

TP 5 REDES

Integrantes: Giovani Azurduy , Lautaro Larosa

Actividad 1:SSH

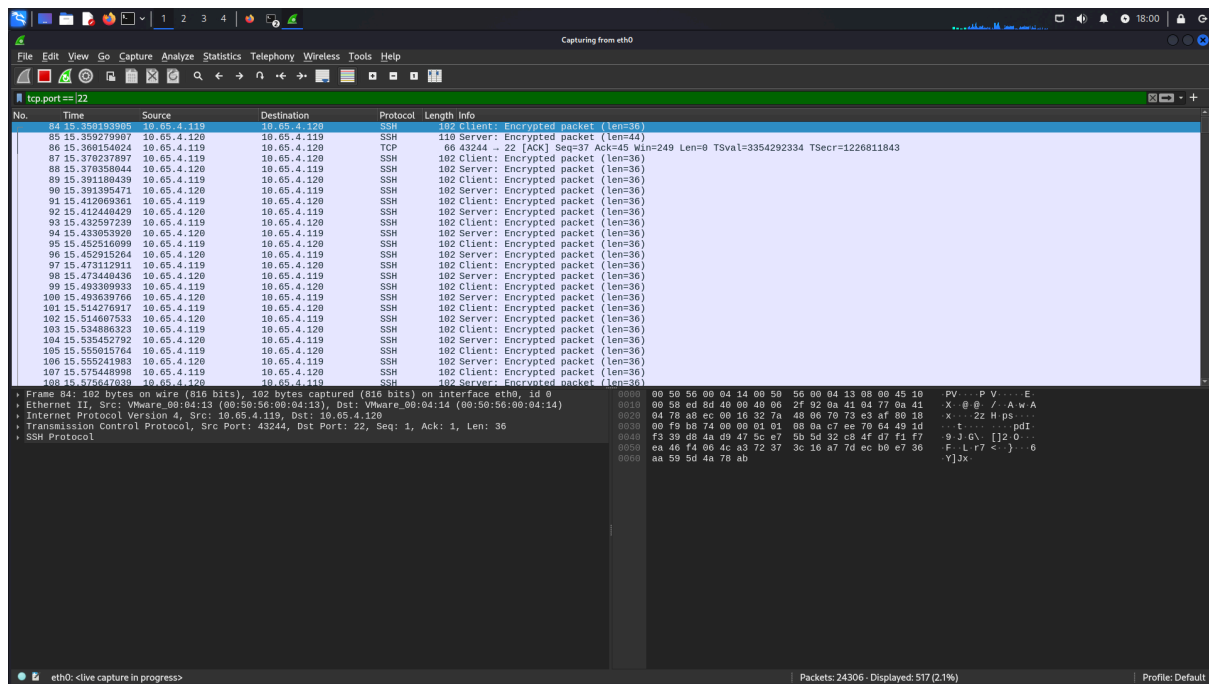
El objetivo principal de la actividad de SSH es aprender a establecer conexiones seguras entre computadoras mediante el protocolo SSH, permitiéndoles administrar sistemas remotos de forma encriptada. Esto incluye ejecutar comandos a distancia, transferir archivos de manera segura con SCP, redirigir interfaces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

```
user@ubuntu:/home/estudiante$ sudo ssh kali@10.65.4.119
The authenticity of host '10.65.4.119 (10.65.4.119)' can't be established.
ED25519 key fingerprint is SHA256:lNaAkav2B5RzGg7BeGTVZoXMZTcwiyp0tEfuF0DrPk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.65.4.119' (ED25519) to the list of known hosts.
kali@10.65.4.119's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 21 14:00:51 2025 from 10.65.4.120
└─(kali@kali)-[~]
└─$ touch juaniArchivo.txt
```

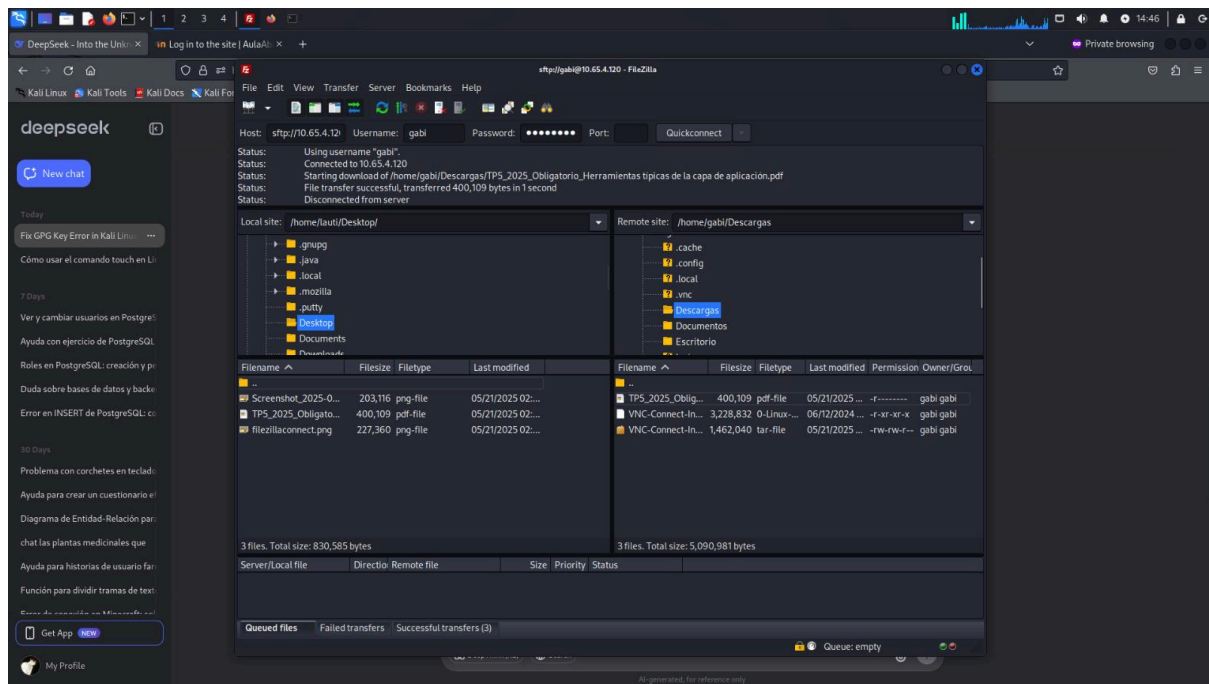
Muestra una conexión SSH establecida desde Ubuntu a una máquina Kali (10.65.4.119).



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.



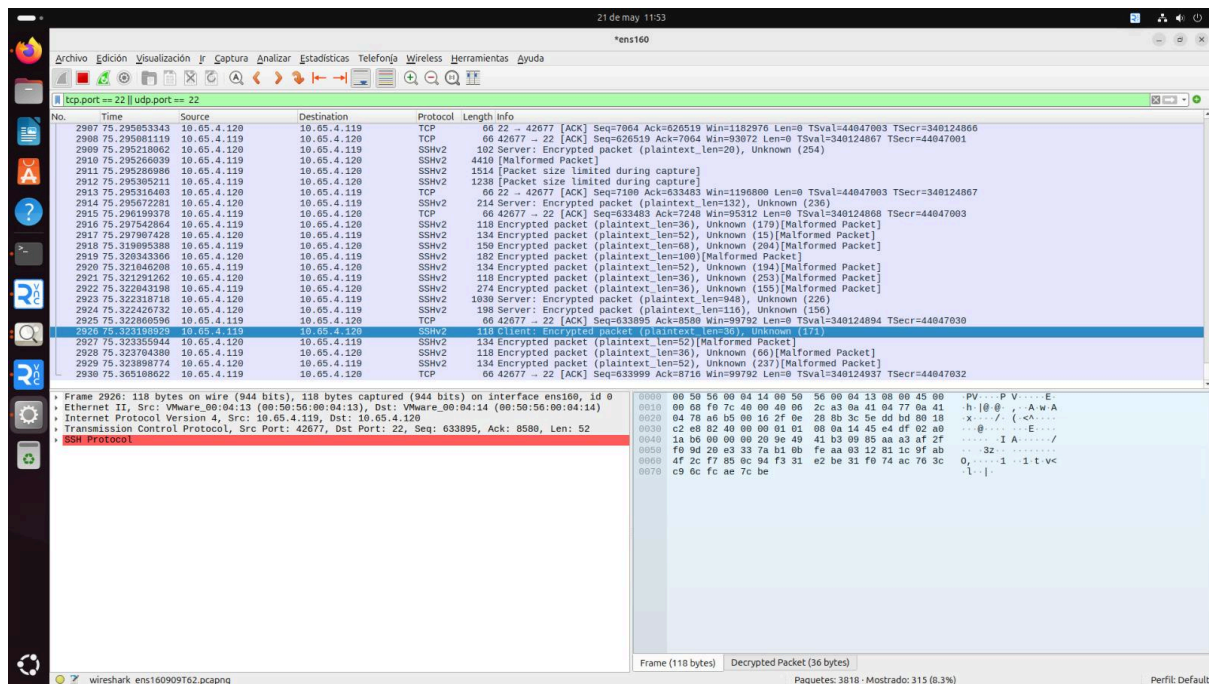
Conexión exitosa al servidor `sftp://10.65.4.120` con usuario `gabi` (puerto SFTP/SSH implícito).

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).



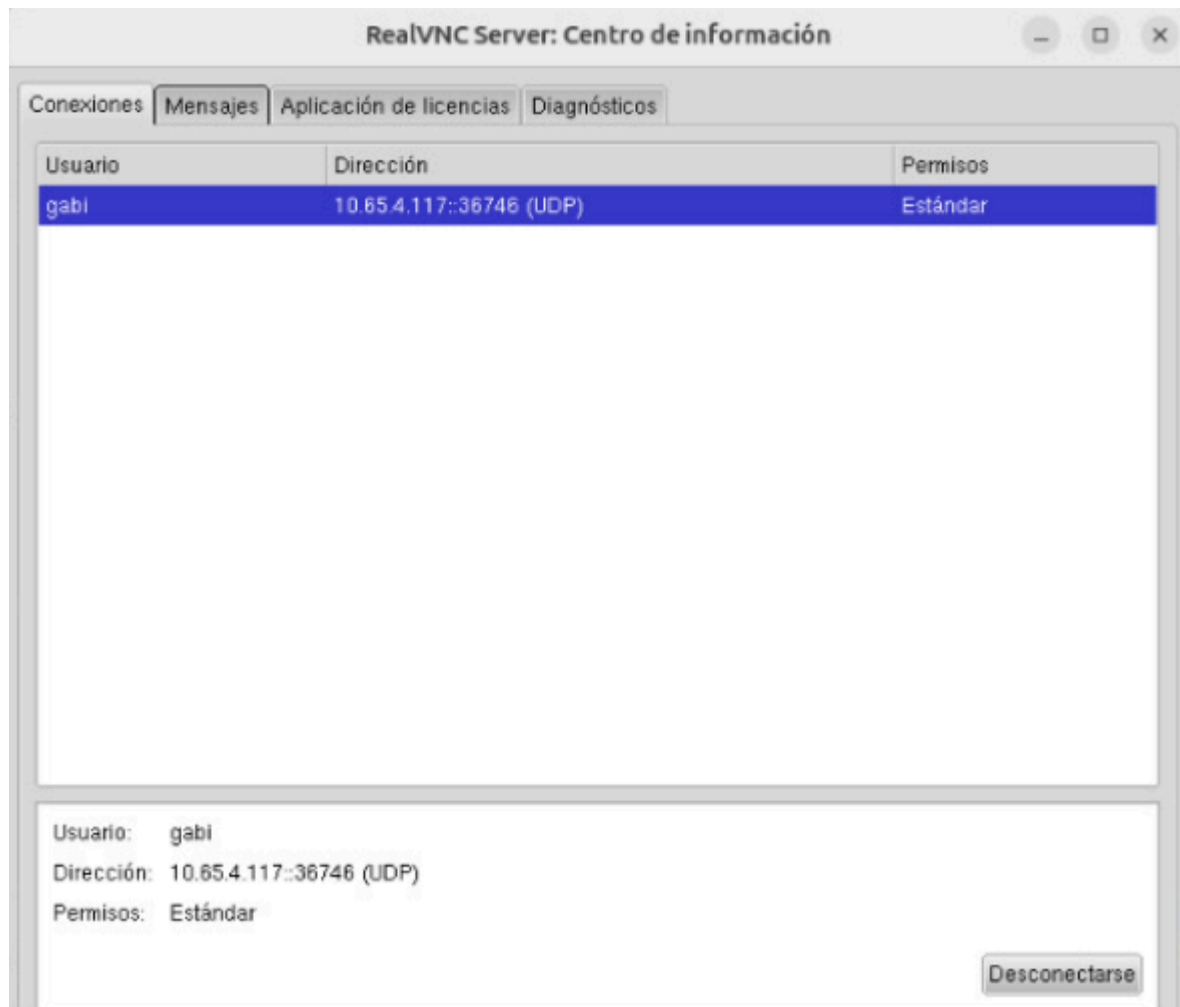
Protocolo: SFTP sobre SSH (puerto 22).

Actividad 3:VNC

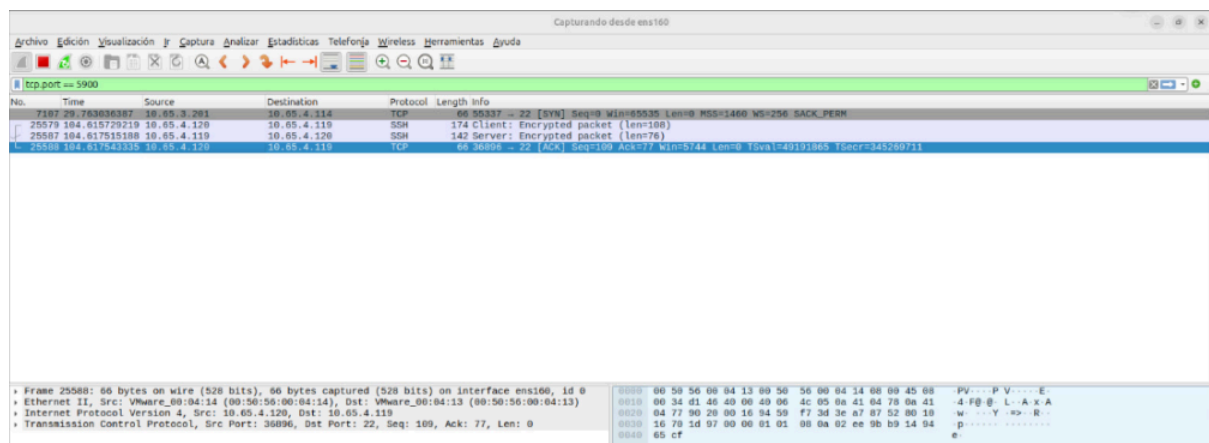
Descripción de la actividad

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.

```
user@ubuntu:/home/estudiante$ sudo rsync -r -v /home/user/Descargas/server.py gabi@10.65.4.120:/home/gabi/Descargas/
gabi@10.65.4.120's password:
sending incremental file list
server.py

sent 2.883 bytes  received 35 bytes  448,92 bytes/sec
total size is 2.789  speedup is 0,96
user@ubuntu:/home/estudiante$
```

Ejecución práctica del comando Rsync

Io	Time	Source	Destination	Protocol	Length	Info
542	15.084142215	10.65.4.117	10.65.4.120	TCP	74	42828 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1683221375 TSecr=0 WS=128
583	15.084326874	10.65.4.120	10.65.4.117	TCP	74	22 -> 42828 [SYN, ACK] Seq=0 Ack=1 Win=65169 Len=0 MSS=1460 SACK_PERM TSval=2721361217 TSecr=1683221375 WS=128
584	15.085110265	10.65.4.117	10.65.4.120	TCP	66	42828 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1683221376 TSecr=2721361217
585	15.085455395	10.65.4.117	10.65.4.120	SSHv2	109	Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11)
586	15.085459686	10.65.4.120	10.65.4.117	TCP	66	22 -> 42828 [ACK] Seq=1 Ack=44 Win=65152 Len=0 TSval=2721361219 TSecr=1683221376
587	15.126438721	10.65.4.120	10.65.4.117	SSHv2	109	Server: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11)
588	15.127175495	10.65.4.117	10.65.4.120	TCP	66	42828 -> 22 [ACK] Seq=44 Ack=44 Win=64256 Len=0 TSval=1683221418 TSecr=2721361269
589	15.127968786	10.65.4.117	10.65.4.120	SSHv2	1662	Client: Key Exchange Init
590	15.128018763	10.65.4.120	10.65.4.117	TCP	66	22 -> 42828 [ACK] Seq=44 Ack=1580 Win=63616 Len=0 TSval=2721361261 TSecr=1683221418
591	15.132294988	10.65.4.120	10.65.4.117	SSHv2	1186	Server: Key Exchange Init
592	15.174263999	10.65.4.117	10.65.4.120	TCP	66	42828 -> 22 [ACK] Seq=1580 Ack=1164 Win=66848 Len=0 TSval=1683221465 TSecr=2721361285
593	15.227528717	10.65.4.117	10.65.4.120	SSHv2	1274	Client: Diffie-Hellman Key Exchange Init
594	15.243842988	10.65.4.120	10.65.4.117	SSHv2	1598	Server: Diffie-Hellman Key Exchange Reply, New Keys
595	15.243645180	10.65.4.117	10.65.4.120	TCP	66	42828 -> 22 [ACK] Seq=2788 Ack=2696 Win=64640 Len=0 TSval=1683221534 TSecr=2721361376
596	15.267711894	10.65.4.117	10.65.4.120	SSHv2	159	Client: New Keys
597	15.308494582	10.65.4.120	10.65.4.117	TCP	66	22 -> 42828 [ACK] Seq=2696 Ack=2872 Win=62464 Len=0 TSval=2721361442 TSecr=1683221558
598	15.308988820	10.65.4.117	10.65.4.120	SSHv2	118	Client: New Keys
599	15.309835237	10.65.4.120	10.65.4.117	TCP	66	22 -> 42828 [ACK] Seq=2696 Ack=2916 Win=62464 Len=0 TSval=2721361442 TSecr=1683221600
600	15.309148024	10.65.4.120	10.65.4.117	SSHv2	118	Server: New Keys
601	15.309638518	10.65.4.117	10.65.4.120	SSHv2	126	Client: New Keys
602	15.31101183	10.65.4.120	10.65.4.117	SSHv2	330	Server: New Keys
603	15.352473319	10.65.4.117	10.65.4.120	TCP	66	42828 -> 22 [ACK] Seq=2976 Ack=3004 Win=64384 Len=0 TSval=1683221643 TSecr=2721361444

Frame 244: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface ens160, id 0

Ethernet II, Src: QuantatComput_a5:60:15 (c8:0a:a9:a5:60:15), Dst: VMware_00:04:01 (08:00:56:00:04:01)

Internet Protocol Version 4, Src: 10.65.4.141, Dst: 10.65.4.101

Transmission Control Protocol, Src Port: 55254, Dst Port: 22, Seq: 1, Ack: 1, Len: 68

SSH Protocol

0000 00 50 56 00 04 01 c8 0a a9 a5 60 15 08 00 45 10 PV.....E..

0010 00 78 39 17 40 00 49 06 e3 e5 0a 41 04 8d 0a 41 x9-0-0...A..

0020 04 05 07 06 00 16 fe 45 7e 1d e6 35 03 a1 80 18 e...E...S...

0030 30 ff af 56 00 00 01 01 00 0a 51 c8 cc ad f2 c3 0-V.....Q....

0040 83 44 7a b0 dd b4 35 f8 b0 9e dc cd ef 11 7f cd 0z...5.....

0050 a4 c1 2c 41 62 5a 05 53 23 19 12 83 30 a1 80 57 ..Ch2-S#...0-W

0060 b5 02 cc 69 66 a0 c9 30 bd 2a bb d4 4f 63 2f f3 ...1F-0-*...dc/

0070 f0 4a cb 3c 00 25 dd 03 88 05 1d 4f 60 1c 41 bb J.<-%-...0h-A-

0080 ef f1 94 a5 0d 399

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.

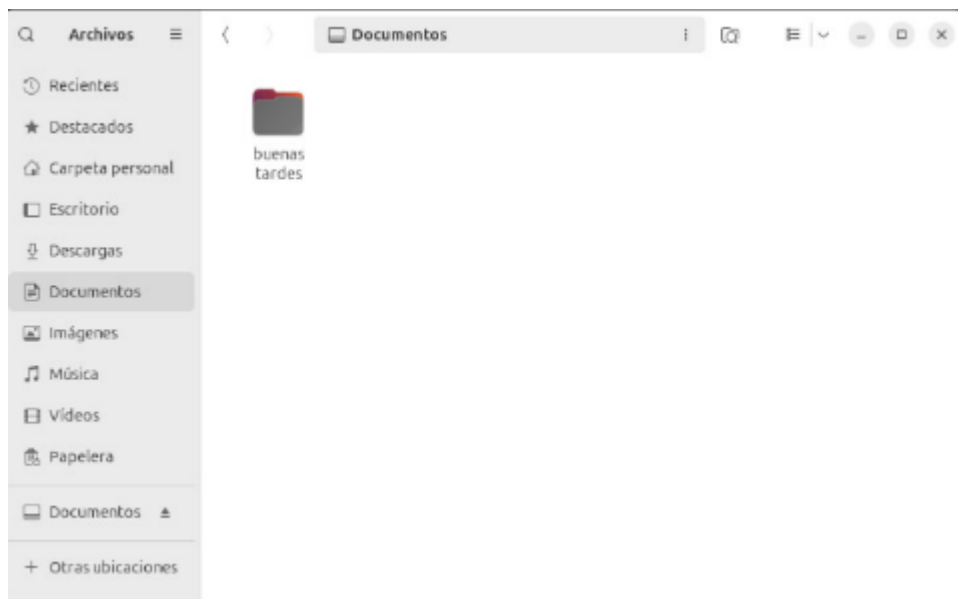
Actividad 5:SSHFS

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.

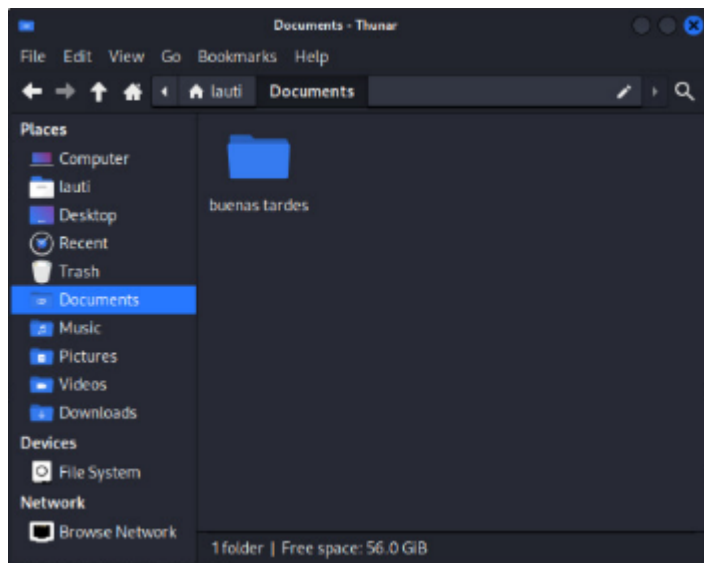
Esta actividad permite comprender cómo SSHFS utiliza el protocolo SSH para proporcionar acceso seguro a sistemas de archivos remotos.

```
gabi@ubuntu:~/Descargas$ sshfs lautl@10.65.4.119:/home/lautl/Documents /home/gabi/Documentos
lautl@10.65.4.119's password:
gabi@ubuntu:~/Descargas$
```

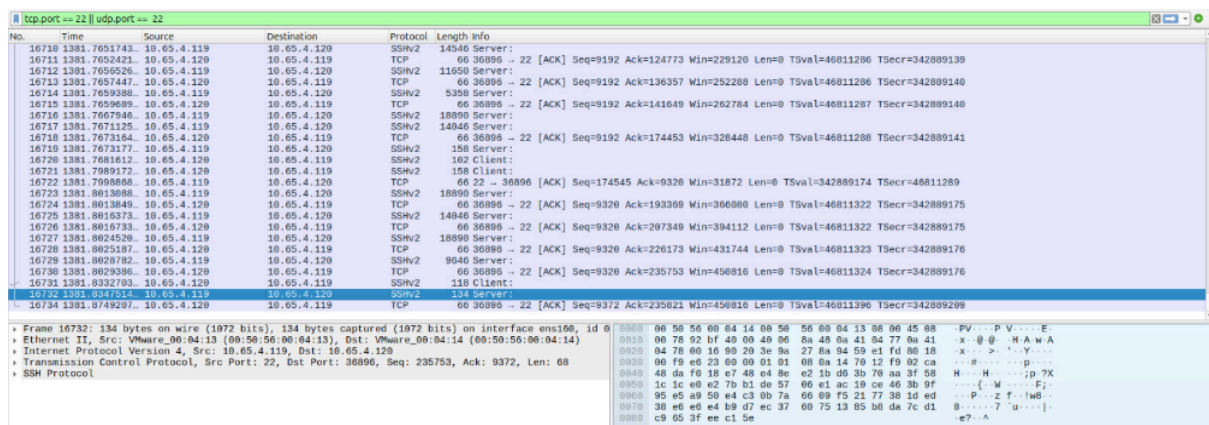
Ejecución del comando sshfs



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.