



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 análisis de paquetes, ya sea a paquetes que mandan la computadora para poder comunicarse, o paquetes que llegan al momento de conectarse con la internet.

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

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

Funciones Esenciales

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

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

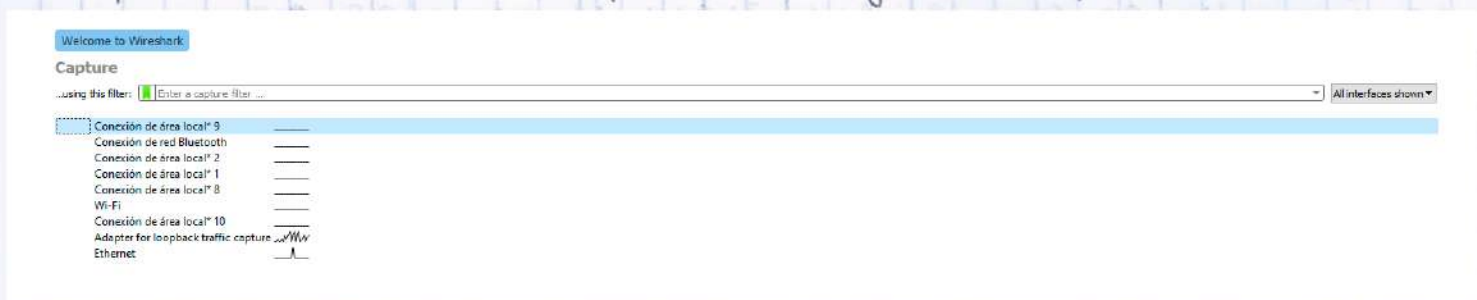


Capturar paquetes

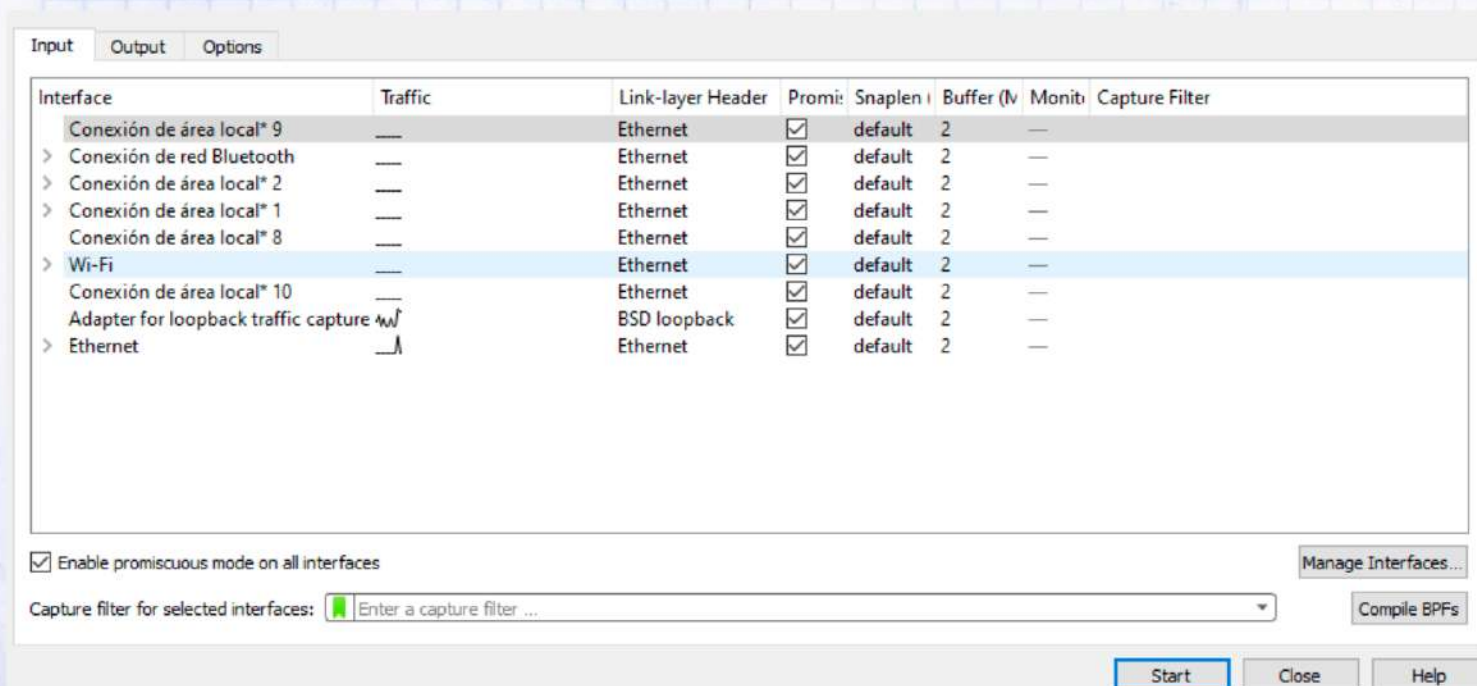
Para empezar a analizar paquetes se necesita enfocar el uso que le daremos a estos análisis, pero primero se necesita hacer unas cosas primero:

- * Asegurarse que el usuario tenga permisos de administrador
- * Escoger una interface de network
- * Capturar de la ubicación correcta

Ya teniendo estas cosas anteriores se abre la aplicación y se muestra la siguiente pantalla



Posteriormente se tendrá que elegir una interfaz para poder capturar paquetes, se pueden seleccionar múltiples interfaces para poder capturar múltiples fuentes



Como analizar paquetes

Una vez que se tienen capturados los paquetes, por default muestra 3 ventanas, la lista de paquetes, los bytes de paquetes y los detalles de paquetes, para poder visualizar 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".

The screenshot shows the Wireshark interface with the 'Ethernet' capture filter. The packet list shows several UDP and TCP packets. The selected packet (No. 1392) is a UDP packet from 192.168.100.2 to 192.168.100.2, port 52784. The details pane shows the packet structure: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes are displayed in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
99606	530.845835	2006:2f0:933f:11:12	2006:2f0:933f:11:12	UDP	84	443 → 49843 Len=22
99607	530.845871	2006:2f0:933f:11:12	2006:2f0:933f:11:12	UDP	92	49843 → 443 Len=30
99608	530.846980	2006:2f0:933f:11:12	2006:2f0:933f:11:12	UDP	91	49843 → 443 Len=29
99609	530.849310	2006:2f0:933f:11:12	2006:2f0:933f:11:12	UDP	84	443 → 49843 Len=22
99610	531.672015	52.233.241.7	192.168.100.2	TLSv1.2	85	Encrypted Alert
99611	531.672085	52.233.241.7	192.168.100.2	TCP	60	443 → 52784 [RST, ACK] Seq=226559 Ack=28297 Win=0 Len=0
99612	531.673606	192.168.100.2	52.233.241.7	TCP	54	52784 → 443 [ACK] Seq=28297 Ack=226560 Win=262400 Len=0
99613	532.320540	192.168.100.2	224.77.77.77	UDP	148	12177 → 12177 Len=106
99614	532.624482	104.244.42.194	192.168.100.2	TLSv1.2	103	Application Data
99615	532.665062	192.168.100.2	104.244.42.194	TCP	54	52590 → 443 [ACK] Seq=4637 Ack=4366 Win=1024 Len=0
99616	534.091700	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TLSv1.2	105	Application Data
99617	534.170807	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TLSv1.2	112	Application Data
99618	534.223107	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TCP	74	52452 → 443 [ACK] Seq=840 Ack=11379 Win=1027 Len=0
99619	534.422114	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TLSv1.2	105	Encrypted Alert
99620	534.422117	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TCP	74	443 → 52784 [FIN, ACK] Seq=4892 Ack=1596 Win=0 Len=0
99621	534.422241	2006:2f0:933f:11:12	2006:2f0:933f:11:12	TCP	74	52784 → 443 [ACK] Seq=1596 Ack=4693 Win=261632 Len=0
99622	535.342620	192.168.100.2	224.77.77.77	UDP	148	12177 → 12177 Len=106

Frame 1392: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{3A413AA5-BE82-4E32-8B7D-52A292121446}, Id 0

Interface name: \Device\NPF_{3A413AA5-BE82-4E32-8B7D-52A292121446}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Jun 6, 2020 22:05:25.685391000 Hora de verano central (México)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1591499125.685391000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 1392 bytes (11136 bits)

Capture Length: 1392 bytes (11136 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: ethertypesipudpdata]

[Coloring Rule Name: UDP]

```
0000 cc 05 77 6a 52 50 04 c4 d0 c3 2d 86 d4 60 00  ...wJRX.....
0010 c1 5e 05 3a 11 40 06 82 f0 91 c1 0f 71 15 bf  ...B{.....cq
0020 1e 5e d7 c3 1d 25 07 f0 b0 40 12 08 6a 00 00  ...s.....
0030 00 00 00 00 20 0e d2 d3 01 b0 05 3a e1 00 89  ........g
0040 44 c0 eb a4 67 7a 37 fc bc 0e c9 f1 22 ec a4 7b  ...Omg7.....{
0050 ff 63 79 b2 54 92 ee b3 d0 36 86 71 7d 48 82  ...cyT.....6qJH
0060 43 7d 58 46 fc 94 08 6a 71 27 7a db bc 37 ac 10  ...CjP...H5...7-
0070 6a a2 f1 73 17 89 0f 36 3d 1d 6c eb 9e a5 7c 8f  ...j's...6...l...|
0080 50 68 f6 a7 1c e8 2c 96 bf 70 db 40 30 ef ae c0  ...Xh.....pH...
0090 58 50 15 58 c3 ba b5 06 f7 ea db f2 2e 96 6d 3f  ...XPX.....m?
00a0 32 32 05 45 23 22 72 65 b5 2f 12 75 7a a1 ba 3b  ...22eE're.../uz...
00b0 6a 5c 43 16 c8 91 c1 95 06 05 00 cc ff c3 04 a7  ...jL.....0.....
00c0 21 75 11 3d 54 b3 9c 02 54 85 b0 15 f3 40 f7 b7  ...uaz.....T...
00d0 27 a6 9e 7a 82 72 66 7c 10 d2 d1 01 3f d6 55 ab  ...'...zrf...-U-
00e0 9b 3f aa 30 a0 8e dc 11 24 a0 9b d9 99 ee 31 66  ...7-0...$.....1f
00f0 f9 59 1d 03 9a e4 b0 fd df c0 c4 15 8b 7d b4  ...Y.....G...-}
0100 bc d2 76 bc 13 f4 f0 86 07 2d 67 1c f7 71 49 d5  ...-.....G...q1-
0110 69 7a 69 08 96 f4 b7 c6 c1 90 68 e5 95 58 c3 f5  ...izi.....h...
0120 19 99 23 2b 59 5e 48 a9 67 9c 6d 32 37 be b7 15  ...&VYH...g-w27n-
0130 77 12 04 39 c3 cd 13 19 5c 87 3d a7 44 7b 4c 46  ...w-9.....\w-D-LF
```

The screenshot shows a Facebook profile for Isaac Ortiz (Quesa). The profile picture is a circular image of a man. The cover photo is a landscape image. The bio section is empty. The 'About' section shows 'Estudió en ESCOM IPN MX', 'Vive en Cuautitlán Izcalli', 'Soltero', and '23 seguidores'. There are several photos in the 'Photos' section.

Isaac Ortiz (Quesa)

Biografía

2 elementos para revisar

Detalles

Agrega una breve presentación para que las personas sepan más sobre ti

Agregar presentación

Estudió en ESCOM IPN MX

Vive en Cuautitlán Izcalli

Soltero

23 seguidores

Editar detalles

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 múltiples fuentes al mismo tiempo
- Fácil de usar
- Muchas herramientas y múltiples funciones
- Se puede operar en todo tipo de sistemas operativos
- Análisis de tráfico y responder
- Capacidad de hacer estadísticas
- No tiene un tutorial integrado
- No posee un analizador que encuentre anomalías en comunicaciones
- Si no se sabe a buen nivel el análisis, el usuario corre el riesgo de perderse con facilidad
- Tiene algunos problemas de pegando paquetes de gran tamaño
- Existe una barrera importante para poder agregar herramientas a la aplicación
- Muchas opciones de configuración de interfaz están escondidas dentro de los menús

Relación / Conclusión

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

Por medio de esta herramienta se puede optimizar aplicaciones creadas por el usuario y al mismo tiempo detectar anomalías 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.