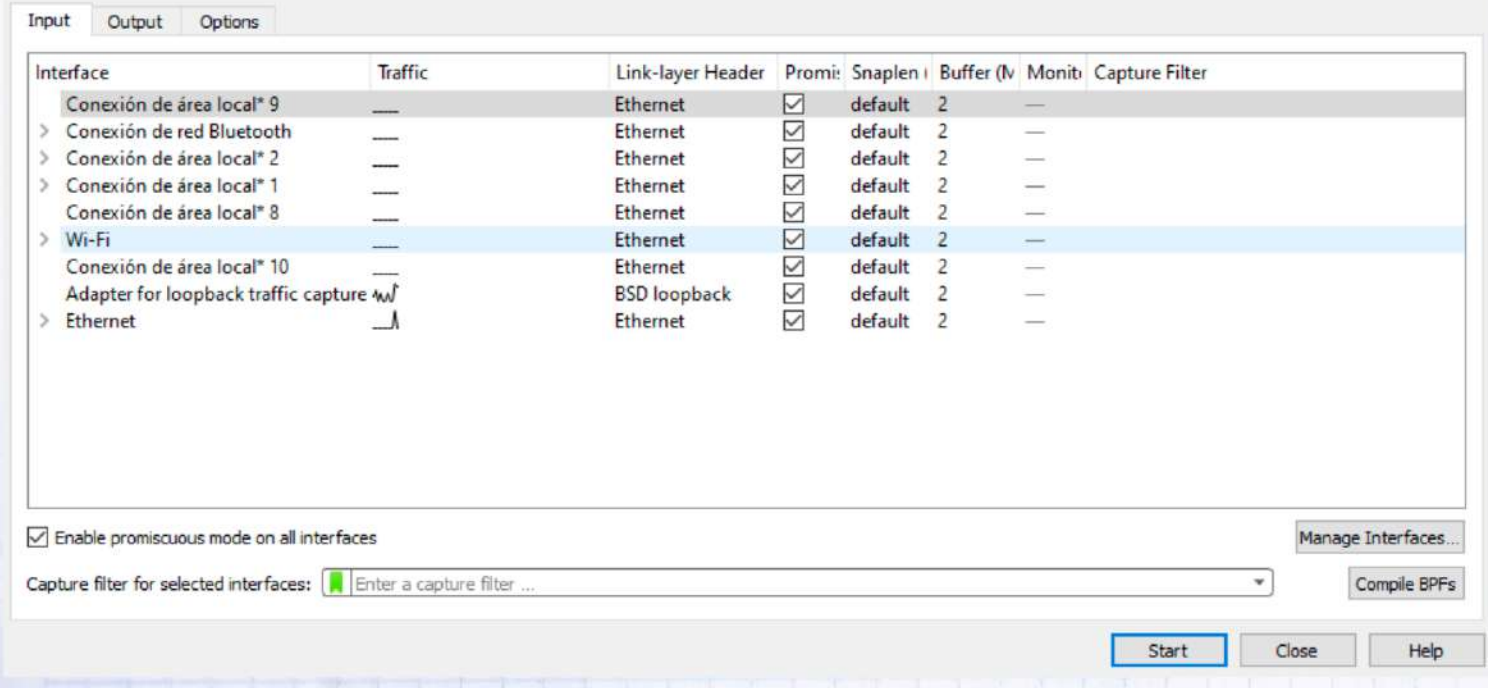
Para empezar a analizar paquetes se necesita enfocar el uso que le daremos a estos analisis, pero primero se necesita hacer unas cosas primero:

* Asegurarse que el usuario tenga permisos de administrador
* Escojer una interface de network
* Capturar de la locación correcta

Ya teniendo esto, como anteriores se abre la aplicación y se nuestra la siguiente pantalla



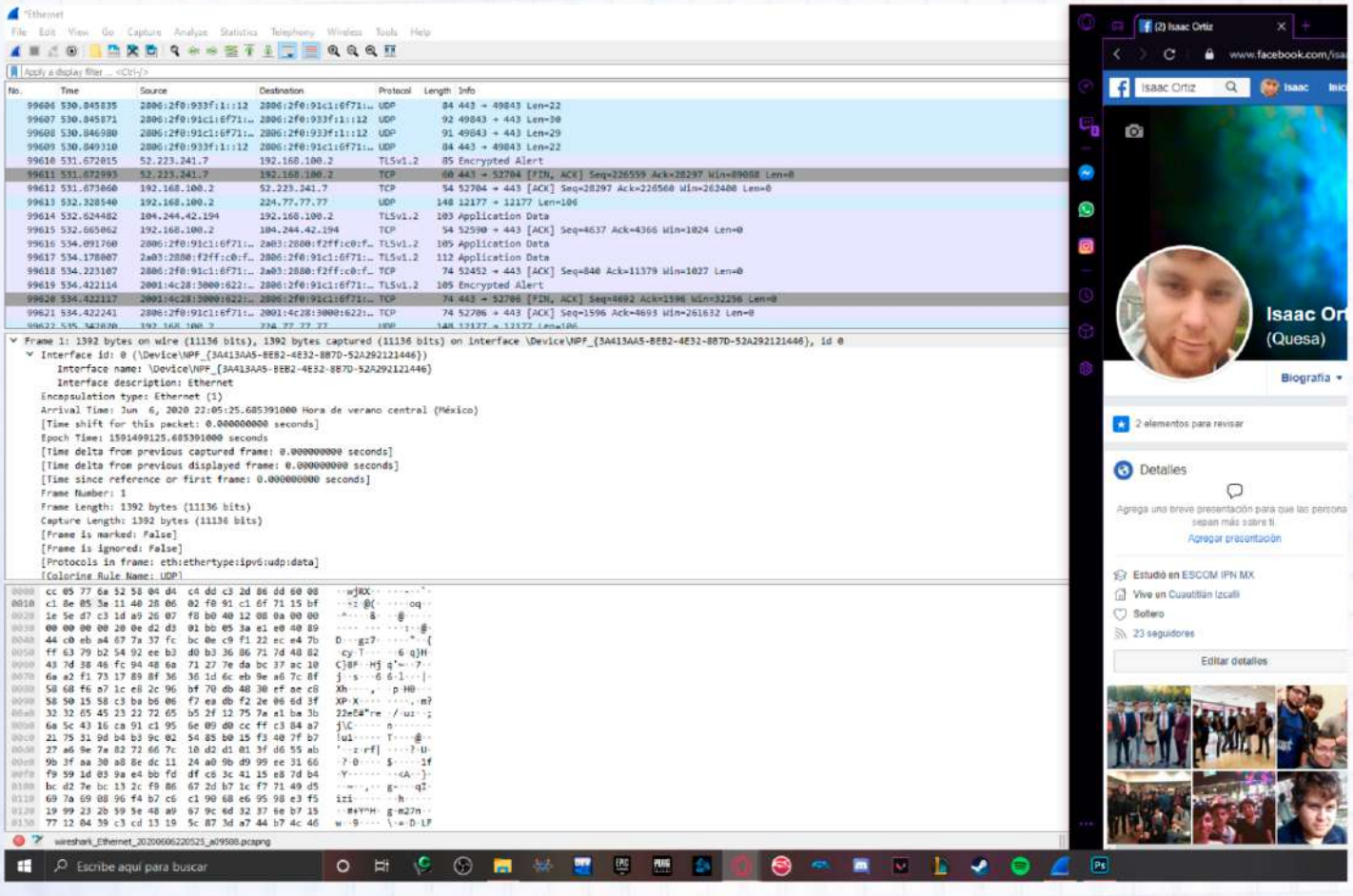
Posteriormente se tendra que elegir una interfaz para poder capturar paquetes, se pueden seleccionar multiples interfaces para poder capturar multiples fuentes



Como analizar paquetes

Una vez que se tienen capturados los paquetes, por default nos trova 3 ventanas, la lista de paquetes, los bytes de paquetes y los detalles de paquetes, para poder visualizar la información solo se da click a un paquete.

- Lista de paquetes, literalmente solo es la ventana donde se muestra una vista general de los paquetes capturados.
- Detalles de paquete, muestra los protocolos que los paquetes estan utilizando.
- Bytes de paquete, por default muestra la información del paquete "seleccionado" en un formato hexadecimal, si se quiere cambiar al formato de bits solo es necesario seleccionarlo en el menu de "context".



Ventajas y desventajas

- Captura todo tipo de paquetes
- Guarda y restaura datos capturados
- Muestra errores y problemas en niveles de protocolo
- Ligero de correr y de tamaño
- Funciones de filtros
- Captura de multiples fuentes al mismo tiempo
- Facil de usar
- Muchas herramientas y multiples funciones
- Se puede ocupar en todo tipo de sistemas operativos
- Analisis de trafico y reportes
- Capacidad de hacer estadisticas

- No tiene un tutorial integrado
- No puede un analizador que muestre anomalias en comunicaciones
- Si no se sabe a buen nivel el analisis, el usuario comun puede perderse con facilidad
- Tiene algunos problemas de, plegando de paquetes de gran tamaño
- Existe una barrera importante para poder agregar herramientas a la aplicación
- Muchas opciones de configuración de interfaz estan demasiado ocultas dentro de los menus

Relación / Conclusión

Con lo aprendido en este último parcial y en general toda la materia se pueden desisfrar varias cosas dentro de la aplicación, como el saber de donde a donde va un paquete o "mensaje", la clase de protocolo que ciertas páginas utilizan a comparación de paginas que no necesitan aplicar metodos para comunicarse con nuestras computadoras.

Por medio de esta herramienta se puede optimizar aplicaciones creadas por el usuario y al mismo tiempo detectar anomalidades en conexiones como lo pueden ser la clonación de direcciones para poder robar datos o la manipulación de protocolos para obtener datos de alguno de los involucrados en las comunicaciones.