LABORATORIO DE REDES TCP-IP

PRÁCTICA N° 3

1. TEMA

SOFTWARE DE CAPTURA DE PAQUETES

2. OBJETIVOS

2.1. Aprender sobre el funcionamiento del analizador de protocolos Wireshark.

3. INFORMACIÓN

Esta práctica de laboratorio se va a realizar utilizando el sistema operativo Windows, y usando la herramienta Wireshark, la cual permite capturar paquetes.

4. TRABAJO PREPARATORIO

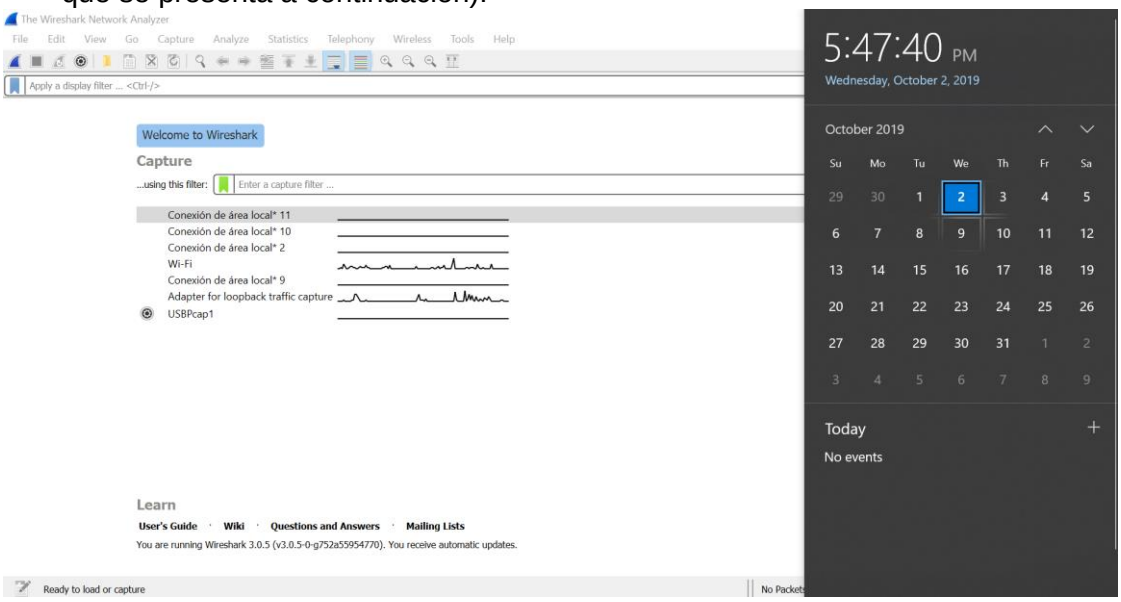
Como parte de este preparatorio, Usted debe realizar las siguientes tareas:

4.1. Investigue qué es el modo promiscuo (aplicable a interfaces de red) (máximo un párrafo

4.2. Investigue qué es un analizador de protocolos, y para qué es útil (máximo 1 página).

4.3. Investigue sobre 2 herramientas, distintas a Wireshark, que permitan realizar análisis de trafico de red, y escriba una breve descripción de estos (máximo un párrafo por cada una).

4.4. Instale Wireshark en su equipo, capture una pantalla en la que se muestre el software instalado, en la captura debe verse la fecha y hora de la captura (similar a la figura que se presenta a continuación):



La última versión estable de Wireshark es 3.0.5. Puede descargarla de: https://www.wireshark.org/download.html

5. EQUIPO Y MATERIALES

Materiales por grupo de trabajo.

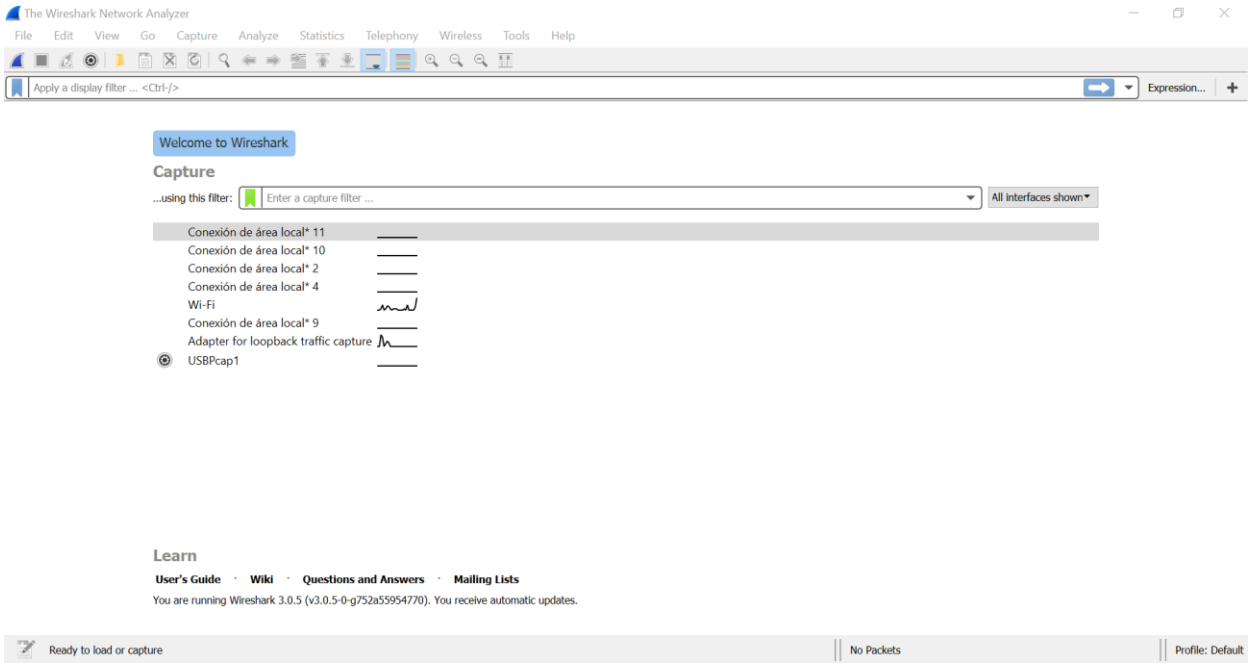
- PC
  - Software Wireshark

6. PROCEDIMIENTO

Establezca y verifique la conectividad a Internet, esto garantiza que su equipo tiene asignado una dirección IP. Para esto abra un explorador web y compruebe que puede acceder a www.google.com. Sino puede hacerlo pida ayuda al instructor.

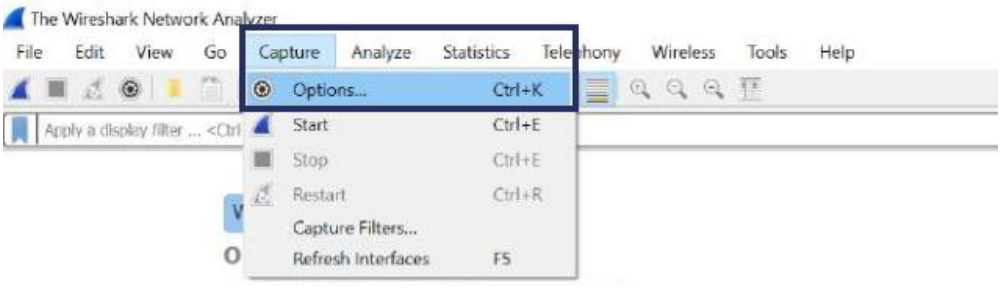
6.1. Uso de Wireshark:

6.1.1. Ejecute el programa, encontrará un enlace directo en su escritorio. Debe ejecutarlo con permisos de administrador, para iniciarlo, presione botón derecho sobre el icono y escoja "Ejecutar como administrador (*Run as administrator*)". Si no ejecuta el programa con privilegios de administrador, no verá ninguna interfaz al momento de querer captura tráfico. Luego de ejecutarlo verá una pantalla similar a la siguiente:

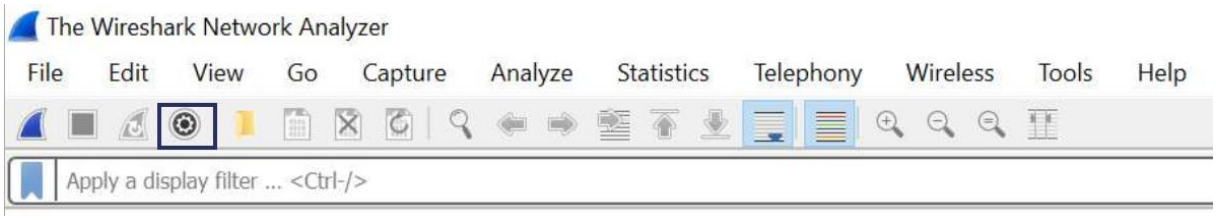


6.1.2. Vamos a usar Wireshark para capturar tráfico. Para iniciar una captura realice **una** de las siguientes tareas:

a. Escoja la opción del menú llamada “Capture”, y en el submenú seleccione la opción “Options”.

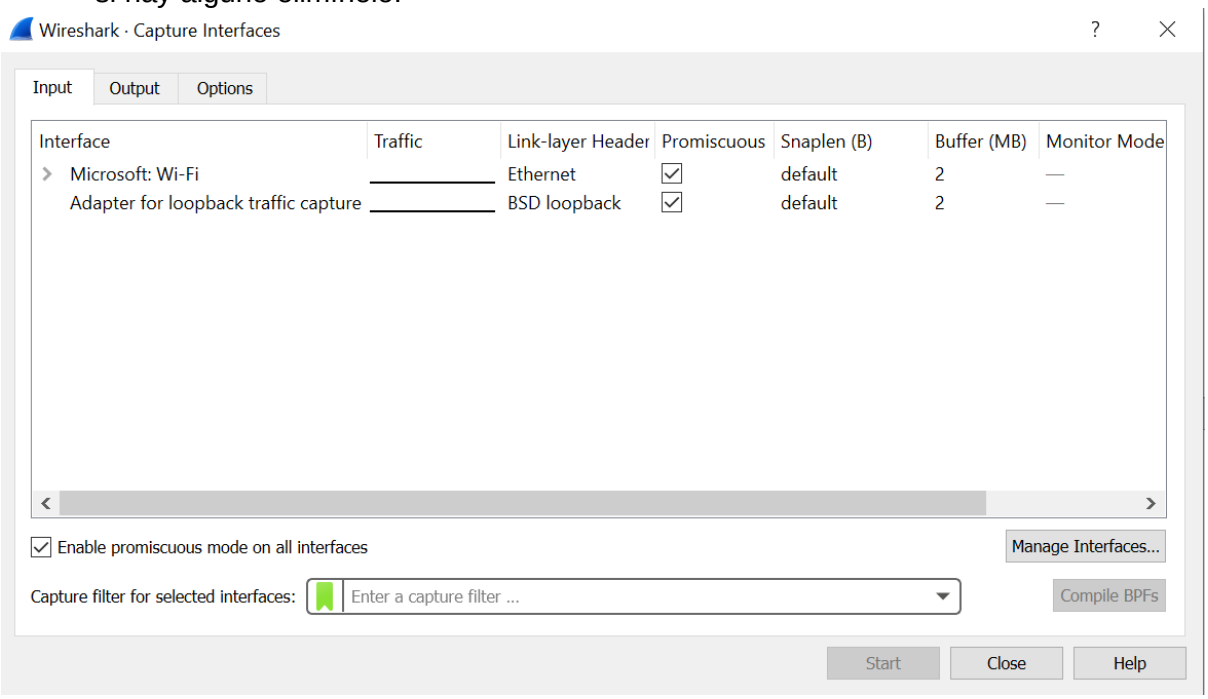


b. En la barra de herramientas, busque el icono que tiene un círculo negro rodeado de una circunferencia negra.

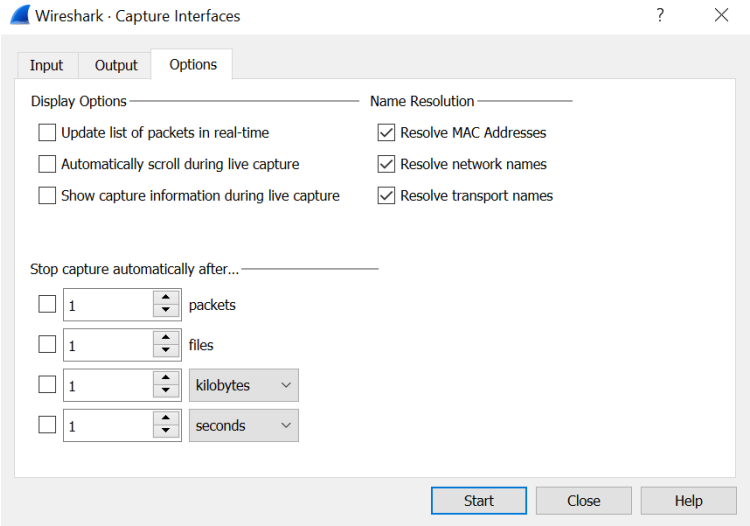


6.1.3. En la ventana “Wireshark: Capture Interfaces” realice lo siguiente:

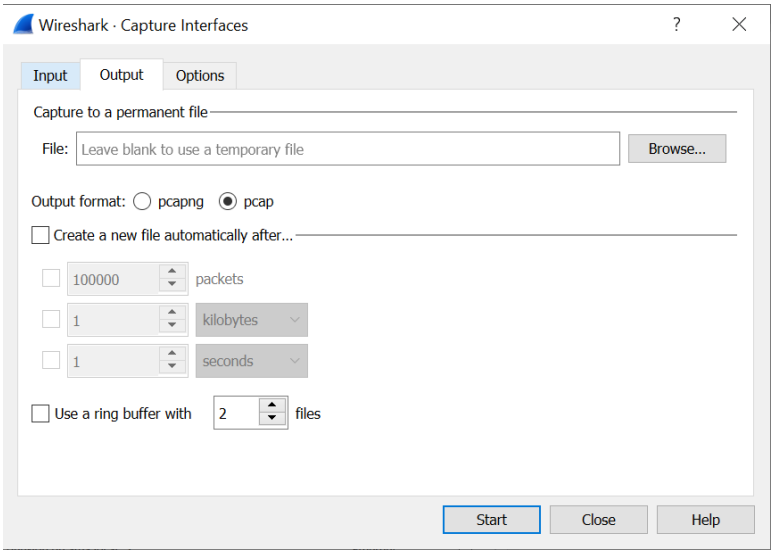
a. Seleccione la tarjeta de red a usar para capturar los paquetes. Es probable que el nombre de la interfaz sea “Conexión de área local”
b. Seleccione la opción para capturar paquetes en modo promiscuo (“Enable promiscuous mode on all interfaces”).
c. Verifique que no haya ningún filtro definido en “Capture filter for selected interfaces”, si hay alguno elimínelo.



d. Verifique que las opciones seleccionadas en “Name Resolution” involucren: direcciones MAC, direcciones de capa de red y direcciones de capa de transporte.
e. Deseleccione las opciones bajo “Display Options”.

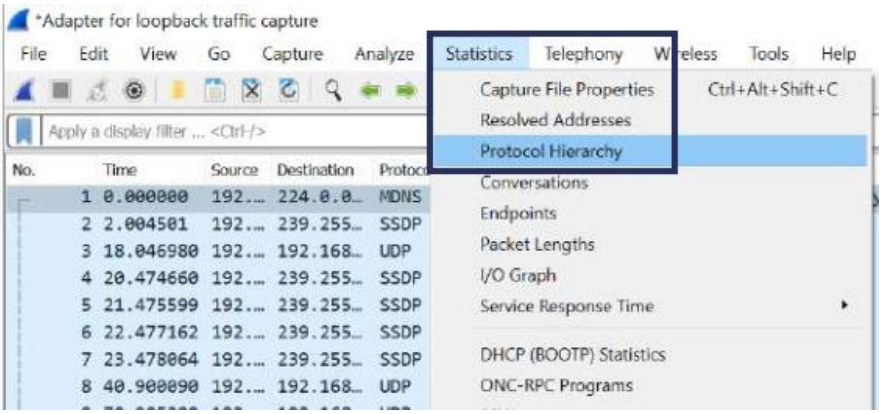


f. Deseleccionar la opción “Use pcap-ng format”.

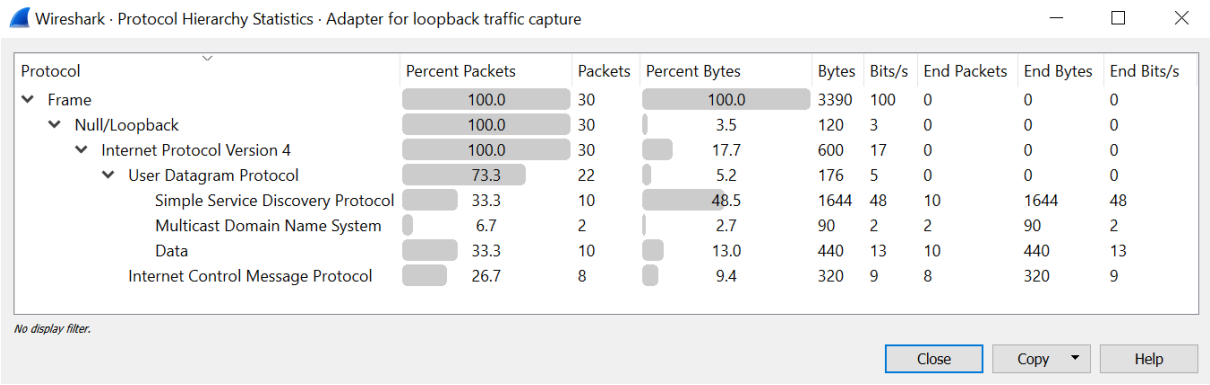


g. Una vez que esté seguro de que todo está de acuerdo con lo indicado, presione “Start”

6.1.4. En su navegador visite algunas páginas y detenga la captura. En el menú escoja la opción “Statistics” y en el submenú la opción “Protocol Hierarchy”.



Se presentará una ventana con información de los paquetes capturados, similar a la siguiente:



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	30	100.0	3390	100	0	0	0
Null/Loopback	100.0	30	3.5	120	3	0	0	0
Internet Protocol Version 4	100.0	30	17.7	600	17	0	0	0
User Datagram Protocol	73.3	22	5.2	176	5	0	0	0
Simple Service Discovery Protocol	33.3	10	48.5	1644	48	10	1644	48
Multicast Domain Name System	6.7	2	2.7	90	2	2	90	2
Data	33.3	10	13.0	440	13	10	440	13
Internet Control Message Protocol	26.7	8	9.4	320	9	8	320	9

6.1.5. Genere una tabla indicando cuantos paquetes fueron capturados en TCP, UDP, ICMP y ARP.

6.1.6. Abra una consola y ejecute los siguientes comandos:

a. ping 127.0.0.1
b. ping www.google.com
c. ping www.epn.edu.ec
d. ping www.facebook.com
e. ping www.youtube.com

6.1.7. Abra un explorador web e ingrese a los siguientes sitios web:

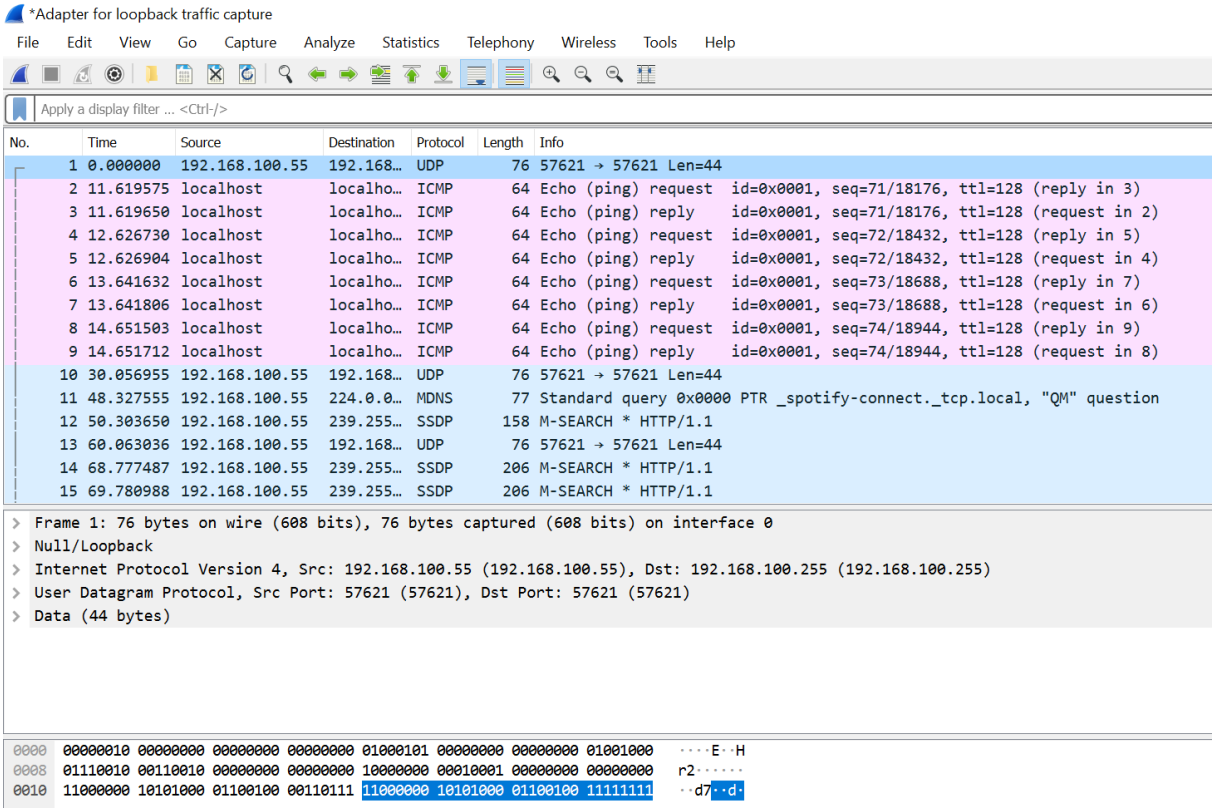
a. www.google.com
b. www.epn.edu.ec
c. www.facebook.com
d. www.youtube.com

6.1.8. Abra una consola y ejecute los siguientes comandos:

a. nslookup 127.0.0.1
b. nslookup www.google.com
c. nslookup www.epn.edu.ec
d. nslookup www.facebook.com
e. nslookup www.youtube.com

6.1.9. Detenga la captura de paquetes, presionando en el botón “Stop”, podrá ver una ventana con resultados similar a la siguiente:

a. En la parte superior de la pantalla principal verá un listado de todos los paquetes con información como: Número de paquete, Tiempo, Origen, Destino, Protocolo, Longitud e Información.



b. Al seleccionar un paquete del listado, en la parte intermedia, aparecerá información detallada de cada campo que conforma el paquete.

```
> Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.100.55 (192.168.100.55), Dst: 192.168.100.255 (192.168.100.255)
> User Datagram Protocol, Src Port: 57621 (57621), Dst Port: 57621 (57621)
> Data (44 bytes)
```

c. Explique la información contenida de dicha sección de cualquiera de los paquetes capturados.

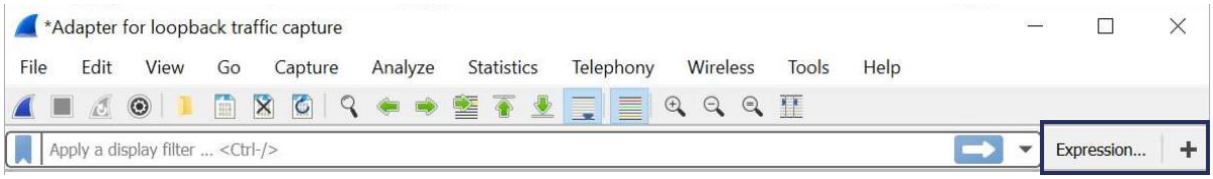
d. En la parte inferior podrá ver la representación en hexadecimal del contenido del paquete, así como la interpretación en formato ASCII.

```
0000  00000010 00000000 00000000 00000000 01000101 00000000 00000000 00111100   ····E··<
0008  00100111 10000001 00000000 00000000 10000000 00000001 00000000 00000000   '·******
0010  01111111 00000000 00000000 00000001 01111111 00000000 00000000 00000001   ********
0018  00001000 00000000 01001101 00010010 00000000 00000001 00000000 01001001   ··M····I
0020  01100001 01100010 01100011 01100100 01100101 01100110 01100111 01101000   abcdefgh
0028  01101001 01101010 01101011 01101100 01101101 01101110 01101111 01110000   ijklmnop
0030  01110001 01110010 01110011 01110100 01110101 01110110 01110111 01100001   qrstuvwa
0038  01100010 01100011 01100100 01100101 01100110 01100111 01101000 01101001   bcdefghi
```

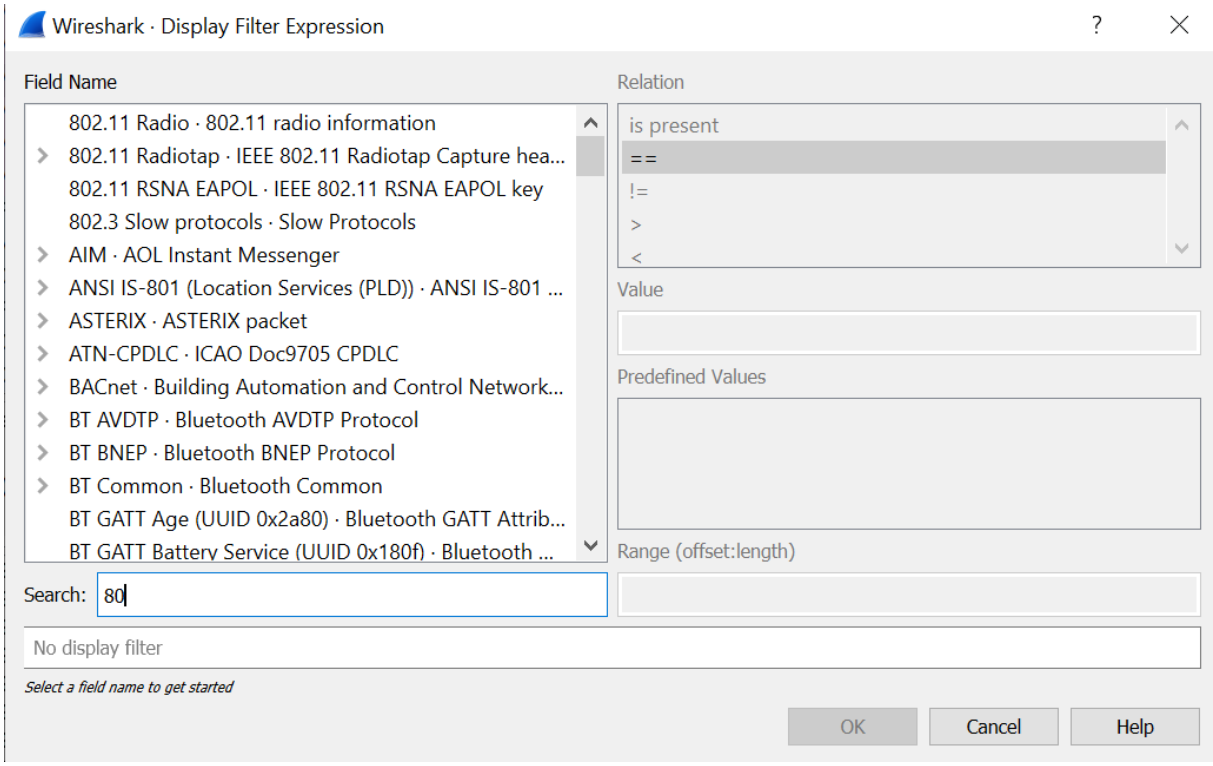
6.1.10. Con base en la información presentada, determine:

a. Número de paquetes enviados a 127.0.0.1.
b. Número de paquetes recibidos en 127.0.0.1.
c. Número de paquetes enviados a www.google.com.
d. Número de paquetes recibidos de www.google.com.
e. Número de paquetes enviados a www.epn.edu.ec.
f. Número de paquetes recibidos de www.epn.edu.ec.
g. Número de paquetes enviados a www.facebook.com.
h. Número de paquetes recibidos de www.facebook.com.
i. Número de paquetes enviados a www.youtube.com.
j. Número de paquetes recibidos de www.youtube.com.
k. ¿Compare esta información con la obtenida por su compañero, es la misma? Comente sobre los resultados obtenidos.

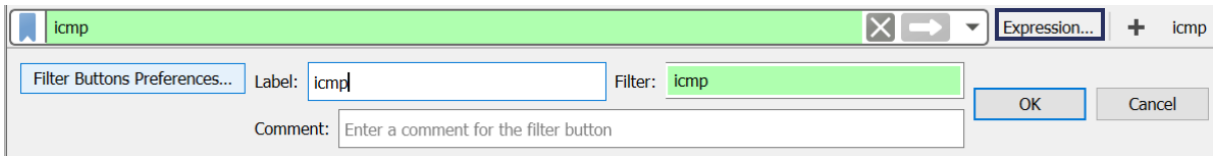
6.1.11. El filtrado de tráfico permite desplegar solo aquellos paquetes que son de nuestro interés. Para esto, en la barra de herramientas se encuentra un combobox denominado “Filter”. Se puede escribir directamente sobre este control la condición que cumplirán los paquetes a ser desplegados, o se puede usar la ventana asociada al botón "Expression…". En esta nueva ventana selecciona el nombre del campo, su relación y el un valor.



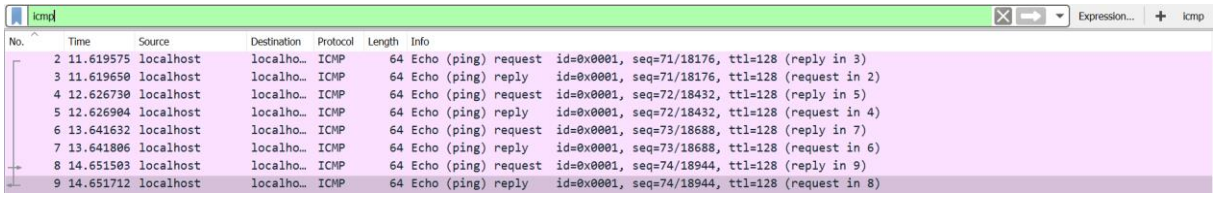
a. A continuación, se muestra el filtro de paquetes especificando al puerto 80 TCP como origen o como destino. Para que un filtro tenga efecto, se debe hacer clic en “Apply”. Si se desea nuevamente mostrar todos los paquetes, se debe hacer clic en “Clear”.



b. Junto al botón “Expressions” se encuentra el botón con signo más (+), presione sobre este botón y se visualizará una sección igual a la que se muestra a continuación, aplique un filtro para presentar paquetes ICMP.



c. Una vez creado el filtro presionar “OK”, el resultado será similar al siguiente.



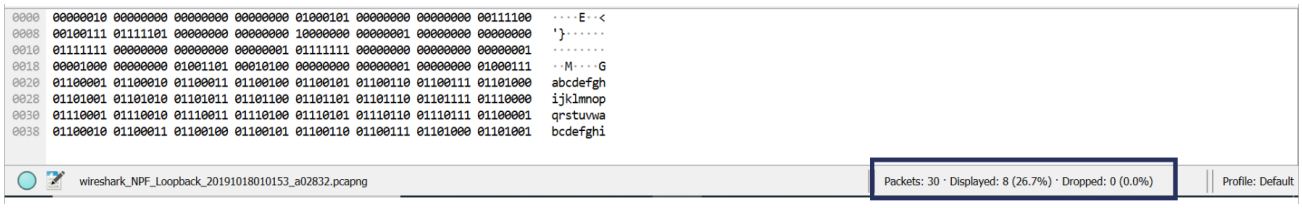
No.	Time	Source	Destination	Protocol	Length	Info
2	11.619575	localhost	localho…	ICMP	64	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 3)
3	11.619650	localhost	localho…	ICMP	64	Echo (ping) reply id=0x0001, seq=71/18176, ttl=128 (request in 2)
4	12.626730	localhost	localho…	ICMP	64	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 5)
5	12.626904	localhost	localho…	ICMP	64	Echo (ping) reply id=0x0001, seq=72/18432, ttl=128 (request in 4)
6	13.641632	localhost	localho…	ICMP	64	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 7)
7	13.641806	localhost	localho…	ICMP	64	Echo (ping) reply id=0x0001, seq=73/18688, ttl=128 (request in 6)
8	14.651503	localhost	localho…	ICMP	64	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 9)
9	14.651712	localhost	localho…	ICMP	64	Echo (ping) reply id=0x0001, seq=74/18944, ttl=128 (request in 8)

d. Presente capturas de pantalla de filtros para paquetes UDP y TCP.

e. Aplique un filtro para presentar paquetes DNS con dirección de destino u origen (Con dominio o dirección debe ser escogida por el estudiante). El resultado puede ser similar al siguiente.

f. Indique cuantos paquetes TCP han sido generados. ¿Compare con la información de su compañero, y responda si es la misma cantidad? Comente sobre los resultados obtenidos. Compare con la información que recolectó en el punto 6.1.9, ¿qué puede concluir?

Esta información se puede encontrar en la parte inferior derecha como se muestra a continuación:



g. Indique cuantos paquetes ICMP han sido generados. ¿Compare con la información de su compañero, y responda si es la misma cantidad?, ¿qué puede concluir?

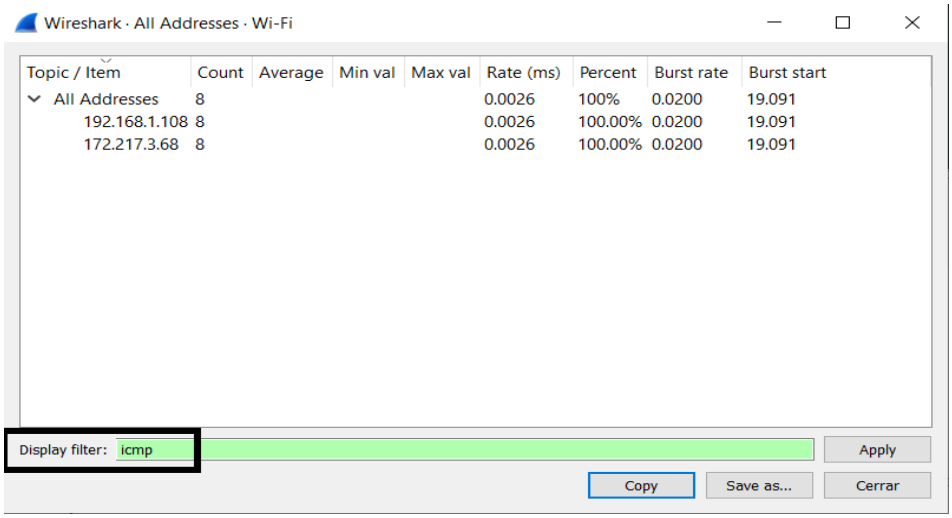
6.1.12. Wireshark posee un conjunto completo de herramientas que permiten obtener estadísticas de los paquetes, entre las cuales están: resúmenes, gráficas, jerarquías de protocolos, conversaciones, etc. Se accede a la mayoría de ellas a través de la opción del menú “Statistics”.

a. En el submenú escoger la opción “Packet Lengths”, se encuentra información similar a lo presentado a continuación. El “Display filter” debe estar configurado en ICMP.

Wireshark · Packet Lengths · Adapter for loopback traffic capture

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	30	113.00	64	206	0.0001	100%	0.0200	11.620
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	20	71.30	64	77	0.0001	66.67%	0.0200	11.620
80-159	2	158.00	158	158	0.0000	6.67%	0.0100	50.304
160-319	8	206.00	206	206	0.0000	26.67%	0.0100	68.777
320-639	0	-	-	-	0.0000	0.00%	-	-
640-1279	0	-	-	-	0.0000	0.00%	-	-
1280-2559	0	-	-	-	0.0000	0.00%	-	-
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

b. En el submenú escoger la opción “IPV4 Statistics” y escoja la opción “All Address”, se encuentra información similar a lo presentado a continuación. El “Display filter” debe estar configurado en ICMP.



c. Obtenga la siguiente información:
   Número de paquetes
   Tamaño promedio
   Tamaño minimo
   Tamaño máximo
   Velocidad (ms)

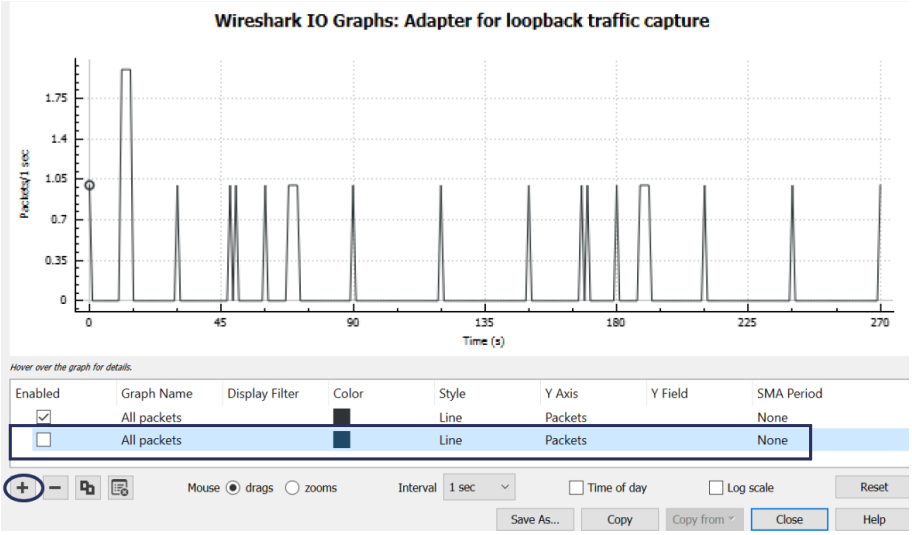
d. Analice la información obtenida en a y en b cual es la diferencia y para que utilizaría cada una de estas opciones.

e. Compare con la información recolectada por su compañero. ¿Qué puede concluir?

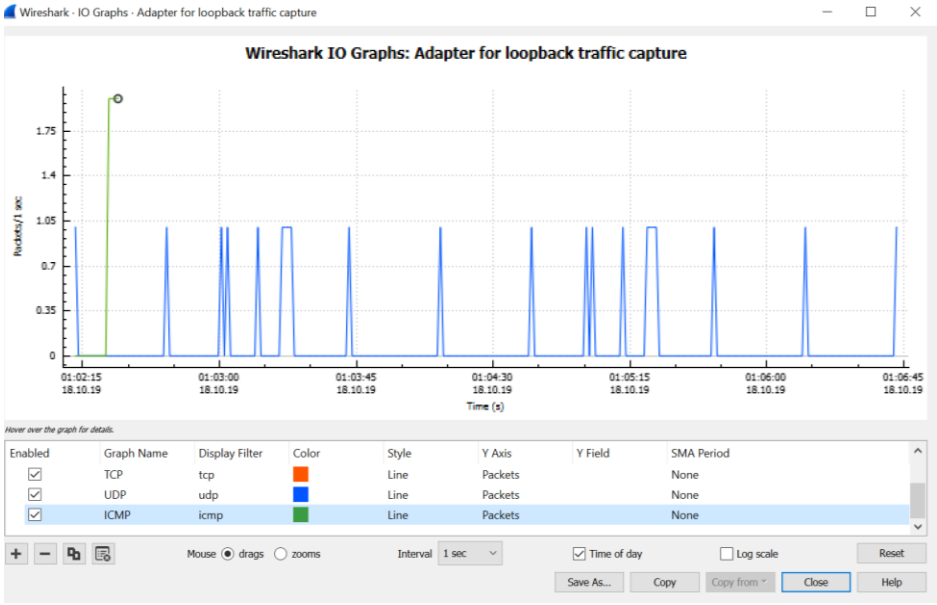
f. Aplicar el filtro TCP y obtenga la misma información del punto c.

6.1.13. Ahora veremos la opción gráficos, para lo cual, haga click en “Statistics” y a continuación escoja “IO Graph”.

a. Para crear filtros primero hacer click en el botón con signo más (+), aparecerá una sección en blanco como se muestra a continuación:



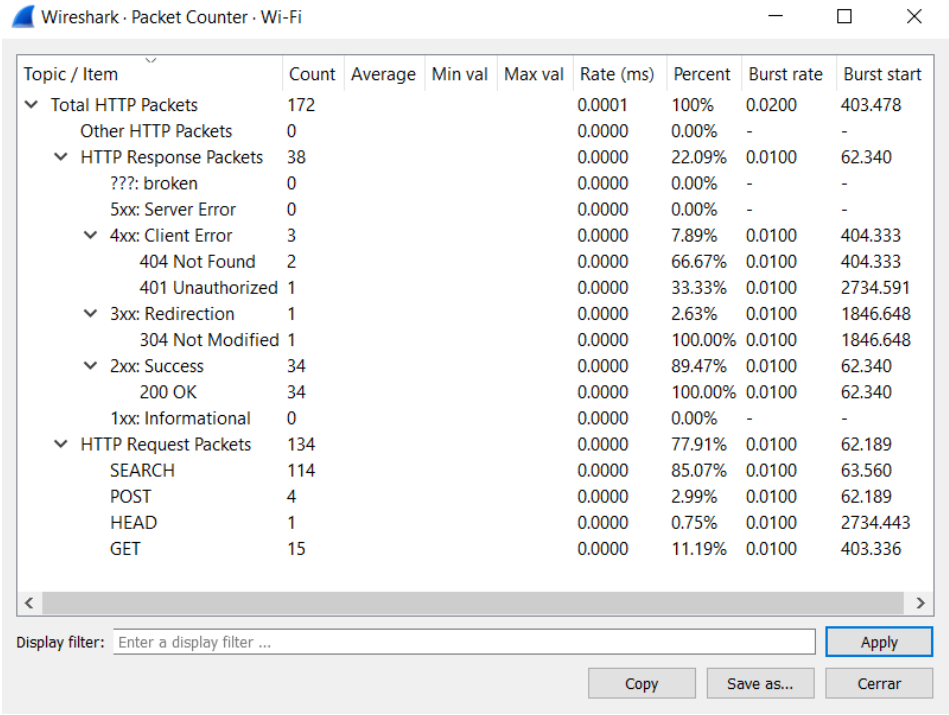
b. A continuación, llenar los campos “Graph Name” indicando el nombre de la gráfica, “Display Filter” indicando el filtro que se desea, en este caso obtener filtros para TCP, UDP e ICMP, y cambiar la propiedad “Color” para poder distinguir los filtros. Se obtendrá una grafica similar a la siguiente:



c. Compare su gráfica con la de su compañero, ¿qué puede concluir?

6.1.14. Ahora veremos las opciones de HTTP que nos proporcionan datos básicos para el análisis de páginas web.

a. Haga click en “Statistics” y a continuación escoja “HTTP” y “Packet Counter”

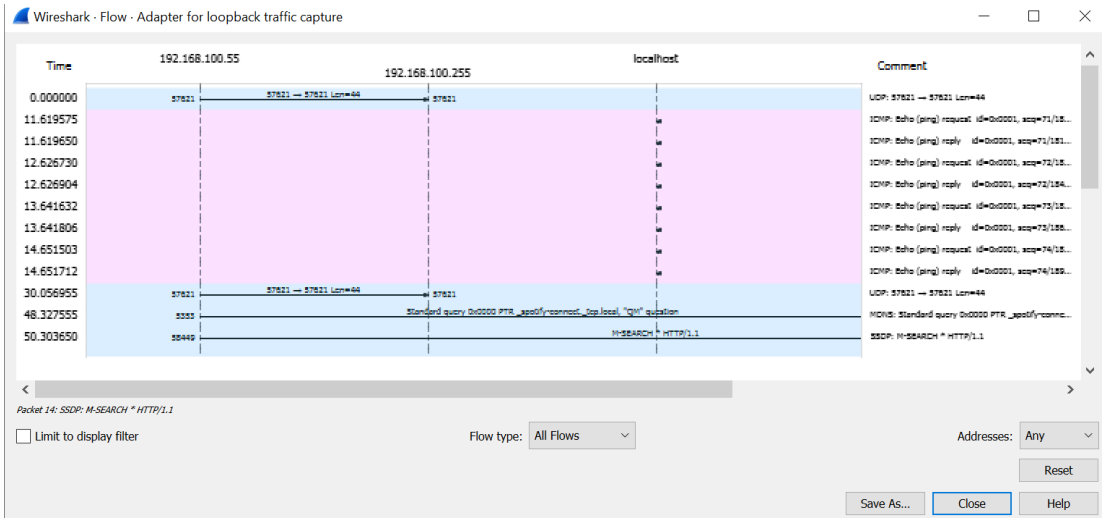


Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	172				0.0001	100%	0.0200	403.478
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	38				0.0000	22.09%	0.0100	62.340
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	3				0.0000	7.89%	0.0100	404.333
404 Not Found	2				0.0000	66.67%	0.0100	404.333
401 Unauthorized	1				0.0000	33.33%	0.0100	2734.591
3xx: Redirection	1				0.0000	2.63%	0.0100	1846.648
304 Not Modified	1				0.0000	100.00%	0.0100	1846.648
2xx: Success	34				0.0000	89.47%	0.0100	62.340
200 OK	34				0.0000	100.00%	0.0100	62.340
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	134				0.0000	77.91%	0.0100	62.189
SEARCH	114				0.0000	85.07%	0.0100	63.560
POST	4				0.0000	2.99%	0.0100	62.189
HEAD	1				0.0000	0.75%	0.0100	2734.443
GET	15				0.0000	11.19%	0.0100	403.336

b. Consulte que significa cada uno de los “Response Packets” obtenidos e interprete para que nos sirve este tipo de información.

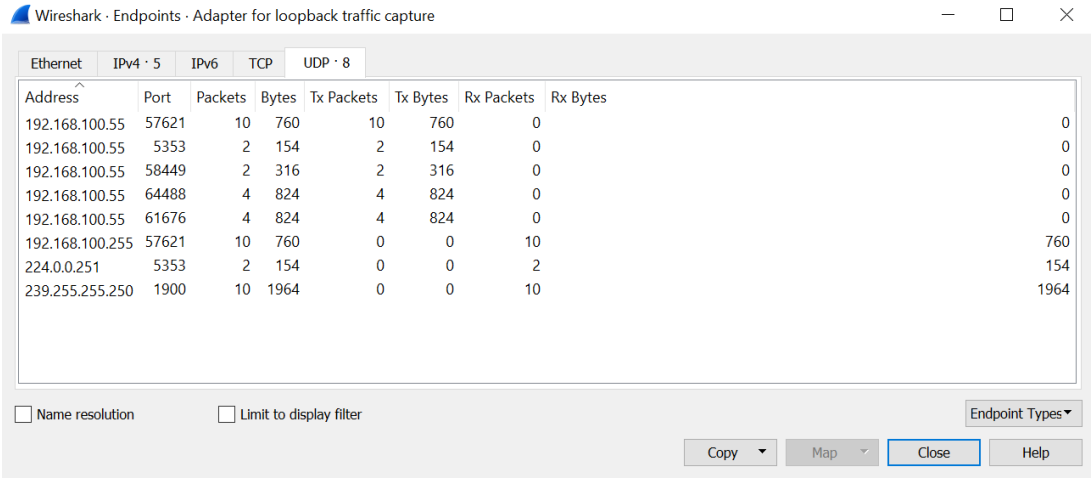
c. Registre los tipos de peticiones que fueron realizadas “HTTP Request Packets” y realice un cuadro comparativo en el que se indique cuáles son las diferencias entre cada una de estas peticiones.

6.1.15. Ahora veremos la opción gráfica de flujo, la cual permite ver el flujo de paquetes entre dos o más equipos, en orden cronológico. Esta opción es muy útil para entender el flujo de paquetes y poder hacer troubleshooting. Para acceder a esta opción vaya a “Statistics” y luego escoja “Flow Graph”, verá una ventana similar a la siguiente:



a. Compare la gráfica obtenida con la de su compañero, ¿qué puede concluir?

6.1.16. Finalmente veremos las gráficas de puntos finales (endpoints) tanto para TCP como para UDP. Para esto, escoja la opción “Statistics” y luego “Endpoints”, verá una ventana similar a la siguiente:



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.100.55	57621	10	760	10	760	0	0
192.168.100.55	5353	2	154	2	154	0	0
192.168.100.55	58449	2	316	2	316	0	0
192.168.100.55	64488	4	824	4	824	0	0
192.168.100.55	61676	4	824	4	824	0	0
192.168.100.255	57621	10	760	0	0	10	760
224.0.0.251	5353	2	154	0	0	2	154
239.255.255.250	1900	10	1964	0	0	10	1964

a. Podrá observar estadísticas de TCP en la viñeta “TCP:#” y de UDP en la viñeta “UDP:#”.

b. Recoja lo siguiente:
   Cantidad de paquetes UDP transmitidos
   Cantidad de bytes UDP transmitidos
   Cantidad de paquetes UDP recibidos
   Cantidad de bytes UDP recibidos
   Cantidad de paquetes TCP transmitidos
   Cantidad de bytes TCP transmitidos
   Cantidad de paquetes TCP recibidos
   Cantidad de bytes TCP recibidos

c. ¿Cuál es el tráfico más prominente recibido? TCP o UDP? ¿Cuál es el tráfico más prominente transmitido? TCP o UDP?

d. Compare con los resultados de su compañero. ¿Qué puede concluir?

7. INFORME

7.1. Consulte que información nos proporciona el menú de “Telephony” del Wireshark, y que utilidad nos brinda la esta información.

7.2. Consulte que información nos proporciona el menú de “Wireless” del Wireshark, y que utilidad nos brinda la esta información
7.3. Presentar las capturas de pantalla obtenidas del desarrollo de la práctica con la debida explicación de ser necesaria.
7.4. Responder a las preguntas presentadas en la práctica.
7.5. Conclusiones y Recomendaciones
7.6. Bibliografía.

8. REFERENCIAS

- Wireshark, “Wireshark Documentation”, http://www.wireshark.org/docs, [Online], revisado en 24/04/2017

Elaborado por: Ing. Víctor H. Reyes C. – Técnico Docente