

Departamento de Ingeniería de Sistemas y Computación Infraestructura de Comunicaciones



Asist. De laboratorio: Nathalia Quiroga

n.quiroga@uniandes.edu.co

GUÍA 1 – TUTORIAL WIRESHARK

1. OBJETIVO (S)

Aprender el funcionamiento básico de un analizador de protocolos, específicamente Wireshark, y comprender los resultados generados por éste, obteniendo así un mayor conocimiento sobre algunos protocolos usados comúnmente en una red.

2. ANALIZADOR DE PROTOCOLOS WIRESHARK

El análisis de paquetes o análisis de protocolos se describe como el proceso de captura y la interpretación de datos en tiempo real a medida que los paquetes circulan a través de una red, esto con el fin de entender mejor lo que está sucediendo en dicha red. Análisis de paquetes se realiza normalmente por un analizador de protocolos, una herramienta que se utiliza para capturar los datos de la red que viajan a través del medio físico (Ejemplo un cable de cobre).

Análisis de paquetes puede ayudarnos a entender las características de la red, saber quién está en una red, determinar quién o qué está utilizando el ancho de banda disponible, identificar las horas pico de uso de red, identificar a posibles ataques o actividad maliciosa, y encontrar aplicaciones no seguras.

Hay varios tipos de programas de detección de paquetes, incluyendo libres y comerciales. Cada programa está diseñado con diferentes objetivos. Algunos de los programas de análisis de paquetes más populares son tcpdump (un programa de línea de comandos), OmniPeek y Wireshark.

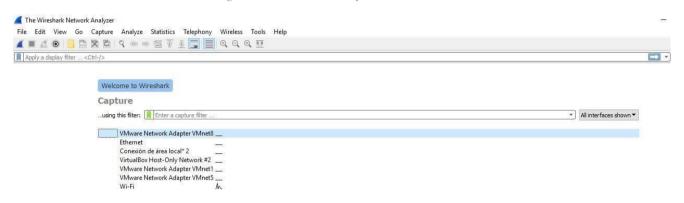
Wireshark es un analizador de paquetes de red (sniffer). Un analizador de paquetes de red intenta capturar paquetes en la red e intenta visualizar los datos de esos paquetes tan detalladamente como sea posible. Se puede pensar en un analizador de paquetes de red como un dispositivo de medida usado para examinar que está pasando al interior de un cable de red.

Wireshark tiene todas las características estándares que se pueden esperar en un analizador de protocolos; su licencia es de código abierto y puede ser ejecutado sobre plataformas como Unix, Linux y Windows. Wireshark sobresale en el número de protocolos que soporta (más de 850). Estos protocolos van desde los más comunes como IP y DHCP hasta protocolos propietarios más avanzados como AppleTalk.

3. USO BÁSICO DE WIRESHARK

Una vez se ejecuta el programa Wireshark, se verá una ventana como la siguiente:

Figura. 1. Ventana inicial software Wireshark.



Para iniciar una captura, seleccionar la palabra en gris "Capture", en la ventana principal. También se puede acceder a esta opción a través del segundo ícono del menú, "Show the capture options".

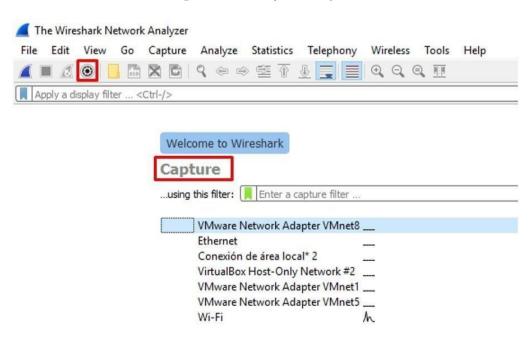


Figura. 2. Iniciar captura de tráfico.

En la ventana que aparece, realizar las siguientes acciones en las tres pestañas:

Seleccione la tarjeta de red a usar para capturar los paquetes.

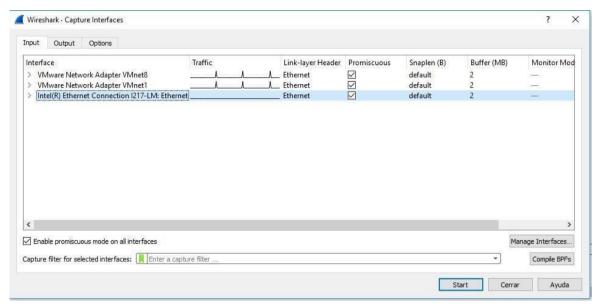
Seleccione la opción para capturar paquetes en modo promiscuo.

Verifique que no haya ningún filtro, en "Capture Filter".

No remueva las selecciones en "Display Options"

Verifique que las opciones seleccionadas en "Name Resolution" involucren las direcciones MAC, las direcciones de capa de red y las direcciones de capa de transporte. Seleccionar la opción "pcap".

Figura. 3. Ventana de selección de interfaz para capturar trafico.



Al hacer click en "Start" se inicia la captura de tráfico que muestra el número de paquetes capturados, con sus respectivos protocolos e información.

Para terminar la captura de paquetes, hacer click en "Stop". Después de esto se podrá observar una ventana de resultados, la misma que se visualizaba previamente durante la captura.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools ■ Ø ● □ □ X □ Q ⊕ ⊕ ≅ T ₺ □ □ Q Q Q Ⅲ Apply a display filter ... <Ctrl-/: Time
886 9.304380
887 9.304790
888 9.313678
889 9.319804
890 9.370209
891 9.370816
892 9.371296
893 9.384463
895 9.384463
895 9.38486 Source Destination iad23s23-in-f195.1e... DESKTOP-NT6967P Length info

1424 Application Data[TCP segment of a reassembled PDU]

54 59223 + https(443) [ACK] Seq-4585 Ack-95981 kin-567 Len-0

76 Standard query 0xa729 A id.google.com.co

66 https(443) + 95924 [ACK] Seq-1 Ack-2 kin-116 Len-0 SLE=1 SRE=2

54 http(80) + 59248 [ACK] Seq-1 Ack-459 win-290 Len-0

842 Response

1424 Application Data[TCP segment of a reassembled PDU]

54 59223 + https(443) [ACK] Seq-4585 Ack-9351 kin-657 Len-0

1424 Application Data[TCP segment of a reassembled PDU]

54 59223 + https(443) [ACK] Seq-4585 Ack-98721 win-567 Len-0

940 Application Data[TCP segment of a reassembled PDU] TLSv1.2 DESKTOP-NT6967P DESKTOP-NT6967P iad23s23-in-f195.1e_ TCP 192.168.43.1 DNS ec2-52-41-78-152.us. DESKTOP-NT6967P 192.16.58.8 DESKTOP-NT6967P 192.16.58.8 DESKTOP-NT6967P ec2-52-41-78-152.us DESKTOP-NT6967P 192.16.58.8 DESKTOP-NT6967P 0CSP DESKTOP-NT6967P 192.16.58.8 TCP 192.16.58.8 TCP 192.16.59.8 TCP 192.16.59.8 TCP 192.16.59.8 TCP 192.16.59.8 TCP 193.16.59.9 TCSV1.2 TCP 193.16.59.8 TCP 193.16.59.9 TCP 193.16.59 TCP iad23s23-in-f195.1e. TCP 896 9.385030 897 9.386595 54 59223 + https(443) [ACK] Seq=4585 Ack=98721 Win=567 Len=0 940 Application Data 1424 Application Data 1424 Application Data 1424 Application Data [TCP segment of a reassembled PDU] 54 59223 + https(443) [ACK] Seq=4585 Ack=108091 Min-1567 Len=0 1424 Application Data[TCP segment of a reassembled PDU] 121 Standard query response 0xa729 A id.google.com.co CNAME id. 54 59223 + https(443) [ACK] Seq=4585 Ack=10461 Win=567 Len=0 1424 Application Data[TCP segment of a reassembled PDU] 54 59223 + https(443) [ACK] Seq=4585 Ack=102831 Win=567 Len=0 1424 Application Data[TCP segment of a reassembled PDU] 54 59223 + https(443) [ACK] Seq=4585 Ack=104281 Win=567 Len=0 65 59224 + https(443) [ACK] Seq=4585 Ack=104281 Win=567 Len=0 65 59224 + https(443) [ACK] Seq=4585 Ack=104281 Win=567 Len=0 65 59224 + https(443) [SYM] Seq=96 Win=17520 Len=0 MSS=1460 WS DESKTOP-NT6967P sync-648-us-west-2... TLSv1.2 iad23s23-in-f195.1e.. DESKTOP-NT6967P TLSv1.2 897 9.386595 898 9.39969 899 9.399591 900 9.399974 901 9.399982 902 9.400256 903 9.400611 904 9.400750 905 9.400210 iad2323-in-f195.1e_ DESKTOP-NT6967P TLSV
DESKTOP-NT6967P iad2323-in-f195.1e_ DESKTOP-NT6967P DISC
192.168.43.1 DESKTOP-NT6967P DISC
182323-in-f195.1e_ DESKTOP-NT6967P TLSV
182323-in-f195.1e_ DESKTOP-NT6967P TLSV
182323-in-f195.1e_ DESKTOP-NT6967P TLSV
DESKTOP-NT6967P iad23232-in-f195.1e_ TCP
182432323-in-f195.1e_ TCP
1824323-in-f195.1e_ TCP
182432-in-f195.1e_ TCP
1824323-in-f195.1e_ TCP DESKTOP-NT6967P iad23s23-in-f19 iad23s23-in-f195.1e_ DESKTOP-NT6967P TLSv1.2 906 9.402204 iad23s23-in-f195.1e.. TCP 907 9.414152 Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: DESKTOP-NIT6967P (40:49:6f:2b:cb:f5), Dst: de:bf:e9:20:19:ca (de:bf:e9:20:19:ca)

Internet Protocol Version 4, Src: DESKTOP-NIT6967P (192.166.43.12), Dst: sec-tws-prod-vip.webex.com (66.163.35.36)

Transmission Control Protocol, Src Port: 59263 (59263), Dst Port: https (443), Seq: 0, Len: 0

Figura. 4. Captura de tráfico corriendo.

El filtrado de tráfico permite desplegar sólo aquellos paquetes de interés para el usuario. Para hacer esto, se usa la barra "**Filter**". Se puede escribir directamente sobre ella la condición sobre los paquetes que debe ser cumplida, o se puede usar la ventana asociada al botón "**Expression...**". Ahí se selecciona el nombre del campo, y su relación con un valor.

A continuación, se muestra el filtro de paquetes que poseen el puerto 80 TCP como origen o como destino. Para que un filtro tenga efecto, se debe hacer click en "Apply". Si se desea nuevamente mostrar todos los paquetes, se debe hacer click en "Clear".

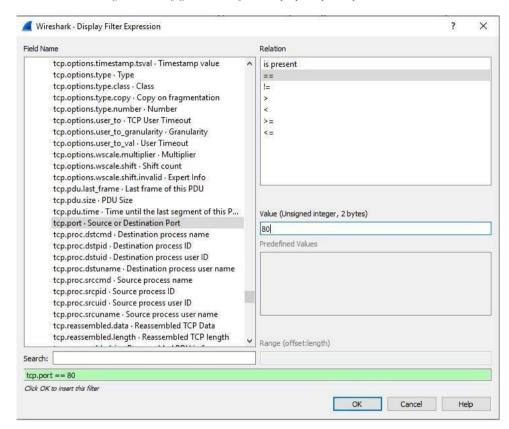


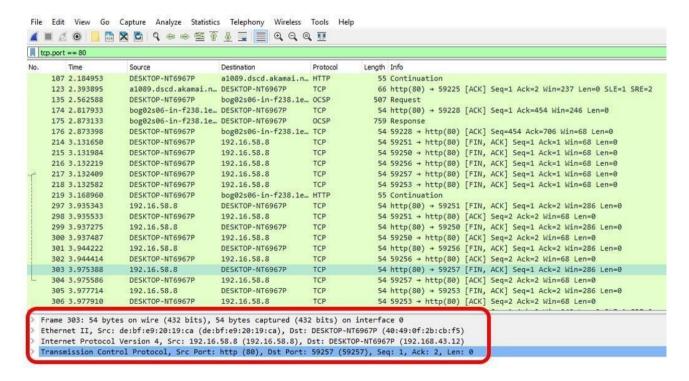
Figura. 5. Configuración de filtro de paquete por el puesto 80.

Figura. 6. Trafico filtrado por el puerto TCP 80.

o.		Time	Source	Destination	Protocol	Length Info
	107	2.184953	DESKTOP-NT6967P	a1089.dscd.akamai.n	HTTP	55 Continuation
	123	2.393895	a1089.dscd.akamai.n	DESKTOP-NT6967P	TCP	66 http(80) → 59225 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=
	135	2.562588	DESKTOP-NT6967P	bog02s06-in-f238.1e	OCSP	507 Request
	174	2.817933	bog02s06-in-f238.1e	DESKTOP-NT6967P	TCP	54 http(80) + 59228 [ACK] Seq=1 Ack=454 Win=246 Len=0
	175	2.873133	bog02s06-in-f238.1e	DESKTOP-NT6967P	OCSP	759 Response
	176	2.873398	DESKTOP-NT6967P	bog02s06-in-f238.1e	TCP	54 59228 + http(80) [ACK] Seq=454 Ack=706 Win=68 Len=0
	214	3.131650	DESKTOP-NT6967P	192.16.58.8	TCP	54 59251 → http(80) [FIN, ACK] Seq=1 Ack=1 Win=68 Len=0
	215	3.131984	DESKTOP-NT6967P	192.16.58.8	TCP	54 59250 → http(80) [FIN, ACK] Seq=1 Ack=1 Win=68 Len=0
	216	3.132219	DESKTOP-NT6967P	192.16.58.8	TCP	54 59256 → http(80) [FIN, ACK] Seq=1 Ack=1 Win=68 Len=0
	217	3.132409	DESKTOP-NT6967P	192.16.58.8	TCP	54 59257 + http(80) [FIN, ACK] Seq=1 Ack=1 Win=68 Len=0
	218	3.132582	DESKTOP-NT6967P	192.16.58.8	TCP	54 59253 → http(80) [FIN, ACK] Seq=1 Ack=1 Win=68 Len=0
	219	3.168960	DESKTOP-NT6967P	bog02s06-in-f238.1e	HTTP	55 Continuation
	297	3.935343	192.16.58.8	DESKTOP-NT6967P	TCP	54 http(80) - 59251 [FIN, ACK] Seq=1 Ack=2 Win=286 Len=0
	298	3.935533	DESKTOP-NT6967P	192.16.58.8	TCP	54 59251 → http(80) [ACK] Seq=2 Ack=2 Win=68 Len=0
	299	3.937275	192.16.58.8	DESKTOP-NT6967P	TCP	54 http(80) + 59250 [FIN, ACK] Seq=1 Ack=2 Win=286 Len=0
	300	3.937487	DESKTOP-NT6967P	192.16.58.8	TCP	54 59250 → http(80) [ACK] Seq=2 Ack=2 Win=68 Len=0
	301	3.944222	192.16.58.8	DESKTOP-NT6967P	TCP	54 http(80) + 59256 [FIN, ACK] Seq=1 Ack=2 Win=286 Len=0
	302	3.944414	DESKTOP-NT6967P	192.16.58.8	TCP	54 59256 → http(80) [ACK] Seq=2 Ack=2 Win=68 Len=0
	303	3.975388	192.16.58.8	DESKTOP-NT6967P	TCP	54 http(80) - 59257 [FIN, ACK] Seq=1 Ack=2 Win=286 Len=0
	304	3.975586	DESKTOP-NT6967P	192.16.58.8	TCP	54 59257 → http(80) [ACK] Seq=2 Ack=2 Win=68 Len=0
	305	3.977714	192.16.58.8	DESKTOP-NT6967P	TCP	54 http(80) + 59253 [FIN, ACK] Seq=1 Ack=2 Win=286 Len=0
	306	3.977910	DESKTOP-NT6967P	192.16.58.8	TCP	54 59253 + http(80) [ACK] Seq=2 Ack=2 Win=68 Len=0

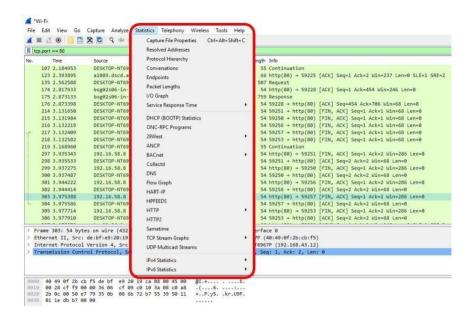
Para el caso particular del protocolo TCP, la información de cada captura es mostrada en cuatro partes: "Frame", "Ethernet", "Internet Protocol", y "Transmission Control Protocol".

Figura. 7. Información en detalle de un registro de captura de trafico.



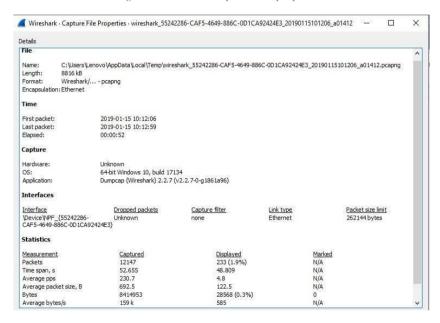
Wireshark posee un completo conjunto de herramientas que permiten obtener estadísticas. Éstas incluyen resúmenes, gráficas, jerarquías de protocolos, conversaciones, etc. Se accede a la mayoría de ellas a través del menú "Statistics".

Figura. 8. Opciones de pestaña Statistics.



La siguiente figura muestra la opción "Capture File Properties". En ella se muestran datos de tráfico capturado y mostrado.

Figura. 9. Ventana Capture File properties.



La siguiente gráfica muestra la opción "Statistics \rightarrow IO Graphs", donde se han seleccionado los parámetros de tráfico TCP para todos los paquetes.

Figura. 10. Ventana I/O Graphs para el trafico TCP.



Las siguientes gráficas se refieren a la configuración de la opción "Flow Graph" y a la muestra de resultados del mismo. Esto muestra el flujo de mensajes entre uno o más sistemas finales, en su orden cronológico.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Capture File Properties Resolved Addresses Apply a display filter Protocol Hierarchy Time Source 524 6.722533 iad23s23-in-f Conversations 525 6.722533 iad23s23-in-f Endpoints 526 6.722534 iad23s23-in-f Packet Lengths 527 6.722535 528 6.722536 iad23s23-in-f iad23s23-in-f I/O Graph DESKTOP-NT696 DESKTOP-NT696 529 6.723306 Service Response Time 530 6.723507 531 6.723593 DESKTOP-NT696 DHCP (BOOTP) Statistics 532 6.724074 iad23s23-in-f ONC-RPC Programs 533 6.724075 iad23s23-in-f 29West 534 6.724075 535 6.724076 iad23s23-in-f iad23s23-in-f ANCP 536 6.724423 DESKTOP-NT696 BACnet DESKTOP-NT696 537 6.728563 Collectd 538 6.735949 DESKTOP-NT696 DNS DESKTOP-NT696 539 6.737429 Flow Graph 541 6.748073 542 6.757995 DESKTOP-NT696 HART-IP DESKTOP-NT696 HPFEEDS 543 6.873271 iad23s23-in-f 544 6.873493 DESKTOP-NT696 545 6.873700 iad23s23-in-f HTTP2 Sametime Frame 20: 54 bytes on wire (432 b Ethernet II, Src: DESKTOP-NT6967P TCP Stream Graphs Internet Protocol Version 4. Src: **UDP Multicast Streams** Transmission Control Protocol, Sr IPv6 Statistics

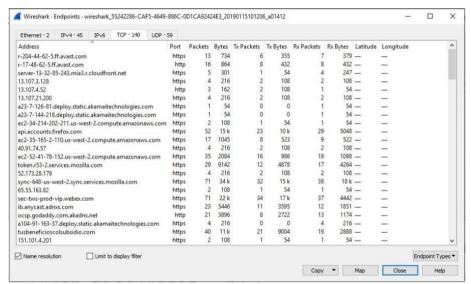
Figura. 11. Herramienta Flow Graph.

Figura. 12. Ventana de Flowgraph para una captura de trafico.



Las siguientes gráficas muestran el uso de la opción "Statistics \rightarrow Endpoints". En ellas se puede observar información referente a cada uno de los endpoints en el caso de los protocolos TCP y UDP.

Figura. 13. Ventana de herramienta Statistics-Endpoints.



4. BIBLIOGRAFÍA

- [1] The Wireshark Field Guide Analyzing and Troubleshooting Network Traffic. Robert Shimonski. Syngress.
- [2] Network Analysis Using Wireshark. Yoram Orzach. Packt Publishing.
- [3] Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th ed.

HISTORIAL DE REVISIONES

Fecha	Autor	Observaciones
05/02/2021	Arnold Andres Lara a.larav@uniandes.edu.co	Ajustes de redacción y actualización del documento
11/02/2020	Arnold Andres Lara a.larav@uniandes.edu.co	Ajustes de redacción.
14/01/2019	Jonatan Legro Pastrana j.legro@uniandes.edu.co	Actualización de la documentación para la versión de Wireshark 2.6.6