# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025

Uso de Wireshark (sniffer)

El manejo de la herramienta WireShark, permite

- 1- Identificar los tipos de paquetes, de acuerdo con su protocolo.
- 2- Analizar el tráfico de datos de las distintas capas que ocurre entre un cliente y un servidor.

Para realizar las siguientes actividades, se necesitará el analizador de protocolo wireshark, que lo pueden descargar del portal de la cátedra (versión 2.2 para Windows) o en la página oficial wireshark.org, luego instalarlo en el equipo que van a utilizar.

Una vez instalado el analizador WireShark, revisen este video tutorial para aprender o reforzar su utilización.

## https://www.youtube.com/watch?v=Y5rZlmmqVQk

Realice una captura de tráfico en la computadora que tiene instalado el analizador.

- Aplicación de filtros. Una vez hecha una captura, visualizar los paquetes de acuerdo a los siguientes filtros
  - a. Visualice los paquetes que provengan de la ip X.X.X.X (una IP que Uds. Identifiquen dentro de la captura)

b. Visualice los paquetes que vayan a la ip X.X.X.X (una IP que Uds. Identifiquen dentro de la captura)

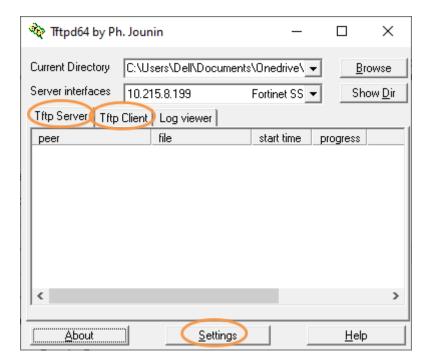
c. Visualice los paquetes que lleven el protocolo ARP

Ejercicio práctico identificación de UDP

1) Descargue del portal de la cátedra el software tftpd32 o tftpd64 de acuerdo con su sistema operativo. Este software puede ejecutarse tanto como servidor o cliente (vea la captura que se encuentra debajo) y dentro del mismo equipo o equipos separados.

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025

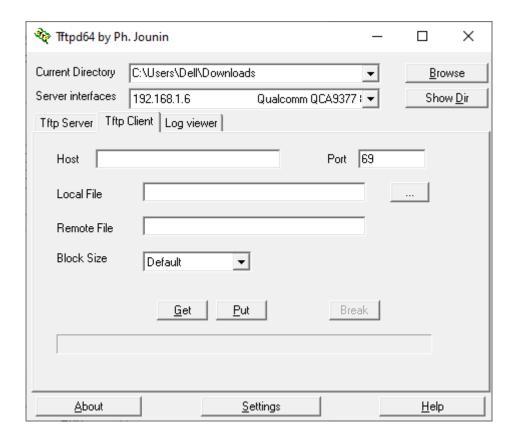


Configure en "setting" los parámetros del servidor (solo el base directory que será una carpeta física dentro del equipo que está ejecutando el servidor). También puede dejar la ruta por defecto que propone el software.

En el "client" configure la IP del server host. En "local" seleccione el archivo a enviar y luego presione "put". Puede ver si se envió en la pestaña "log viewer".

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025



Ahora ejecute WireShark, comience a capturar en la interface correspondiente, vuelva a ejecutar el envío de un archivo y detenga la captura.

Aclaración: si el server y client están en la misma PC, en Wireshark debe capturar la interfaz "loopback" (misma PC)

#### **OBJETIVO:**

Realizar una transferencia de archivo usando el protocolo TFTP (Trivial File Transfer Protocol) y analizar la comunicación capturada con Wireshark, especialmente para observar el uso del protocolo UDP en la capa de transporte.



Configurar el servidor TFTP

r Por qué: Para que el cliente tenga un destino al cual enviar el archivo.

## Cómo:

Abrí el programa Tftpd64.

En la pestaña Tftp Server, seleccioná (o dejá por defecto) una carpeta local en Current Directory donde se recibirán los archivos.

Elegí la interfaz de red correcta:

Si estás trabajando en la misma PC (como en tu caso), elegí 127.0.0.1 o localhost.

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025

## 2 Configurar el cliente TFTP

📌 Por qué: El cliente es el que iniciará la transferencia del archivo hacia el servidor.

#### Cómo:

Ir a la pestaña Tftp Client.

En Host, escribí la IP del servidor (ej. 127.0.0.1 si es la misma máquina).

En Local File, seleccioná el archivo que querés enviar (en tu caso: PRUEBA2).

En Remote File, podés escribir el mismo nombre u otro.

Presioná Put para enviar.

## 3 Captura con Wireshark

Por qué: Para analizar cómo se transmite un archivo usando UDP, bloque por bloque.

#### Cómo:

Abrí Wireshark.

Seleccioná la interfaz Loopback (porque cliente y servidor están en la misma PC).

Iniciá la captura antes de hacer el envío del archivo.

Hacé la transferencia desde Tftpd64.

Una vez finalizado el envío, detené la captura.

## 4 Filtrar el tráfico en Wireshark

📌 Por qué: Para ver solo los paquetes relevantes al análisis.

## Cómo:

Usá este filtro: udp o más específico: tftp

¿Qué vemos en la captura?

De acuerdo a tu imagen:

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile - Joaquín Nepotti Redes y Comunicaciones de Datos II

Año 2025

Tipo de paquete	Contenido	Función
Write Request	Solicita enviar el archivo PRUEBA2	Inicia la transferenc ia
Option Ack	El servidor acepta las opciones (como el tamaño tsize=171384)	Negociació n
Data Packet, Block 1 a 10	Contienen fragmentos del archivo enviado	Transferen cia real de datos
Acknowledgem ent, Block 1 a	Confirmaciones por parte del servidor de que recibió	Asegura la fiabilidad

# 🔽 RESPUESTAS DIRECTAS A LAS PREGUNTAS DEL EJERCICIO

¿Qué protocolo de transporte se utilizó para el envío del archivo?  $\blacktriangleright$  UDP, como se observa en la capa de transporte (Src Port: 50183  $\rightarrow$  Dst Port: 69).

correctamente cada bloque

Identifique IP:puerto del servidor y del cliente.
➤ Cliente: 127.0.0.1:50183
➤ Servidor: 127.0.0.1:69

¿Qué protocolo de aplicación hizo la transferencia del archivo? ¿Qué parámetro usó para identificarlo?

➤ Protocolo: TFTP

Práctico Nº 7

➤ Parámetros: Nombre del archivo (PRUEBA2), opcode, block, tsize.

¿Qué tamaño en KB tiene el envío?

¿Cuántos bloques fueron enviados?

➤ Se enviaron bloques — como se observa en los paquetes Data Packet.

#### CONCLUSIÓN

Este ejercicio te permite comprender cómo:

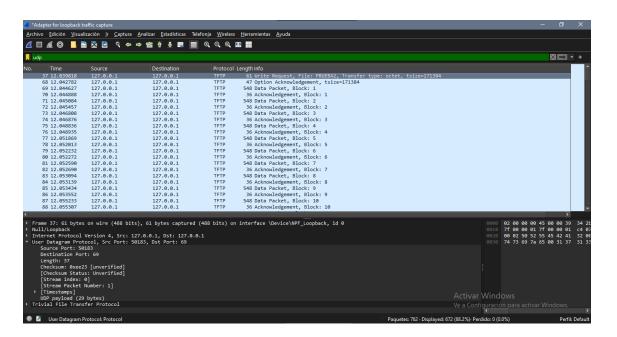
Un protocolo simple como TFTP transfiere archivos usando UDP.

Cada paquete DATA tiene una confirmación (ACK) correspondiente.

El tráfico se puede observar claramente en Wireshark, incluso en loopback.

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025



2) Ventajas de y desventajas de UDP

# Ventajas de UDP

Ventaja	Descripción
Menor retardo	No realiza comprobaciones ni espera confirmaciones, lo que lo hace más rápido. Ideal para tiempo real.
✓ Menor sobrecarga	Los encabezados de UDP son más livianos (8 bytes), lo que reduce el tamaño de los paquetes.
Soporta difusión y multidifusión	Permite enviar datos a múltiples destinos al mismo tiempo, útil para servicios como streaming o descubrimiento de dispositivos.
✓ Ideal para aplicaciones en tiempo real	Como llamadas VoIP, juegos online o videoconferencias, donde es preferible perder algún paquete antes que retrasar toda la transmisión.
✓ Implementación sencilla	Su estructura es simple y fácil de programar o analizar.

# Docentes: Gabriel Filippa - Franco Cian - Marcelo T. Gentile – Joaquín Nepotti Redes y Comunicaciones de Datos II

Práctico № 7 Año 2025

<b>X</b> Desventajas	de UDP
----------------------	--------

Desventaja	Descripción
X No garantiza entrega	Los datagramas pueden perderse, duplicarse o llegar desordenados. No hay confirmación de recepción.
No hay control de congestión	Puede saturar la red fácilmente si se usa en exceso o sin regulación.
➤ No detecta errores complejos	Solo posee un checksum básico. No asegura que los datos lleguen íntegros o completos.
X No mantiene conexión	No hay sesión establecida entre emisor y receptor, lo que puede dificultar el seguimiento de los datos.
➤ No es adecuado para transferencias críticas	No es recomendable para transmisión de archivos, correos o páginas web (para eso se usa TCP).