Informe trabajo práctico N° 5

Integrantes: Valerio Perla, Perea Trinidad, Suden Paulina

Actividad 1:

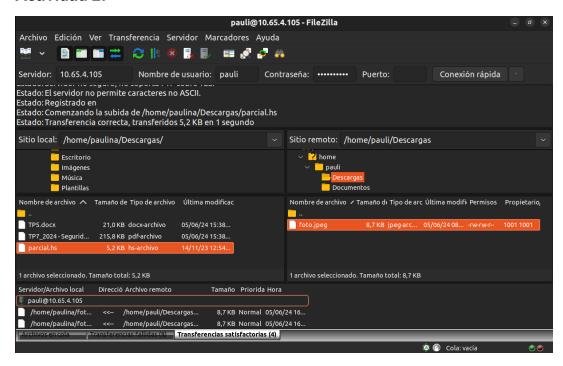
```
pauli@ubuntu:~$ hostname -I
10.65.3.119 172.17.0.1
pauli@ubuntu:~$ ls ~/Descargas
'TP5_2024 - Herramientas típicas de la capa de aplicación (1).pdf'
pauli@ubuntu:~$ top | grep firefox
   5877 pauli 20 0 11,5g 524656 220012 S 2,0 4,1 2:04.18 firefox 5877 pauli 20 0 11,5g 524912 220012 S 2,6 4,1 2:04.26 firefox 5877 pauli 20 0 11,5g 524912 220012 S 0,3 4,1 2:04.27 firefox
pauli@ubuntu:~$ pgrep -l firefox
5877 firefox
pauli@ubuntu:~$ kill 5877
pauli@ubuntu:-$ scp /home/pauli/TP7Redes.pdf pauli@10.65.3.119:/home/pauli/Documentos
pauli@10.65.3.119's password:
scp: stat local "/home/pauli/TP7Redes.pdf": No such file or directory
pauli@ubuntu:-$ scp /home/pauli/TP5.docx pauli@10.65.3.119:/home/pauli/Documentos
pauli@10.65.3.119's password:
TP5.docx
                                                    100% 20KB 5.1MB/s 00:00
```

Paquetes visualizados mediante Wireshark:

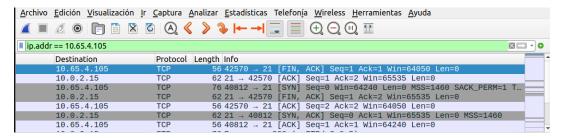
No.	Time	Source	Destination	Protocol	Length Info
	79 37.859840732	10.65.3.120	10.65.3.119	TCP	76 46646 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S/
	80 37.860746069	10.65.3.119	10.65.3.120	TCP	76 22 - 46646 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
	81 37.860773386	10.65.3.120	10.65.3.119	TCP	68 46646 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
	82 37.861049190	10.65.3.120	10.65.3.119	SSHv2	109 Client: Protocol (SSH-2.0-OpenSSH_9.3p1 Ubuntu-1ul
1	83 37.861694127	10.65.3.119	10.65.3.120	TCP	68 22 → 46646 [ACK] Seq=1 Ack=42 Win=65152 Len=0 TSv
1	84 37.865069793	10.65.3.119	10.65.3.120	SSHv2	109 Server: Protocol (SSH-2.0-OpenSSH_9.3p1 Ubuntu-1ul
1	85 37.865090111	10.65.3.120	10.65.3.119	TCP	68 46646 → 22 [ACK] Seq=42 Ack=42 Win=64256 Len=0 TS
1	86 37.865411699	10.65.3.120	10.65.3.119	SSHv2	1604 Client: Key Exchange Init
	87 37.870646696	10.65.3.119	10.65.3.120	SSHv2	1180 Server: Key Exchange Init
	88 37.912867239	10.65.3.120	10.65.3.119	TCP	68 46646 → 22 [ACK] Seq=1578 Ack=1154 Win=64128 Len=
	89 37.922288566	10.65.3.120	10.65.3.119	SSHv2	1276 Client: Diffie-Hellman Key Exchange Init
	90 37.937012070	10.65.3.119	10.65.3.120	SSHv2	1632 Server: Diffie-Hellman Key Exchange Reply, New Key
	91 37.937039101	10.65.3.120	10.65.3.119	TCP	68 46646 → 22 [ACK] Seq=2786 Ack=2718 Win=64000 Len=
1	92 37.955460068	10.65.3.120	10.65.3.119	SSHv2	84 Client: New Keys
	93 37.997471607	10.65.3.119	10.65.3.120	TCP	68 22 → 46646 [ACK] Seq=2718 Ack=2802 Win=64128 Len=
	94 37.997487388	10.65.3.120	10.65.3.119	SSHv2	112 Client:
	95 37.998409371	10.65.3.119	10.65.3.120	TCP	68 22 → 46646 [ACK] Seq=2718 Ack=2846 Win=64128 Len=
	96 37.998409448	Cisco_37:1c:19		RLDP	62 Network Loop Detection
	97 37.998426660	10.65.3.119	10.65.3.120	SSHv2	112 Server:
	98 37.998532430	10.65.3.120	10.65.3.119	SSHv2	136 Client:
	99 38.007111751	10.65.3.119	10.65.3.120	SSHv2	120 Server:

En esta actividad lo que hicimos fue, conectar dos máquinas mediante un cliente SSH y un servidor SSH y realizar distintas acciones tales como ver archivos en la carpeta de descarga, enviar archivos de una computadora a otra, entre otras.

Actividad 2:

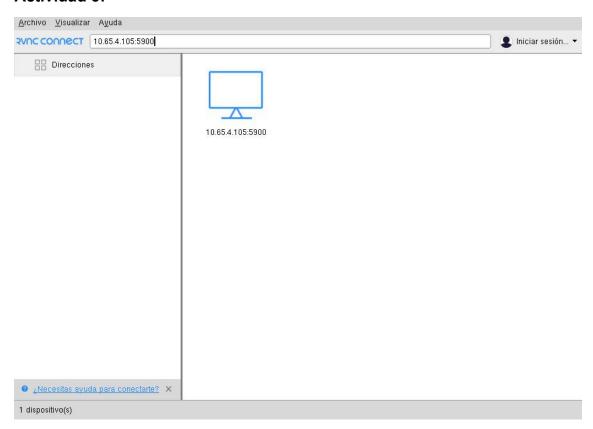


Paquetes visualizados mediante Wireshark:

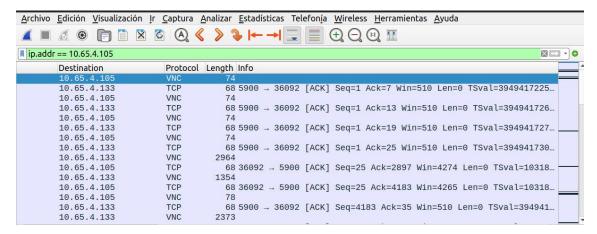


En esta actividad, desde la computadora cliente con FileZilla podemos ver los archivos del sitio remoto y del local, y realizar transferencias entre ambos, como se puede ver en la imagen.

Actividad 3:



Paquetes visualizados mediante Wireshark:



Acá, desde Real VNC, ubicamos la maquina a la que queremos conectar a través de su ip y puerto como está establecido en la parte superior de la imagen, y luego, se nos abre una pestaña en la que podemos ver la computadora con dicha ip desde nuestra computadora, y podemos realizar distintas acciones sobre esa computadora.

Actividad 4:

```
paulina@ubuntu:-$ rsync -r -v /home/paulina/Descargas/ pauli@10.65.4.105:/home/pauli/Documentos/
pauli@10.65.4.105's password:
sending incremental file list
TP5.docx
TP7_2024 - Seguridad en redes.pdf
parcial.hs
sent 242.164 bytes received 73 bytes 44.043,09 bytes/sec
total size is 241.850 speedup is 1,00
paulina@ubuntu:-$ rsync -r -v pauli@10.65.4.105:/home/pauli/Descargas/ /home/paulina/Descargas/
pauli@10.65.4.105's password:
receiving incremental file list
foto.jpeg
sent 43 bytes received 8.772 bytes 1.356,15 bytes/sec
total size is 8.662 speedup is 0,98
paulina@ubuntu:-$
```

Paquetes visualizados mediante Wireshark:

```
SSH<sub>V</sub>2
                                                       112 Client: Encrypted packet (len=44)
1.133
                 10,65,4,105
1.105
                 10.65.4.133
                                           SSHv2
                                                       112 Server: Encrypted packet (len=44)
                                                       112 Client: Encrypted packet (len=44)
                 10.65.4.105
1.133
                                           SSHv2
1.105
                 10.65.4.133
                                           SSHv2
                                                       128 Server: Encrypted packet (len=60)
1.133
                 10.65.4.105
                                           SSH<sub>V</sub>2
                                                       112 Client: Encrypted packet (len=44)
244 Server: Encrypted packet (len=176)
                                           SSHv2
1.105
                 10.65.4.133
1.133
                 10.65.4.105
                                           SSH<sub>V</sub>2
                                                       104 Client: Encrypted packet (len=36)
                 10.65.4.105
1.133
                                           SSHv2
                                                       128 Client: Encrypted packet (len=60)
```

En esta actividad, al instalar un servidor Rsync en ambas computadoras, se establece una conexión que facilita la copia y actualización de archivos de manera bidireccional, asegurando que las carpetas y archivos estén alineados entre las dos máquinas. En la imagen, se ve como se realizó una copia desde una computadora a la otra en ambas direcciones.

Actividad 5:

```
pauli@ubuntu:~$ sshfs pauli@10.65.3.120:/home/pauli/compartida /home/pauli/carpetamontaje
pauli@10.65.3.120's password:
pauli@ubuntu:~$ umount /home/pauli/carpetamontaje
```

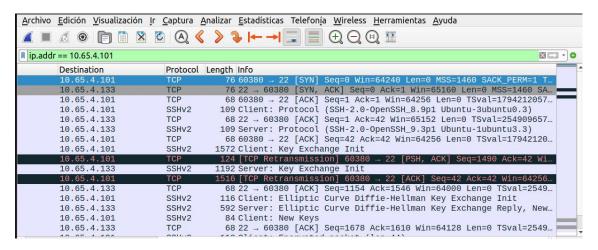
Paquetes visualizados mediante Wireshark:

No.	Time	Source	Destination	Protocol	Length Info
	221 28.267270211	10.65.3.119	142.251.133.197	TCP	68 57914 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=3390954578 TS
	222 28.455264721	10.65.3.119	142.251.133.67	TCP	68 [TCP Dup ACK 19#1] 51514 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSv
	223 28.472420983				68 [TCP Dup ACK 26#2] 80 → 51514 [ACK] Seq=1 Ack=2 Win=273 Len=0 TSv
	224 29.999569912	Cisco_37:1c:19		RLDP	62 Network Loop Detection
	225 31.256170660	10.65.3.119	10.65.3.120	SSHv2	104 Client:
	226 31.258124088	10.65.3.120	10.65.3.119	SSHv2	192 Server:
	227 31.258167942	10.65.3.119	10.65.3.120	TCP	68 57364 → 22 [ACK] Seq=4846 Ack=5138 Win=64128 Len=0 TSval=41902005
	228 31.258740007	10.65.3.119	10.65.3.120	SSHv2	104 Client:
	229 31.258796770	10.65.3.119	10.65.3.120	SSHv2	128 Client:
	230 31.258838163	10.65.3.119	10.65.3.120	TCP	68 57364 → 22 [FIN, ACK] Seq=4942 Ack=5138 Win=64128 Len=0 TSval=419
	231 31.260231644	10.65.3.120	10.65.3.119	TCP	68 22 → 57364 [ACK] Seq=5138 Ack=4943 Win=64128 Len=0 TSval=24505627
	232 31.276773426	10.65.3.120	10.65.3.119	TCP	68 22 → 57364 [FIN, ACK] Seq=5138 Ack=4943 Win=64128 Len=0 TSval=245
	233 31.276925576	10.65.3.119	10 65 3 120	TCP	68 57364 - 22 [ACK] Seg=4943 Ack=5139 Win=64128 Len=0 TSval=41902006

En esta actividad, montamos la carpeta "carpetamontaje" de una computadora a la carpeta "compartida" de la otra computadora. Lo que podemos observar es que los archivos que tenemos en carpetamontaje, se "clonan" en la carpeta "compartida". Además, si se realiza alguna modificación, o se elimina algún archivo, podemos ver que los cambios se ven en ambas carpetas.

Actividad 6:

```
paulina@ubuntu:-$ scp PaulinaSuden.txt redes@10.65.4.101:/home/redes/
redes@10.65.4.101's password:
PaulinaSuden.txt 100% 18 0.6KB/s 00:00
```



En esta actividad transferimos el archivo PaulinaSuden.txt a una computadora Raspberry Pi con su ip: 10.65.4.101 a través de SHH.