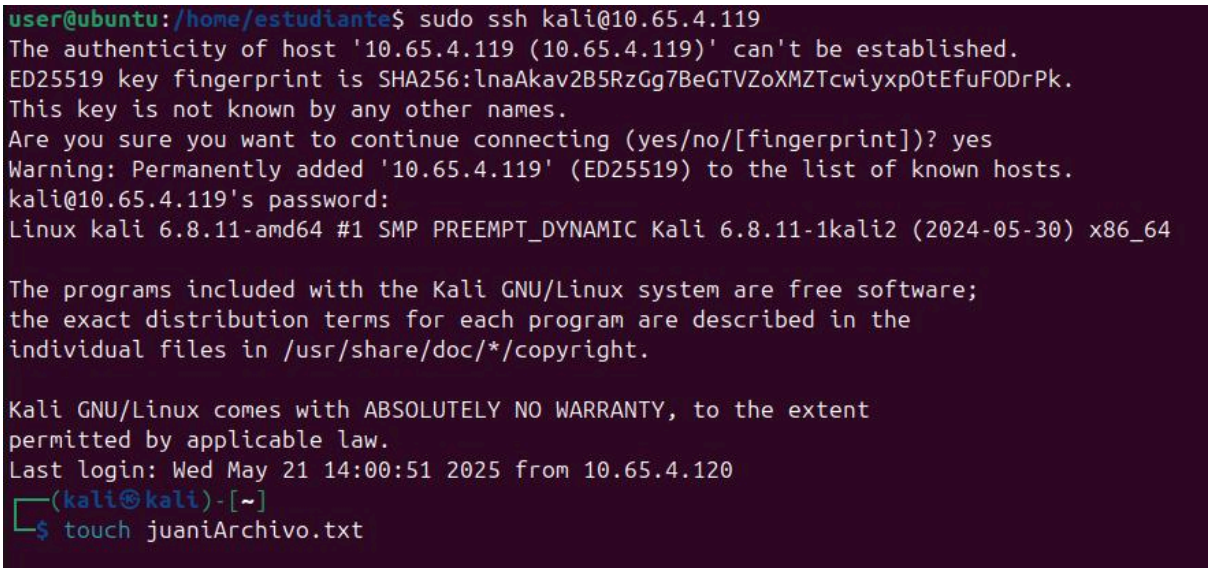
TP 5 REDES

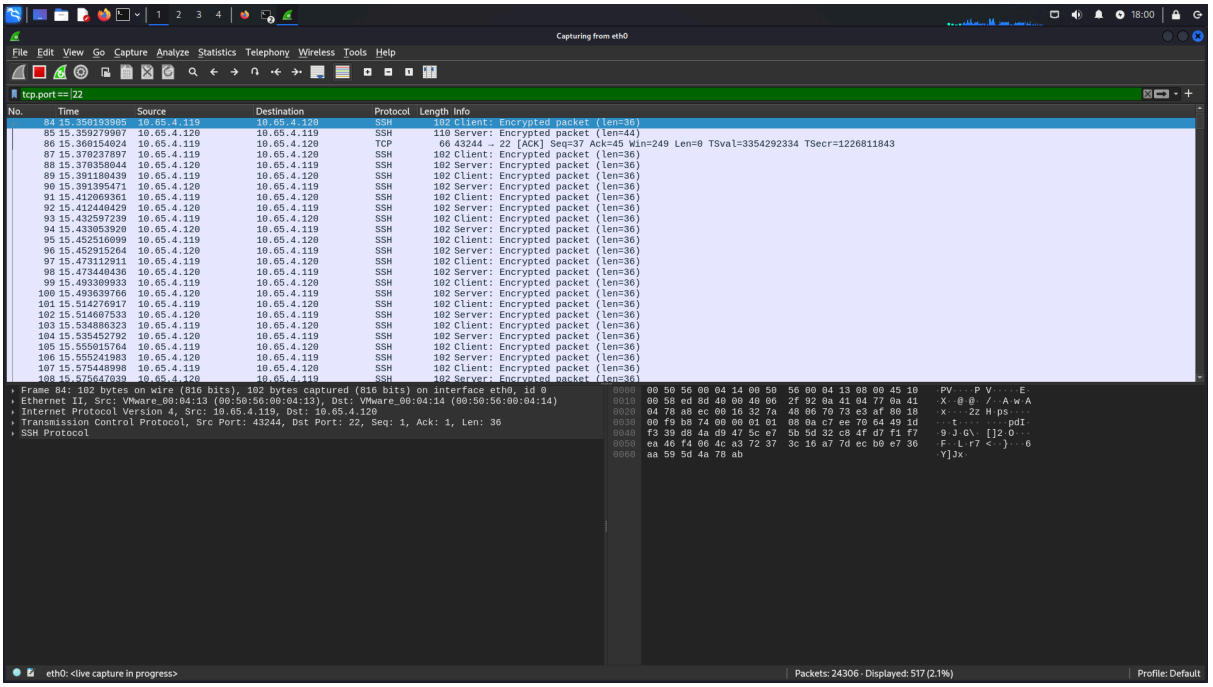
Integrantes: Giovani Azurduy , Lautaro Larosa

Actividad 1:SSH

El objetivo principal de la actividad de SSH es aprender a establecer conexiones seguras entre computadoras mediante el protocolo SSH, permitiéndoles administrar sistemas remotos de forma encriptada. Esto incluye ejecutar comandos a distancia, transferir archivos de manera segura con SCP, redirigir interfaces gráficas, y analizar el tráfico cifrado para comprender su funcionamiento y ventajas de seguridad.



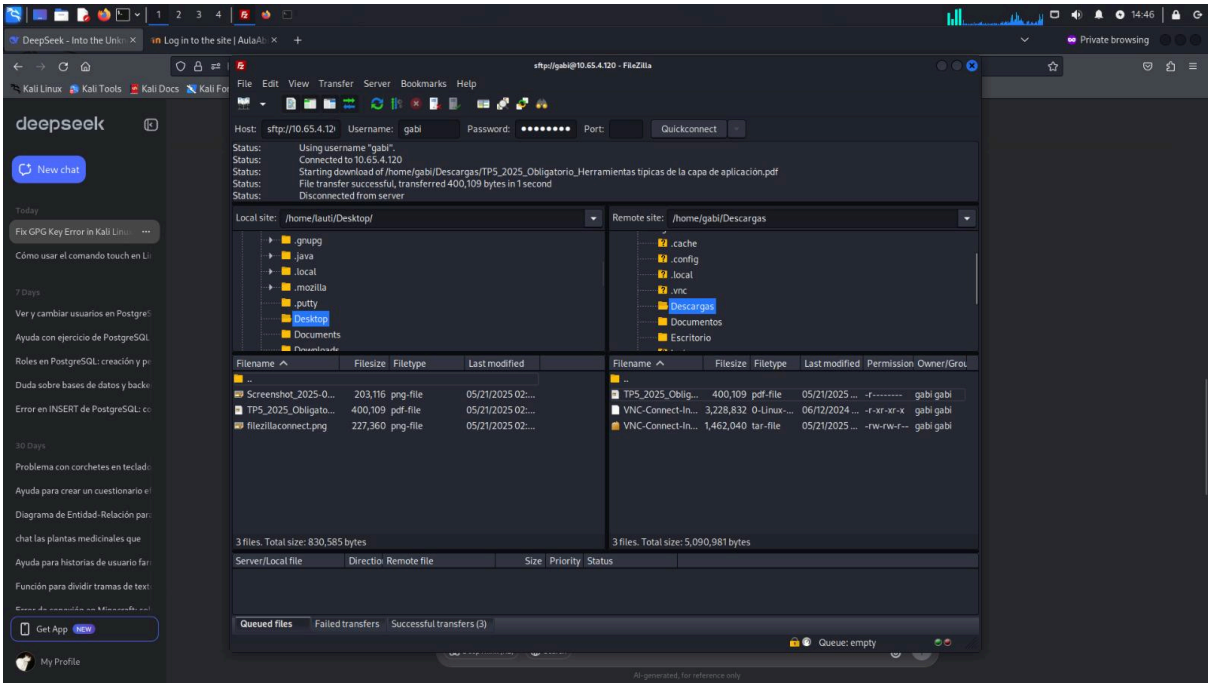
Muestra una conexión SSH establecida desde Ubuntu a una máquina Kali (10.65.4.119).



Captura paquetes cifrados entre IPs 10.65.4.110 (cliente) y 10.65.4.120 (servidor).

Actividad 2:FTP

El objetivo principal de la actividad de FTP es enseñar la configuración y uso básico de servidores FTP tradicionales para transferencia de archivos, destacando sus limitaciones de seguridad al transmitir datos sin cifrado, con el fin de que los estudiantes comprendan la importancia de utilizar alternativas seguras como SFTP o FTPS en entornos reales.

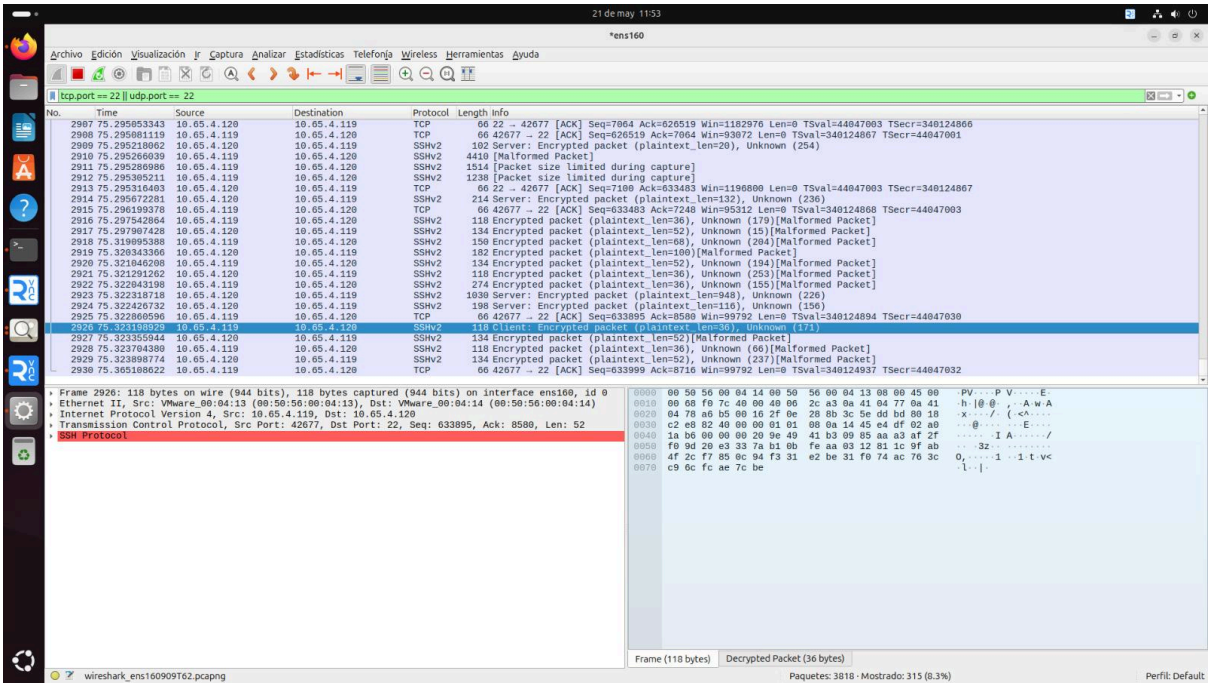


Conexión exitosa al servidor `sftp://10.65.4.120` con usuario `gabi` (puerto SFTP/SSH implícito).
Transferencia exitosa:

- Descarga del archivo `TP5_2025_Obligatorio_Herramientas.pdf` (400 KB en 1 segundo).

Estructura de directorios:

- **Local**: Muestra carpetas como `Desktop`, `Documents` en `/home/lauti/`.
- **Remoto**: Contenido de `/home/gabi/Descargas` (archivos PDF, imágenes, VNC).



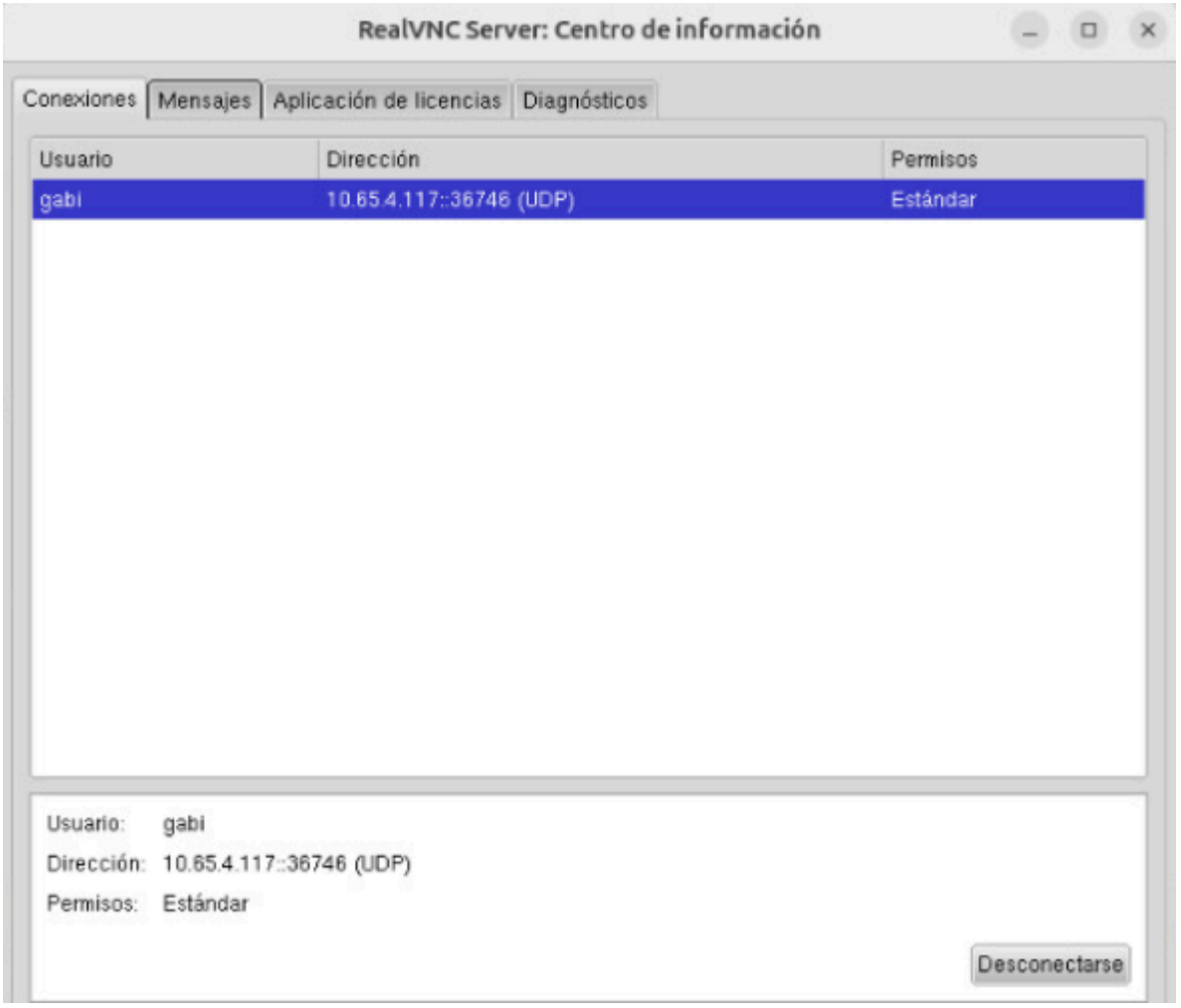
Protocolo: SFTP sobre SSH (puerto 22).

Actividad 3:VNC

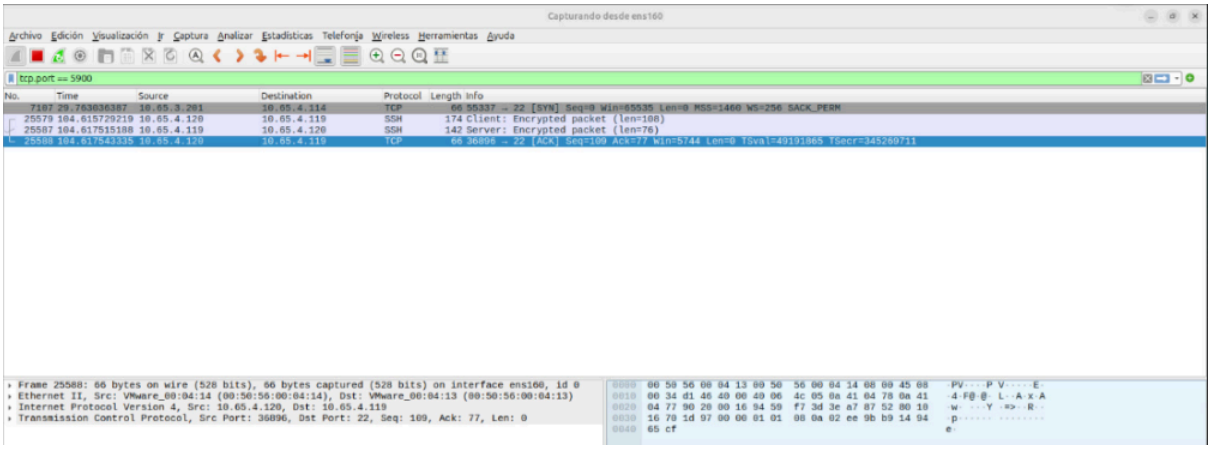
Descripción de la actividad

La Actividad 3 consiste en la implementación y análisis de una conexión VNC (Virtual Network Computing), que es un sistema de visualización remota que permite controlar una computadora (servidor) desde otra (cliente) a través de una red.

Esta actividad permite comprender cómo funciona el protocolo VNC, qué puertos utiliza (como el 5900 para la conexión principal), y cómo se transmite la información gráfica y de control entre las máquinas.



Configuración Básica de los puertos vnc

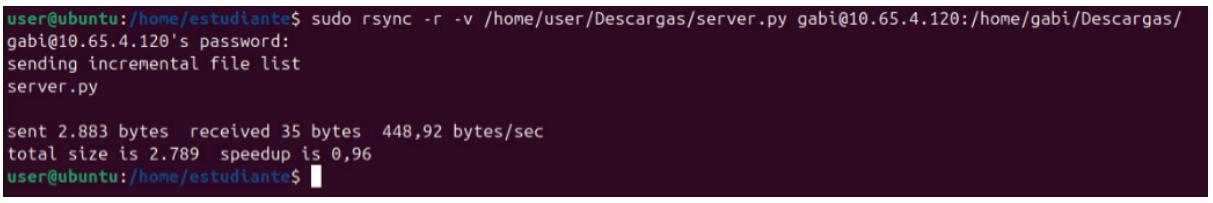


- Muestra el intercambio técnico entre cliente y servidor VNC
- Indica parámetros de la conexión TCP subyacente
- Demuestra cómo se negocian opciones de red durante la comunicación

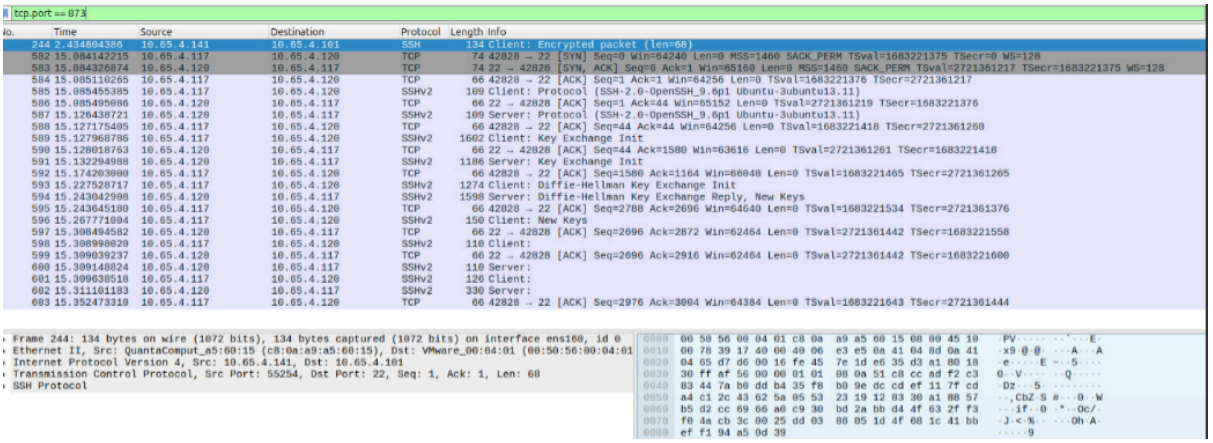
Actividad 4:Rsync

La Actividad 4 consiste en la implementación y análisis del protocolo Rsync, una herramienta de sincronización y transferencia de archivos eficiente que sólo transmite las diferencias entre archivos.

Esta actividad permite comprender cómo Rsync optimiza la transferencia de archivos y qué protocolos utiliza para la comunicación entre sistemas.



Ejecución práctica del comando Rsync

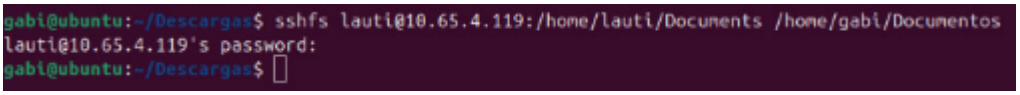


El análisis de Wireshark reveló que Rsync puede operar sobre SSH (como en este caso) o directamente sobre su propio protocolo, mostrando el proceso completo desde el establecimiento de la conexión TCP hasta el intercambio de claves criptográficas y la transferencia de datos.

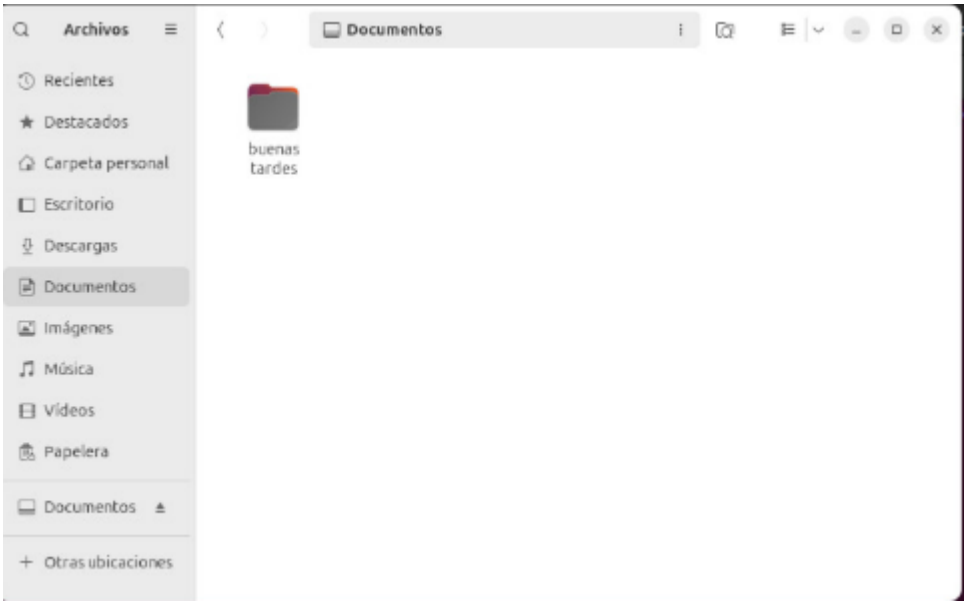
Actividad 5:SSHFS

La Actividad 5 consiste en la implementación y análisis de SSHFS (SSH Filesystem), que permite montar sistemas de archivos remotos a través de una conexión SSH segura.

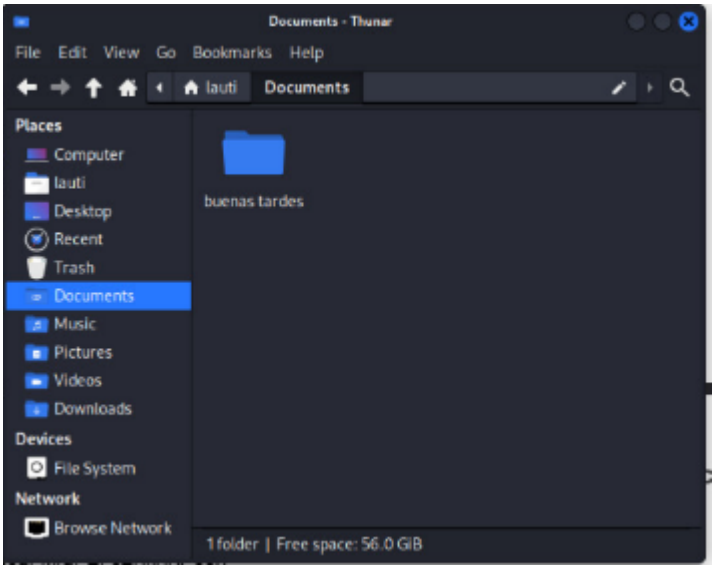
Esta actividad permite comprender cómo SSHFS utiliza el protocolo SSH para proporcionar acceso seguro a sistemas de archivos remotos.



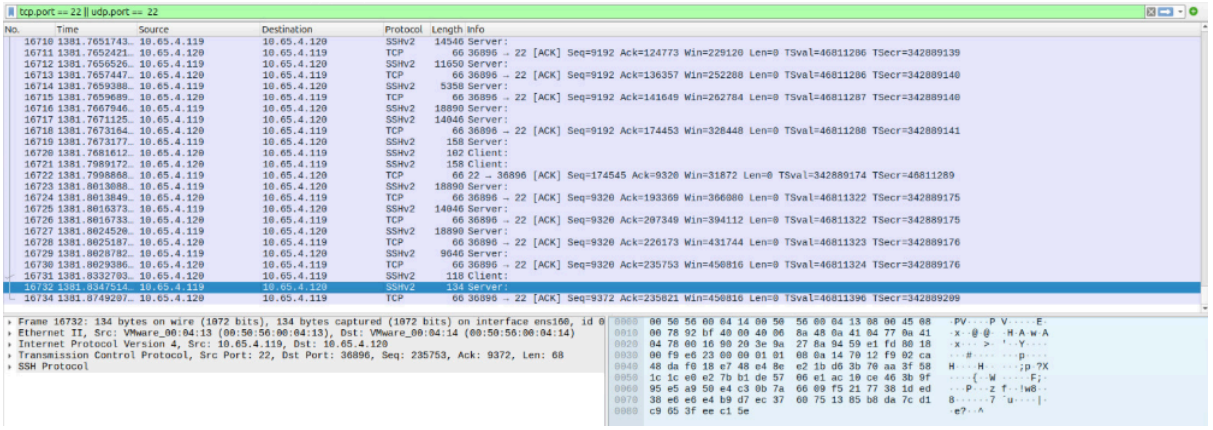
Ejecución del comando sshfs



Muestra el directorio local /home/gabi/Documentos montado via SSHFS.



Muestra el directorio remoto original (/home/Lauti/Documentos) en el servidor.



El análisis de Wireshark mostró la naturaleza cifrada del tráfico (evidenciado por los datos ilegibles), confirmando la seguridad de la solución. A diferencia de Rsync que sincroniza archivos puntualmente, SSHFS mantiene una conexión persistente permitiendo trabajar con archivos remotos como si fueran locales.