

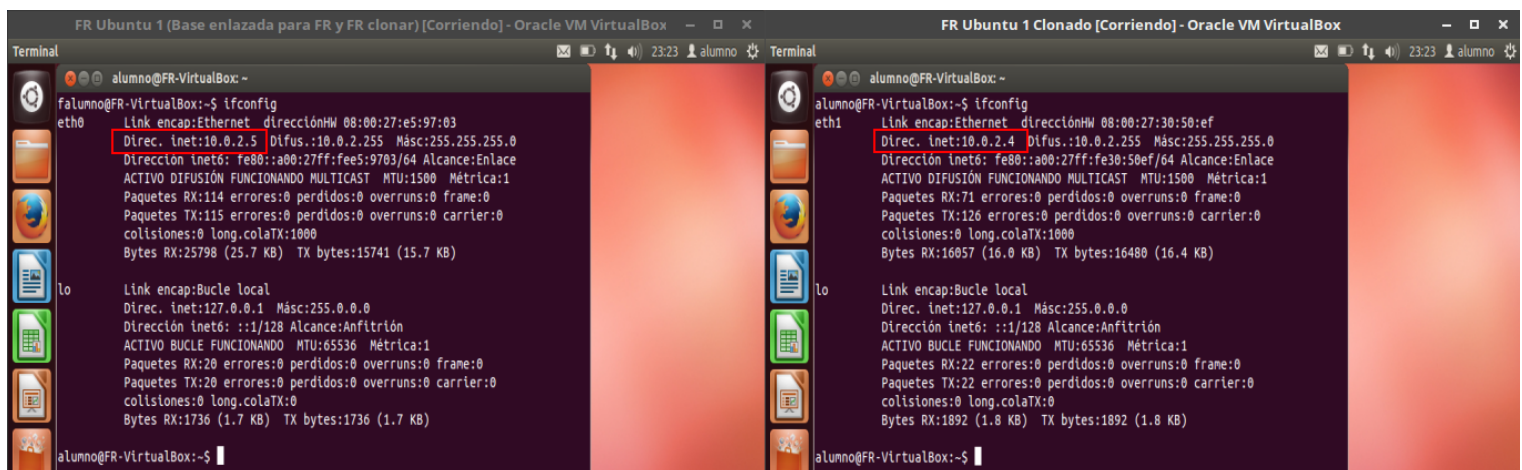
Entrega cuestiones C1

1. **Actividad 1:** capturas de telnet y ssh con wireshark entre las dos máquinas virtuales ¿podemos sacar información de los paquetes telnet? pista: mirar el contenido de varios paquetes seguidos.

Telnet

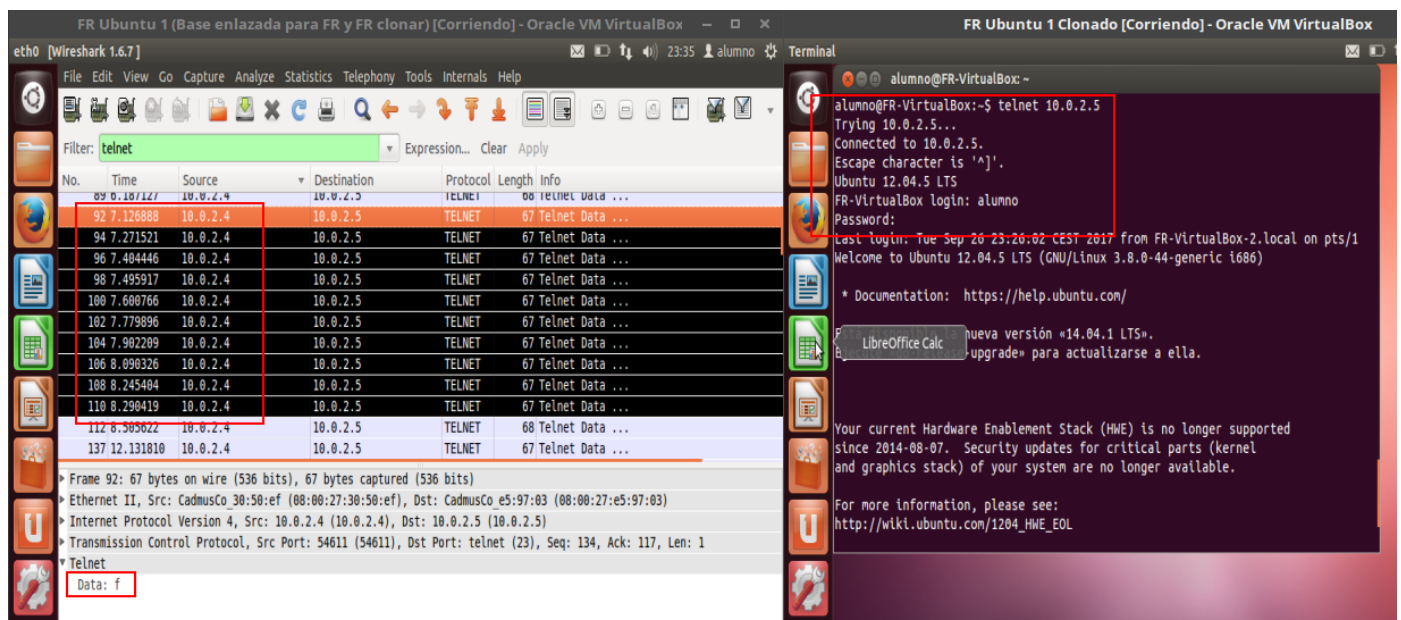
Primero hemos conectado las dos máquinas virtuales mediante una “Red NAT” con la cual, ambas “se ven” en la red y por tanto, puede haber conexión entre ellas.

Vemos en la siguiente imagen que cada maquina virtual tiene una IP distinta pero en el mismo rango de red.



Ahora abrimos el Wireshark (poniendo a esnifar el tráfico) en una de las dos máquinas y realizamos una conexión telnet a través del terminal hacia la otra máquina.

Podemos ver, por ejemplo, la contraseña letra por letra en los paquetes enviados desde la dirección IP de donde se realizó la conexión telnet (10.0.2.4), en mi caso son todos los paquetes marcados en negro.



SSH

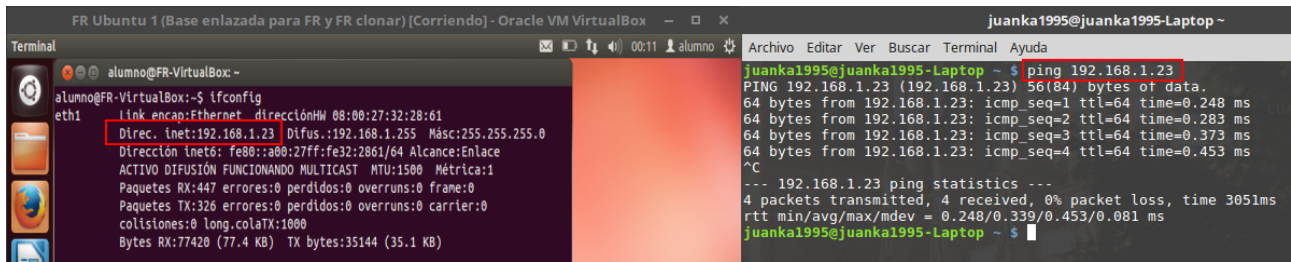
Ahora realizamos el mismo proceso con SSH y nos damos cuenta de que los paquetes van cifrados por lo que no es posible obtener información.

The screenshot displays two windows from an Oracle VM VirtualBox environment. The left window is Wireshark 1.6.7, capturing traffic on the eth0 interface. The filter is set to 'ssh'. The packet list shows several SSH packets. Packet 12, at time 0.010160, is selected and highlighted in orange. Its details pane shows 'SSH Version 2 (encryption:aes128-ctr mac:hmac-md5 compression:none)'. The right window is a terminal titled 'alumno@FR-VirtualBox: ~'. It shows the command 'ssh 10.0.2.5' being executed. The terminal output indicates that the authenticity of the host '10.0.2.5' cannot be established, showing the ECDSA key fingerprint and a warning to add it to the list of known hosts. The user is prompted for a password, and the terminal shows 'Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.8.0-44-generic i686)'.

2. Actividad 2: Actividad 2: poner la red de una MV en adaptador puente e intentar capturar tráfico del dispositivos host.

Lo primero es añadir la red puente a la maquina virtual y seguidamente comprobar que exista conexión entre el Host y la virtual.

The screenshot shows the 'FR Ubuntu 1 - Configuración' window, specifically the 'Red' (Network) settings. The 'Adaptador 1' tab is selected. The 'Habilitar adaptador de red' checkbox is checked. The 'Conectado a:' dropdown menu is set to 'Adaptador puente'. Below this, the 'Nombre' field is 'wlp3s0'. In the 'Avanzadas' section, the 'Tipo de adaptador' is 'Intel PRO/1000 MT Desktop (82540EM)', the 'Modo promiscuo' is 'Denegar', and the 'Dirección MAC' is '080027322861'. The 'Cable conectado' checkbox is checked. There is a 'Reenvío de puertos' button at the bottom.

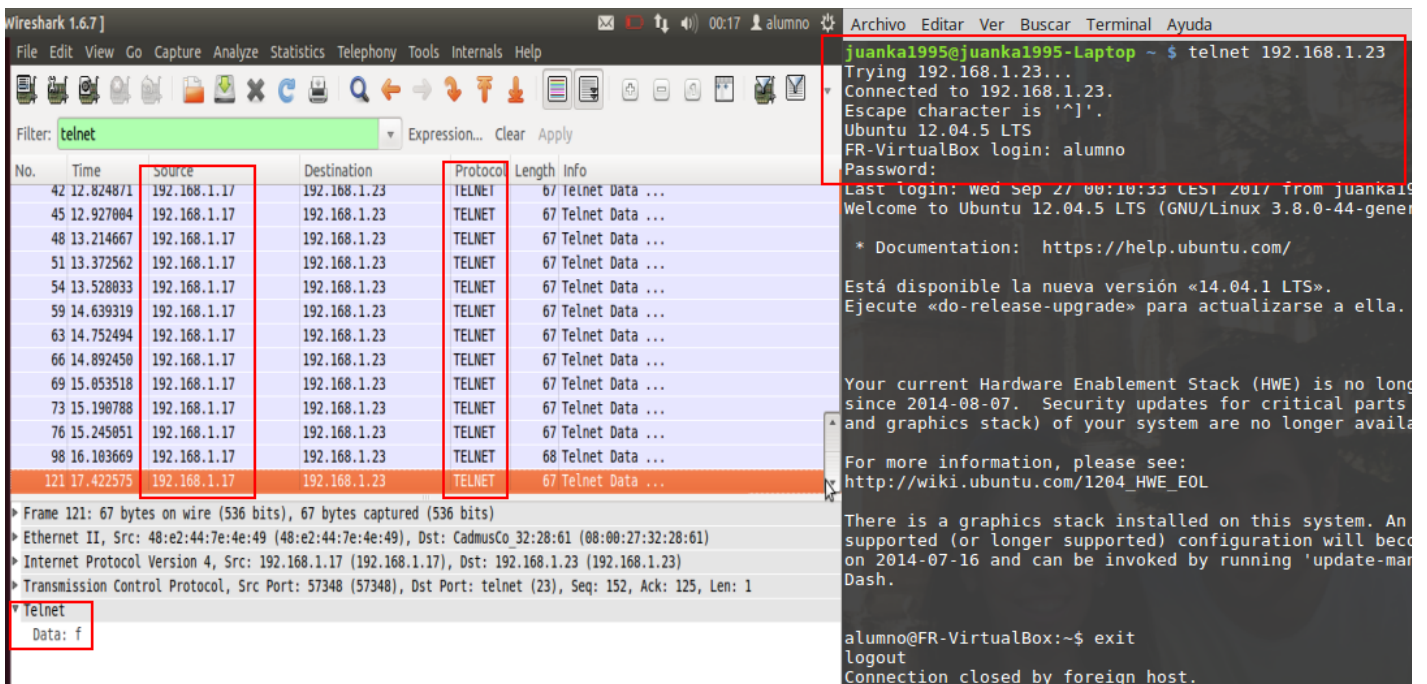


The screenshot shows two terminal windows. The left window, titled 'alumno@FR-VirtualBox:~', displays the output of the 'ifconfig' command for the 'eth1' interface. The right window, titled 'juanka1995@juanka1995-Laptop ~', shows the output of a 'ping' command to 192.168.1.23.

```
alumno@FR-VirtualBox:~$ ifconfig
eth1:
    link encap:Ethernet  direcciónHW 08:00:27:32:28:61
    Dirección inet:192.168.1.23  Difus.:192.168.1.255  Másc:255.255.255.0
    Dirección lnets6: fe80::a00:27ff:fe32:2861/64 Alcance:Enlace
    ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
    Paquetes RX:447 errores:0 perdidos:0 overruns:0 frame:0
    Paquetes TX:326 errores:0 perdidos:0 overruns:0 carrier:0
    colisiones:0 long.colatX:1000
    Bytes RX:77420 (77.4 KB)  TX bytes:35144 (35.1 KB)
```

```
juanka1995@juanka1995-Laptop ~$ ping 192.168.1.23
PING 192.168.1.23 (192.168.1.23) 56(84) bytes of data:
64 bytes from 192.168.1.23: icmp_seq=1 ttl=64 time=0.248 ms
64 bytes from 192.168.1.23: icmp_seq=2 ttl=64 time=0.283 ms
64 bytes from 192.168.1.23: icmp_seq=3 ttl=64 time=0.373 ms
64 bytes from 192.168.1.23: icmp_seq=4 ttl=64 time=0.453 ms
^C
--- 192.168.1.23 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.248/0.339/0.453/0.081 ms
juanka1995@juanka1995-Laptop ~$
```

Una vez comprobado esto lanzamos el wireshark y podemos probar a realizar un Telnet desde el anfitrión hacia el virtual y ver que efectivamente podemos esnifar el trafico de red del anfitrión.



The screenshot shows the Wireshark 1.6.7 interface. The packet list on the left shows a series of Telnet data packets from 192.168.1.17 to 192.168.1.23. The packet details pane on the right shows the selected packet (No. 121) as a Telnet data packet. The packet bytes pane at the bottom shows the raw data 'f'.

Filter: telnet

No.	Time	Source	Destination	Protocol	Length	Info
42	12.824871	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
45	12.927084	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
48	13.214667	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
51	13.372562	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
54	13.528033	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
59	14.639319	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
63	14.752494	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
66	14.892450	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
69	15.053518	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
73	15.190788	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
76	15.245051	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...
98	16.103669	192.168.1.17	192.168.1.23	TELNET	68	Telnet Data ...
121	17.422575	192.168.1.17	192.168.1.23	TELNET	67	Telnet Data ...

Frame 121: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)

Ethernet II, Src: 48:e2:44:7e:4e:49 (48:e2:44:7e:4e:49), Dst: CadmusCo 32:28:61 (08:00:27:32:28:61)

Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 192.168.1.23 (192.168.1.23)

Transmission Control Protocol, Src Port: 57348 (57348), Dst Port: telnet (23), Seq: 152, Ack: 125, Len: 1

Telnet

Data: f

```
juanka1995@juanka1995-Laptop ~$ telnet 192.168.1.23
Trying 192.168.1.23...
Connected to 192.168.1.23.
Escape character is '^J'.
Ubuntu 12.04.5 LTS
FR-VirtualBox login: alumno
Password:
Last login: wed Sep 27 00:10:33 CEST 2017 from juanka19
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.8.0-44-gener

* Documentation: https://help.ubuntu.com/

Está disponible la nueva versión «14.04.1 LTS».
Ejecute «do-release-upgrade» para actualizarse a ella.

Your current Hardware Enablement Stack (HWE) is no long
since 2014-08-07. Security updates for critical parts
and graphics stack) of your system are no longer availa

For more information, please see:
http://wiki.ubuntu.com/1204_HWE_EOL

There is a graphics stack installed on this system. An
supported (or longer supported) configuration will beco
on 2014-07-16 and can be invoked by running 'update-mar
Dash.

alumno@FR-VirtualBox:~$ exit
logout
Connection closed by foreign host.
```