

Informe del Trabajo Práctico N.º 5

Herramientas y protocolos de la capa de aplicación

Introducción

El presente trabajo práctico tuvo como objetivo experimentar con diferentes **herramientas reales utilizadas en la capa de aplicación** del modelo TCP/IP, basadas en el modelo **cliente-servidor**. A través de cinco actividades, se configuraron servicios como SSH, FTP, VNC, Rsync y SSHFS entre dos computadoras conectadas en una misma red local. Se analizaron los paquetes intercambiados con **Wireshark** y se exploraron los mecanismos de funcionamiento, transferencia de archivos y seguridad.

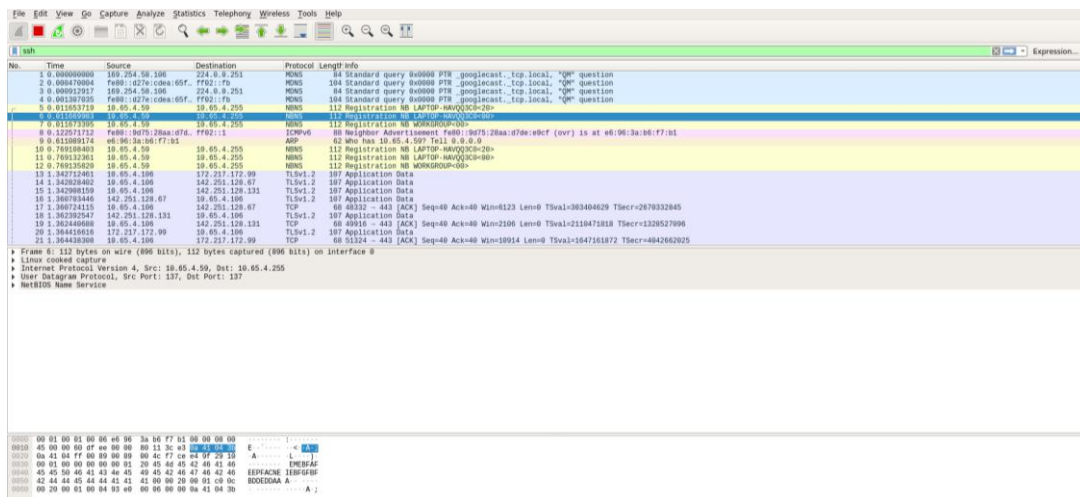
Actividad 1 – SSH

Se instaló y configuró un **servidor SSH** en una computadora con Linux y se establecieron conexiones desde un cliente remoto utilizando el comando ssh.

Acciones realizadas:

- Obtención de IP remota.
- Visualización y modificación de archivos en el escritorio remoto (touch, rm).
- Cierre de procesos con top, grep y kill.
- Apagado remoto con sudo shutdown -h now.
- Transferencia de archivos usando scp.
- Ejecución de programas gráficos mediante redirección X (ssh -X usuario@IP, luego firefox, cheese, etc).

```
tp5redes@ubuntu: ~/Escritorio
tp5redes@ubuntu:~$ cd Escritorio
tp5redes@ubuntu:~/Escritorio$ touch prueba.txt
tp5redes@ubuntu:~/Escritorio$ scp /home/tp5redes/Escritorio/prueba.txt caposlcc@
10.65.4.110:/home/caposlcc/Escritorio
The authenticity of host '10.65.4.110 (10.65.4.110)' can't be established.
ED25519 key fingerprint is SHA256:BBX4dTf1Q64pByo8VukFIJ0hkOUzXcIJLAMNYs1BwxU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.65.4.110' (ED25519) to the list of known hosts.
caposlcc@10.65.4.110's password:
prueba.txt                                100% 0    0.0KB/s  00:00
tp5redes@ubuntu:~/Escritorio$
```



Actividad 2 – FTP

Se instaló un **servidor vsftpd** y se utilizó **FileZilla** como cliente para transferir archivos en ambos sentidos entre las dos computadoras.

Acciones realizadas:

- Transferencia de archivos desde cliente a servidor y viceversa.
- Verificación de permisos de escritura en el servidor (write_enable=YES).

Estado: El servidor no permite caracteres no ASCII.

Estado: Registrado en

Estado: Comenzando la subida de /home/Usuario/Imágenes/Screenshot_2025-05-14_14-33-57.jpg

Estado: Transferencia correcta, transferidos 85.115 bytes en 3 segundos

Estado: Desconectado del servidor

Sitio local: /home/Usuario/Imágenes/

Sitio remoto: /home/test

..

ScreenShot_2025-05-14_14-33-57.jpg

Nombre de archivo | Tamaño de archivo | Tipo de archivo | Última modificac

1 archivo seleccionado. Tamaño total: 85.115 bytes

home

test

Nombre de archivo | Tamaño de archivo | Tipo de archivo | Última modificac | Permisos

Public | Directorio | 14/05/25 06:00 | drwxr-xr-x | 1

Templates | Directorio | 14/05/25 06:00 | drwxr-xr-x | 1

1 archivo seleccionado. Tamaño total: 0 bytes

Servidor/Archivo local

Dirección Archivo remoto

Tamaño

Prioridad

Hora

test@10.65.4.106

/home/Usuario/Imágenes/ejemplo.png <-- /home/test/ejemplo.png 0 Normal 14/05/25 15:...

test@10.65.4.106

/home/Usuario/Imágenes/Screenshot_2025-05-14_14-33-57.jpg --> /home/test/Screenshot... 85.115 Normal 14/05/25 16:...

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

10.65.4.106

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1155	515.104317620	10.65.4.106	10.65.4.106	FTP	76	Request: AUTH TLS
1160	515.104317620	10.65.4.106	10.65.4.106	FTP	106	Response: 530 Please login with USER and PASS.
1170	516.044819660	10.65.4.106	10.65.4.106	FTP	76	Request: AUTH SSL
1171	516.044819660	10.65.4.106	10.65.4.106	FTP	106	Response: 530 Please login with USER and PASS.
1180	525.225508280	10.65.4.106	10.65.4.106	FTP	76	Request: USER test
1189	525.225508280	10.65.4.106	10.65.4.106	FTP	102	Response: 331 Please specify the password.
1204	526.47835447	10.65.4.106	10.65.4.106	FTP	76	Request: PASS 1234
1209	526.265652771	10.65.4.106	10.65.4.106	FTP	91	Response: 230 Login successful.
1207	526.558439441	10.65.4.106	10.65.4.106	FTP	74	Request: SYST
1209	526.558439441	10.65.4.106	10.65.4.106	FTP	87	Response: 215 UNIX Type: L8
1210	527.000209047	10.65.4.106	10.65.4.106	FTP	74	Request: FEAT
1211	527.000209047	10.65.4.106	10.65.4.106	FTP	83	Response: 211 Features:
1212	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Request: EPRT
1213	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Response: EPRT
1214	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Request: MDTM
1215	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Response: MDTM
1216	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Request: PASV
1217	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Response: PASV
1218	527.000209047	10.65.4.106	10.65.4.106	FTP	75	Request: TYPE
1219	527.000209047	10.65.4.106	10.65.4.106	FTP	77	Response: 211 End
1221	527.299489880	10.65.4.106	10.65.4.106	FTP	73	Request: PWD
1222	527.299489880	10.65.4.106	10.65.4.106	FTP	111	Response: 257 "/home/test" is the current directory
1223	527.304827241	10.65.4.106	10.65.4.106	FTP	73	Request: TYPE I
1224	527.304827241	10.65.4.106	10.65.4.106	FTP	99	Response: 280 Switching to Binary mode.
1227	527.304827241	10.65.4.106	10.65.4.106	FTP	74	Request: LIST
1228	527.304827241	10.65.4.106	10.65.4.106	FTP	117	Response: 227 Entering Passive Mode (10,65,4,106,138,94).
1229	528.381322222	10.65.4.106	10.65.4.106	FTP	74	Request: LIST
1230	528.381322222	10.65.4.106	10.65.4.106	FTP	107	Response: 150 Here comes the directory listing.
1231	529.47179971802	10.65.4.106	10.65.4.106	FTP	82	Response: 226 Directory send OK.
1244	529.800575450	10.65.4.106	10.65.4.106	FTP	86	Request: MDTM ejemplo.png
1245	529.800575450	10.65.4.106	10.65.4.106	FTP	86	Response: 213 200804140205
1099	695.790211851	10.65.4.106	10.65.4.106	FTP	88	Response: 220 FTPD 3.0.3
1761	695.790211851	10.65.4.106	10.65.4.106	FTP	76	Request: AUTH TLS
1763	695.790211851	10.65.4.106	10.65.4.106	FTP	106	Response: 530 Please login with USER and PASS.
1764	695.790211851	10.65.4.106	10.65.4.106	FTP	76	Request: AUTH SSL
1765	695.790211851	10.65.4.106	10.65.4.106	FTP	106	Response: 530 Please login with USER and PASS.
1767	695.854388789	10.65.4.106	10.65.4.106	FTP	76	Request: USER test
1768	695.854388789	10.65.4.106	10.65.4.106	FTP	102	Response: 331 Please specify the password.
1712	695.860413887	10.65.4.106	10.65.4.106	FTP	91	Response: 230 Login successful.
1713	695.860413887	10.65.4.106	10.65.4.106	FTP	84	Request: CWD /home/test
1715	695.860413887	10.65.4.106	10.65.4.106	FTP	105	Response: 250 Directory successfully changed.
1716	695.860413887	10.65.4.106	10.65.4.106	FTP	73	Request: PWD
1717	695.860413887	10.65.4.106	10.65.4.106	FTP	111	Response: 257 "/home/test" is the current directory
1719	695.902874789	10.65.4.106	10.65.4.106	FTP	76	Request: TYPE I
1720	695.902874789	10.65.4.106	10.65.4.106	FTP	99	Response: 280 Switching to Binary mode.
1722	695.904982329	10.65.4.106	10.65.4.106	FTP	74	Request: PASV
1723	695.904982329	10.65.4.106	10.65.4.106	FTP	118	Response: 227 Entering Passive Mode (10,65,4,106,248,157).
1724	695.907700707	10.65.4.106	10.65.4.106	FTP	109	Request: STOR Screenshot_2025-05-14_14-33-57.jpg
1725	695.907700707	10.65.4.106	10.65.4.106	FTP	92	Response: 550 Permission denied.
1730	695.91543747	10.65.4.106	10.65.4.106	CTP	53	Shutdown: CWD /home/test (0 bytes)

Frame 1545: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.65.4.106, Dst: 10.65.4.69

Transmission Control Protocol, Src Port: 21, Dst Port: 47832, Seq: 1, Ack: 1, Len: 28

File Transfer Protocol (FTP)

(Current working directory: /)

00 04 00 01 00 06 00 58 56 00 04 04 7a 2a 08 00

0000 40 00 00 00 20 00 00 00 00 00 00 00 00 00 00

E H- g - A J

Actividad 3 – VNC

Se instaló un servidor VNC (x11vnc) y se accedió remotamente desde un cliente RealVNC Viewer.

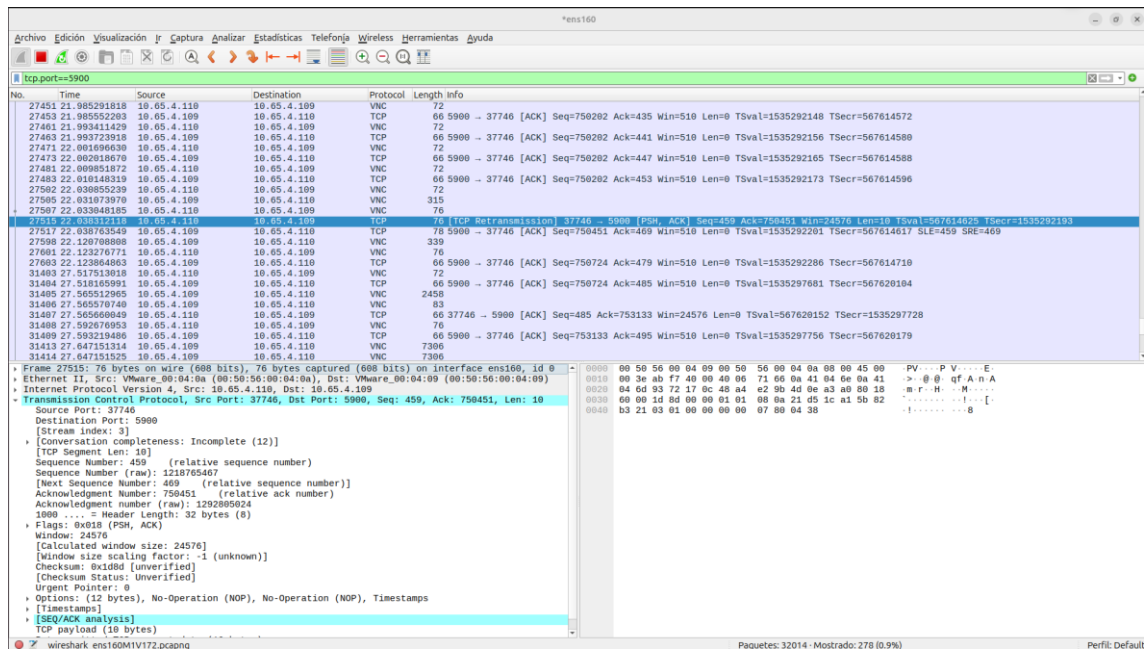
Acciones realizadas:

- Visualización remota del escritorio.
- Control de la computadora servidor (movimiento de archivos, apertura de aplicaciones).

Integrantes: Martina Nahman y Emiliano Germani



Integrantes: Martina Nahman y Emiliano Germani



Actividad 4 – Rsync

Se utilizó **rsync** para sincronizar carpetas entre dos computadoras (Linux a Linux) que estaban en la misma red. Es decir, **lo que se agregaba, modificaba o eliminaba en una carpeta en una PC, se replicaba automáticamente en la otra**, manteniendo ambas carpetas idénticas.

¿Cómo se hizo?

- Se creó una carpeta con algunos archivos en una computadora.
- Luego, desde la otra computadora, se ejecutó el comando **rsync** para copiar esa carpeta por red.
- Cuando se agregaron nuevos archivos a la carpeta original, se volvió a ejecutar **rsync**, y los nuevos archivos aparecieron **automáticamente** en la otra computadora.
- No fue necesario copiar uno por uno: **rsync** detecta los cambios y solo transfiere lo nuevo o modificado.

Acciones realizadas:

- Sincronización de carpetas locales y remotas.
- Uso de banderas **-r** (recursiva), **-v** (verbo) y **--delete** para mantener estructuras espejo.


```
estudiante@ubuntu: ~  
jun 04 10:14:34 ubuntu systemd[1]: rsync.service - fast remote file copy progra>  
jun 04 11:00:54 ubuntu systemd[1]: rsync.service - fast remote file copy progra>  
  
estudiante@ubuntu:~$ mkdir ~/prueba_rsync  
echo "Hola Mundo" > ~/prueba_rsync/archivo1.txt  
echo "Otro archivo" > ~/prueba_rsync/archivo2.txt  
estudiante@ubuntu:~$ rsync -r -v ~/prueba_rsync/ caposlcc@10.65.4.110:/home/capo  
slcc/pruebatp5/  
The authenticity of host '10.65.4.110 (10.65.4.110)' can't be established.  
ED25519 key fingerprint is SHA256:BBX4dTf1Q64pByo8VukFIJ0hkOUzXcIJLAMNYs1BwxU.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? lcc12345678  
9  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '10.65.4.110' (ED25519) to the list of known hosts.  
caposlcc@10.65.4.110's password:  
sending incremental file list  
archivo1.txt  
archivo2.txt  
  
sent 197 bytes  received 54 bytes  11,16 bytes/sec  
total size is 24  speedup is 0,10  
estudiante@ubuntu:~$
```

Archivos

Recientes

★ Destacados

Carpeta personal

Escritorio

Descargas

Documentos

Imágenes

Música

Videos

Papelera

+ Otras ubicaciones

Carpeta personal / pruebatp5

archivo1.txt

archivo2.txt

Integrantes: Martina Nahman y Emiliano Germani

No.	Time	Source	Destination	Protocol	Length	Info
2044	129.052643853	10.05.4.110	10.05.4.109	TCP	66	22 → 37792 [ACK] Seq=3084 Ack=3132 Win=62464 Len=0 TSval=568591606 TSecr=1536269140
2045	129.099642375	10.05.4.110	10.05.4.109	SSHv2	94	Server:
2046	129.100254328	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=3132 Ack=3032 Win=64384 Len=0 TSval=1536269228 TSecr=568591653
2047	129.100919382	10.05.4.109	10.05.4.110	SSHv2	178	Client:
2048	129.100942036	10.05.4.110	10.05.4.109	TCP	66	22 → 37792 [ACK] Seq=3032 Ack=3244 Win=62464 Len=0 TSval=568591654 TSecr=1536269229
2049	129.170295905	10.05.4.110	10.05.4.109	SSHv2	694	Server:
2050	129.211766087	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=3244 Ack=3660 Win=63872 Len=0 TSval=1536269340 TSecr=568591724
2051	129.211796162	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2052	129.212495616	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=3244 Ack=3704 Win=63872 Len=0 TSval=1536269340 TSecr=568591765
2053	129.212998075	10.05.4.109	10.05.4.110	SSHv2	870	Client:
2054	129.213021545	10.05.4.110	10.05.4.109	TCP	66	22 → 37792 [ACK] Seq=3704 Ack=4048 Win=61096 Len=0 TSval=568591767 TSecr=1536269341
2055	129.213773396	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2056	129.214881037	10.05.4.109	10.05.4.110	SSHv2	110	Client:
2057	129.218674122	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2058	129.220090603	10.05.4.110	10.05.4.109	SSHv2	142	Server:
2059	129.221024805	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=4092 Ack=3896 Win=63872 Len=0 TSval=1536269349 TSecr=568591772
2060	129.225943248	10.05.4.109	10.05.4.110	SSHv2	134	Client:
2061	129.226163249	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2062	129.227623399	10.05.4.109	10.05.4.110	SSHv2	174	Client:
2063	129.227662684	10.05.4.110	10.05.4.109	SSHv2	142	Server:
2064	129.228254072	10.05.4.109	10.05.4.110	SSHv2	214	Client:
2065	129.228847938	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2066	129.229362196	10.05.4.109	10.05.4.110	SSHv2	110	Client:
2067	129.229514522	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2068	129.230669745	10.05.4.109	10.05.4.110	SSHv2	110	Client:
2069	129.230835471	10.05.4.110	10.05.4.109	SSHv2	110	Server:
2070	129.251789903	10.05.4.110	10.05.4.109	SSHv2	242	Server:
2071	129.252460437	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=4512 Ack=4324 Win=63744 Len=0 TSval=1536269380 TSecr=568591784
2072	129.252606238	10.05.4.109	10.05.4.110	SSHv2	102	Client:
2073	129.252726825	10.05.4.110	10.05.4.109	SSHv2	126	Client:
2074	129.252778020	10.05.4.110	10.05.4.109	TCP	66	22 → 37792 [ACK] Seq=4324 Ack=4608 Win=62464 Len=0 TSval=568591806 TSecr=1536269381
2075	129.252826805	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [FIN, ACK] Seq=4608 Ack=4324 Win=63744 Len=0 TSval=1536269391 TSecr=568591784
2076	129.257490828	10.05.4.110	10.05.4.109	TCP	66	22 → 37792 [FIN, ACK] Seq=4324 Ack=4609 Win=62464 Len=0 TSval=568591811 TSecr=1536269381
2077	129.257893291	10.05.4.109	10.05.4.110	TCP	66	37792 → 22 [ACK] Seq=4609 Ack=4325 Win=63744 Len=0 TSval=1536269386 TSecr=568591811

[TCP Segment Len: 0]
Sequence Number: 4324 (relative sequence number)
Sequence Number (raw): 2819858419
[Next Sequence Number: 4325 (relative sequence number)]
Acknowledgment Number: 4609 (relative ack number)
Acknowledgment number (raw): 3225632143
1000 ... = Header Length: 32 bytes (8)
Flags: 0x011 (FIN, ACK)
Window: 488
[Calculated window size: 62464]
[Window size scaling factor: 128]
Checksum: 0x1d83 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
wireshark_ens160b7KZ72.pcapng Paquetes: 2852 - Mostrado: 114 (4.0%) Perfil: Default

Actividad 5 – SSHFS

Se utilizó **SSHFS** para montar el sistema de archivos de una computadora sobre otra mediante SSH.

Acciones realizadas:

- Montaje de carpeta remota con sshfs usuario@IP:/ruta /punto_montaje
- Modificación y creación de archivos desde el cliente.
- Verificación de cambios reflejados en el servidor.
- Desmontaje con umount.

Integrantes: Martina Nahman y Emiliano Germani

The image shows a Linux desktop environment with a terminal window and a Wireshark network traffic analysis window.

Terminal Window:

```
caposlcc@ubuntu:~$ man:ssh config($)  
Process: 10453 ExecStartPre=/usr/sbin/ssh -t (code=exited, status=0/SUCCESS)  
Main PID: 10453 (sshd)  
Tasks: 1 (limit: 14794)  
Memory: 2.2M (peak: 20.7M)  
CPU: 47ms  
CGroup: /system.slice/ssh.service  
└─10453 "sshd: /usr/sbin/ssh -D [listener] 0 of 10-100 startups"  
  
jun 04 11:07:45 ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell server.  
jun 04 11:08:07 ubuntu sshd[10454]: Accepted password for caposlcc from 10.65.4.109  
jun 04 11:08:07 ubuntu sshd[10454]: pam_unix(sshd:session): session opened for caposlcc  
jun 04 11:11:00 ubuntu sshd[10861]: Accepted password for caposlcc from 10.65.4.109  
jun 04 11:11:00 ubuntu sshd[10861]: pam_unix(sshd:session): session opened for caposlcc  
jun 04 11:11:01 ubuntu sshd[10861]: pam_unix(sshd:session): session closed for caposlcc  
jun 04 11:11:51 ubuntu sshd[10989]: Accepted password for caposlcc from 10.65.4.109  
jun 04 11:11:51 ubuntu sshd[10989]: pam_unix(sshd:session): session opened for caposlcc  
jun 04 11:11:51 ubuntu sshd[10989]: pam_unix(sshd:session): session closed for caposlcc  
  
caposlcc@ubuntu:~$ mkdir -p /home/estudiante/compartida  
mkdir: no se puede crear el directorio «/home/estudiante»: Permiso denegado  
caposlcc@ubuntu:~$ mkdir -p /home/caposlcc/compartida
```

Wireshark Window:

The Wireshark window shows a packet capture on the interface `ens160`. The filter is `tcp.port==22`. The packet list shows several SSH packets (TCP 22) between 10.65.4.109 and 10.65.4.110. The packet details pane shows the structure of an SSH packet, including the header and the encrypted payload.

No.	Time	Source	Destination	Protocol	Length	Info
3554	10.663357767	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=601 Ack=193 Win=487 Len=0 TSval=1537064547 TSecr=569326974
3653	10.755548220	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
3655	10.756170453	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
3656	10.756622193	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=781 Ack=325 Win=487 Len=0 TSval=1537064641 TSecr=569327068
3791	10.889367681	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
3793	10.890538444	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
3794	10.891689607	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=881 Ack=1057 Win=487 Len=0 TSval=1537064775 TSecr=569327282
4195	20.285563766	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
4197	20.285851824	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
4198	20.286239978	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=901 Ack=1108 Win=487 Len=0 TSval=1537065170 TSecr=569327597
4320	20.408911239	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
4322	20.409259149	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
4323	20.409677810	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=1001 Ack=1321 Win=487 Len=0 TSval=1537065294 TSecr=569327721
4896	20.982457345	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
4898	20.983412248	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
4900	20.983822000	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=1101 Ack=1453 Win=487 Len=0 TSval=1537065868 TSecr=569328295
4901	20.98459183	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
4904	20.985716906	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
4906	20.986691882	10.65.4.109	10.65.4.110	SSH	142	Client: Encrypted packet (len=76)
4908	20.987867398	10.65.4.110	10.65.4.109	SSH	142	Server: Encrypted packet (len=76)
4910	20.989454418	10.65.4.109	10.65.4.110	SSH	106	Client: Encrypted packet (len=100)
4913	20.991534064	10.65.4.110	10.65.4.109	SSH	198	Server: Encrypted packet (len=132)
4916	20.993288984	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4918	20.993889402	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4919	20.994886549	10.65.4.109	10.65.4.110	SSH	158	Client: Encrypted packet (len=92)
4921	20.995522663	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4923	20.996449782	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4925	20.997341753	10.65.4.110	10.65.4.109	SSH	142	Server: Encrypted packet (len=76)
4944	21.014839955	10.65.4.109	10.65.4.110	SSH	142	Client: Encrypted packet (len=76)
4945	21.014939515	10.65.4.110	10.65.4.109	SSH	142	Server: Encrypted packet (len=76)
4946	21.015857526	10.65.4.109	10.65.4.110	TCP	66	22 → 47786 [ACK] Seq=2005 Ack=1789 Win=488 Len=0 TSval=1537065899
4947	21.015121239	10.65.4.110	10.65.4.109	SSH	142	Client: Encrypted packet (len=76)
4948	21.015432208	10.65.4.109	10.65.4.110	SSH	238	Server: Encrypted packet (len=164)
4951	21.016635313	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4952	21.017113283	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4954	21.018386698	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4956	21.018769155	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4958	21.020119821	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4960	21.020493919	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4961	21.021269858	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4963	21.021528386	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4964	21.022513782	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4966	21.022830886	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4971	21.026457282	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4973	21.026816536	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
4975	21.027629385	10.65.4.109	10.65.4.110	SSH	150	Client: Encrypted packet (len=84)
4976	21.027972787	10.65.4.110	10.65.4.109	SSH	134	Server: Encrypted packet (len=68)
5020	21.069513488	10.65.4.109	10.65.4.110	TCP	66	47786 → 22 [ACK] Seq=2453 Ack=2645 Win=488 Len=0 TSval=1537065954 TSecr=569328340

Frame 4976: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface ens160, id 0
Ethernet II, Src: VMware 00:04:0a:00:56:00:04:09, Dst: VMware 00:04:09:00:56:00:04:09
Internet Protocol Version 4, Src: 10.65.4.109, Dst: 10.65.4.109
Wireshark_ens160LSV72.pcapng

Paquetes: 7052 · Mostrado: 65 (0.9%) Perfil: Default

Conclusión

Este trabajo práctico permitió experimentar de forma directa con herramientas esenciales de administración remota, transferencia de archivos y sincronización en redes, todas funcionando sobre la **capa de aplicación del modelo TCP/IP**. El análisis con Wireshark complementó la experiencia brindando una visión concreta de cómo fluyen los datos entre cliente y servidor, reforzando conceptos de seguridad, puertos y protocolos. Herramientas como SSH, FTP, VNC, Rsync y SSHFS son fundamentales tanto en redes domésticas como en entornos empresariales y de administración de servidores.