Trabajo Práctico 5 - Redes - Rando - 14004

Tomás Rando

Mayo 2024

1 Introducción

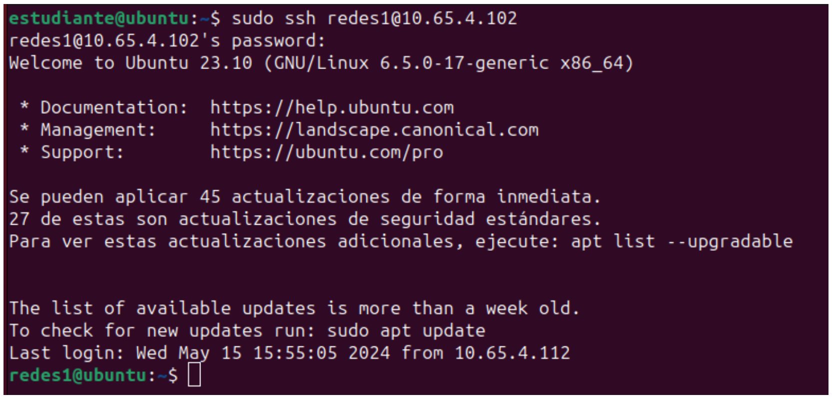
Se realiza el informe correspondiente al trabajo práctico número 5 de la materia "Redes de computadoras" del año 2024. En el mismo se realizaron todas las actividades, es decir, la 1, 2, 3, 4, 5 y 6.

Índice

2 Actividades

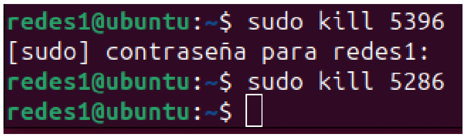
2.1 1. SSH

Se muestran imágenes de como se realizó la conexión entre dos computadoras del laboratorio de la facultad de ingeniería. Además, se muestra como se usaron comandos (kill) en la otra computadora y como se transfirieron archivos mediante scp. Por último, se agrega una imagen de algunos paquetes obtenidos mediante wireshark.



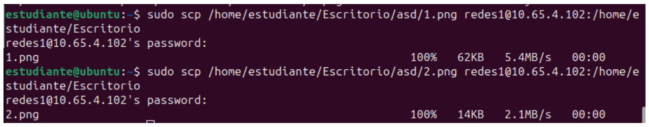
```
estudiante@ubuntu:~$ sudo ssh redes1@10.65.4.102
redes1@10.65.4.102's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Se pueden aplicar 45 actualizaciones de forma inmediata.
27 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Wed May 15 15:55:05 2024 from 10.65.4.112
redes1@ubuntu:~$ 
```

Figure 1: Realizando conexión



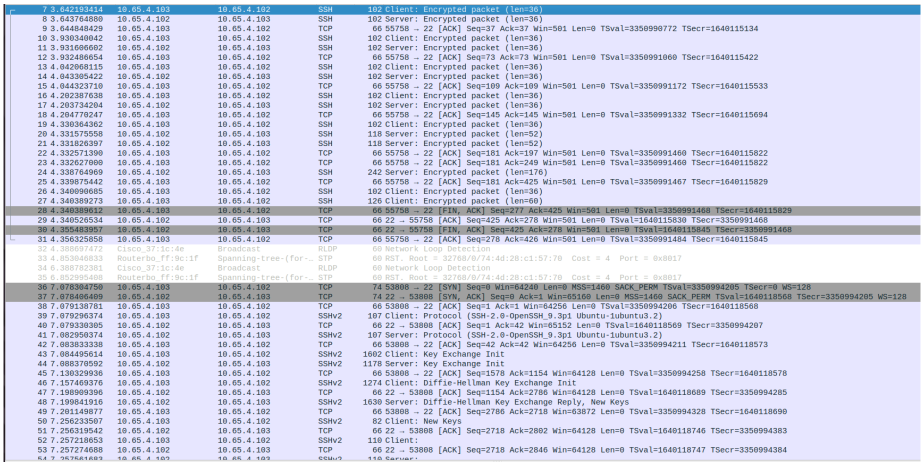
```
redes1@ubuntu:~$ sudo kill 5396
[sudo] contraseña para redes1:
redes1@ubuntu:~$ sudo kill 5286
redes1@ubuntu:~$ 
```

Figure 2: Utilizando kill



```
estudiante@ubuntu:~$ sudo scp /home/estudiante/Escritorio/asd/1.png redes1@10.65.4.102:/home/e
studiante/Escritorio
redes1@10.65.4.102's password:
1.png                                                100%   62KB   5.4MB/s   00:00
estudiante@ubuntu:~$ sudo scp /home/estudiante/Escritorio/asd/2.png redes1@10.65.4.102:/home/e
studiante/Escritorio
redes1@10.65.4.102's password:
2.png                                                100%   14KB   2.1MB/s   00:00
```

Figure 3: Transfiriendo archivos con scp

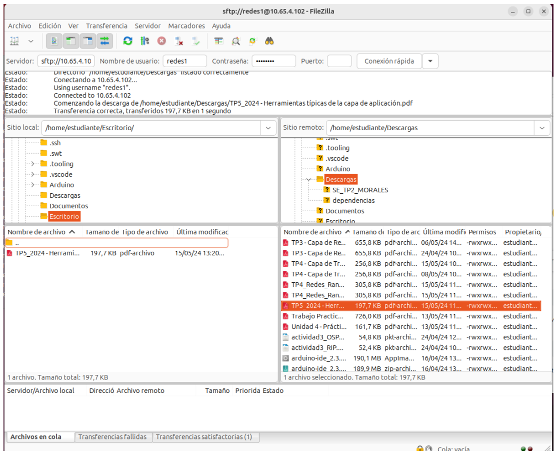


```
 7 3.642193414  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
 8 3.643764880  10.65.4.102          10.65.4.103          SSH      102 Server: Encrypted packet (len=36)
 9 3.644848429  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=37 Ack=37 Win=501 Len=0 TSval=3350990772 TSecr=1640115134
10 3.930340042  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
11 3.931606602  10.65.4.102          10.65.4.103          SSH      102 Server: Encrypted packet (len=36)
12 3.932486654  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=73 Ack=73 Win=501 Len=0 TSval=3350991060 TSecr=1640115422
13 4.042068115  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
14 4.043305422  10.65.4.102          10.65.4.103          SSH      102 Server: Encrypted packet (len=36)
15 4.044323710  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=109 Ack=109 Win=501 Len=0 TSval=3350991172 TSecr=1640115533
16 4.202387638  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
17 4.203734204  10.65.4.102          10.65.4.103          SSH      102 Server: Encrypted packet (len=36)
18 4.204770247  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=145 Ack=145 Win=501 Len=0 TSval=3350991332 TSecr=1640115694
19 4.330364362  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
20 4.331575558  10.65.4.102          10.65.4.103          SSH      118 Server: Encrypted packet (len=52)
21 4.331826397  10.65.4.102          10.65.4.103          SSH      118 Server: Encrypted packet (len=52)
22 4.332571390  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=181 Ack=197 Win=501 Len=0 TSval=3350991460 TSecr=1640115822
23 4.332627000  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=181 Ack=249 Win=501 Len=0 TSval=3350991460 TSecr=1640115822
24 4.338764969  10.65.4.102          10.65.4.103          SSH      242 Server: Encrypted packet (len=176)
25 4.339875442  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=181 Ack=425 Win=501 Len=0 TSval=3350991467 TSecr=1640115829
26 4.340090685  10.65.4.103          10.65.4.102          SSH      102 Client: Encrypted packet (len=36)
27 4.340389273  10.65.4.103          10.65.4.102          SSH      126 Client: Encrypted packet (len=60)
28 4.340389612  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [FIN, ACK] Seq=277 Ack=425 Win=501 Len=0 TSval=3350991468 TSecr=1640115829
29 4.340526534  10.65.4.102          10.65.4.103          TCP       66 22 → 55758 [ACK] Seq=425 Ack=278 Win=501 Len=0 TSval=1640115830 TSecr=3350991468
30 4.355483957  10.65.4.102          10.65.4.103          TCP       66 22 → 55758 [FIN, ACK] Seq=425 Ack=278 Win=501 Len=0 TSval=1640115845 TSecr=3350991468
31 4.356325858  10.65.4.103          10.65.4.102          TCP       66 55758 → 22 [ACK] Seq=278 Ack=426 Win=501 Len=0 TSval=3350991484 TSecr=1640115845
32 4.388697472  Cisco_37:1c:4e       Broadcast            RLDP      60 Network Loop Detection
33 4.853046833  Routerbo_ff:9c:1f    Spanning-tree-(for-… STP       60 RST. Root = 32768/0/74:4d:28:c1:57:70  Cost = 4  Port = 0x8017
34 6.388782381  Cisco_37:1c:4e       Broadcast            RLDP      60 Network Loop Detection
35 6.852995408  Routerbo_ff:9c:1f    Spanning-tree-(for-… STP       60 RST. Root = 32768/0/74:4d:28:c1:57:70  Cost = 4  Port = 0x8017
36 7.078304750  10.65.4.103          10.65.4.102          TCP       74 53808 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3350994205 TSecr=0 WS=128
37 7.078406409  10.65.4.102          10.65.4.103          TCP       74 22 → 53808 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1640118568 TSecr=3350994205 WS=128
38 7.079138781  10.65.4.103          10.65.4.102          TCP       66 53808 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3350994206 TSecr=1640118568
39 7.079296374  10.65.4.103          10.65.4.102          SSHv2    107 Client: Protocol (SSH-2.0-OpenSSH_9.3p1 Ubuntu-1ubuntu3.2)
40 7.079330305  10.65.4.102          10.65.4.103          TCP       66 22 → 53808 [ACK] Seq=1 Ack=42 Win=65152 Len=0 TSval=1640118569 TSecr=3350994207
41 7.082950374  10.65.4.102          10.65.4.103          SSHv2    107 Server: Protocol (SSH-2.0-OpenSSH_9.3p1 Ubuntu-1ubuntu3.2)
42 7.083833338  10.65.4.103          10.65.4.102          TCP       66 53808 → 22 [ACK] Seq=42 Ack=42 Win=64256 Len=0 TSval=3350994211 TSecr=1640118573
43 7.084495614  10.65.4.103          10.65.4.102          SSHv2   1602 Client: Key Exchange Init
44 7.088370592  10.65.4.102          10.65.4.103          SSHv2   1178 Server: Key Exchange Init
45 7.130329936  10.65.4.103          10.65.4.102          TCP       66 53808 → 22 [ACK] Seq=1578 Ack=1154 Win=64128 Len=0 TSval=3350994258 TSecr=1640118578
46 7.157469376  10.65.4.103          10.65.4.102          SSHv2   1274 Client: Diffie-Hellman Key Exchange Init
47 7.198909396  10.65.4.102          10.65.4.103          TCP       66 22 → 53808 [ACK] Seq=1154 Ack=2786 Win=64128 Len=0 TSval=1640118689 TSecr=3350994285
48 7.199841916  10.65.4.102          10.65.4.103          SSHv2   1630 Server: Diffie-Hellman Key Exchange Reply, New Keys
49 7.201149877  10.65.4.103          10.65.4.102          TCP       66 53808 → 22 [ACK] Seq=2786 Ack=2718 Win=63872 Len=0 TSval=3350994328 TSecr=1640118690
50 7.256233507  10.65.4.103          10.65.4.102          SSHv2     82 Client: New Keys
51 7.256319542  10.65.4.102          10.65.4.103          TCP       66 22 → 53808 [ACK] Seq=2718 Ack=2802 Win=64128 Len=0 TSval=1640118746 TSecr=3350994383
52 7.257218653  10.65.4.103          10.65.4.102          SSHv2    110 Client:
53 7.257274688  10.65.4.102          10.65.4.103          TCP       66 22 → 53808 [ACK] Seq=2718 Ack=2846 Win=64128 Len=0 TSval=1640118747 TSecr=3350994384
54 7.257561683  10.65.4.102          10.65.4.103          SSHv2    110 Server:
```

Figure 4: Paquetes con Wireshark

2.2 2. FTP

Se muestran imágenes de la conexión realizada y de los paquetes obtenidos. Nuevamente entre dos computadoras de la facultad de ingeniería.



Servidor: sftp://10.65.4.10 Nombre de usuario: redes1 Contraseña: •••••••• Puerto:

```
Estado:    Directorio "/home/estudiante/Descargas" listado correctamente
Estado:    Conectando a 10.65.4.102...
Estado:    Using username "redes1".
Estado:    Connected to 10.65.4.102
Estado:    Comenzando la descarga de /home/estudiante/Descargas/TP5_2024 - Herramientas típicas de la capa de aplicación.pdf
Estado:    Transferencia correcta, transferidos 197,7 KB en 1 segundo
```

Sitio local: /home/estudiante/Escritorio/

.ssh
.swt
.tooling
.vscode
Arduino
Descargas
Documentos
Escritorio

Sitio remoto: /home/estudiante/Descargas

.swt
.tooling
.vscode
Arduino
Descargas
SE_TP2_MORALES
dependencias
Documentos
Escritorio

Nombre de archivo	Tamaño de	Tipo de archivo	Última modificac
..			
TP5_2024 - Herrami...	197,7 KB	pdf-archivo	15/05/24 13:20...

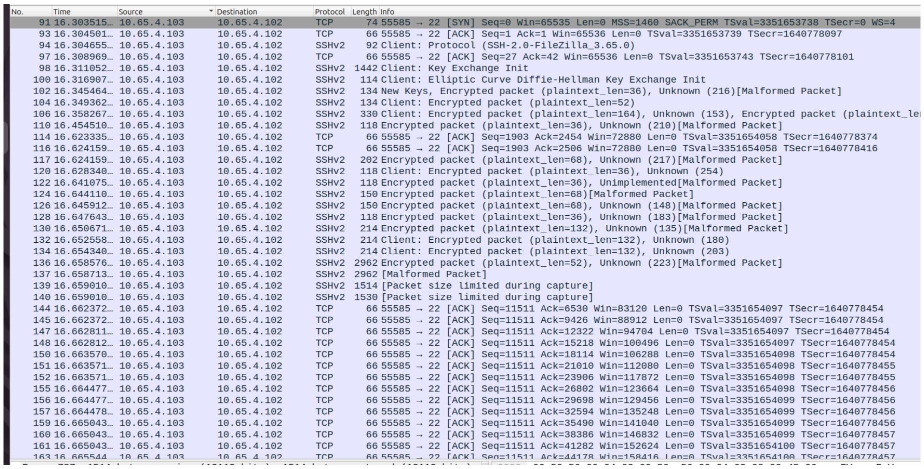
1 archivo. Tamaño total: 197,7 KB

Nombre de archivo	Tamaño d	Tipo de arc	Última modifi	Permisos	Propietario,
TP3 - Capa de Re...	655,8 KB	pdf-archi...	06/05/24 14...	-rwxrwx...	estudiant...
TP3 - Capa de Re...	655,8 KB	pdf-archi...	24/04/24 10...	-rwxrwx...	estudiant...
TP4 - Capa de Tr...	256,8 KB	pdf-archi...	15/05/24 10...	-rwxrwx...	estudiant...
TP4 - Capa de Tr...	256,8 KB	pdf-archi...	08/05/24 10...	-rwxrwx...	estudiant...
TP4_Redes_Ran...	305,8 KB	pdf-archi...	15/05/24 11...	-rwxrwx...	estudiant...
TP4_Redes_Ran...	305,8 KB	pdf-archi...	15/05/24 11...	-rwxrwx...	estudiant...
TP5_2024 - Herr...	197,7 KB	pdf-archi...	15/05/24 11...	-rwxrwx...	estudiant...
Trabajo Practic...	726,0 KB	pdf-archi...	13/05/24 11...	-rwxrwx...	estudiant...
Unidad 4 - Prácti...	161,7 KB	pdf-archi...	13/05/24 11...	-rwxrwx...	estudiant...
actividad3_OSP...	54,8 KB	pkt-archi...	24/04/24 12...	-rwxrwx...	estudiant...
actividad3_RIP....	52,4 KB	pkt-archi...	24/04/24 10...	-rwxrwx...	estudiant...
arduino-ide_2.3....	190,1 MB	AppIma...	16/04/24 13...	-rwxrwx...	estudiant...
arduino-ide_2.3....	189,9 MB	zip-archi...	16/04/24 13...	-rwxrwx...	estudiant...

1 archivo seleccionado. Tamaño total: 197,7 KB

Servidor/Archivo local	Direcció	Archivo remoto	Tamaño	Priorida	Estado

Figure 5: Utilizando FTP

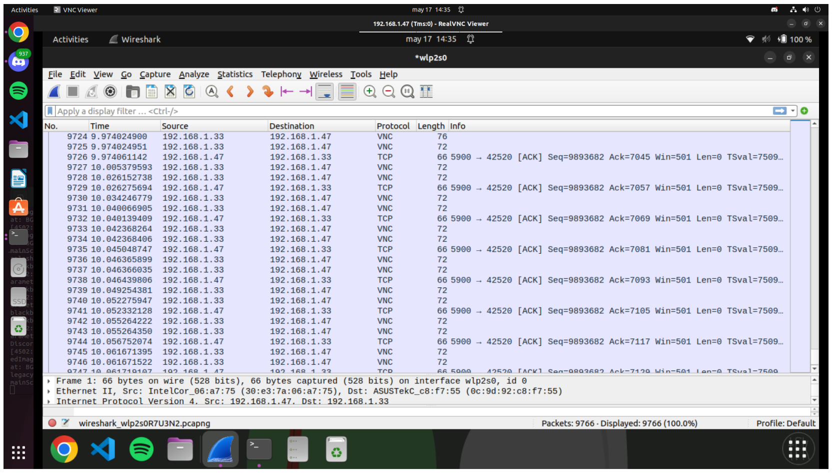


```
No.  Time          Source        Destination   Protocol Length Info
  91 16.303515…   10.65.4.103   10.65.4.102   TCP        74 55585 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=3351653738 TSecr=0 WS=4
  93 16.304501…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3351653739 TSecr=1640778097
  94 16.304655…   10.65.4.103   10.65.4.102   SSHv2      92 Client: Protocol (SSH-2.0-FileZilla_3.65.0)
  97 16.308969…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=27 Ack=42 Win=65536 Len=0 TSval=3351653743 TSecr=1640778101
  98 16.311052…   10.65.4.103   10.65.4.102   SSHv2    1442 Client: Key Exchange Init
 100 16.316907…   10.65.4.103   10.65.4.102   SSHv2     114 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
 102 16.345464…   10.65.4.103   10.65.4.102   SSHv2     134 New Keys, Encrypted packet (plaintext_len=36), Unknown (216)[Malformed Packet]
 104 16.349362…   10.65.4.103   10.65.4.102   SSHv2     134 Client: Encrypted packet (plaintext_len=52)
 106 16.358267…   10.65.4.103   10.65.4.102   SSHv2     330 Client: Encrypted packet (plaintext_len=164), Unknown (153), Encrypted packet (plaintext_le
 110 16.454510…   10.65.4.103   10.65.4.102   SSHv2     118 Encrypted packet (plaintext_len=36), Unknown (210)[Malformed Packet]
 114 16.623335…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=1903 Ack=2454 Win=72880 Len=0 TSval=3351654058 TSecr=1640778374
 116 16.624159…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=1903 Ack=2506 Win=72880 Len=0 TSval=3351654058 TSecr=1640778416
 117 16.624159…   10.65.4.103   10.65.4.102   SSHv2     202 Encrypted packet (plaintext_len=68), Unknown (217)[Malformed Packet]
 120 16.628340…   10.65.4.103   10.65.4.102   SSHv2     118 Client: Encrypted packet (plaintext_len=36), Unknown (254)
 122 16.641075…   10.65.4.103   10.65.4.102   SSHv2     118 Encrypted packet (plaintext_len=36), Unimplemented[Malformed Packet]
 124 16.644110…   10.65.4.103   10.65.4.102   SSHv2     150 Encrypted packet (plaintext_len=68)[Malformed Packet]
 126 16.645912…   10.65.4.103   10.65.4.102   SSHv2     150 Encrypted packet (plaintext_len=68), Unknown (148)[Malformed Packet]
 128 16.647643…   10.65.4.103   10.65.4.102   SSHv2     118 Encrypted packet (plaintext_len=36), Unknown (183)[Malformed Packet]
 130 16.650671…   10.65.4.103   10.65.4.102   SSHv2     214 Encrypted packet (plaintext_len=132), Unknown (135)[Malformed Packet]
 132 16.652558…   10.65.4.103   10.65.4.102   SSHv2     214 Client: Encrypted packet (plaintext_len=132), Unknown (180)
 134 16.654340…   10.65.4.103   10.65.4.102   SSHv2     214 Client: Encrypted packet (plaintext_len=132), Unknown (203)
 136 16.658576…   10.65.4.103   10.65.4.102   SSHv2    2962 Encrypted packet (plaintext_len=52), Unknown (223)[Malformed Packet]
 137 16.658713…   10.65.4.103   10.65.4.102   SSHv2    2962 [Malformed Packet]
 139 16.659010…   10.65.4.103   10.65.4.102   SSHv2    1514 [Packet size limited during capture]
 140 16.659010…   10.65.4.103   10.65.4.102   SSHv2    1530 [Packet size limited during capture]
 144 16.662372…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=6530 Win=83120 Len=0 TSval=3351654097 TSecr=1640778454
 145 16.662372…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=9426 Win=88912 Len=0 TSval=3351654097 TSecr=1640778454
 147 16.662811…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=12322 Win=94704 Len=0 TSval=3351654097 TSecr=1640778454
 148 16.662812…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=15218 Win=100496 Len=0 TSval=3351654097 TSecr=1640778454
 150 16.663570…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=18114 Win=106288 Len=0 TSval=3351654098 TSecr=1640778454
 151 16.663571…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=21010 Win=112080 Len=0 TSval=3351654098 TSecr=1640778455
 152 16.663571…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=23906 Win=117872 Len=0 TSval=3351654098 TSecr=1640778455
 155 16.664477…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=26802 Win=123664 Len=0 TSval=3351654098 TSecr=1640778456
 156 16.664477…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=29698 Win=129456 Len=0 TSval=3351654099 TSecr=1640778456
 157 16.664478…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=32594 Win=135248 Len=0 TSval=3351654099 TSecr=1640778456
 159 16.665043…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=35490 Win=141040 Len=0 TSval=3351654099 TSecr=1640778456
 160 16.665043…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=38386 Win=146832 Len=0 TSval=3351654099 TSecr=1640778457
 161 16.665043…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=41282 Win=152624 Len=0 TSval=3351654100 TSecr=1640778457
 163 16.665544…   10.65.4.103   10.65.4.102   TCP        66 55585 → 22 [ACK] Seq=11511 Ack=44178 Win=158416 Len=0 TSval=3351654100 TSecr=1640778457
```

Figure 6: Paquetes con Wireshark

2.3 3. VNC

En este caso todo se muestra en una única imagen. En esta se observa la conexión entre dos computadoras propias y la aplicación wireshark siendo ejecutada en la computadora host.

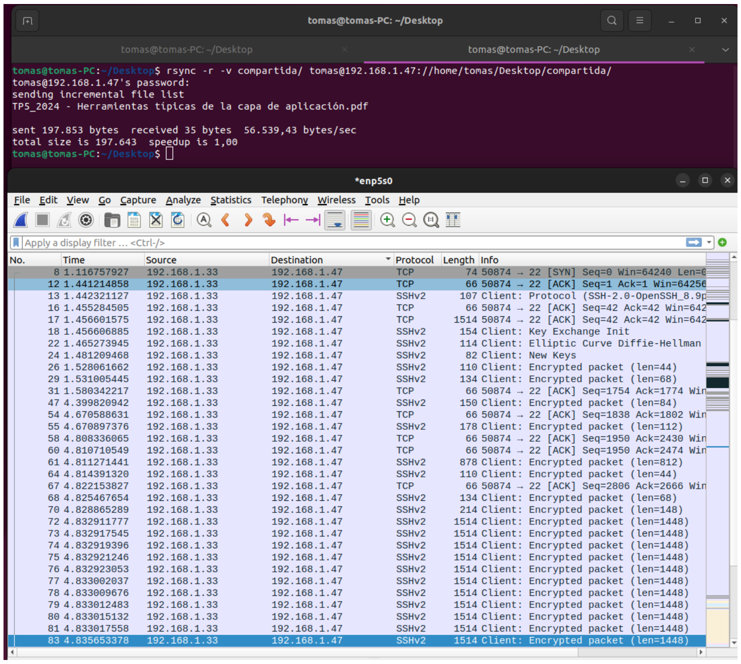

Activities
VNC Viewer
may 17 14:35
192.168.1.47 (Tms:0) - RealVNC Viewer
Activities
Wireshark
may 17 14:35
100 %
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time          Source          Destination     Protocol  Length  Info
  9724 9.974024900   192.168.1.33    192.168.1.47    VNC         76
  9725 9.974024951   192.168.1.33    192.168.1.47    VNC         72
  9726 9.974061142   192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7045 Win=501 Len=0 TSval=7509…
  9727 10.005379593  192.168.1.33    192.168.1.47    VNC         72
  9728 10.026152738  192.168.1.33    192.168.1.47    VNC         72
  9729 10.026275694  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7057 Win=501 Len=0 TSval=7509…
  9730 10.034246779  192.168.1.33    192.168.1.47    VNC         72
  9731 10.040066905  192.168.1.33    192.168.1.47    VNC         72
  9732 10.040139409  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7069 Win=501 Len=0 TSval=7509…
  9733 10.042368264  192.168.1.33    192.168.1.47    VNC         72
  9734 10.042368406  192.168.1.33    192.168.1.47    VNC         72
  9735 10.045048747  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7081 Win=501 Len=0 TSval=7509…
  9736 10.046365899  192.168.1.33    192.168.1.47    VNC         72
  9737 10.046366035  192.168.1.33    192.168.1.47    VNC         72
  9738 10.046439806  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7093 Win=501 Len=0 TSval=7509…
  9739 10.049254381  192.168.1.33    192.168.1.47    VNC         72
  9740 10.052275947  192.168.1.33    192.168.1.47    VNC         72
  9741 10.052332128  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7105 Win=501 Len=0 TSval=7509…
  9742 10.055264222  192.168.1.33    192.168.1.47    VNC         72
  9743 10.055264350  192.168.1.33    192.168.1.47    VNC         72
  9744 10.056752074  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7117 Win=501 Len=0 TSval=7509…
  9745 10.061671395  192.168.1.33    192.168.1.47    VNC         72
  9746 10.061671522  192.168.1.33    192.168.1.47    VNC         72
  9747 10.061719107  192.168.1.47    192.168.1.33    TCP         66 5900 → 42520 [ACK] Seq=9893682 Ack=7129 Win=501 Len=0 TSval=7509…

› Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp2s0, id 0
› Ethernet II, Src: IntelCor_06:a7:75 (30:e3:7a:06:a7:75), Dst: ASUSTekC_c8:f7:55 (0c:9d:92:c8:f7:55)
› Internet Protocol Version 4, Src: 192.168.1.47, Dst: 192.168.1.33

wireshark_wlp2s0R7U3N2.pcapng        Packets: 9766 · Displayed: 9766 (100.0%)        Profile: Default
```

Figure 7: Conexión VNC

2.4 4. Rsync

En este caso se observa como se realiza la sincronización entre dos carpetas y abajo de esto el programa wireshark con los paquetes capturados durante esa sincronización.


tomas@tomas-PC: ~/Desktop
tomas@tomas-PC: ~/Desktop
tomas@tomas-PC: ~/Desktop
*enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

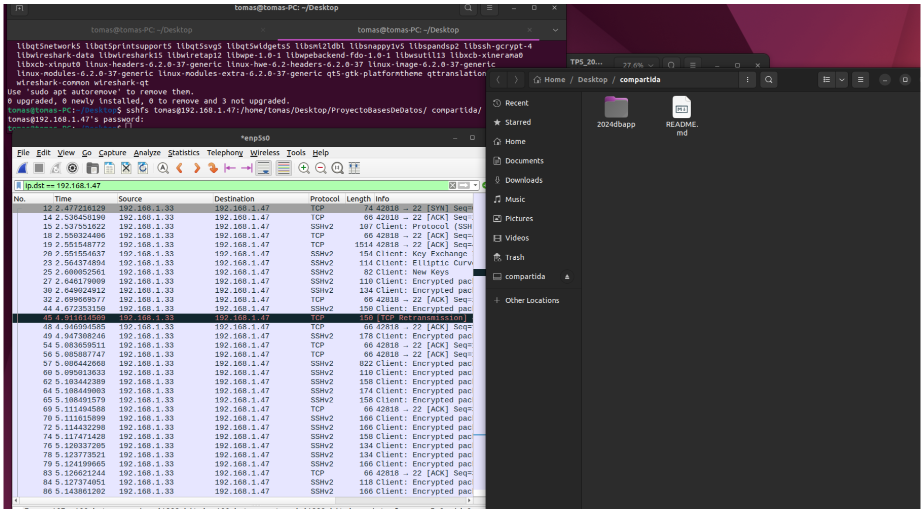
```
tomas@tomas-PC:~/Desktop$ rsync -r -v compartida/ tomas@192.168.1.47://home/tomas/Desktop/compartida/
tomas@192.168.1.47's password:
sending incremental file list
TP5_2024 - Herramientas típicas de la capa de aplicación.pdf

sent 197.853 bytes  received 35 bytes  56.539,43 bytes/sec
total size is 197.643  speedup is 1,00
tomas@tomas-PC:~/Desktop$
```

No.	Time	Source	Destination	Protocol	Length	Info
8	1.116757927	192.168.1.33	192.168.1.47	TCP	74	50874 → 22 [SYN] Seq=0 Win=64240 Len=0
12	1.441214858	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=1 Ack=1 Win=64256
13	1.442321127	192.168.1.33	192.168.1.47	SSHv2	107	Client: Protocol (SSH-2.0-OpenSSH_8.9p
16	1.455284505	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=42 Ack=42 Win=642
17	1.456601575	192.168.1.33	192.168.1.47	TCP	1514	50874 → 22 [ACK] Seq=42 Ack=42 Win=642
18	1.456606885	192.168.1.33	192.168.1.47	SSHv2	154	Client: Key Exchange Init
22	1.465273945	192.168.1.33	192.168.1.47	SSHv2	114	Client: Elliptic Curve Diffie-Hellman
24	1.481209468	192.168.1.33	192.168.1.47	SSHv2	82	Client: New Keys
26	1.528061662	192.168.1.33	192.168.1.47	SSHv2	110	Client: Encrypted packet (len=44)
29	1.531005445	192.168.1.33	192.168.1.47	SSHv2	134	Client: Encrypted packet (len=68)
31	1.580342217	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=1754 Ack=1774 Win
47	4.399820942	192.168.1.33	192.168.1.47	SSHv2	150	Client: Encrypted packet (len=84)
54	4.670588631	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=1838 Ack=1802 Win
55	4.670897376	192.168.1.33	192.168.1.47	SSHv2	178	Client: Encrypted packet (len=112)
58	4.808336065	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=1950 Ack=2430 Win
60	4.810710549	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=1950 Ack=2474 Win
61	4.811271441	192.168.1.33	192.168.1.47	SSHv2	878	Client: Encrypted packet (len=812)
64	4.814391320	192.168.1.33	192.168.1.47	SSHv2	110	Client: Encrypted packet (len=44)
67	4.822153827	192.168.1.33	192.168.1.47	TCP	66	50874 → 22 [ACK] Seq=2806 Ack=2666 Win
68	4.825467654	192.168.1.33	192.168.1.47	SSHv2	134	Client: Encrypted packet (len=68)
70	4.828865289	192.168.1.33	192.168.1.47	SSHv2	214	Client: Encrypted packet (len=148)
72	4.832911777	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
73	4.832917545	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
74	4.832919396	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
75	4.832921246	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
76	4.832923053	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
77	4.833002037	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
78	4.833009676	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
79	4.833012483	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
80	4.833015132	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
81	4.833017558	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)
83	4.835653378	192.168.1.33	192.168.1.47	SSHv2	1514	Client: Encrypted packet (len=1448)

Figure 8: Utilización de Rsync

2.5 5. SSHFS

Se muestra en una imagen el comando utilizado para realizar la conexión, la carpeta en la que se montó la carpeta externa y wireshark con los paquetes capturados



tomas@tomas-PC: ~/Desktop
tomas@tomas-PC: ~/Desktop
tomas@tomas-PC: ~/Desktop
*enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Home / Desktop / compartida
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
compartida
Other Locations
2024dbapp
README.md

```
  libqt5network5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark15 libwiretap12 libwpe-1.0-1 libwpebackend-fdo-1.0-1 libwsutil13 libxcb-xinerama0
  libxcb-xinput0 linux-headers-6.2.0-37-generic linux-hwe-6.2-headers-6.2.0-37 linux-image-6.2.0-37-generic
  linux-modules-6.2.0-37-generic linux-modules-extra-6.2.0-37-generic qt5-gtk-platformtheme qttranslation
  wireshark-common wireshark-qt
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
tomas@tomas-PC:~/Desktop$ sshfs tomas@192.168.1.47:/home/tomas/Desktop/ProyectoBasesDeDatos/ compartida/
tomas@192.168.1.47's password:
```

ip.dst == 192.168.1.47

No.	Time	Source	Destination	Protocol	Length	Info
12	2.477216129	192.168.1.33	192.168.1.47	TCP	74	42818 → 22 [SYN] Seq=
14	2.536458190	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
15	2.537551622	192.168.1.33	192.168.1.47	SSHv2	107	Client: Protocol (SSH
18	2.550324406	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
19	2.551548772	192.168.1.33	192.168.1.47	TCP	1514	42818 → 22 [ACK] Seq=
20	2.551554637	192.168.1.33	192.168.1.47	SSHv2	154	Client: Key Exchange
23	2.564374894	192.168.1.33	192.168.1.47	SSHv2	114	Client: Elliptic Curv
25	2.600052561	192.168.1.33	192.168.1.47	SSHv2	82	Client: New Keys
27	2.646179009	192.168.1.33	192.168.1.47	SSHv2	110	Client: Encrypted pac
30	2.649024912	192.168.1.33	192.168.1.47	SSHv2	134	Client: Encrypted pac
32	2.699669577	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
44	4.672353150	192.168.1.33	192.168.1.47	SSHv2	150	Client: Encrypted pac
45	4.911614509	192.168.1.33	192.168.1.47	TCP	150	[TCP Retransmission]
48	4.946994585	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
49	4.947308246	192.168.1.33	192.168.1.47	SSHv2	178	Client: Encrypted pac
54	5.083659511	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
56	5.085887747	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
57	5.086442668	192.168.1.33	192.168.1.47	SSHv2	822	Client: Encrypted pac
60	5.095013633	192.168.1.33	192.168.1.47	SSHv2	110	Client: Encrypted pac
62	5.103442389	192.168.1.33	192.168.1.47	SSHv2	158	Client: Encrypted pac
64	5.108449003	192.168.1.33	192.168.1.47	SSHv2	174	Client: Encrypted pac
65	5.108491579	192.168.1.33	192.168.1.47	SSHv2	158	Client: Encrypted pac
69	5.111494588	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
70	5.111615899	192.168.1.33	192.168.1.47	SSHv2	166	Client: Encrypted pac
72	5.114432298	192.168.1.33	192.168.1.47	SSHv2	166	Client: Encrypted pac
74	5.117471428	192.168.1.33	192.168.1.47	SSHv2	158	Client: Encrypted pac
76	5.120337205	192.168.1.33	192.168.1.47	SSHv2	134	Client: Encrypted pac
78	5.123773521	192.168.1.33	192.168.1.47	SSHv2	134	Client: Encrypted pac
79	5.124199665	192.168.1.33	192.168.1.47	SSHv2	166	Client: Encrypted pac
83	5.126621244	192.168.1.33	192.168.1.47	TCP	66	42818 → 22 [ACK] Seq=
84	5.127374051	192.168.1.33	192.168.1.47	SSHv2	118	Client: Encrypted pac
86	5.143861202	192.168.1.33	192.168.1.47	SSHv2	166	Client: Encrypted pac

Figure 9: Conexión SSHFS

2.6 6. Transferencia a Raspberry Pi

Esta actividad será realizada y mostrada al profesor en horario de clases ya que necesita ser realizada con una Raspberry Pi provista por la cátedra.