

Informe Laboratorio 1: Captura y Análisis de Paquetes con Wireshark

Sección 1 Grupo 1

Paula Villaroel; Ezequiel Morales; Dylan Barahona
paula.villaroel@mail_udp.cl; ezequiel.morales@mail_udp.cl; dylan.barahona@mail_udp.cl

Septiembre de 2024

Índice

1. Equipos y materiales	2
2. Actividades	2
2.1. Identificación de su entorno de red, sus elementos y parámetros de configuración.	2
2.2. Captura de paquetes ping	7
2.3. Captura y análisis de TPDUs (Transport protocol data unit)	11
2.4. Captura de paquetes HTTP y HTTPS	14
3. Dificultades encontradas	18
4. Conclusiones	19

1. Equipos y materiales

El equipo utilizado para realizar esta experiencia de laboratorio corresponde al computador de Dylan Barahona.

Especificaciones:

CPU: AMD Ryzen 3 3300X

RAM: 16GB

OS: WINDOWS 10

Los materiales necesarios son tener un modem en fisico, en este caso sera utilizado el del integrante Dylan Barahona.

2. Actividades

2.1. Identificación de su entorno de red, sus elementos y parámetros de configuración.

Esta actividad le ayudará a identificar los distintos elementos que componen su infraestructura de red LAN (o WLAN - Wireless Local Area Network) al interior de su hogar y la configuración de los parámetros de red de los distintos equipos. Las actividades que debe realizar son:

1. Identifique físicamente el dispositivo denominado Router o MODEM. Tome una fotografía del equipo, indique su marca y modelo. Describa físicamente el dispositivo indicando los puertos LAN y/o WAN.

Respuesta: El modem que se dispone en mi hogar es el ARRIS TG2492LG-VTR. A continuación se muestra en la figura 1, el modelo del mismo:



Figura 1: Modelo del modem VTR



Figura 2: Puertos LAN, de telefonía y cable de cobre para canales, en el televisor.

Como se puede apreciar en la figura 2, se tienen 2 entradas para telefonía fija y 4 entradas para puertos LAN, el equipo no tiene ningún puerto WLAN. Por último se tiene una entrada tipo cobre para la señal digital de canales.

2. Indique el ISP (Internet service provider) contratado.

Respuesta: El ISP contratado es VTR

3. Indique el SSID (Service Set Identifier) de su WLAN.

Respuesta: El SSID se muestra representado en la figura 1. Por lo tanto el SSID es VTR-0526636

4. Identifique los parámetros de red su computador o dispositivo móvil conectado a la red. Debe indicar: dirección MAC, dirección IP, máscara de red, dirección IP del gateway y DNS.

2 ACTIVIDADES

Respuesta: Para esta actividad se considera el computador del integrante Dylan, y su respectivo celular. Luego se procede a indicar lo solicitado. También gran parte de la información se saco dentro de la pagina oficial de VTR, entrando a las configuraciones del modem, como se muestra a continuacion en los dispositivos conectados:

Lista de clientes Attached

Dirección IP	Nombre	Dirección MAC	Tipo	Expiración	Don't Steer
192.168.0.2	Dylan	00:D8:61:7A:1C: DA	Ethernet	2024-09-08 08:55:46.0 0	<input type="checkbox"/>
192.168.0.3	A34-de-Dylan	BA:EE:6D:95:DA: 63	Wireless 50	2024-09-08 08:55:55.0 0	<input type="checkbox"/>
2800:150:118:2668:39B4:2009:431: A3D8	A34-de-Dylan	BA:EE:6D:95:DA: 63	Wireless 50	0-00-00 00:00:00.00	<input type="checkbox"/>
2800:150:118:2668:B81A:CF06:BD6 9:42AC	Dylan	00:D8:61:7A:1C: DA	Ethernet	0-00-00 00:00:00.00	<input type="checkbox"/>
FE80::B8EE:6dff:FE95:DA63	A34-de-Dylan	BA:EE:6D:95:DA: 63	Wireless 50	0-00-00 00:00:00.00	<input type="checkbox"/>
FE80::EC9D:526E:23BB:BEB3	Dylan	00:D8:61:7A:1C: DA	Ethernet	0-00-00 00:00:00.00	<input type="checkbox"/>

Figura 3: Lista de clientes conectados, indica direccion IPv4, IPV6 y MAC

1) Computador:

Dirección MAC: 00:D8:61:7A:1C:DA

Direccion IPV4: 192.168.0.2

Direccion IPV6 (TEMPORAL): 2800:150:118:2668:B81A:CF06:BD69:42AC

Direccion IPV6 (VINCULO): FE80::EC9D:526E:23BB:BEB3

Para obtener la direccion IP del gateway y el DNS se tiene la siguiente figura, que a través de las configuraciones de red de windows se pueden obtener estos datos.

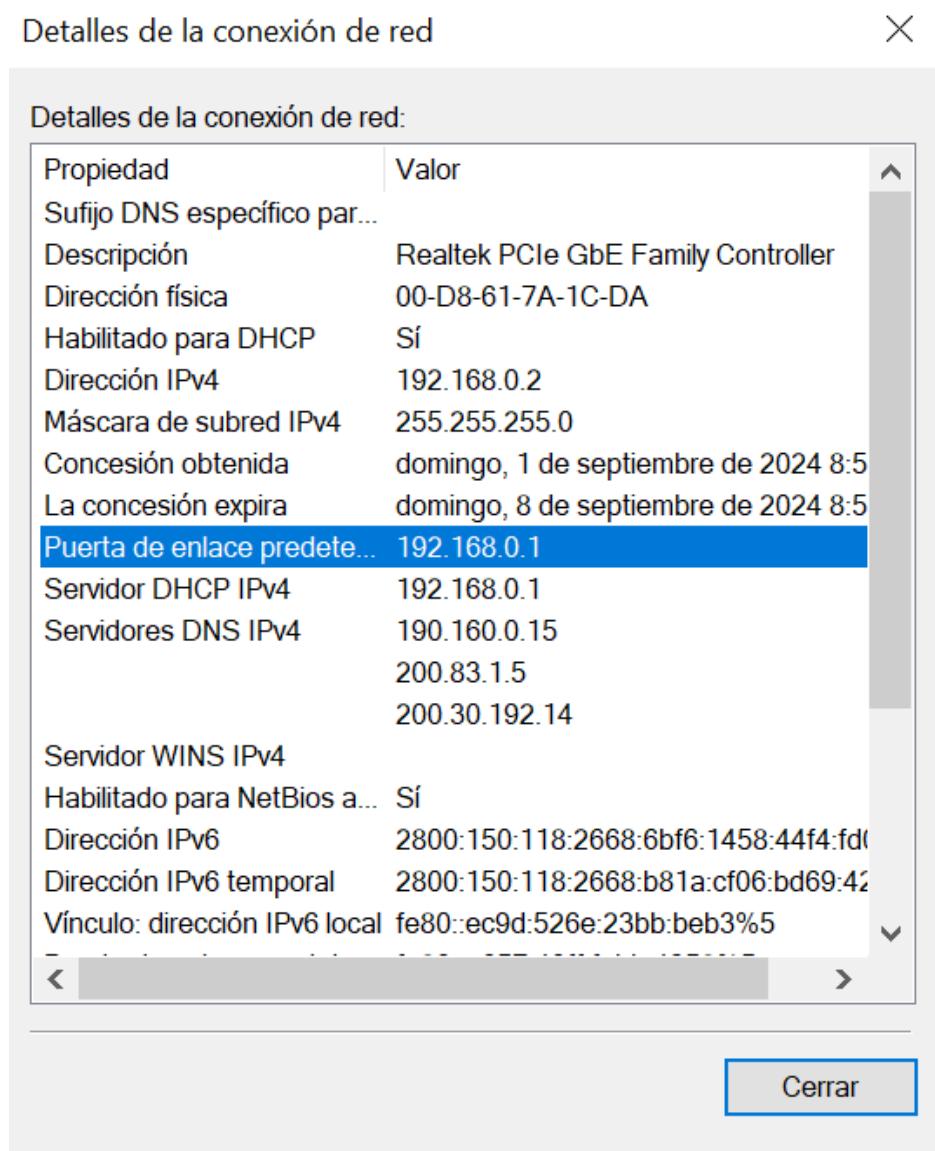


Figura 4: Informacion de la red

1) Computador:

DNS IVP4:

DNS 1 = 190.160.0.15

DNS 2 = 200.83.1.5

DNS 3 = 200.30.192.14

DNS IVP6:

DNS 1 = 2800:150:e:2::15

DNS 2 = 2800:150:e:4::5

DNS 3 = 2800:150:e:3::14

DNS 4 = 2800:150:e:2::15

DNS 5 = 2800:150:e:4::5

DNS 6 = 2800:150:e:3::14

Dirección IP gateway = 192.168.0.1

A continuacion se presentera lo solicitado, para el celular de Dylan (Samsung A34 5G), se utilizara la figura 3, para indicar las direcciones IP y MAC

2) Celular:

Dirección IPV4 = 192.168.0.2

Dirección IPV6 (TEMPORAL) = 2800:150:118:2668:39B4:2009:431:A3D8

Dirección IPV6 (VINCULO) = FE80::B8EE:6DFF:FE95:DA63

La dirección IP gateway se repite entre dispositivos conectados a la misma red, de igual manera pasa con el DNS ya que estos dos son proporcionados directamente por el ISP, luego:

Dirección IP gateway = 192.168.0.1

DNS IVP4:

DNS 1 = 190.160.0.15

DNS 2 = 200.83.1.5

DNS 3 = 200.30.192.14

DNS IVP6:

DNS 1 = 2800:150:e:2::15

DNS 2 = 2800:150:e:4::5

DNS 3 = 2800:150:e:3::14

DNS 4 = 2800:150:e:2::15

DNS 5 = 2800:150:e:4::5

DNS 6 = 2800:150:e:3::14

Para obtener la MAC del celular se usa la figura 3:

MAC = BA:EE:6D:95:DA:63

Por ultimo es posible obtener la MAC asociada al router eso usando el comando arp -a en cmd y sabiendo nuestra IP Gateway, como la IP Gateway es 192.168.0.1, anteriormente mencionada.

La MAC del router es: e4:57:40:bb:43:58

5. Realice el diagrama de la topología lógica de su red. Para esto debe identificar los distintos equipos o dispositivos conectados a la red indicando su dirección IP y MAC.

Respuesta: A continuacion en la figura 5 se muestra el diagrama de red.

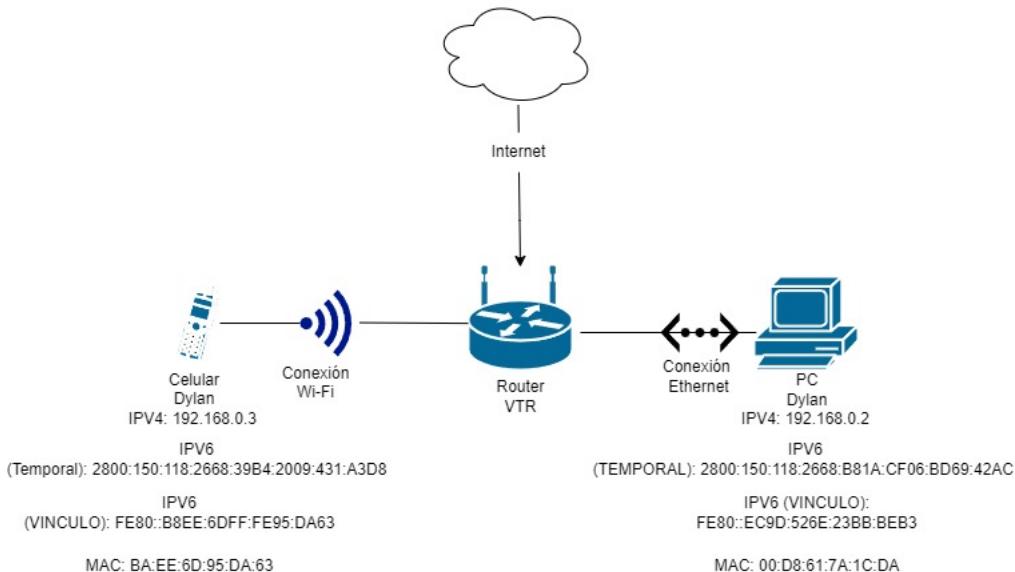


Figura 5: Diagrama de red local del integrante Dylan Barahona.

Es importante señalar que la topología en particular es de estrella. También el ISP proporciona direcciones IPV6 temporales, es por ello que se indica la dirección IPV6 como temporal, al momento de realizar el informe esa es la dirección IPV6 del momento. Respecto a las IPV4 estas son dinámicas, variando la cantidad de dispositivos conectados. Por último la MAC del celular es aleatoria.

2.2. Captura de paquetes ping

En esta actividad Ud. deberá generar y capturar paquetes del tipo ping (protocolo ICMP). Para realizar esto usted deberá abrir una ventana de consola o CMD. A continuación deberá tipar el comando `$ ping www.google.com` y comenzar inmediatamente la captura en Wireshark una vez que tenga suficientes paquete ping capturados detenga la captura y responda lo siguiente:

- Indique el filtro utilizado para desplegar los mensajes del tipo "ping".

Respuesta: En el programa Wireshark se utilizó el siguiente filtro para obtener los ping:
`"(icmpv6 && ipv6.dst == 2800:150:118:2668:b81a:cf06:bd69:42ac) |||(icmpv6&&ipv6.src == 2800 : 150 : 118 : 2668 : b81a : cf06 : bd69 : 42ac)"`

A continuación se muestra una captura de los paquetes protocolo ICMPV6 junto con el filtro, indicado anteriormente:

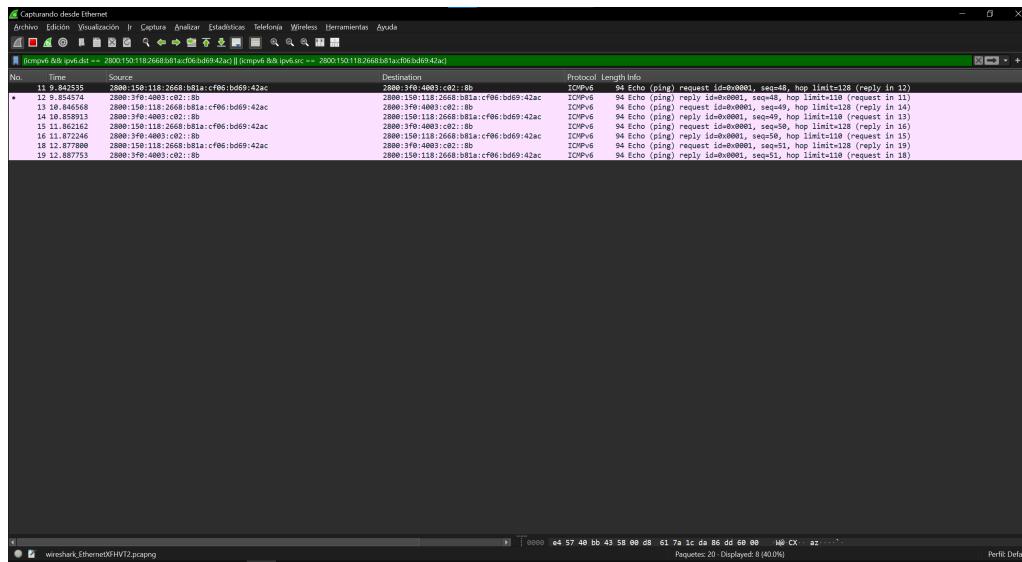


Figura 6: Captura de paquetes PING a través del protocolo ICMPV6 en WireShark

2. ¿Cuántos paquetes del tipo "ping" ha capturado?. Respuesta: En este caso se han capturado 8 paquetes en total. 4 de solicitud, 4 de respuesta.
3. ¿Cuáles son las direcciones MACs de origen y destino de los frames?.

Para los paquetes de request:

Mac Origen: 00:d8:61:7a:1c:da Mac Destino: e4:57:40:bb:43:58

Para los paquetes de reply:

Mac Origen: e4:57:40:bb:43:58 Mac Destino: 00:d8:61:7a:1c:da

A continuacion imagenes de las mac de request y reply:

Request:

```
▶ Frame 11: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
└─ Ethernet II, Src: MicroStarINT_7a:1c:da (00:d8:61:7a:1c:da), Dst: ARRISGroup_bb:43:58 (e4:57:40:bb:43:58)
    └─ Destination: ARRISGroup_bb:43:58 (e4:57:40:bb:43:58)
    └─ Source: MicroStarINT_7a:1c:da (00:d8:61:7a:1c:da)
        Type: IPv6 (0x86dd)
        [Stream index: 3]
    └─ Internet Protocol Version 6, Src: 2800:150:118:2668:b81a:cf06:bd69:42ac, Dst: 2800:3f0:4003:c02::8b
    └─ Internet Control Message Protocol v6
```

Figura 7: MAC origen y destino paquetes request

Reply:

```
▶ Frame 12: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
└─ Ethernet II, Src: ARRISGroup_bb:43:58 (e4:57:40:bb:43:58), Dst: MicroStarINT_7a:1c:da (00:d8:61:7a:1c:da)
    └─ Destination: MicroStarINT_7a:1c:da (00:d8:61:7a:1c:da)
    └─ Source: ARRISGroup_bb:43:58 (e4:57:40:bb:43:58)
        Type: IPv6 (0x86dd)
        [Stream index: 3]
    └─ Internet Protocol Version 6, Src: 2800:3f0:4003:c02::8b, Dst: 2800:150:118:2668:b81a:cf06:bd69:42ac
    └─ Internet Control Message Protocol v6
```

Figura 8: MAC origen y destino paquetes reply

4. Realizando un estudio de las direcciones MAC capturadas, ¿reconoce alguna de ellas?.

Respuesta: Haciendo un análisis de las figuras 7 y 8, note que la MAC: e4:57:40:bb:43:58 corresponde a la del modem VTR, esto también se indica pues en el wireshark sale como ARRIS-Group, dando a entender claramente que es el modem. Para la mac: 00:D8:61:7A:1C:DA, note que esta corresponde a la mac del computador, en este caso se señala a la compañía MSI, la cual es la marca de mi placa madre, y por tanto a la tarjeta de red integrada a la placa madre.

5. ¿Cuáles son las direcciones IPs de origen y destino de esos paquetes?. ¿Cuál es la dirección IP del servidor?. ¿Cuál es la dirección IP de su computador?. Respuesta:

Para cada paquete request y reply, se tendrá las direcciones de origen y destino invertidos, esto es claro, ya que si yo me comunico con A hacia B en forma de request, B debe confirmarme la comunicación desde B hacia A como una reply.

Habiendo hecho esa analogía se indica las direcciones de destino y origen, primero para los paquetes request, utilizaremos la figura 6, para ello:

Origen: 2800:150:118:2668:B81A:CF06:BD69:42AC

Destino: 2800:3f0:4003:c02::8b

Paquetes reply:

Origen: 2800:3f0:4003:c02::8b

Destino: 2800:150:118:2668:B81A:CF06:BD69:42AC

Note que la dirección 2800:150:118:2668:B81A:CF06:BD69:42AC corresponde a la IPV6 del computador de Dylan, por lo tanto esta es la ip del computador y la otra 2800:3f0:4003:c02::8b corresponde a la IP del servidor, en este caso de la compañía de Google.

6. ¿Qué protocolo utiliza el comando "ping".

Respuesta: El comando ping utiliza el protocolo ICMP, este puede estar en sus versiones IMPV4 o IMPV6, depende netamente del equipo y la configuración del router, en este caso para Dylan utiliza IMPV6 ya que tiene asociada una IPV6.

7. Indique el tamaño (en Bytes) del paquete.

Respuesta: El tamaño de los paquetes es de 94 Bytes, revisar figura 6

8. Realice una inspección en el campo de datos del "ping". Indique su contenido.

Respuesta: Se tiene la siguiente figura

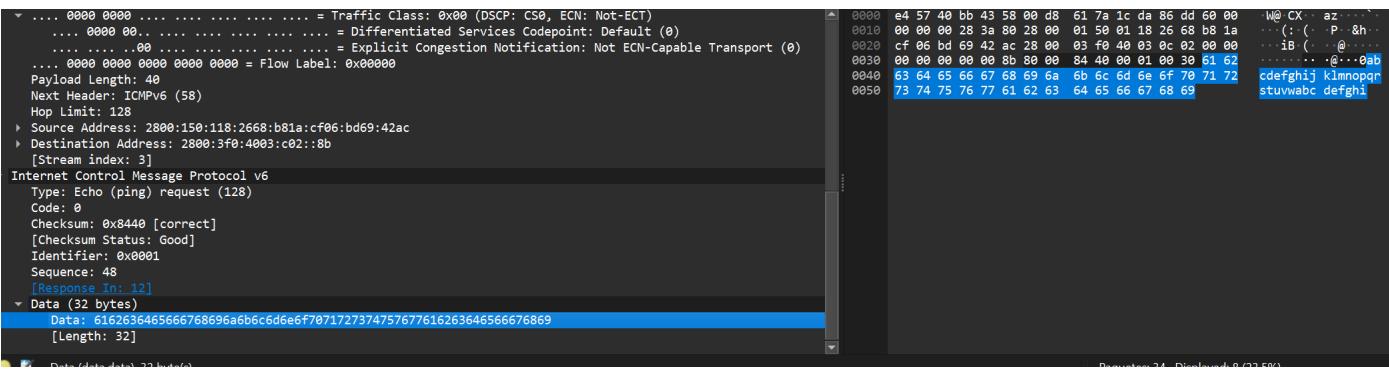


Figura 9: Contenido del ping

Observe que lo que realmente se esta mandando entre origen y destino es una cadena de caracteres de 32 de largo, el string que se esta mandando es el: ".abcde...ijklmnopqrstuvwxyz", note que en data eso si se tiene el siguiente numero: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869 Lo que significa esto es que cada numero en hexadecimal corresponde a una letra en el codigo ASCII, por ejemplo 61 en hexadecimal haciendo la transformacion en decimal es 97 y eso corresponde a la letra 'a' justamente la que aparece al principio del string.

- Explique el funcionamiento del "ping".^eindique cuáles son las principales razones de su uso.

Respuesta:

Por lo aprendido en esta sección el ping funciona de la siguiente manera:

- A través de la dirección IPV6 del computador y la MAC de la tarjeta de red se realiza una petición en forma de string al modem a través de su MAC, el modem acepta esta solicitud y la envía a la IPV6 del servidor de destino.
- Luego de enviar la solicitud a la IPV6 del servidor de destino, la IPV6 acepta la solicitud y reenvia la respuesta string hasta llegar a la MAC del modem, finalmente el modem envía la respuesta string al computador a través de la IPV6 y su MAC.
- Finalmente de obtener la respuesta se indica el tiempo en el que se logró esto generalmente utilizando la unidad milisegundos
- Esto se va repitiendo dependiendo de cuantas solicitudes haga el usuario a través de la terminal cmd.

Es importante que durante todo este proceso el protocolo a utilizar sera el ICMP en sus versiones 4 o 6 dependiendo del equipo en cuestión y la configuración del modem.

Las principales funciones y razones de usar la función ping, es: uno, saber si estamos conectados a internet, ya que como se necesita obtener una respuesta del servidor, en caso de no llegar esta, puede ser que no estemos conectados a internet.

Dos, nos permite saber si una página en cuestión o servidor está operativo, ya que de mandar una solicitud y no tener respuesta, puede ser que el sitio no exista, o bien ya no se encuentre operativo.

Tres, nos permite saber si estamos perdiendo paquetes, es decir nuestro internet esta inestable, si mandamos paquetes asegurandonos de que realmente estemos conectados a internet, pero no obtengamos reply, probablemente estemos perdiendo paquetes.

Cuatro, nos permite saber el tiempo de respuesta entre nuestra conexión y un destino determinado.

Esas serian las principales razones de usar ping.

2.3. Captura y análisis de TPDUs (Transport protocol data unit)

Esta actividad tiene por objetivo la captura y el análisis de segmentos y datagramas TCP y UDP. Los protocolos TCP y UDP están definidos en la capa de transporte y sirven de apoyo a la transmisión de los datos generados en la capa de aplicación. En esta actividad usted deberá ejecutar o correr aplicaciones de red que utilicen el protocolo de transporte UDP y TCP.

Es importante mencionar antes de comenzar la actividad que la IPV6 del equipo de Dylan cambio, esto se debio a que se le fue el internet por unos segundos, y después le volvio, como su ISP le asigna IPV6 temporales por nueva conexion, se le asigna otra nueva.

Dicho eso la nueva IPV6 del equipo de Dylan es:

IPV6 = 2800:150:118:2668:8d3c:48e8:873b:33

Lo demás sigue siendo lo mismo expuesto en la anterior actividad, las MAC no cambian pues son unicos y el DNS es unico de VTR.

En el caso de la IPV4 sigue siendo la misma tambien: **192.168.0.2**

Con eso dicho comienza la actividad.

- Ejecute alguna aplicación de red y realice la captura de datagramas UDP. Nota: debe indicar la aplicación utilizada además del filtro de despliegue.

Respuesta: La aplicación de red que se ejecutara será Google Chrome, se reproducira un video de una canción (si desea escucharla le dejo el link, sino pues no la escuche):

<https://youtu.be/rnYodiJO6k?si=PZ9io-VcK39iyfE6>

El filtro usado es udp

- Seleccione uno de los datagrama y complete la tabla con la información solicitada. Respuesta: Se muestra la siguiente figura en la cual se selecciono un paquete protocolo UDP, a través de Google Chrome y Youtube.

origen / destino	protocolo	destino	origen	protocolo	destino	origen	protocolo	destino
6305 70.716816	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	1292 443 → 65310 Len=1230				
6306 70.717842	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	88 443 → 53082 Len=26				
6307 70.722840	2800:150:118:2668:8d3c:48e8:873b:33	2800:3f0:4003:c00::5b	UDP	95 53082 → 443 Len=33				
6308 70.722820	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	92 443 → 53082 Len=30				
6309 70.728873	2800:150:118:2668:8d3c:48e8:873b:33	2800:3f0:4003:c00::5b	UDP	95 53082 → 443 Len=33				
6310 70.730321	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	138 443 → 53082 Len=76				
6311 70.730555	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	85 443 → 53082 Len=23				
6312 70.737448	2800:150:118:2668:8d3c:48e8:873b:33	2800:3f0:4003:c00::5b	UDP	99 53082 → 443 Len=37				
6313 70.749265	2800:3f0:4003:c00::5b	2800:150:118:2668:8d3c:48e8:873b:33	UDP	88 443 → 53082 Len=26				

Figura 10: Datagrama Protocolo UDP WireShark

Se selecciona el datagrama el cual esta destacado con negro.

Se procede a llenar la tabla:

Capa Modelo	Campo	Valor del Campo
Capa de Enlace	Dirección MAC de Destino	00:d8:61:7a:1c:da
	Dirección MAC de Origen	e4:57:40:bb:43:58
	FCS	False
Capa de Transporte	Protocolo IP	Solo IPV6
	Dirección IP de Destino	2800:150:118:2668:8d3c:48e8:873b:33
	Dirección IP de Origen	2800:3f0:4003:c00::5b
	Protocolo de Transporte	UDP
	Número de Puerto de Destino	65310

2. De la misma manera ejecute alguna aplicación de red y realice la captura de segmentos TCP.
 Nota: debe indicar la aplicación utilizada además del filtro de despliegue.

Respuesta: Se realizara el mismo experimento que con los paquetes UDP, se abrirá Google Chrome y se reproducirá la canción anteriormente mencionada en YouTube. El filtro a usar será TCP.

3. Seleccione uno de los segmentos y complete la tabla con la información solicitada.

Respuesta: Se muestra la siguiente figura para los paquetes TCP.

287 47.875841	2800:150:118:2668:8d3c:48e8:873b:33	2800:3f0:4003:c02::bc	TCP	75 [TCP Keep-Alive] 59625 + 5228 [ACK] Seq=1 Ack=1 Win=1025
288 47.888084	2800:3f0:4003:c02::bc	2800:150:118:2668:8d3c:48e8:873b:33	TCP	86 [TCP Keep-Alive ACK] 5228 → 59625 [ACK] Seq=1 Ack=2 Win=1025
290 48.313735	192.168.0.2	104.18.41.33	TCP	55 [TCP Keep-Alive] 60169 → 443 [ACK] Seq=1 Ack=1 Win=1025
291 48.326139	104.18.41.33	192.168.0.2	TCP	66 [TCP Keep-Alive ACK] 443 → 60169 [ACK] Seq=1 Ack=2 Win=1023
292 48.728129	2800:150:118:2668:8d3c:48e8:873b:33	2603:1030:48c:e::	TCP	75 62539 → 443 [ACK] Seq=1 Ack=1 Win=1023 Len=1
293 48.851163	2603:1030:48c:e::	2800:150:118:2668:8d3c:48e8:873b:33	TCP	86 443 → 62539 [ACK] Seq=1 Ack=2 Win=7201 Len=0 SRE=1
335 53.804311	192.168.0.2	34.120.52.64	TCP	55 [TCP Keep-Alive] 59932 → 443 [ACK] Seq=1 Ack=1 Win=1025
336 53.816124	34.120.52.64	192.168.0.2	TCP	66 [TCP Keep-Alive ACK] 443 → 59932 [ACK] Seq=1 Ack=2 Win=1025
340 54.976493	2800:150:118:2668:8d3c:48e8:873b:33	2606:4700::6811:2069	TCP	75 [TCP Keep-Alive] 60170 → 443 [ACK] Seq=1 Ack=1 Win=1025
341 54.990227	2606:4700::6811:2069	2800:150:118:2668:8d3c:48e8:873b:33	TCP	86 [TCP Keep-Alive ACK] 443 → 60170 [ACK] Seq=1 Ack=2 Win=1025

Figura 11: Datagrama protocolo TCP WireShark

Se selecciona el datagrama que está destacado en negro y se procede a llenar la tabla:

Capa Modelo	Campo	Valor del Campo
Capa de Enlace	Dirección MAC de Destino	00:d8:61:7a:1c:da
	Dirección MAC de Origen	e4:57:40:bb:43:58
	FCS	False
Capa de Transporte	Protocolo IP	IPV4 y IPV6
	Dirección IP de Destino	2800:150:118:2668:8d3c:48e8:873b:33
	Dirección IP de Origen	2800:3f0:4003:c00::5b
	Protocolo de Transporte	TCP
	Número de Puerto de Destino	59625

4. Investigue cuáles son las principales diferencias existentes entre los protocolos TCP y UDP.

Respuesta: La principal diferencia entre el protocolo TCP y UDP, tiene que ver con la rapidez y confiabilidad de la transmisión. Mientras que el protocolo TCP tiene una transmisión

confiable, es decir, se asegura que los paquetes sean recibidos, y en caso de que no sea así, se puedan retransmitir, sin embargo esto hace que los paquetes TCP sean muchísimo más lentos, ya que tienen que asegurar esta confiabilidad de recepción y respuesta, mientras tanto los paquetes a través de protocolos UDP no tiene una transmisión confiable, pues se envían montones de paquetes y no se asegura si estos fueron correctamente enviados, para UDP lo importante es hacer llegar la información de la manera más rápida, no de fiarse en la confiabilidad de la transmisión.

Por ende se tienen las siguientes fortalezas y debilidades:

TCP:

Fortalezas:

Excelente protocolo para transmitir información sensible que se necesita asegurarse de que sea confiable y llegue de manera completa.

Excelente protocolo para establecer comunicaciones en forma de conexiones.

Mucho más seguro en términos de la seguridad de la información que UDP

Gran comprobación de errores

Mecanismos de retransmisión de información ante errores

Debilidades:

Lentitud para transmitir la información

Necesita sí o sí una conexión preestablecida para transmitir la información

UDP:

Fortalezas:

Gran rapidez para transmitir información

No necesita una conexión preestablecida para transmitir la información

Debilidades:

Debido a la poca confiabilidad que existe en la transmisión y en la nula comprobación de errores existe una probabilidad de perder información.

No tiene mecanismos para retransmitir la información en caso de pérdida de la misma.

En general es más inseguro que TCP

Por último se puede decir que utilizar cada protocolo depende netamente de la actividad que se desea realizar, por ejemplo para videojuegos y servicios de streaming UDP es una buena opción por la rapidez en la que se necesita la información. Para tareas como, enviar correos electrónicos, mandar archivos por la web, entre otros, es mejor el protocolo TCP por la confiabilidad que da para transmitir toda la información y de manera más segura que UDP.

2.4. Captura de paquetes HTTP y HTTPS

Los protocolos HTTP y HTTPS son protocolos definidos en la capa de aplicación. Estos protocolos de comunicación permiten la transferencia de información a través de archivos del tipo HTML. Estas aplicaciones de red presentan un esquema del tipo cliente/servidor. El servidor (se le suele llamar un servidor web) le envía un mensaje de respuesta a los clientes. Ejemplos de cliente son los navegadores web o browsers.

1. Para iniciar la captura de mensajes HTTP primero deberá encontrar un servidor web HTTP. Una vez identificado dicho servidor realice una conexión y comience la captura de mensajes. Una vez terminada la sesión seleccione un filtro de despliegue e indique: ¿cuántos paquetes ha capturado?. ¿Cuáles son las direcciones IP de origen y destino de esos paquetes?. ¿Cuáles son los puertos de origen y destino?.

Respuesta: El sitio web HTTP que se encontró y se utilizó es el siguiente: <http://httpforever.com/>

Se pudieron capturar los siguientes paquetes HTTP entrando a esa página web, como se muestra en la figura:

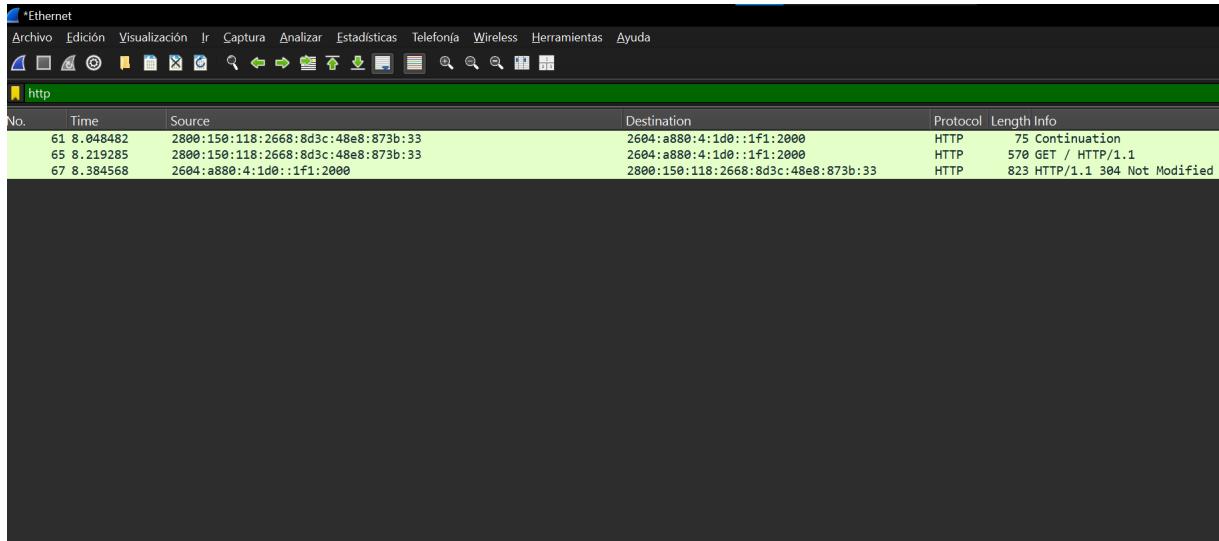


Figura 12: Paquetes HTTP capturados por Wireshark

Se pudieron capturar en total 3 paquetes.

Las direcciones de destino y origen dependen si el paquete es una request o una reply.

Para el caso de una request se tiene:

IPv6 Origen: 2800:150:118:2668:8d3c:48e8:873b:33 IPv6 Destino: 2604:a880:4:1d0::1f1:2000

Para el caso de una reply se tiene:

IPv6 Origen: 2604:a880:4:1d0::1f1:2000 IPv6 Destino: 2800:150:118:2668:8d3c:48e8:873b:33

Los puertos de origen y destino son específicamente:

Si es una request:

Puerto Origen: 60513

Puerto Destino: 80

Si es una reply:

Puerto Origen: 80

Puerto Destino: 60513

Note que el puerto de una petición HTTP siempre tiene el 80 por defecto.

- Utilice la herramienta de Wireshark para extraer el flujo de datos establecido en una sesión TCP. Para esto seleccione ".Analyze" del menú principal y luego seleccione "Follow HTTP Stream". Describa el tipo de información desplegada.

Respuesta:

En la siguiente figura, se muestra los datos que se lograron extraer de una solicitud http del sitio anteriormente mencionado

```

GET / HTTP/1.1
Host: httpforever.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 22 Mar 2023 14:54:48 GMT
If-None-Match: W/"642b1b5b-1040"
Priority: u=0, i

HTTP/1.1 304 Not Modified
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 01 Sep 2024 19:35:19 GMT
Last-Modified: Wed, 22 Mar 2023 14:54:48 GMT
Connection: keep-alive
Etag: "642b1b5b-1040"
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
Content-Security-Policy: default-src 'self'; script-src cdnjs.cloudflare.com 'self'; style-src cdnjs.cloudflare.com 'self' fonts.googleapis.com 'unsafe-inline'; font-src fonts.googleapis.com fonts.gstatic.com cdnjs.cloudflare.com 'self'; font-variant-axes-ancestors 'none'; report-uri https://scottelme.report-uri.com/r/d/csp/enforce"
me-ancestors 'none'; report-uri https://scottelme.report-uri.com/r/d/csp/enforce"

```

Figura 13: Datos extraídos de un paquete protocolo HTTP con Wireshark

Se muestran datos tales como el servidor donde esta alojado el cual parece ser una plataforma de Linux, en este caso Ubuntu.

Se muestran datos la ultima modificación que se hizo en el sitio web, la cual fue el Miércoles 23 de Marzo del año 2023

Se muestran algunas configuraciones del sitio, que no es necesario solicitar el acceso a la camara, micfrono, entre otros.

Los otros datos en rojo corresponden a los datos donde se realizo la solicitud la cual seria mi computador, se realizo la solicitud a través del navegador Mozilla Firefox, los lenguajes aceptados el cual uno de ellos es es-CL dando cuenta que podria uno inferir que el navegador del que realizo la solicitud es de Chile.

Se indica tambien que se realizo una solicitud insegura en este caso catalogado con un 1.

3. De la misma manera, para iniciar la captura de mensajes HTTPS primero deberá encontrar un servidor web HTTPS. Una vez identificado dicho servidor realice una conexión y comience la captura de los mensajes. Una vez terminada la sesión seleccione un filtro de despliegue e indique: ¿cuántos paquetes ha capturado?. ¿Cuáles son las direcciones IP de origen y destino de esos paquetes?. ¿Cuáles son los puertos de origen y destino?.

Respuesta: Se utilizara el sitio oficial de GitHub para capturar paquetes HTTPS. Se pudieron capturar los siguientes paquetes como muestra la siguiente figura:

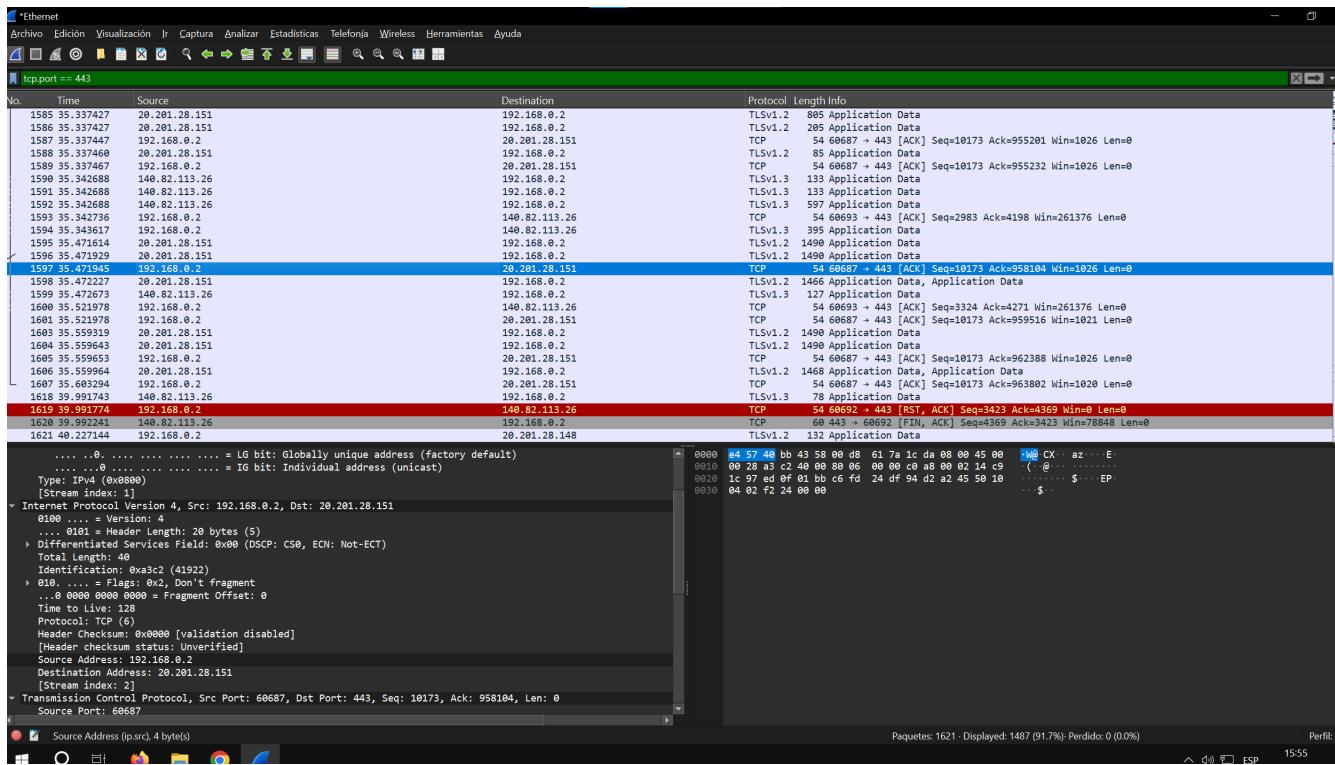


Figura 14: Datos extraidos de un paquete protocolo HTTPS con Wireshark

Se pudieron capturar aproximadamente 1600 paquetes, lo cual es bastante.

La dirección ip de origen y destino depende si es una request o una reply.

En el caso de request:

IP ORIGEN: 192.168.0.2 (La del equipo)

IP DESTINO: 20.201.28.151 (Corresponde A GitHub Sao Paulo, Brasil)

En el caso de una reply:

IP ORIGEN: 20.201.28.151

IP DESTINO: 192.168.0.2

Note que en el caso del sitio web de GitHub se trabaja con la IPV4.

Los puertos de origen y destino tambien varian dependiendo de si es una request o una reply.

En el caso de una request:

Puerto Origen: 60687

Puerto Destino: 443

En el caso de una reply:

Puerto Origen: 443

Puerto Destino: 60687

Note que los protocolos HTTPS siempre tienen como puerto el 443, incluso hubo que utilizar el filtro tcp.port == 443 para poder analizar solicitudes del protocolo HTTPS

4. Utilice la herramienta de Wireshark para extraer el flujo de datos establecido en una sesión TCP. Para esto seleccione "Analyze" del menú principal y luego seleccione "Follow TCP Stream". Describa el tipo de información desplegada.

Respuesta:

A continuacion se presenta la siguiente figura que muestra los datos de una peticion en protocolo HTTP.



3 DIFICULTADES ENCONTRADAS

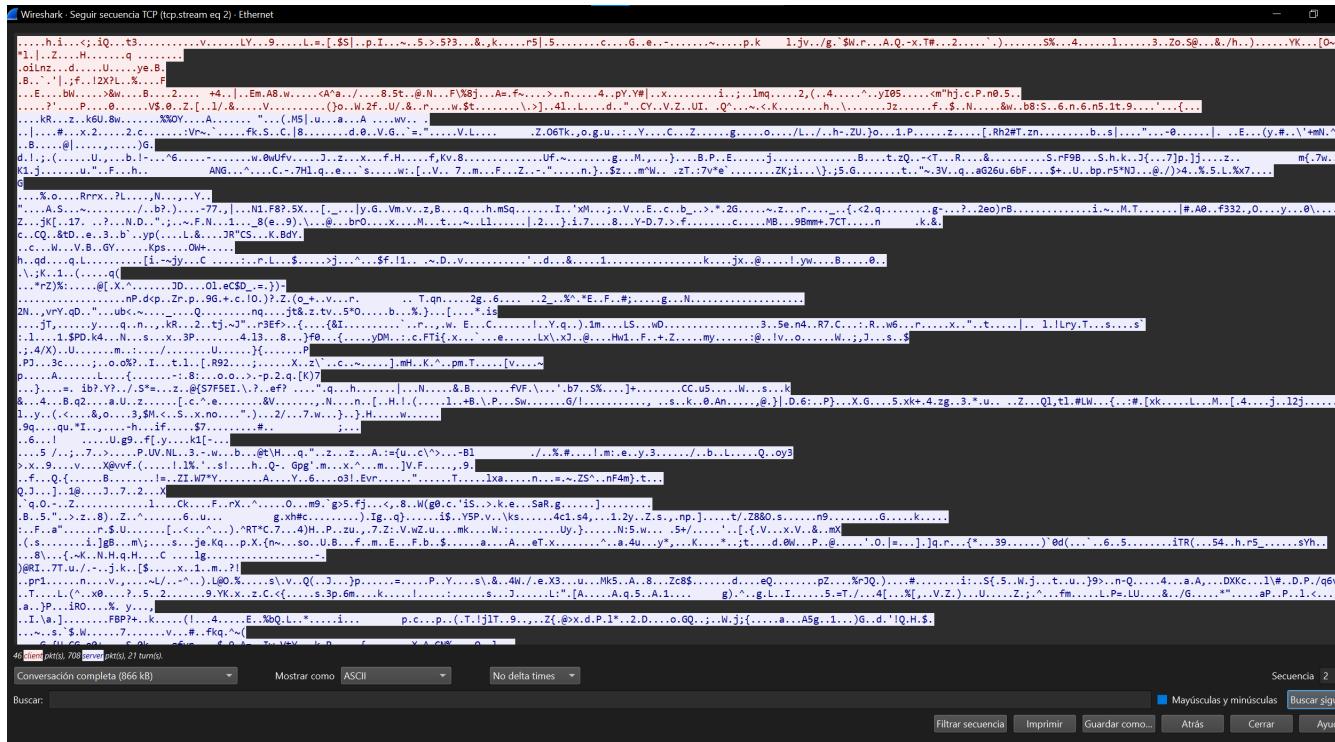


Figura 15: Datos extraídos de un paquete protocolo HTTPS con Wireshark

Note que la información obtenida esta totalmente cifrada, por lo cual es ilegible, dando cuenta que el protocolo HTTPS esta protegido a diferencia del protocolo HTTP.

5. Indique las principales diferencias entre los protocolos HTTP y HTTPS.

Respuesta: Note que la principal diferencia entre los protocolos HTTP y HTTPS viene en base a la seguridad de la información.

Mientras que HTTP esta escrito en texto plano y es posible interceptar los paquetes para ser leidos con un "sniffer" como WireShark. HTTPS esta totalmente cifrado y aunque puedan ser interceptados los paquetes con un sniffer estos apareceran totalmente ilegibles.

3. Dificultades encontradas

La mayor dificultad que se presento en el laboratorio fue que al pasar de la actividad 2.1 (ping) a la actividad 2.2 (analisis de paquetes TCP/UDP) la direccion IPV6 del equipo de Dylan cambio por lo tanto hubo que reestructurar todo para realizar la actividad de la 2.2, volver a indicar la IPV6, concluir acerca de las MAC'S entre otro. Otra dificultad que se presento es la nula experiencia que se tiene con el "sniffer" WireShark por lo tanto costo al principio lograr capturar los paquetes ICMPV6.

4. Conclusiones

En este laboratorio se tuvo un primer acercamiento al capturamiento de paquetes a través del sniffer Wireshark, se aprendió mucho mejor acerca del protocolo ICMP propio de los ping, además de entender la naturaleza de los mismos y para qué casos es utilizado, también se aprendió sobre los protocolos TCP y UDP de mejor manera a través de sus diferencias, fortalezas y debilidades. Por último también se aprendió mucho más acerca de los protocolos HTTP y HTTPS, contrastando cada uno en términos de seguridad de la información.