Informe Laboratorio 1: Análisis y Captura de Paquetes usando Wireshark

Sección 1

Benjamín Morales Pizarro
e-mail: benjamin.morales3@mail.udp.cl

14 abril de 2022

Índice

1. Equipos y materiales

A continuación se utiliza la herramienta Wireshark para analizar y capturar paquetes a través de la red desde mi computadora, la cual está conectada a internet mediante un cable Ethernet.

2. Desarrollo de las actividades

```
C:\Users\benja>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : benjamin
   Sufijo DNS principal  . . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Killer E2400 Gigabit Ethernet Controller
   Dirección física. . . . . . . . . . . . . : 4C-CC-6A-0C-22-7A
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::51e4:56a1:92b8:de0e%15(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.100(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : martes, 12 de abril de 2022 9:37:22
   La concesión expira . . . . . . . . . . . : martes, 12 de abril de 2022 18:46:35
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 105696362
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-29-6A-70-BE-4C-CC-6A-0C-22-7A
   Servidores DNS. . . . . . . . . . . . . . : 200.28.4.129
                                       200.28.4.130
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

Adaptador de Ethernet Ethernet 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : TAP-Windows Adapter V9
   Dirección física. . . . . . . . . . . . . : 00-FF-D5-74-39-CE
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
```

Figura 1. Información sobre el dispositivo

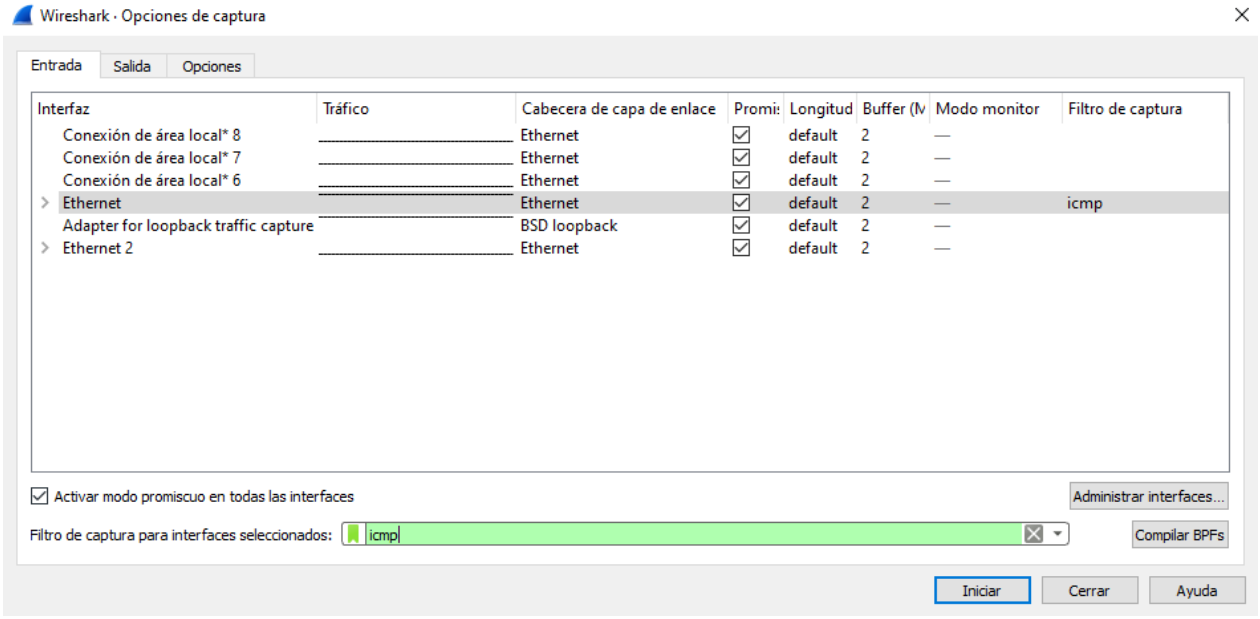

Figura 2. Selección de filtros, en este caso ICMP

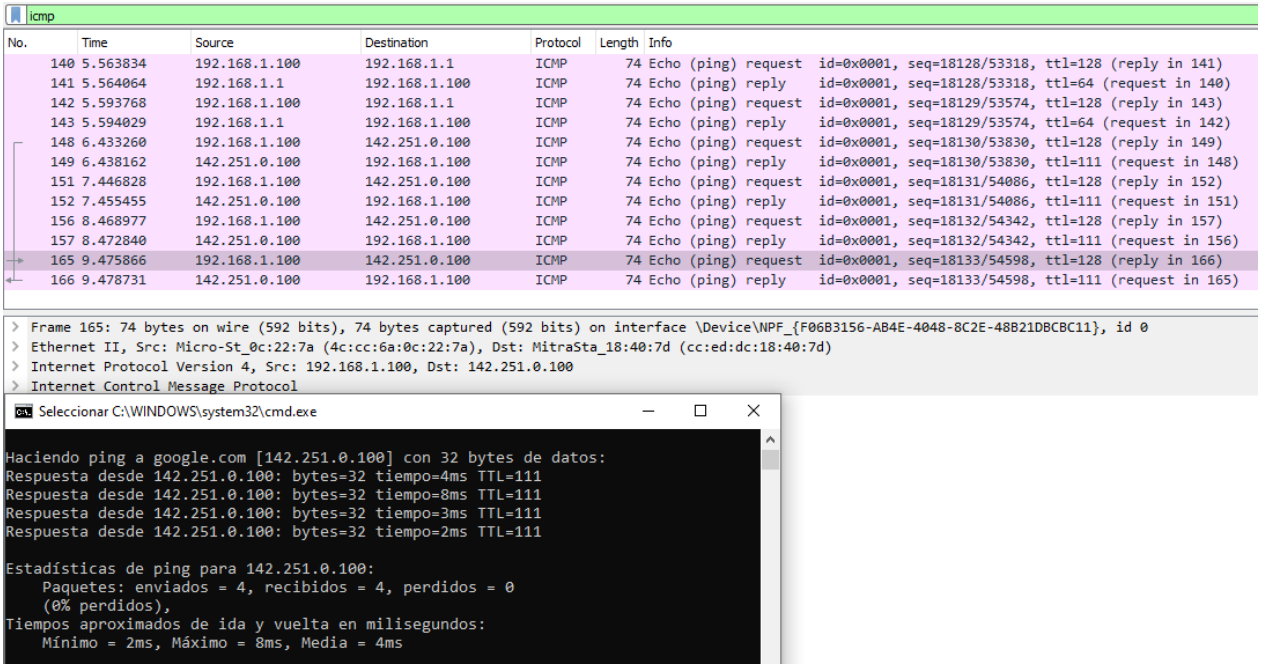

Figura 3. Ping a Google.com

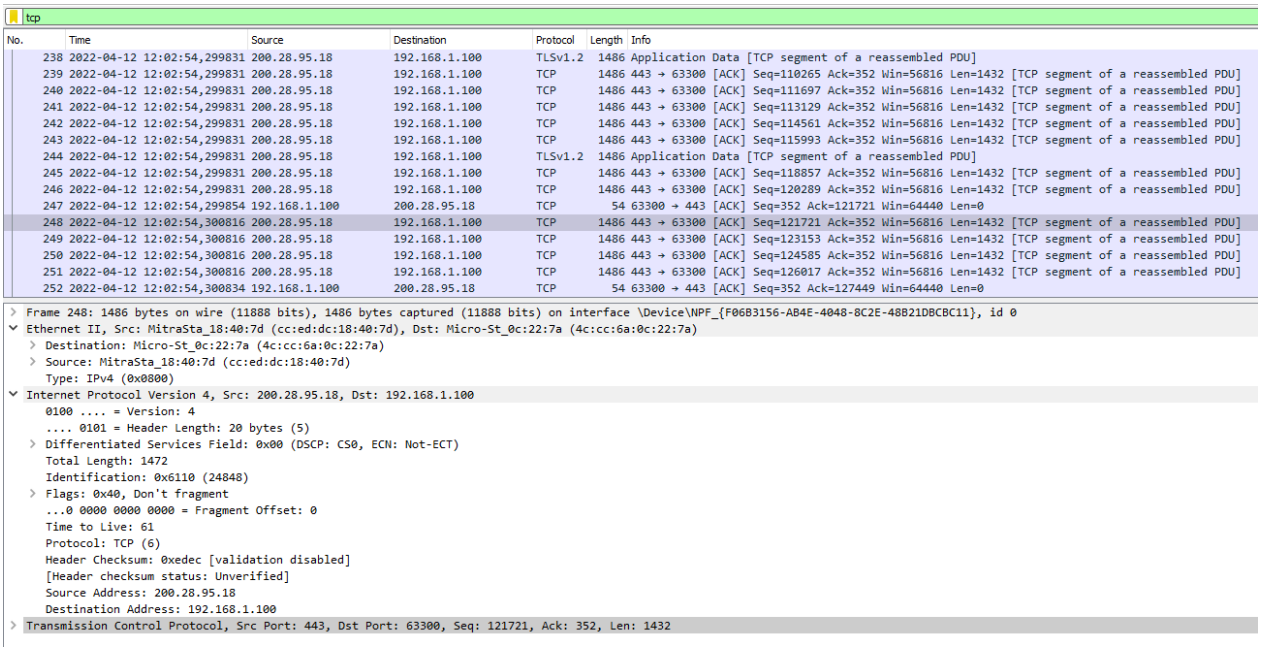

Figura 4. Tráfico TCP

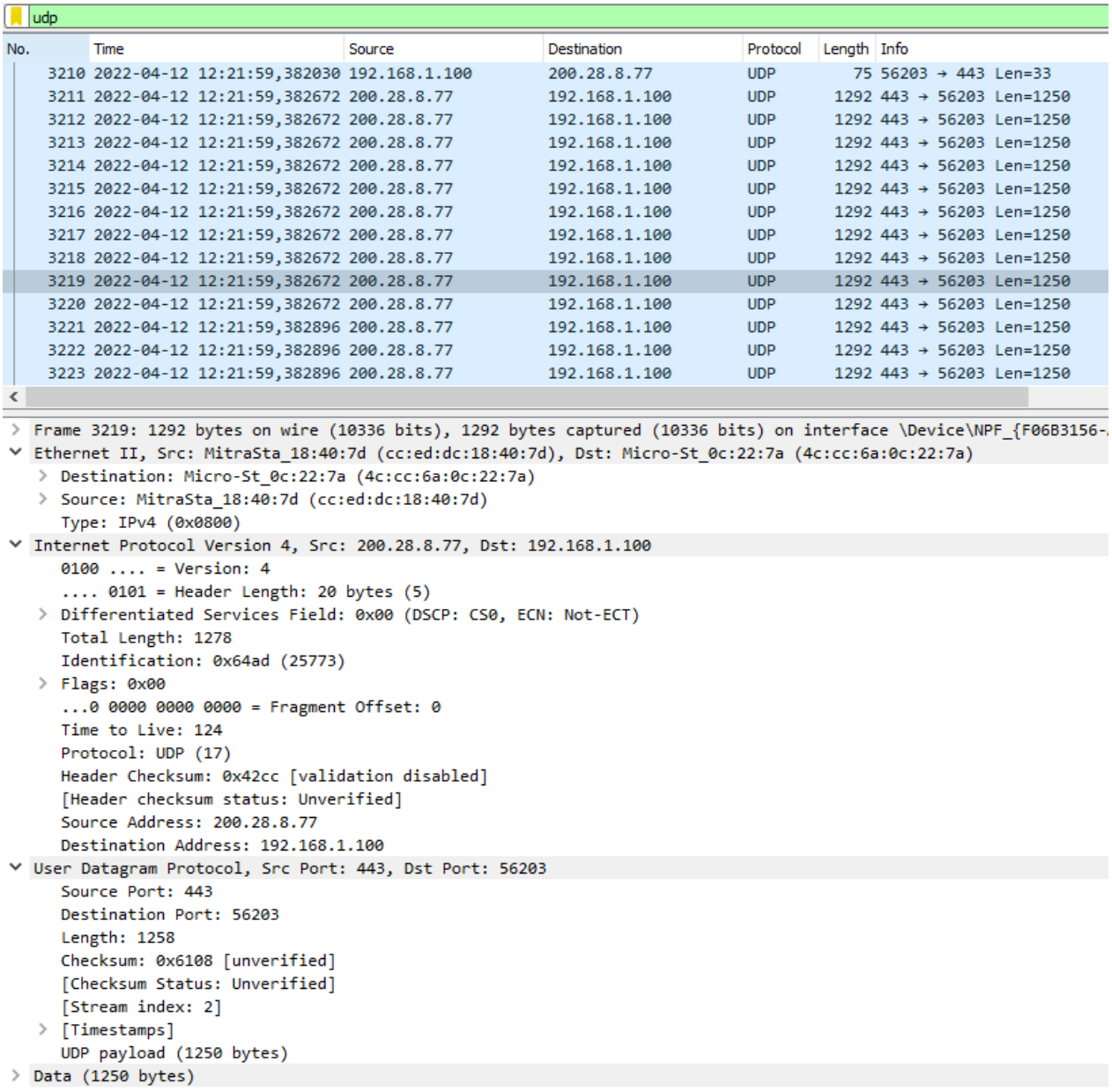

Figura 5. Tráfico UDP

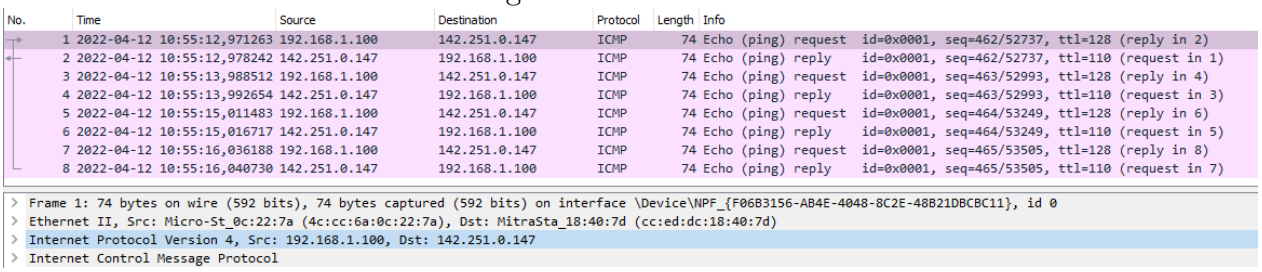

Figura 6. Paquetes ICMP

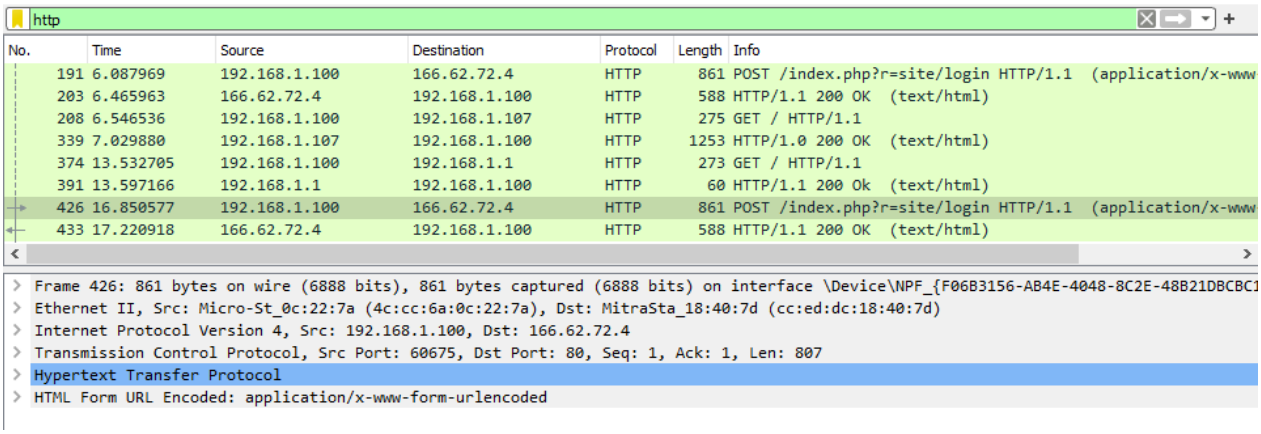

Figura 7. Tráfico HTTP

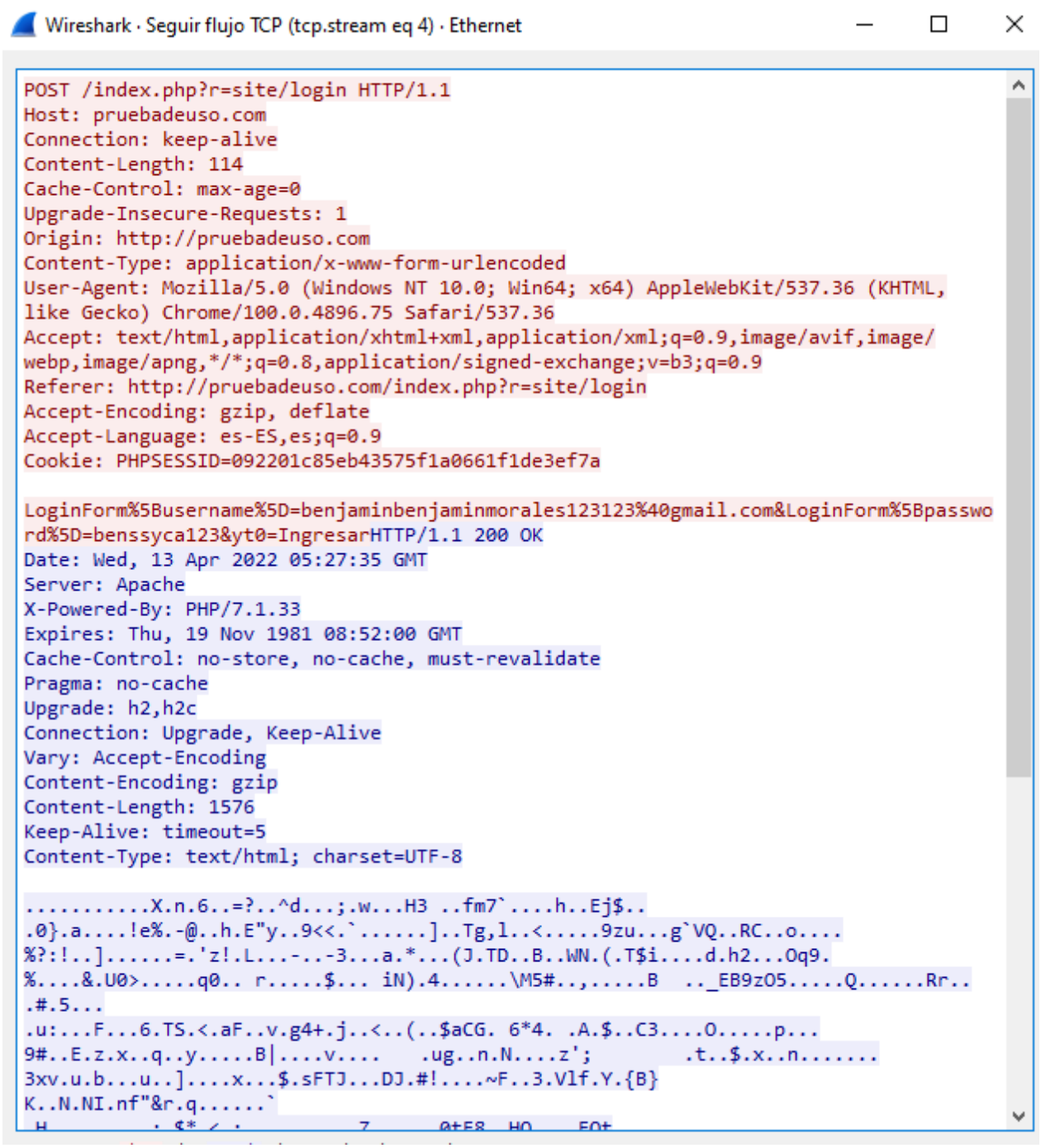

Figura 8. Seguimiento TCP

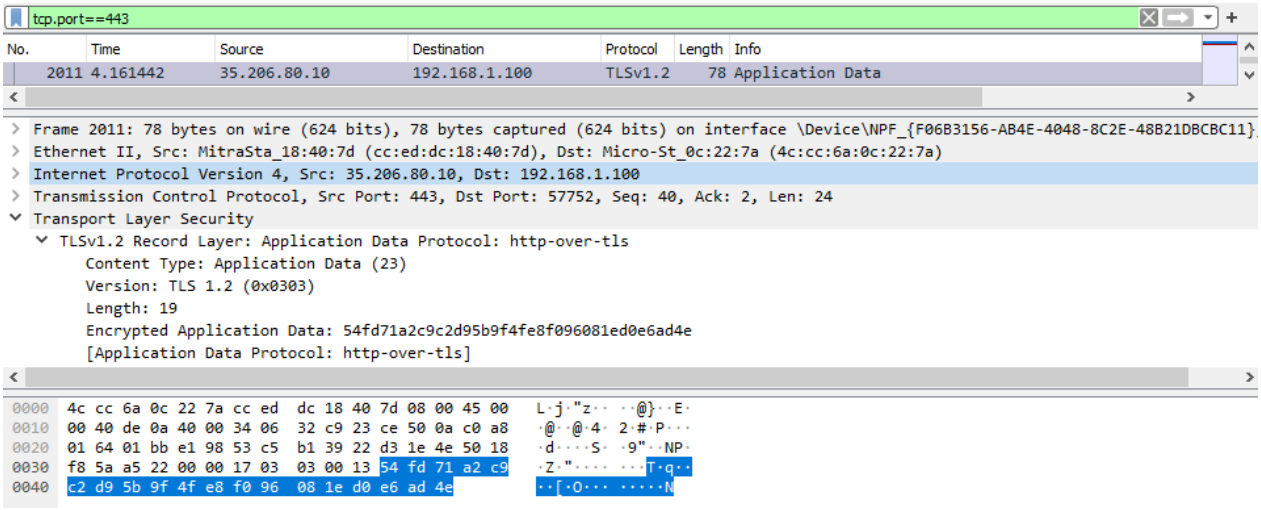

Figura 9. Tráfico HTTPS

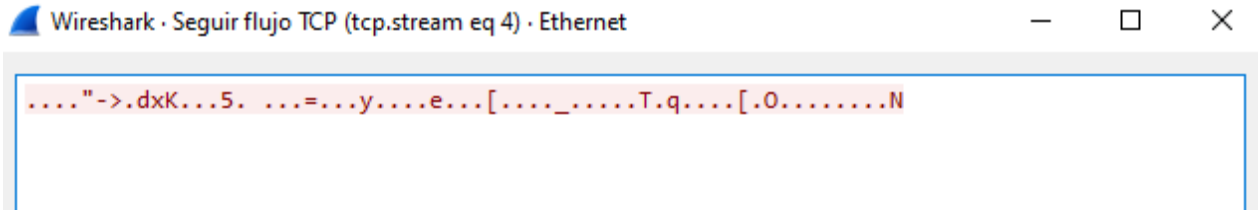

Figura 10. Seguimiento TCP

Figura 11. Router por delante

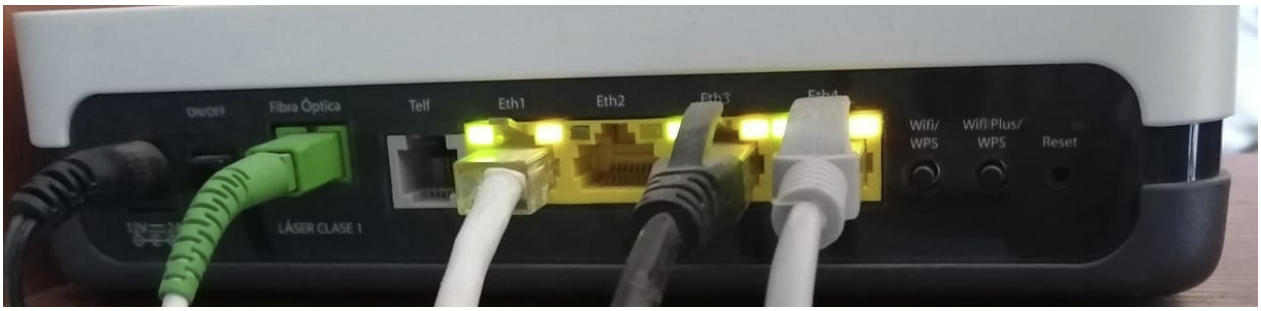

Figura 12. Puertos del router

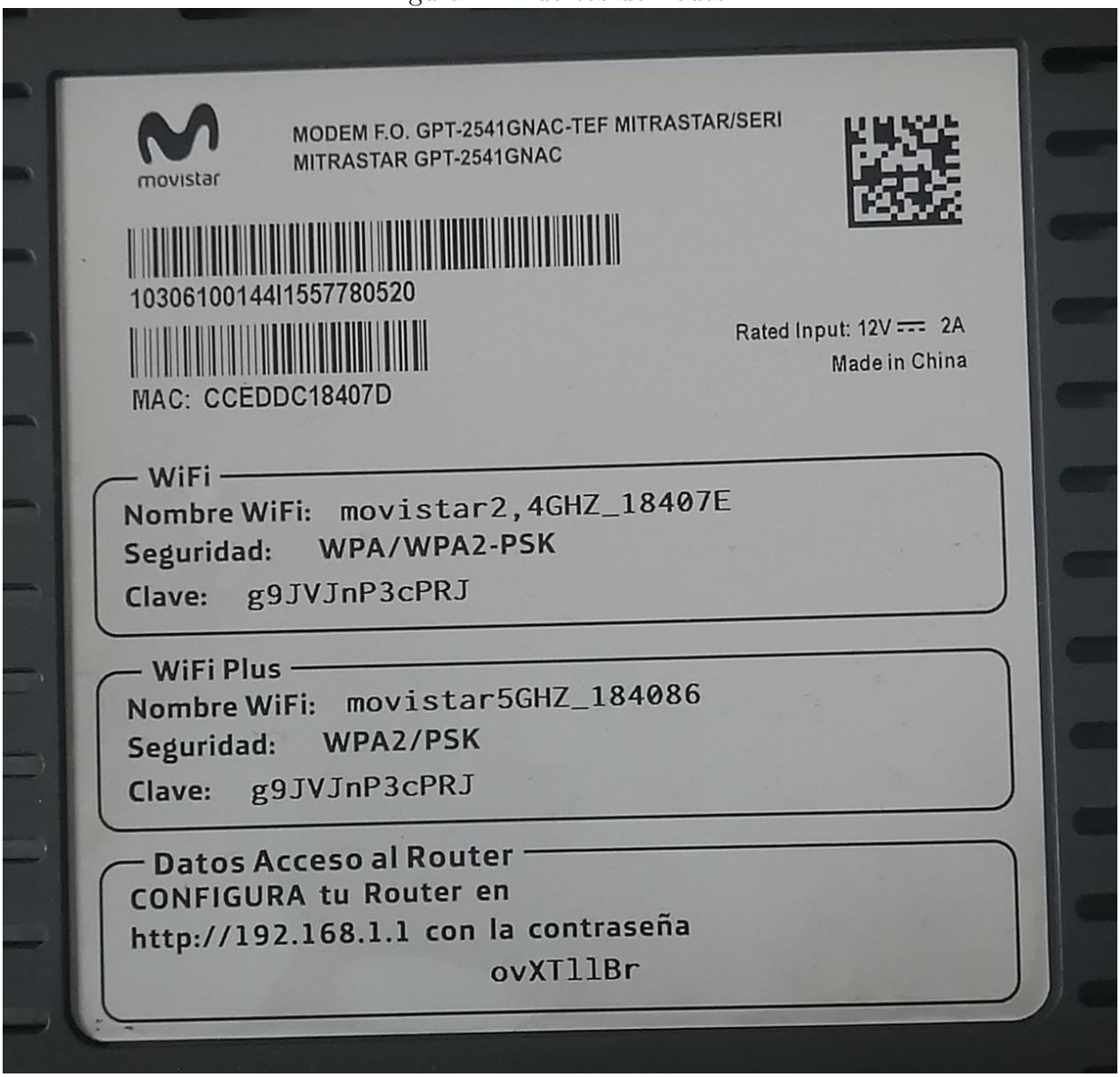

Figura 13. Información del router

2.1. Identificación de su entorno de red

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**:

   El dispositivo contiene cuatro puertos para Ethernet (figura 12). Tres puertos están siendo usados para conectarse a distintos computadores a través de cables. Además, se puede apreciar el cable de fibra óptica a la izquierda (WAN). EL router es de marca Movistar y su modelo es MitraStar GPT-2541GNAC (HGU).

2. **Indique el ISP (*Internet service provider*) contratado**: Movistar Chile.

3. **Indique el SSID (*Service Set Identifier*) de su WLAN**: Actualmente es "Beto-Luna".

4. **Dirección MAC**: 4C – CC – 6A – 0C – 22 - 7A

5. **Dirección IP**: 192.168.1.100

6. **Máscara de red**: 255.255.255.0

7. **Dirección IP del gateway**: 192.168.1.1

8. **DNS**: 200.28.4.129, 200.28.4.130

9. **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**:

   - Dispositivo 1 (ordenador): **MAC** (4c-cc-6a-0c-22-7a) **IP** (192.168.1.100).
   - Dispositivo 2 (ordenador): **MAC** (d0-7e-35-9a-fd-7b) **IP** (192.168.1.87).
   - Dispositivo 3 (celular): **MAC** (e0-24-81-b1-0a-b8) **IP** (192.168.1.88).
   - Dispositivo 4 (ordenador): **MAC** (bc-ee-7b-9c-69-8d) **IP** (192.168.1.120).
   - Dispositivo 5 (celular): **MAC** (50-8e-49-00-47-e6) **IP** (192.168.1.113).

2.2. Captura de paquetes ping

1. **Indique el filtro utilizado para desplegar los mensajes del tipo "*ping*"**: Se utiliza el filtro ïcmp"(ver figura 2).

2. **¿Cuántos paquetes del tipo "*ping*" ha capturado?**: Se han capturado cuatro paquetes (ver figura 3).

3. **¿Cuáles son las direcciones MACs de origen y destino de los frames?**: De origen es 4c:cc:6a:0c:22:7a y de destino es cc:ed:dc:18:40:7d (ver figura 3).

4. **Realizando un estudio de las direcciones MAC capturadas, ¿reconoce alguna de ellas?**: Reconozco mi dirección MAC. Esto sucede ya que se envía una request al servidor de Google.com desde mi dispositivo, por lo que se transfieren paquetes desde mi computadora y WireShark lo muestra.

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?**: La dirección IP del servidor es 142.251.0.100 y de mi computador es 192.168.1.100 (ver figura 3).

6. **¿Qué protocolo utiliza el comando "*ping*"?**: Utiliza el protocolo ICMP.

7. **Indique el tamaño (en Bytes) del paquete**: 32 bytes (ver figura 3).

8. **Realice una inspección en el campo de datos del "*ping*" e indique su contenido**: Al observar la figura 3, se presenta el protocolo utilizado en estos paquetes, las direcciones IP de origen y destino (al momento de enviar y recibir), además de las direcciones MAC. Es posible ver el tamaño de estos paquetes, cuántos han sido enviados, recibidos y el promedio de ida y vuelta de estos paquetes enviados a google.com en ms a través del comando ping.

9. **Explique el funcionamiento del "*ping*" e indique cuáles son las principales razones de su uso**: El comando ping se utiliza para ver si un servidor responde a paquetes enviados, verificando si está activo. Ayuda a determinar el estado de un host remoto, lo cual a través del protocolo ICMP se solicita una respuesta. Se muestra información como el transcurso en ms, paquetes enviados y direcciones IP (ver figura 3).

2.3. Captura y análisis de TPDUs

1. **Ejecute alguna aplicación de red utilizada y filtro de despliegue**: Se utiliza la aplicación YouTube para capturar TCP con el filtro "tcp". Para los UDP, se utiliza la aplicación Roblox (app online) con el filtro udp.

2. **Principales diferencias existente entre los protocolos TCP y UDP**: La principal diferencia es el sistema de verificación de la transmisión de la información entre el emisor y receptor, el cual posee el protocolo TCP. Este está orientado a la conexión y verifica la correcta transmisión de datos (por lo que lo hace más seguro).El protocolo UDP tiene una mayor velocidad de transmisión pero menos precisión al transmitir datos. Además,

el tamaño de la cabecera del protocolo TCP es de 20 bytes, y 8 bytes el de UDP, debido a que TCP contiene más información para verificar los datos transmitidos.

Capa Modelo	Campo	Valor del Campo
Capa de Enlace	Dirección MAC de Destino	4c:cc:6a:0c:22:7a
	Dirección MAC de Origen	cc:ed:dc:18:40:7d
	FCS	
Capa de Red	Protocolo IP	Internet Protocol Version 4 (IPv4)
	Dirección IP de Destino	192.168.1.100
	Dirección IP de Origen	200.28.95.18
Capa de Transporte	Protocolo de Transporte	Transmisision Control Protocol (TCP)
	Número de Puerto de Destino	63300
	Número de Puerto de Origen	443

2.4. Captura de paquetes HTTP y HTTPS

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**?:

   La primera conexión se realiza con el sitio web "http://pruebadeuso.com". Se utiliza el filtro "http"para analizar estos paquetes transferidos. La IP de origen es 192.168.1.100 (mi dispositivo) y de destino 166.62.72.4, además, el puerto de origen es 60675 y de destino 80 (ver figura 7). Se han capturado 451 paquetes.

2. **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**:

   La información desplegada es amplia. Se muestra el Host y la información sobre la web, y lo más importante, el usuario y contraseña ingresados en la página. Esta información observada en la figura 8, no está encriptada y puede observarse sin problemas a través de Wireshark, lo que lo hace menos segura.

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?:

La conexión se realiza con el sitio web "https://mudivino.com". Se utiliza el filtro "tcp.port==443", ya que se conecta con este puerto en específico, y se ubica el protocolo TLSv.1.2 para obtener la información del inicio de sesión en la web. Al observar la figura 9, la dirección IP de origen es 35.206.80.10 y de destino 192.168.1.100. El puerto de origen es 443 y de destino 57752. Se han caputado 3006 paquetes.

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**:

   La información que se muestra parece estar encriptada, no se sabe el usuario o contraseña, toda la información está segura (en comparación con HTTP) ya que no se logra observar en la figura 10.

5. **Principales diferencias entre los protocolos HTTP y HTTPS**:

   "La principal diferencia entre HTTP y HTTPS es la seguridad. El protocolo HTTPS impide que otros usuarios puedan interceptar la información confidencial que se transfiere entre el cliente y el servidor web a través de Internet."(María Acibeiro,2021). Otras diferencias son que HTTP utiliza el puerto 80, no está encriptado, no requiere certificados SSL y no utiliza conexión segura, por otro lado, HTTPS manda la información por el puerto 443, está encriptado, requiere SSL y utiliza conexión segura.

Conclusiones y comentarios

Se concluye que mediante la herramienta Wireshark es posible analizar distintos paquetes a través de distintos protocolos (TCP, UDP, HTTP,HTTPS,ICMP). Se reconocen las direcciones MAC e IP, puertos y flujo de información segura e insegura, además de características de los dispositivos. Además, se observaron las funciones del comando ping y características de los protocolos mencionados.
Wireshark es bastante útil e intuitivo, fácil de utilizar y sencillo para aprender.

Referencias

1. Andrew S. Tanenbaum y David J. Wetherall. Redes de computadoras. 5ta Ed.,Pearson Educación, 2012

2. IBM. (12 abril, 2021). Protocolo de mensajes de control de Internet (Internet Control Message Protocol). https://www.ibm.com/docs/es/aix/7.2?topic=protocols-internet-control-message-protocol

3. Ilma V. (13 Noviembre, 2019). TCP vs. UDP, comparamos los dos protocolos. https://nordvpn.com/es/blog/protocolo-tcp-udp/#:text=La%20principal%20diferencia%20entre%20TCP,protocolo%20UDP%20no%20lo%20es

4. María A. (6 julio, 2021). ¿Cuál es la diferencia entre HTTP y HTTPS?. https://es.godaddy.com/blog/diferencia-entre-http-y-https/

5. Victoria R. (26 Julio, 2017). Entienda qué son el HTTP y el HTTPS y sus diferencias. https://www.segurisoft.es/encriptacion/diferencia-http-https/