

# Servicios de Red

## Práctica 3

### Aplicaciones sobre TCP/UDP

Himar Alonso Díaz

17 de abril de 2006

## Contenido

<b>1. Introducción</b>	<b>2</b>
<b>2. Ejercicios relacionados</b>	<b>2</b>
2.1. Mirar la dirección IP y el nombre de un equipo . . . . .	2
2.2. Efectuar una conexión TELNET . . . . .	2
2.3. Listar las conexiones locales y los procesos que las controlan . . . . .	3
2.4. Escanear los servicios (puertos TCP más comunes) que ofrece una máquina remota . . . . .	4
2.5. Hacer una conexión FTP . . . . .	5
2.6. Interceptar una contraseña mediante el uso de Ethereal . . . . .	6
2.7. Hacer una conexión SSH y configurar la misma usando certificados de clave pública/privada . . . . .	7
2.8. Hacer peticiones DNS y WHOIS . . . . .	9
2.9. Hacer peticiones HTTP 1.0 y 1.1 usando TELNET . . . . .	11
2.10. Hacer FTPs tanto activos como pasivos usando TELNET . . . . .	13
2.11. Enviar y recibir correos usando TELNET . . . . .	15
<b>3. Cuestiones específicas</b>	<b>16</b>
3.1. Crear un subdirectorio en nuestra cuenta de la máquina remota y poner en ella algunos ficheros. ¿Cómo hacemos para traernos por FTP todo el directorio? . . . . .	16
3.1.1. Utilizando el comando FTP: <code>mget</code> . . . . .	16
3.1.2. Utilizando el programa <code>wget</code> . . . . .	17
3.1.3. Utilizando un cliente FTP avanzado en modo gráfico . . . . .	18
3.2. Identificar las máquinas de la subred del laboratorio que están encendidas y los servicios que están prestando. ¿Podemos hacerlo con un solo comando? . . . . .	18
3.3. ¿Es posible hacer un FTP <i>activo</i> usando como cliente una máquina dentro de la red de la Universidad y como servidor una máquina de afuera? Dicho de otra manera, ¿puede la máquina externa conocer la IP de nuestro nodo dentro de la Universidad? . . . . .	20
3.3.1. Caso genérico . . . . .	20
3.3.2. Haciendo uso de NAT . . . . .	20

# 1. Introducción

El objetivo de esta práctica es conocer el funcionamiento del *nivel de transporte* (TCP y UDP), para lo cual utilizaremos varias aplicaciones que nos permitirán realizar un análisis completo de los distintos protocolos.

Este documento consta de dos secciones principales:

- En la primera se recogen de forma detallada todos los pasos seguidos durante el desarrollo de la práctica (comandos, accesos, *logs*, capturas de pantalla, ...).
- En la segunda se da contestación a las cuestiones específicas.

## 2. Ejercicios relacionados

### 2.1. Mirar la dirección IP y el nombre de un equipo

- Una forma rápida y sencilla de comprobar nuestra IP es observar la configuración del interfaz de red con el comando `$ifconfig eth0`. El nombre del equipo está almacenado en la variable de entorno `HOSTNAME`. Para mostrar el contenido de esta variable utilizamos el comando de bash `$echo $HOSTNAME`. Este es el resultado que se observa por pantalla:

```
camilo:/home/himar# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:03:0D:30:EE:00
          inet addr:192.168.100.33  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::203:dff:fe30:ee00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21855 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35647 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23649317 (22.5 MiB)  TX bytes:37636847 (35.8 MiB)
          Interrupt:3 Base address:0x6c00

camilo:/home/himar# echo $HOSTNAME
camilo
camilo:/home/himar#
```

- La IP es “192.168.100.33” y el nombre del equipo “camilo”.

### 2.2. Efectuar una conexión TELNET

- En la primera conexión TELNET lo que vamos a hacer es crear un fichero en la máquina remota. La forma más rápida de crear un fichero en GNU/Linux es utilizando el comando `$touch mifichero`:

```
camilo:/home/himar# telnet 192.168.100.13
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
Ubuntu 5.10 "Breezy Badger" tx11.tx.teleco.ulpgc.es
tx11 login: halonso
Password:
Last login: Mon Apr  3 12:30:40 2006 from 192.168.100.33 on pts/6
Linux tx11 2.6.12-9-386 #1 Mon Oct 10 13:14:36 BST 2005 i686 GNU/Linux

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
```

```
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
```

```
halonso@tx11:~$ ls -l
total 0
halonso@tx11:~$ touch mifichero
halonso@tx11:~$ ls -l
total 0
-rw-r--r-- 1 halonso users 0 2006-04-03 12:35 mifichero
halonso@tx11:~$ exit
logout
Connection closed by foreign host.
camilo:/home/himar#
```

- En una segunda conexión TELNET comprobaremos que existe el fichero `mifichero` y lo borraremos:

```
camilo:/home/himar# telnet 192.168.100.13
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
Ubuntu 5.10 "Breezy Badger" tx11.tx.teleco.ulpgc.es
tx11 login: halonso
Password:
Last login: Mon Apr  3 12:33:19 2006 from 192.168.100.33 on pts/5
Linux tx11 2.6.12-9-386 #1 Mon Oct 10 13:14:36 BST 2005 i686 GNU/Linux
```

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

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
```

```
halonso@tx11:~$ ls -l
total 0
-rw-r--r-- 1 halonso users 0 2006-04-03 12:35 mifichero
halonso@tx11:~$ rm mifichero
halonso@tx11:~$ ls -l
total 0
halonso@tx11:~$
```

## 2.3. Listar las conexiones locales y los procesos que las controlan

- En el siguiente fragmento puede observarse un listado de conexiones y procesos observados al entrar por TELNET a la máquina remota. Las dos primeras líneas muestran la conexión TCP con el *host* “camilo”, desde el cual estamos accediendo de forma remota.

```
halonso@tx11:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 camilo:49241           camilo:32771           ESTABLISHED
tcp        0      0 camilo:32771           camilo:49241           ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State                  I-Node Path
unix    9      [ ]                 DGRAM                  -                       3282  /dev/log
unix    3      [ ]                 STREAM                 CONNECTED               15269 /tmp/.ICE-unix/dcop3552-1144059170
unix    3      [ ]                 STREAM                 CONNECTED               15268
unix    3      [ ]                 STREAM                 CONNECTED               15259 /tmp/.ICE-unix/dcop3552-1144059170
unix    3      [ ]                 STREAM                 CONNECTED               1525
unix    3      [ ]                 STREAM                 CONNECTED               15255
(...)
```

- A continuación filtraremos el contenido de los procesos y las conexiones activas, con las siguientes opciones de filtrado:

- -p Procesos que gestionan las conexiones
  - -u Conexiones UDP
  - -t Conexiones TCP
  - -a Conexiones en estado “LISTEN all”
- Obsérvese que hay varias conexiones TCP activas con varios *hosts* del laboratorio, que tienen su nombre de máquina registrado. También se puede ver la conexión que realicé yo desde mi ordenador, que al no tener el nombre registrado en la red, muestra la dirección IP (192.168.100.33):

```

halonso@tx11:~$ netstat -puta
(No info could be read for "-p": geteuid()=1005 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:32770                 *:*                     LISTEN      -
tcp        0      0 localhost.localdo:32772 *:*                     LISTEN      -
tcp        0      0 localhost.localdo:32773 *:*                     LISTEN      -
tcp        0      0 localhost.localdo:mysql *:*                     LISTEN      -
tcp        0      0 *:submission           *:*                     LISTEN      -
tcp        0      0 *:netbios-ssn          *:*                     LISTEN      -
tcp        0      0 *:pop3                  *:*                     LISTEN      -
tcp        0      0 *:sunrpc                *:*                     LISTEN      -
tcp        0      0 *:10000                 *:*                     LISTEN      -
tcp        0      0 *:ftp                   *:*                     LISTEN      -
tcp        0      0 *:telnet                *:*                     LISTEN      -
tcp        0      0 localhost.localdoma:ipp *:*                     LISTEN      -
tcp        0      0 *:smtp                  *:*                     LISTEN      -
tcp        0      0 *:microsoft-ds         *:*                     LISTEN      -
tcp        0      0 tx11.tx.teleco.u:telnet tx10.tx.teleco.ul:56770 TIME_WAIT   -
tcp        0      0 localhost.localdo:50063 localhost.localdo:32772 ESTABLISHED-
tcp        0      0 tx11.tx.teleco.u:telnet tx8.tx.teleco.ulp:60462 ESTABLISHED-
tcp        0      0 tx11.tx.teleco.u:telnet 192.168.100.33:47841 ESTABLISHED-
tcp        0      0 localhost.localca:ftp-data localhost.localdo:32813 TIME_WAIT   -
tcp        0      0 tx11.tx.teleco:ftp-data tx11.tx.teleco.ul:32814 TIME_WAIT   -
tcp        0      0 tx11.tx.teleco:ftp-data tx11.tx.teleco.ul:32815 TIME_WAIT   -
tcp        0      0 localhost.localdo:32772 localhost.localdo:50063 ESTABLISHED-
tcp        0      0 tx11.tx.teleco:ftp-data tx11.tx.teleco.ul:32816 TIME_WAIT   -
tcp        0      0 tx11.tx.teleco.ul:59159 tx11.tx.teleco.ulpg:ftp TIME_WAIT   -
tcp        0      0 localhost.localdoma:ftp localhost.localdo:49942 TIME_WAIT   -
tcp        0      0 tx11.tx.teleco.u:telnet tx2.tx.teleco.ulp:58686 ESTABLISHED-
tcp        0      0 tx11.tx.teleco.u:telnet tx1.tx.teleco.ulp:37079 ESTABLISHED-
tcp        0      0 tx11.tx.teleco.u:telnet tx9.tx.teleco.ulp:46687 TIME_WAIT   -
tcp        0      0 tx11.tx.teleco.u:telnet tx5.tx.teleco.ulp:60945 ESTABLISHED-
tcp        0      0 tx11.tx.teleco.u:telnet tx7.tx.teleco.ulp:42847 ESTABLISHED-
tcp6       0      0 *:www                   *:*                     LISTEN      -
tcp6       0      0 *:ssh                   *:*                     LISTEN      -
tcp6       0      0 tx11.tx.teleco.ulpg:ssh operador.tx.teleco:2158 ESTABLISHED-
tcp6       0      0 tx11.tx.teleco.ulpg:ssh operador.tx.teleco:2364 ESTABLISHED-
udp        0      0 *:32768                 *:*                     -
udp        0      0 tx11.tx.tele:netbios-ns *:*                     -
udp        0      0 *:netbios-ns           *:*                     -
udp        0      0 tx11.tx.tel:netbios-dgm *:*                     -
udp        0      0 *:netbios-dgm          *:*                     -
udp        0      0 *:10000                 *:*                     -
udp        0      0 *:800                   *:*                     -
udp        0      0 *:bootpc                *:*                     -
udp        0      0 *:sunrpc                *:*                     -
halonso@tx11:~$

```

## 2.4. Escanear los servicios (puertos TCP más comunes) que ofrece una máquina remota

- Para escanear los servicios que ofrece una máquina remota desde la máquina local utilizaremos el comando `$nmap (IP)`. Escanearemos los puertos del servidor que hemos estado utilizando (cuya dirección IP es 192.168.100.33):

```

camilo:/home/himar# nmap 192.168.100.13

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-04-03 13:24 GMT
Interesting ports on 192.168.100.13:
(The 1660 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
587/tcp   open  submission
10000/tcp open  snet-sensor-mgmt
32770/tcp open  sometimes-rpc3
MAC Address: 00:05:1C:00:F1:85 (Xnet Technology)

Nmap finished: 1 IP address (1 host up) scanned in 4.266 seconds
camilo:/home/himar#

```

- Como cabía esperar, el servidor tiene activados, entre otros, los puertos que dan servicio a las aplicaciones que estamos analizando en esta práctica.

## 2.5. Hacer una conexión FTP

- A continuación haremos una conexión mediante FTP a la máquina remota y entraremos como usuario anónimo (*anonymous*). En el directorio “/pub” encontraremos un fichero con el nombre `telnet_packets`, que inspeccionaremos en el siguiente apartado con Ethereal.

```

camilo:/home/himar# ftp 192.168.100.13
Connected to 192.168.100.13.
220 tx11.tx.teleco.ulpgc.es FTP server ready.
Name (192.168.100.13:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password: *****
230-Welcome, archive user anonymous@192.168.100.33 !
230-
230-The local time is: Mon Apr  3 13:42:42 2006
230-
230-This is an experimental FTP server.  If have any unusual problems,
230-please report them via e-mail to <root@tx11.tx.teleco.ulpgc.es>.
230-
230-If you do have problems, please try using a dash (-) as the first
230-character of your password -- this will turn off the continuation
230-messages that may be confusing your FTP client.
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is current directory.
ftp> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
ftp> cd pub
250 CWD command successful.
ftp> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
ftp> get telnet_packets
local: telnet_packets remote: telnet_packets

```

```

200 PORT command successful.
150 Opening BINARY mode data connection for telnet_packets (59989 bytes).
226 Transfer complete.
59989 bytes received in 0.01 secs (5845.4 kB/s)
ftp> bye
221-You have transferred 59989 bytes in 1 files.
221-Total traffic for this session was 61565 bytes in 5 transfers.
221-Thank you for using the FTP service on tx11.tx.teleco.ulpgc.es.
221 Goodbye.
camilo:/home/himar#

```

## 2.6. Interceptar una contraseña mediante el uso de Ethereal

- *Ethereal* (ver Figura 1) es una herramienta de escaneo de paquetes de red, muy útil para comprobaciones sobre el nivel de seguridad de una red. En este apartado vamos a utilizar un escaneo que ha sido realizado anteriormente, y ha sido guardado en un fichero que es precisamente el que hemos obtenido en el apartado anterior, mediante la conexión FTP.
- Nuestro objetivo es averiguar la contraseña que ha introducido un usuario al realizar una conexión por TELNET. A pesar de la gran utilidad que tiene este protocolo, su principal problema, y es por eso que no se utiliza hoy en día, es que la información no viaja de forma *encriptada*, es decir, que cualquier persona que intercepte los paquetes –como se ha hecho para crear el archivo `telnet_packets`– podrá averiguar qué datos se están enviando.

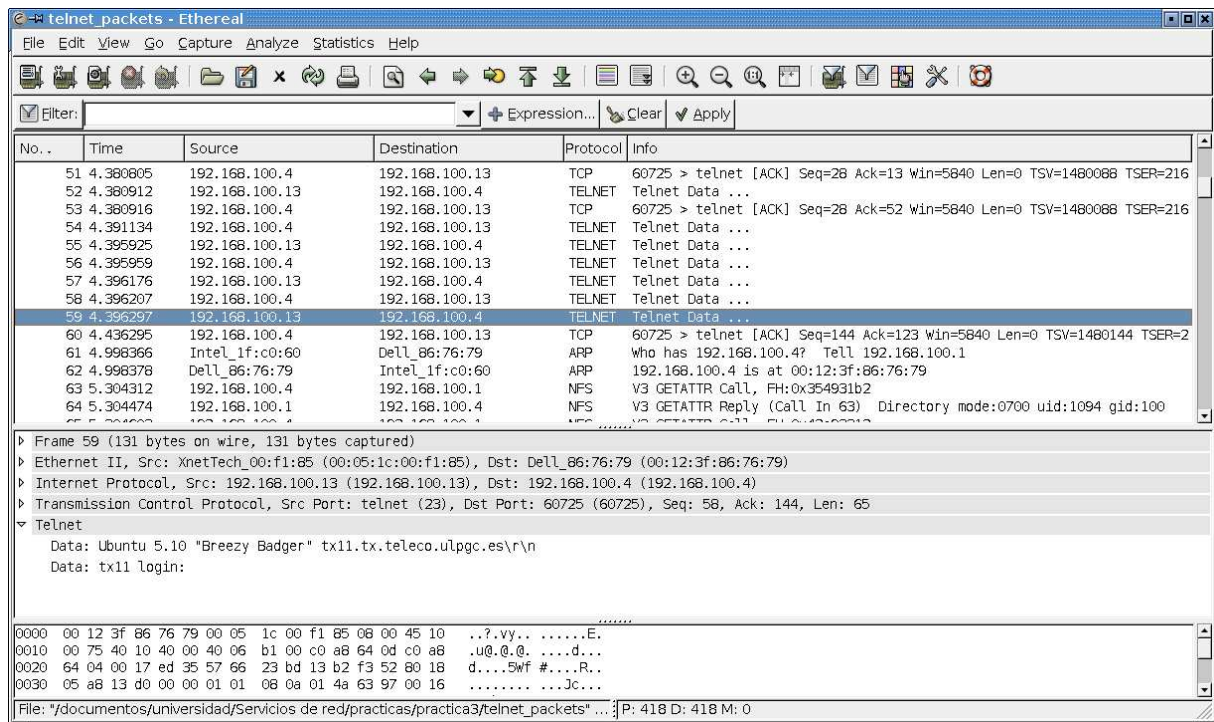


Figura 1: Captura de la aplicación *Ethereal*

Como podemos ver en la ventana del *Ethereal*, tenemos un campo para filtrar la búsqueda, en el que escribiremos “TELNET” para visualizar sólo los paquetes que utilizan este servicio. Mirando su contenido, obtenemos una secuencia como la que

se muestra en la Figura 2. El servidor TELNET pide la contraseña y muestra por pantalla la palabra “Password”, y el usuario introduce la contraseña “12345” y pulsa *Enter* (cuyo código es “\r\000”).

<pre> ▶ Frame 125 (76 bytes on wire, 76 bytes captured) ▶ Ethernet II, Src: XnetTech_00:f1:85 (00:0c:29:00:f1:85), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.13 (192.168.100.13), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 157, Len: 10 ▼ Telnet   Data: Password:  ▶ Frame 151 (67 bytes on wire, 67 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 158, Len: 2 ▼ Telnet   Data: 2  ▶ Frame 155 (67 bytes on wire, 67 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 159, Len: 2 ▼ Telnet   Data: 4 </pre>	<pre> ▶ Frame 149 (67 bytes on wire, 67 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 158, Len: 1 ▼ Telnet   Data: 1  ▶ Frame 153 (67 bytes on wire, 67 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 160, Len: 2 ▼ Telnet   Data: 3  ▶ Frame 165 (67 bytes on wire, 67 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: Dell_86:76:79 (00:12:3f:86:76:79) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.4 (192.168.100.4) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 161, Len: 2 ▼ Telnet   Data: 5 </pre>
<pre> ▶ Frame 167 (68 bytes on wire, 68 bytes captured) ▶ Ethernet II, Src: Dell_86:76:79 (00:12:3f:86:76:79), Dst: XnetTech_00:f1:85 (00:0c:29:00:f1:85) ▶ Internet Protocol, Src: 192.168.100.4 (192.168.100.4), Dst: 192.168.100.13 (192.168.100.13) ▶ Transmission Control Protocol, Src Port: 60725 (60725), Dst Port: telnet (23), Seq: 157, Ack: 158, Len: 10 ▼ Telnet   Data: \r\000 </pre>	

Figura 2: Vemos los paquetes IP que contienen la contraseña con *Ethereal*

## 2.7. Hacer una conexión SSH y configurar la misma usando certificados de clave pública/privada

- En esta sección describiré paso a paso cómo he configurado los certificados para acceder por SSH a mi servidor personal (nombre de red: *debian*), basándome en lo aprendido en las clases de prácticas:

1. En primer lugar generamos la clave en la máquina local:

```

himar@camilo:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/himar/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): *****
Enter same passphrase again: *****
Your identification has been saved in /home/himar/.ssh/id_dsa.
Your public key has been saved in /home/himar/.ssh/id_dsa.pub.
The key fingerprint is:
83:c6:2f:23:52:ab:5c:8f:84:10:6f:7f:7b:5e:62:0f himar@camilo
himar@camilo:~$

```

2. Subimos la clave al servidor, utilizando *scp*:

```

himar@camilo:~$ scp ./ssh/id_dsa.pub debian:/home/himar
Warning: the RSA host key for 'debian' differs from the key for the IP address '192.168.1.1'
Offending key for IP in /home/himar/.ssh/known_hosts:11
Matching host key in /home/himar/.ssh/known_hosts:13

```

```
Are you sure you want to continue connecting (yes/no)? yes
Password: *****
id_dsa.pub                                100% 602      0.6KB/s   00:00
himar@camilo:~$
```

3. Configuramos el archivo con la clave y asignamos los permisos, para evitar que otros usuarios puedan acceder a la clave:

```
himar@camilo:~$ ssh himar@debian
Warning: the RSA host key for 'debian' differs from the key for the IP address '192.168.1.1'
Offending key for IP in /home/himar/.ssh/known_hosts:11
Matching host key in /home/himar/.ssh/known_hosts:13
Are you sure you want to continue connecting (yes/no)? yes
Password:
Linux debian 2.6.11.7 #1 Thu May 5 13:42:28 GMT 2005 i686 GNU/Linux

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Tue Jun 13 17:29:45 2006
himar@debian:~$ mkdir .ssh
himar@debian:~$ mv id_dsa.pub ../ssh/authorized_keys2
himar@debian:~$ chmod 700 .ssh
himar@debian:~$ cd .ssh
himar@debian:~/ssh$ chmod 600 authorized_keys2
himar@debian:~$ exit
logout
Connection to debian closed.
himar@camilo:~$
```

4. Por último configuramos el agente, y comprobamos que podemos acceder sin necesidad de introducir la contraseña en adelante:

```
himar@camilo:~$ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-StLXLC4007/agent.4007; export SSH_AUTH_SOCK;
SSH_AGENT_PID=4008; export SSH_AGENT_PID;
echo Agent pid 4008;
himar@camilo:~$ SSH_AUTH_SOCK=/tmp/ssh-StLXLC4007/agent.4007; export SSH_AUTH_SOCK;
himar@camilo:~$ SSH_AGENT_PID=4008; export SSH_AGENT_PID;
himar@camilo:~$ echo Agent pid 4008;
Agent pid 4008
himar@camilo:~$ ssh-add
Enter passphrase for /home/himar/.ssh/id_dsa:
Identity added: /home/himar/.ssh/id_dsa (/home/himar/.ssh/id_dsa)
himar@camilo:~$ ssh himar@debian
Warning: the RSA host key for 'debian' differs from the key for the IP address '192.168.1.1'
Offending key for IP in /home/himar/.ssh/known_hosts:11
Matching host key in /home/himar/.ssh/known_hosts:13
Are you sure you want to continue connecting (yes/no)? yes
Linux debian 2.6.11.7 #1 Thu May 5 13:42:28 GMT 2005 i686 GNU/Linux

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Tue Jun 13 17:40:53 2006 from debian
himar@debian:~$ exit
logout
Connection to debian closed.
himar@camilo:~$
```

## 2.8. Hacer peticiones DNS y WHOIS

- Para este apartado utilizaré mi web personal ([www.himaronso.com](http://www.himaronso.com)). Mediante los comandos `host`, `dig` y `whois` veremos qué información podemos obtener:

- Con `host` podemos obtener la dirección IP a partir del nombre:

```
himar@camilo:~$ host himaronso.com
himaronso.com      A      64.111.125.144
himar@camilo:~$
```

- Con `dig` podemos obtener también la dirección IP, y además los servidores de nombres que tienen esa información:

```
himar@camilo:~$ dig himaronso.com

; <<>> DiG 9.3.2 <<>> himaronso.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6017
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
himaronso.com.                IN      A

;; ANSWER SECTION:
himaronso.com.                14400  IN      A      64.111.125.144

;; AUTHORITY SECTION:
himaronso.com.                73171  IN      NS     ns2.dreamhost.com.
himaronso.com.                73171  IN      NS     ns3.dreamhost.com.
himaronso.com.                73171  IN      NS     ns1.dreamhost.com.

;; ADDITIONAL SECTION:
ns1.dreamhost.com.           43202  IN      A      66.33.206.206
ns2.dreamhost.com.           43202  IN      A      66.201.54.66
ns3.dreamhost.com.           43202  IN      A      66.33.216.216

;; Query time: 315 msec
;; SERVER: 212.40.224.74#53(212.40.224.74)
;; WHEN: Tue Jun 13 18:02:46 2006
;; MSG SIZE rcvd: 161

himar@camilo:~$
```

- Finalmente, con `whois` podemos obtener información sobre el registro del dominio, y el propietario:

```
himar@camilo:~$ whois himaronso.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: HIMARALONSO.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: NS3.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS1.DREAMHOST.COM
Status: REGISTRAR-LOCK
EPP Status: clientDeleteProhibited
EPP Status: clientTransferProhibited
EPP Status: clientUpdateProhibited
Updated Date: 03-Jan-2006
Creation Date: 20-Nov-2005
```

Expiration Date: 20-Nov-2010

>>> Last update of whois database: Tue, 13 Jun 2006 12:54:14 EDT <<<

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name..... himaralonso.com  
Creation Date..... 2005-11-21  
Registration Date.... 2005-11-21  
Expiry Date..... 2010-11-21  
Organisation Name... Himar Alonso Díaz  
Organisation Address.  
Organisation Address.  
Organisation Address. Las Palmas de Gran Canaria  
Organisation Address. 35004  
Organisation Address. Las Palmas  
Organisation Address. SPAIN

Admin Name..... Himar Alonso Díaz  
Admin Address.....  
Admin Address..... Las Palmas de Gran Canaria  
Admin Address..... 35004  
Admin Address..... Las Palmas  
Admin Address..... SPAIN  
Admin Email..... himaralonso@himaralonso.com  
Admin Phone.....  
Admin Fax.....

Tech Name..... YahooDomains TechContact  
Tech Address..... 701 First Ave.  
Tech Address.....  
Tech Address..... Sunnyvale  
Tech Address..... 94089  
Tech Address..... CA  
Tech Address..... UNITED STATES  
Tech Email..... domain.tech@YAHOO-INC.COM  
Tech Phone..... +1.6198813096  
Tech Fax.....  
Name Server..... ns1.dreamhost.com  
Name Server..... ns2.dreamhost.com  
Name Server..... ns3.dreamhost.com

## 2.9. Hacer peticiones HTTP 1.0 y 1.1 usando TELNET

- La primera conexión HTTP la haremos al servidor local (IP 192.168.100.13), que dispone de un servidor web *Apache* con una página web de prueba. Accediendo por TELNET obtenemos el código HTML de la misma:

```
himar@camilo:~$ telnet 192.168.100.13 80
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
GET /
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Test Page for Apache Installation</title>
</head>
<!-- Background white, links blue (unvisited), navy (visited), red
(active) -->
<body bgcolor="#FFFFFF" text="#000000" link="#0000FF"
vlink="#000080" alink="#FF0000">
<p>If you can see this, it means that the installation of the <a
href="http://www.apache.org/foundation/preFAQ.html">Apache web
server</a> software on this system was successful. You may now add
content to this directory and replace this page.</p>

<hr width="50%" size="8" />
<h2 align="center">Seeing this instead of the website you
expected?</h2>

<p>This page is here because the site administrator has changed the
configuration of this web server. Please <strong>contact the person
responsible for maintaining this server with questions.</strong>
The Apache Software Foundation, which wrote the web server software
this site administrator is using, has nothing to do with
maintaining this site and cannot help resolve configuration
issues.</p>

<hr width="50%" size="8" />
<p>The Apache <a href="/manual/">documentation</a> has been included
with this distribution.</p>

<p>You are free to use the image below on an Apache-powered web
server. Thanks for using Apache!</p>

<div align="center"></div>
</body>
</html>

Connection closed by foreign host.
himar@camilo:~$
```

- En un navegador web como *Mozilla Firefox* podemos visualizar mejor el contenido de la web (Figura 3), ya que de esta manera sólo podemos ver el código.
- Hay páginas web que dependiendo de dónde proceda la petición nos mostrará un contenido u otro. En el siguiente ejemplo comprobaremos cómo al solicitar por TELNET “www.google.com” se nos redirige hacia la web local “www.google.es”:

```
himar@camilo:~$ telnet www.google.com 80
Trying 66.102.9.99...
Connected to www.l.google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.google.com

HTTP/1.1 302 Found
```

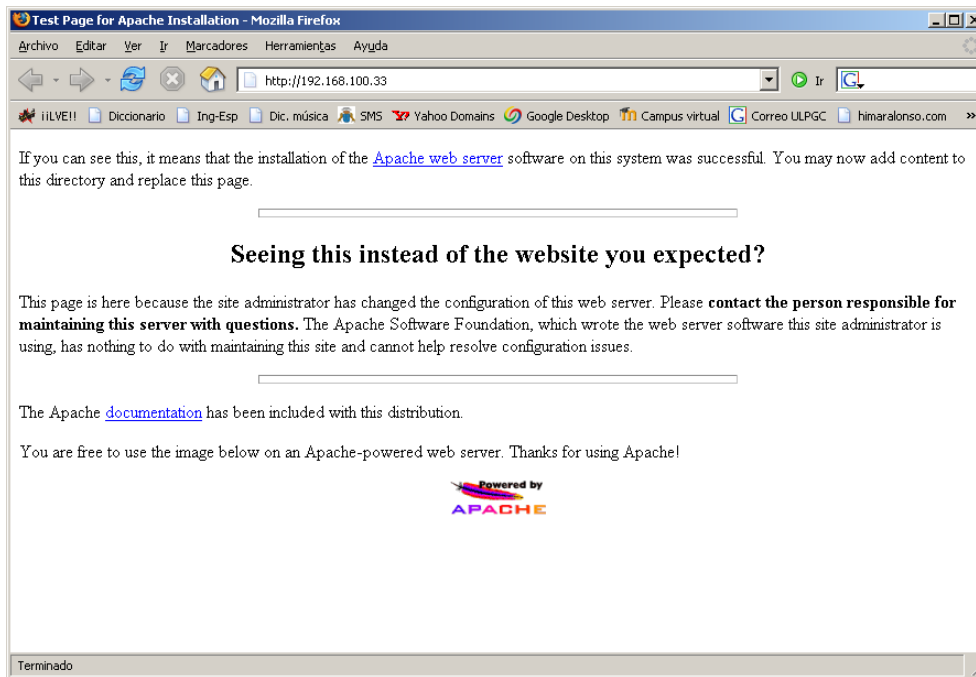


Figura 3: Visualización de la página web de prueba con *Mozilla Firefox*

```

Location: http://www.google.es/
Cache-Control: private
Set-Cookie: PREF=ID=570333c1349a44f8:TM=1145878870:LM=1145878870:S=LuSWE0hAfnKhEk7x;
            expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.com
Content-Type: text/html
Server: GWS/2.1
Content-Length: 218
Date: Mon, 24 Apr 2006 11:41:10 GMT

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.es/">here</A>.
</BODY></HTML>

Connection closed by foreign host.
himar@camilo:~$

```

- Sin embargo, al solicitar una web local, aunque no sea la nuestra, por ejemplo “[www.google.fr](http://www.google.fr)”, no se nos redirecciona a ningún otro sitio, sino que se nos proporciona el código HTML directamente:

```

himar@camilo:~$ telnet www.google.com 80
Trying 66.102.9.99...
Connected to www.l.google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.google.fr

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Set-Cookie: PREF=ID=2e446c02c51d70f1:TM=1145879000:LM=1145879000:S=KVMroLNtmHXAdm3f;
            expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.fr
Server: GWS/2.1
Transfer-Encoding: chunked

```

Date: Mon, 24 Apr 2006 11:43:20 GMT

```
c84
<html><head><meta http-equiv="content-type" content="text/html; charset=ISO-8859-1"><title>Google...
body,td,a,p,.h{font-family:arial,sans-serif;}
.h{font-size: 20px;}
.q{color:#0000cc;}
/-->
</style>
<script>
<!--
function sf(){document.f.q.focus();}
// -->
</script>
</head><body bgcolor=#ffffff text=#000000 link=#0000cc vlink=#551a8b alink=#ff0000 onLoad=sf() ...
<form action=/search name=f><table border=0 cellspacing=0 cellpadding=4><tr><td nowrap>...
0
Connection closed by foreign host.
himar@camilo:~$
```

## 2.10. Hacer FTPs tanto activos como pasivos usando TELNET

- En primer lugar haremos una conexión mediante FTP *activo* al servidor, para descargar la imagen que se encuentra en el directorio remoto “/pub/imagen.gif”. Al utilizar el modo activo, nosotros indicaremos a qué puerto deben ser enviados los datos (mediante el comando PORT). Tendremos que utilizar dos consolas, en una de ellas haremos la conexión por TELNET y en la otra “escucharemos” la información que nos llega por el puerto 25678, que es el que hemos elegido para transferir los datos.
- El programa para escuchar la información del puerto tendremos que ejecutarlo en otra consola, en lo que hacemos la conexión TELNET:
  - `$tcplisten 25678 >imagen.gif`
- Para utilizar el comando PORT tenemos que descomponer el número del puerto:  $25678 = 100 \times 256 + 78$ , de modo que la sentencia deberá ser:
  - `PORT 192,168,100,33,100,78`

```
himar@camilo:~$ telnet 192.168.100.13 21
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
220 ProFTPD 1.2.10 Server (tx11) [192.168.100.13]
USER anonymous
331 Anonymous login ok, send your complete email address as your password.
PASS anonymous
230-Welcome, archive user anonymous@192.168.100.33 !
230-
230-The local time is: Mon Apr 24 12:13:15 2006
230-
230-This is an experimental FTP server. If have any unusual problems,
230-please report them via e-mail to <root@tx11.tx.teleco.ulpgc.es>.
230-
230-If you do have problems, please try using a dash (-) as the first
230-character of your password -- this will turn off the continuation
230-messages that may be confusing your FTP client.
230 Anonymous access granted, restrictions apply.
PORT 192,168,100,33,100,78
200 PORT command successful
CWD pub
250 CWD command successful
RETR imagen.gif
```

```

150 Opening ASCII mode data connection for imagen.gif (2347 bytes)
226 Transfer complete.
QUIT
221 Goodbye.
Connection closed by foreign host.
himar@camilo:~$

```

- Al terminar la transferencia tendremos la imagen guardada en el directorio local, con el nombre “imagen.gif”, y la podremos visualizar (Figura 4).



Figura 4: Imagen obtenida por FTP

- Si queremos hacer una conexión en modo *pasivo* tendremos que indicar al servidor que nos proporcione un puerto para enviar los datos. Utilizaremos el comando PASV. Haremos una conexión FTP nuevamente para descargar la misma imagen, pero esta vez en modo pasivo.
- Debemos esperar el mensaje del servidor indicándonos por qué puerto nos enviará los datos, para hacer el cálculo. En nuestro caso resultó ser 192,168,100,13,197,176, así que el puerto es:  $197 \times 256 + 176 = 50608$ . De modo que en esta ocasión la sentencia de `tcplisten` debe ser:

- `$tcplisten 50608 >imagen.gif`

```

himar@camilo:~$ telnet 192.168.100.13 21
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
220 ProFTPD 1.2.10 Server (tx11) [192.168.100.13]
USER anonymous
331 Anonymous login ok, send your complete email address as your password.
PASS anonymous
230-Welcome, archive user anonymous@192.168.100.33 !
230-
230-The local time is: Mon Apr 24 13:14:16 2006
230-
230-This is an experimental FTP server. If have any unusual problems,
230-please report them via e-mail to <root@tx11.tx.teleco.ulpgc.es>.
230-
230-If you do have problems, please try using a dash (-) as the first
230-character of your password -- this will turn off the continuation
230-messages that may be confusing your FTP client.
230 Anonymous access granted, restrictions apply.
PASV
227 Entering Passive Mode (192,168,100,13,197,176).
CWD pub
250 CWD command successful
RETR imagen.gif
150 Opening ASCII mode data connection for imagen.gif (2347 bytes)
226 Transfer complete.
QUIT
221 Goodbye.
Connection closed by foreign host.
himar@camilo:~$

```

- En el apartado de cuestiones específicas se explican algunos problemas que pueden surgir al intentar acceder con FTP activo, y la solución que se puede dar.

## 2.11. Enviar y recibir correos usando TELNET

- Enviaremos un correo electrónico utilizando TELNET a través del puerto 25 (SMTP):

```
himar@camilo:~$ telnet 192.168.100.13 25
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
220 tx11.tx.teleco.ulpgc.es ESMTP Sendmail 8.13.5/8.13.5/Debian-3; ...
from: 192.168.100.33(OK)-192.168.100.33
HELO 192.168.100.33
250 tx11.tx.teleco.ulpgc.es Hello 192.168.100.33, pleased to meet you
MAIL FROM: himar@192.168.100.33
250 2.1.0 himar@192.168.100.33... Sender ok
RCPT TO: halonso@tx11
250 2.1.5 halonso@tx11... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
E-mail de prueba.
.
250 2.0.0 xe5P8peFkx09362 Message accepted for delivery
QUIT
221 2.0.0 tx11.tx.teleco.ulpgc.es closing connection
Connection closed by foreign host.
himar@camilo:~$
```

- Para leer el correo electrónico utilizaremos POP3 (puerto 110) a través de TELNET:

```
himar@camilo:~$ telnet 192.168.100.13 110
Trying 192.168.100.13...
Connected to 192.168.100.13.
Escape character is '^]'.
+OK
USER halonso
+OK
PASS 44719924
+OK
LIST
+OK
1 523
.
RETR 1
+OK
Return-Path: <himar@192.168.100.33>
Received: from 192.168.100.33
        by tx11.tx.teleco.ulpgc.es (8.13.5/8.13.5/Debian-3) with SMTP id xe5P8peFkx09362
        for halonso@tx11; Thu, 25 May 2006 09:53:14 +0100
Date: Mon, 22 May 2006 12:50:35 +0100
From: himar@192.168.100.33
Message-Id: <200605221250.xe5P8peFkx09362@tx11.tx.teleco.ulpgc.es>
To: undisclosed-recipients;;

E-mail de prueba.
.
DELE 1
+OK
LIST
+OK
.
QUIT
+OK
Connection closed by foreign host.
```

## 3. Cuestiones específicas

### 3.1. Crear un subdirectorio en nuestra cuenta de la máquina remota y poner en ella algunos ficheros. ¿Cómo hacemos para traernos por FTP todo el directorio?

Como para casi todo, hay muchas maneras de hacerlo, de las cuales mencionaré sólo tres, que considero son las más interesantes, según el entorno en el que nos encontremos.

#### 3.1.1. Utilizando el comando FTP: mget

La instrucción `help` nos muestra una lista de los comandos FTP que podemos utilizar. Para el primer ejemplo mostraré un acceso a mi servidor FTP personal. En el directorio raíz hay una carpeta con el nombre “carpeta” y dentro de ésta, hay tres ficheros con los nombres “fichero1”, “fichero2” y “fichero3”. Utilizaré el `mget` de dos maneras posibles:

- `>mget fichero1, fichero2,...` → Descarga la lista de archivos.
- `>mget directorio` → Descarga todos los archivos de “directorio”.

```
camilo:/home/himar# ftp himaralonso.com
Conectado a himaralonso.com.
220 ProFTPD 1.3.0rc2 Server (DreamHost FTP) [64.111.125.144]
Usuario (himaralonso.com:(none)): himaralonso
331 Password required for himaralonso.
Contraseña: *****
230 User himaralonso logged in.
ftp> help
!                delete          literal          prompt          send
?                debug            ls               put             status
append          dir              mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get              mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir

ftp> cd carpeta
250 CWD command successful

ftp> mget fichero1 fichero2
200 Type set to A
mget fichero1? y
200 PORT command successful
150 Opening ASCII mode data connection for fichero1
226 Transfer complete.
mget fichero2? y
200 PORT command successful
150 Opening ASCII mode data connection for fichero2
226 Transfer complete.

ftp> cd ..
250 CWD command successful

ftp> mget carpeta
200 Type set to A
mget carpeta/fichero1? y
200 PORT command successful
150 Opening ASCII mode data connection for carpeta/fichero1
226 Transfer complete.
mget carpeta/fichero2? y
200 PORT command successful
150 Opening ASCII mode data connection for carpeta/fichero2
226 Transfer complete.
```

```

mget carpeta/fichero3? y
200 PORT command successful
150 Opening ASCII mode data connection for carpeta/fichero3
226 Transfer complete.
ftp> bye
221 Goodbye.

```

```
camilo:/home/himar#
```

### 3.1.2. Utilizando el programa wget

El programa `wget` es una aplicación en modo texto que nos permite realizar descargas mediante HTTP o FTP. Entre las múltiples opciones de descarga incluye la *descarga recursiva*. Para ello utilizaremos `$wget -r (URL)`. Por simplificar el ejemplo, he utilizado un servidor FTP público al cual se accede de manera anónima. Nótese que “uemacs” es una carpeta que contiene varios archivos:

```

camilo:/home/himar# wget -r ftp://ftp.kernel.org/pub/linux/kernel/uemacs
--13:43:23-- ftp://ftp.kernel.org/pub/linux/kernel/uemacs
      => 'ftp.kernel.org/pub/linux/kernel/.listing'
Resolving ftp.kernel.org... 204.152.191.5, 204.152.191.37
Connecting to ftp.kernel.org|204.152.191.5|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.      ==> PWD ... done.
==> TYPE I ... done.   ==> CWD /pub/linux/kernel ... done.
==> PASV ... done.     ==> LIST ... done.

      [ <=>                               ] 1.397      --.--K/s

13:43:26 (48.17 MB/s) - 'ftp.kernel.org/pub/linux/kernel/.listing' saved [1397]

Removed 'ftp.kernel.org/pub/linux/kernel/.listing'.
--13:43:26-- ftp://ftp.kernel.org/pub/linux/kernel/uemacs/uemacs
      => 'ftp.kernel.org/pub/linux/kernel/uemacs/.listing'
==> CWD /pub/linux/kernel/uemacs ... done.
==> PASV ... done.     ==> LIST ... done.

      [ <=>                               ] 399      --.--K/s

13:43:27 (14.81 MB/s) - 'ftp.kernel.org/pub/linux/kernel/uemacs/.listing' saved
[399]

Removed 'ftp.kernel.org/pub/linux/kernel/uemacs/.listing'.
--13:43:27-- ftp://ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2
      => 'ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2'
==> CWD /pub/linux/kernel/uemacs ... done.
==> PASV ... done.     ==> RETR em-4.0.15-1t.tar.bz2 ... done.
Length: 165.601 (162K)

100%[=====] 165.601      33.35K/s      ETA 00:00

13:43:33 (33.28 KB/s) - 'ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2' saved [165601]

--13:43:33-- ftp://ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2.sign
      => 'ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2.sign'

==> CWD /pub/linux/kernel/uemacs ... done.
==> PASV ... done.     ==> RETR em-4.0.15-1t.tar.bz2.sign ... done.
Length: 248

100%[=====] 248      --.--K/s

13:43:34 (40.12 KB/s) - 'ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.bz2.sign' saved [248]

--13:43:34-- ftp://ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.gz
      => 'ftp.kernel.org/pub/linux/kernel/uemacs/em-4.0.15-1t.tar.gz'
==> CWD /pub/linux/kernel/uemacs ... done.
==> PASV ... done.     ==> RETR em-4.0.15-1t.tar.gz ... done.
Length: 209.681 (205K)

```

```

100%[=====>] 209.681      56.48K/s   ETA 00:00

13:43:38 (56.35 KB/s) - 'ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.gz' saved [209681]

--13:43:38--  ftp://ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.gz.sign
              => 'ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.gz.sign'
==> CWD /pub/linux/kernel/ueemacs ... done.
==> PASV ... done.      ==> RETR em-4.0.15-lt.tar.gz.sign ... done.
Length: 248

100%[=====>] 248          --.--K/s

13:43:39 (17.40 KB/s) - 'ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.gz.sign' saved [248]

--13:43:39--  ftp://ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.sign
              => 'ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.sign'
==> CWD /pub/linux/kernel/ueemacs ... done.
==> PASV ... done.      ==> RETR em-4.0.15-lt.tar.sign ... done.
Length: 248

100%[=====>] 248          --.--K/s

13:43:40 (27.77 KB/s) - 'ftp.kernel.org/pub/linux/kernel/ueemacs/em-4.0.15-lt.tar.sign' saved [248]

FINISHED --13:43:40--
Downloaded: 376.026 bytes in 5 files

camilo:/home/himar#

```

### 3.1.3. Utilizando un cliente FTP avanzado en modo gráfico

Sin duda la forma más sencilla y cómoda cuando estamos en un entorno gráfico es utilizar un cliente FTP gráfico. En este caso he accedido al mismo servidor que antes, donde podemos ver la carpeta “ueemacs” en la máquina remota (Figura 5, a la derecha). Arrastrándola hacia un directorio local, como se muestra con la flecha, conseguiremos traer a la máquina local el directorio y todos los ficheros que contenga. Esto se consigue con una secuencia de comandos FTP:

- CWD → Para acceder al directorio.
- LIST → Para ver su contenido.
- RETR → El cliente *Filezilla* ejecuta un bucle con esta instrucción, para descargar todos los archivos individualmente.

## 3.2. Identificar las máquinas de la subred del laboratorio que están encendidas y los servicios que están prestando. ¿Podemos hacerlo con un solo comando?

Yo he utilizado dos comandos: uno para comprobar qué máquinas están encendidas, y el otro para escanear los puertos.

1. Para comprobar qué máquinas están encendidas en el laboratorio, hacemos \$ping a todos los ordenadores de la subred:

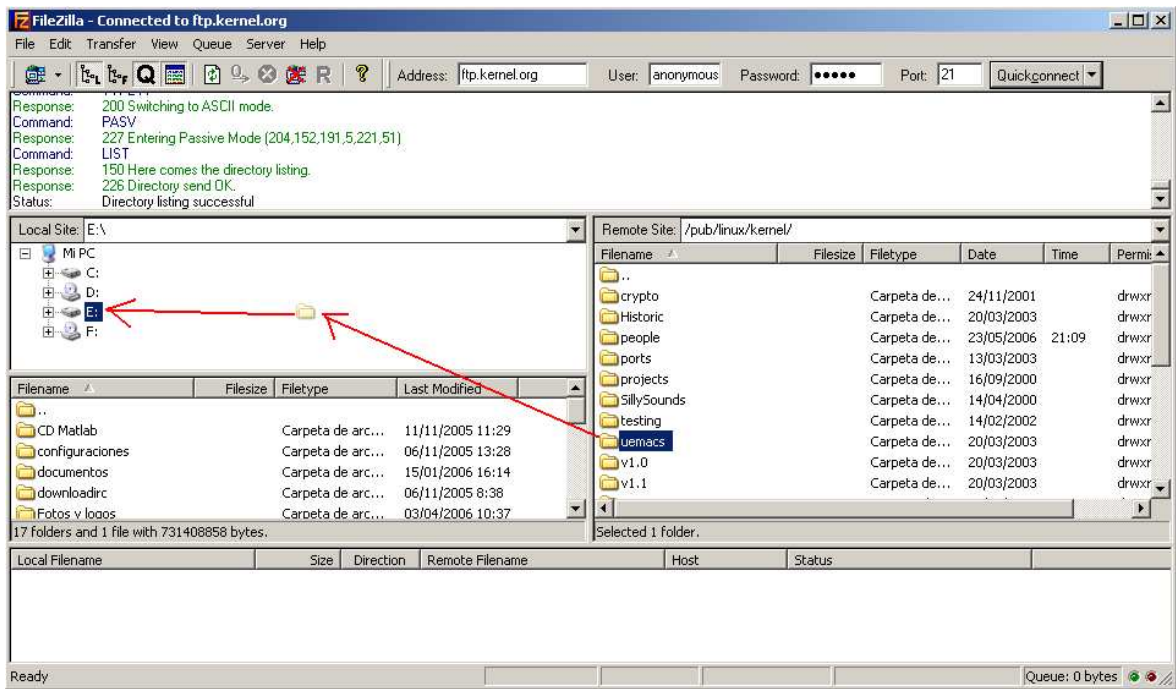


Figura 5: Captura del cliente FTP gráfico *Filezilla*

```

himar@camilo:~$ ping 192.168.100.255
PING 192.168.100.255 (192.168.100.255): 56 data bytes
64 bytes from 192.168.100.5: icmp_seq=0 ttl=64 time=0.6 ms
64 bytes from 192.168.100.6: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.8: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.4: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.1: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.11: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.10: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.9: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=0.7 ms (DUP!)
64 bytes from 192.168.100.12: icmp_seq=0 ttl=64 time=1.2 ms (DUP!)
64 bytes from 192.168.100.3: icmp_seq=0 ttl=64 time=1.2 ms (DUP!)
(...)

--- 192.168.100.255 ping statistics ---
4 packets transmitted, 4 packets received, +40 duplicates, 0% packet loss
round-trip min/avg/max = 0.1/0.3/1.2 ms

himar@camilo:~$

```

2. Una vez sabemos qué máquinas están encendidas, utilizamos *\$nmap* para escanear los puertos. Yo hice el escáner de tres de las máquinas remotas. Para automatizar tareas, en caso de que fuera necesario, se podría hacer un *script* que ejecutara varios comandos de forma secuencial:

```

himar@camilo:~$ nmap 192.168.100.1

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-04-24 12:23 GMT
Interesting ports on 192.168.100.1:
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
113/tcp   open  auth
139/tcp   open  netbios-ssn

```

```

445/tcp open  microsoft-ds
600/tcp open  ipcserver
631/tcp open  ipp
656/tcp open  unknown
693/tcp open  unknown
1010/tcp open unknown
1014/tcp open unknown
1024/tcp open kdm
2049/tcp open  nfs

Nmap finished: 1 IP address (1 host up) scanned in 0.341 seconds

himar@camilo:~$ nmap 192.168.100.254

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-04-24 12:23 GMT
Interesting ports on 192.168.100.254:
(The 1669 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
113/tcp   open  auth

Nmap finished: 1 IP address (1 host up) scanned in 0.284 seconds

himar@camilo:~$ nmap 192.168.100.9

Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-04-24 12:24 GMT
Interesting ports on 192.168.100.9:
(The 1669 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
800/tcp   open  mdbus_daemon

Nmap finished: 1 IP address (1 host up) scanned in 0.247 seconds
himar@camilo:~$

```

### 3.3. ¿Es posible hacer un FTP *activo* usando como cliente una máquina dentro de la red de la Universidad y como servidor una máquina de afuera? Dicho de otra manera, ¿puede la máquina externa conocer la IP de nuestro nodo dentro de la Universidad?

#### 3.3.1. Caso genérico

La respuesta más genérica a esta pregunta sería “en principio no”. En el caso de segunda pregunta la respuesta es “rotundamente no”, el servidor nunca podrá saber cuál es la IP de nuestro equipo en la subred del laboratorio.

**Argumento:** Cuando accedemos por FTP a un servidor externo y ejecutamos el comando PORT (IP), es decir, intentamos acceder en modo *activo*, el parámetro IP es la dirección IP de nuestra máquina local (192.168.100.X), que es *inaccesible* para los servidores de Internet, ya que éstos sólo pueden visualizar la IP *pública* (que en nuestro caso es 193.145.145.108<sup>1</sup>).

#### 3.3.2. Haciendo uso de NAT

Sin embargo, si disponemos de un router con NAT (*Network Adress Translation*), sí que podríamos acceder a un servidor FTP en modo *activo*.

---

<sup>1</sup>En webs del estilo <http://www.showmyip.com> podemos obtener este dato

**Argumento:** Cuando accedemos por FTP a un servidor externo y ejecutamos el comando PORT (IP), la instrucción es reconvertida por el router, que cambia el campo IP –que contiene la IP de nuestra máquina en la subred del laboratorio– por la dirección IP *pública* del router. De este modo, cuando el servidor externo nos envía información, lo hace a través del router, el cual, de manera inversa, envía el paquete a la máquina local.