

Informe Laboratorio 1: Captura y Analisis de Paquetes con Wireshark

Sección 7 Grupo 4

Alumnos: Sebastian Quintero, Sebastian Saldivia, Lucas Herrada, Matias Caceres
e-mail: sebastian.quintero@mail.udp.cl; lucas.herrada@mail.udp.cl.

Abril de 2025

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	5
2.3. Captura y análisis de TPDU's (Transport protocol data unit)	8
2.4. Captura de paquetes HTTP y HTTPS	10
3. Dificultades encontradas	11
4. Conclusiones	11

1. Equipos y materiales

Este experimento se realizó gracias a que contamos con un computador, junto al programa de detección de paquetes Wireshark. También se accedió a un router para obtener los dispositivos conectados a la red.

Lista de Materiales

Tabla 1: Lista de materiales

Ítem	Descripción	Cantidad
1	Router inalámbrico doméstico	1
2	Computadora personal (PC)	1
3	Aplicación: Wireshark (software)	1

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.

El router modelo HG5853SF color blanco tiene unas dimensiones de 22cm x 14,5cm x 4cm con 4 puertos LAN y 1 puerto WAN

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



Figura 1: Router.



Figura 2: Puertos Router.

2. Indique el ISP (Internet service provider) contratado

R: El proveedor de servicio de internet es "Mundo Pacifico".

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

R: El SSID actual es "Herrada huawei".

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

a) Dirección MAC: EC-8E-B5-9D-F8-3E

b) Dirección IP: 192.168.101.6

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

- c) Máscara de red: 255.255.255.0
- d) Dirección IP del gateway: 192.168.101.1
- e) DNS: 8.8.8.8

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Ethernet Connection I219-LM
Dirección física. . . . . : EC-8E-B5-9D-F8-3E
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv4. . . . . : 192.168.101.6(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 31 de marzo de 2025 16:01:42
La concesión expira . . . . . : jueves, 3 de abril de 2025 16:01:42
Puerta de enlace predeterminada . . . . . : 192.168.101.1
Servidor DHCP . . . . . : 192.168.101.1
Servidores DNS. . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Figura 3: Configuración de red

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.

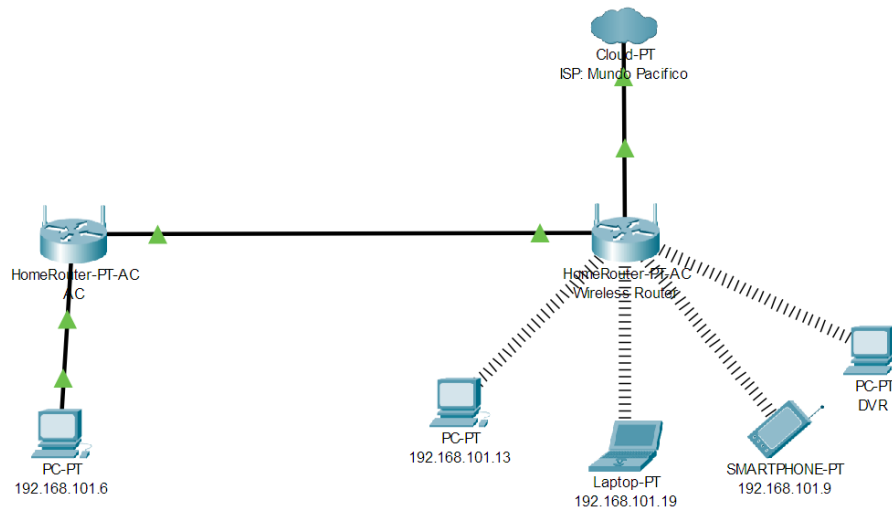


Figura 4: Diagrama de la topología lógica de la red

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 tipear 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:

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

R: Para visualizar únicamente los paquetes generados por la herramienta "ping", se utilizó el filtro ICMP en Wireshark. Este filtro permite desplegar únicamente los paquetes pertenecientes al ICMP, que es el protocolo utilizado para la comunicación de mensajes de control en redes IP.

2. ¿Cuántos paquetes del tipo "ping" ha capturado?.

R: Durante la captura de tráfico en Wireshark, se registró un total de 8 paquetes ICMP. De estos, 4 correspondieron a solicitudes enviadas desde el computador de origen hacia el destino, mientras que los otros 4 paquetes son respuestas generadas por el servidor en respuesta a cada solicitud.

3. ¿Cuáles son las direcciones MACs de origen y destino de los frames?.

R: MAC origen: ec:8e:b5:9d:f8:3e

MAC destino: 58:25:75:2e:0f:91

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

R: Si, la direccion MAC de origen es la misma que el computador.

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?.

R: IP origen (Computador): 192.168.101.6

IP destino (Servidor): 142.251.0.103

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

R: El comando ping utiliza el Internet Control Message Protocol (ICMP), pertenece a la capa de red que se emplea principalmente para el diagnóstico y prueba de conectividad entre dispositivos dentro de una red. permite el envío de mensajes de control, solicitudes y respuestas de eco, con el propósito de determinar si un host específico es accesible y medir el tiempo de respuesta entre ellos.

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

R: El tamaño del paquete son de 74 Bytes.

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

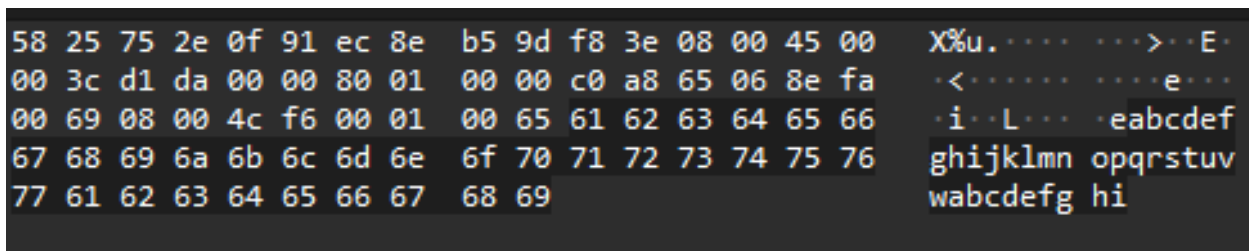


Figura 5: Contenido del paquete/ping.

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

R: el comando ping es utilizado para verificar la conexión entre dos dispositivos de red, por ejemplo, si quiero confirmar que mi PC está correctamente conectado a mi router, utilizo el comando ping para verificar esta comunicación, el comando funciona enviando un paquete ICMP hacia la dirección de destino que hayamos colocado, si el dispositivo recibe el paquete, este responderá con un paquete ICMP de respuesta para nuestro PC.

2.3. Captura y análisis de TPDU's (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.

1. Ejecute alguna aplicación de red y realice la captura de datagramas UDP. Nota: debe indicar la aplicación utilizada además del filtro de despliegue.
2. Seleccione uno de los datagrama y complete la tabla con la información solicitada.
3. 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.
4. Seleccione uno de los segmentos y complete la tabla con la información solicitada.
5. Investigue cuáles son las principales diferencias existente entre los protocolos TCP y UDP.

R: Se seleccionaron dos aplicaciones para poder analizar los paquete TCP y UDP, para TCP se utilizo un navegador (Opera GX) y se accedio a una pagina (deepseek), para UDP se utilizo el servicio de Youtube Music a traves de navegador, aunque realmente Youtube Music no usa el protocolo UDP, utiliza QUIC el cual es una variacion del protocolo con mayor seguridad y rapidez de transmision, asi que el paquete analizado es un paquete QUIC.

Durante el analisis se vio una principal diferencia entre TCP y UDP o en este caso, QUIC, la principal era que el protocolo TCP enviaba mensajes de verificacion preguntando si el paquete habia llegado sin errores a destino y si no debia ser reenviado, este tipo de mensajes no se presentaban con el protocolo QUIC, en el analisis solo se vieron paquetes QUIC sin mensajes de verificacion. A continuacion se expone una tabla con las diferencias entre TCP y UDP:

Tabla 2: Comparación entre TCP y UDP

Característica	TCP	UDP
Orientación a la conexión	Sí (handshake SYN/ACK)	No
Fiabilidad	Garantizada (ACK, retransmisiones)	No garantizada
Control de flujo	Sí (ventana deslizante)	No
Orden de paquetes	Secuenciado	No ordenado
Velocidad	Más lento (overhead)	Más rápido
Uso típico	HTTP, FTP, SSH	VoIP, DNS, video streaming

Tabla de Paquete TCP

Capa Modelo	Campo	Valor del Campo
Capa de Enlace	Dirección MAC de Destino	44:48:b9:46:58:78
	Dirección MAC de Origen	3c:7c:3f:da:3c:0b
	FCS	0x45810000
Capa de Transporte	Protocolo IP	ipv4
	Dirección IP de Destino	104.18.27.90
	Dirección IP de Origen	192.168.1.82
	Protocolo de Transporte	TCP
	Número de Puerto de Destino	443

Tabla de Paquete QUIC

Capa Modelo	Campo	Valor del Campo
Capa de Enlace	Dirección MAC de Destino	44:48:b9:46:58:78
	Dirección MAC de Origen	3c:7c:3f:da:3c:0b
	FCS	0xfbfa211e
Capa de Transporte	Protocolo IP	ipv4
	Dirección IP de Destino	35.186.224.31
	Dirección IP de Origen	192.168.1.82
	Protocolo de Transporte	QUIC
	Número de Puerto de Destino	54280

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?.

R: Se capturaron 2 paquetes con el protocolo HTTP. Dichos paquetes tienen como dirección IP 192.168.101.6 y 96.7.128.175 (IP del PC utilizado y IP del servidor respectivamente). Los puertos de origen son 56564 (origen) y 80 (destino).

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.

R: Al abrir la ventana emergente, se puede visualizar el código fuente de la página, que incluye su estructura en HTML y CSS. Esto ocurre porque la página utiliza el protocolo HTTP, lo que significa que no cuenta con un certificado de seguridad SSL. Como resultado, su código fuente no está cifrado, permitiendo que cualquier usuario, al igual que nosotros, pueda acceder y examinarlo fácilmente.

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?.

R: Se capturaron 23 paquetes con el protocolo HTTPS. Dichos paquetes tienen como dirección IP 192.168.101.6 y 23.192.228.84 (IP de origen y IP de destino respectivamente). Los puertos de origen son 56637 (origen) y 433 (destino).

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.

R: Al analizar la captura de tráfico, se puede notar que los datos aparecen cifrados. Esto se debe a que la página utiliza el protocolo HTTPS, lo que indica que cuenta con un certificado de seguridad TLS. Como consecuencia, la información transmitida está protegida, evitando que terceros puedan acceder a su contenido de manera legible.

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

R: El protocolo HTTP transmite los datos sin ningún tipo de cifrado y opera a través del puerto 80, lo que significa que no cuenta con un certificado de seguridad para garantizar la confiabilidad del sitio. En cambio, HTTPS protege la información mediante cifrado, ofreciendo una comunicación más segura. Además, utiliza el puerto 443 y requiere un certificado de seguridad para validar la autenticidad del sitio web.

3. Dificultades encontradas

A la hora de realizar este informe, una de las principales complicaciones que tuvimos como grupo fue el bajo conocimiento y práctica en el programa Wireshark, así como la falta de conocimiento de protocolos y el funcionamiento de dicho programa. También sufrimos complicaciones en el CMD, donde debíamos buscar o acceder a ciertos datos desconociendo comandos o formas eficientes de realizar esto, ya que no se ha estudiado ni practicado de forma tan recurrente en clases, por lo que debimos aprender sobre la práctica, haciendo el proceso más lento.

4. Conclusiones

Podemos concluir que, gracias a las diferentes actividades prácticas propuestas en esta guía, se lograron profundizar en los conocimientos vistos en clase y entender de mejor manera conceptos tales como:

- Estructura de un datagrama.
- Flujo de datos de una red.
- Análisis de tráfico.
- Manejo de software de tipo sniffers.

También esta guía ayudó a poder entender cómo funciona la transmisión de datos de algunas aplicaciones tales como Youtube Music, conocer parámetros de red de un dispositivo en una red y reconocer puertos de diferentes servicios web. Pese a algunas complicaciones debido a que ningún miembro del grupo tenía experiencia en actividades de análisis de paquetes y en general pocos conocimientos en redes, se lograron cumplir con los objetivos de aprendizaje principales los cuales son:

- Comprender el funcionamiento y la utilidad del analizador de protocolos Wireshark.
- Capturar y analizar los paquetes de datos que circulan en su entorno de red.
- Comprender en profundidad la estructura de los datagramas de red.