

# Manual SSH

# Índice

- 1) Instalar y desinstalar servidor SSH
- 2) Iniciar, reiniciar y parar servidor SSH
- 3) Configurar servidor SSH
- 4) Conectar por terminal a servidor
- 5) Ver que usuarios están conectado al servidor
- 6) Cerrar conexión a un cliente
- 7) Ver fingerprint
- 8) Borrar fingerprint Windows
- 9) Borrar fingerprint Linux
- 10) Borrar claves
- 11) Crear claves
- 12) Error al conectarse al servidor SSH al tener claves nuevas
- 13) Validar SSH clave pública Servidor Linux Cliente Windows
- 14) Agente SSH Servidor Linux Cliente Windows
- 15) Ejecutar aplicaciones X remotas a través de SSH Servidor Linux Cliente Linux
- 16) Ejecutar aplicaciones X remotas a través de SSH Servidor Linux Cliente Windows
- 17) SCP Enviar archivos Servidor Linux Cliente Linux
- 18) SCP Enviar archivos Servidor Windows Cliente Linux
- 19) Tunel SSH Servicio daytime Servidor Linux Cliente Windows

SSH es un protocolo de comunicación seguro que utiliza el puerto 22 TCP.

## 1) Instalar y desinstalar servidor SSH



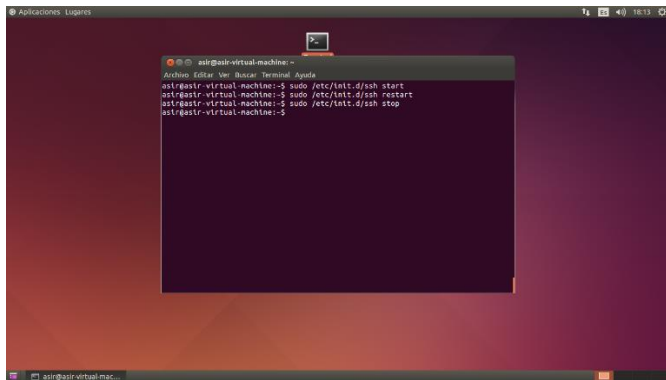
```
asir@asir-virtual-machine:~$ sudo apt-get install openssh-server
Archivos Editar Ver Buscar Terminal Ayuda
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  libick-connector ncurses-term openssh-client openssh-sftp-server
  python-requests python-urllib3 ssh-import-id
Paquetes sugeridos:
  libpam-ssh keychain monkeysphere rssh molly-guard
Se instalarán los siguientes paquetes NOVEDOS:
  libick-connector ncurses-term openssh-server openssh-sftp-server
  python-requests python-urllib3 ssh-import-id
Se actualizarán los siguientes paquetes:
  openssh-client
1 actualizados, 7 se instalarán, 0 para eliminar y 327 no actualizados.
Se necesitan descargar 999 KB/1.03 KB de archivos.
Se utilizarán 3.856 KB de espacio de disco adicional después de esta operación.
¿Deese continuar? [Y/n] y
Des13 http://es.archive.ubuntu.com/ubuntu/ trusty/main libick-connector amd64 0
4.1-3.1ubuntu2 (18,5 KB)
Des12 http://es.archive.ubuntu.com/ubuntu/ trusty/main ncurses-term all 5.9-12014
0110-1ubuntu1 (243 KB)
Des13 http://es.archive.ubuntu.com/ubuntu/ trusty-updates/main openssh-sftp-ser
```



```
asir@asir-virtual-machine:~$ sudo apt-get purge openssh-server
Archivos Editar Ver Buscar Terminal Ayuda
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los siguientes paquetes se ELIMINARÁN:
  openssh-server
0 actualizados, 0 se instalarán, 1 para eliminar y 327 no actualizados.
Se liberarán 911 KB después de esta operación.
¿Deese continuar? [Y/n] y
asir@asir-virtual-machine:~$ sudo apt-get purge openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los siguientes paquetes se ELIMINARÁN:
  openssh-server
0 actualizados, 0 se instalarán, 1 para eliminar y 327 no actualizados.
Se liberarán 911 KB después de esta operación.
¿Deese continuar? [Y/n] y
Leyendo la base de datos ... 172075 ficheros o directorios instalados actualmen
te.)
Removing openssh-server (1:0.4p1-2ubuntu2.3) ...
ssh stop/waiting
Purging configuration files for openssh-server (1:0.4p1-2ubuntu2.3) ...
```

Instalar servidor SSH **sudo apt-get install openssh-server**  
Desinstalar servidor SSH **sudo apt-get purge openssh-server**

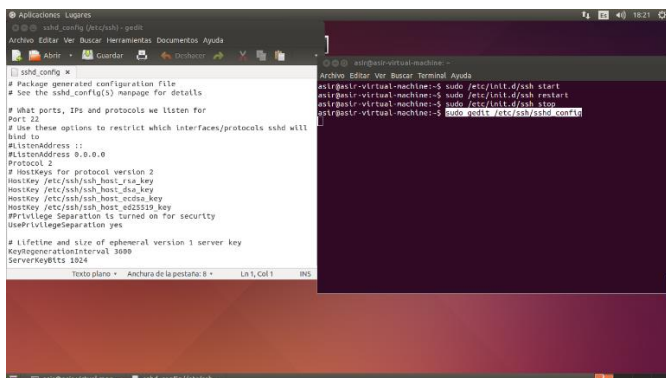
## 2) Iniciar, reiniciar y parar servidor SSH



```
asir@asir-virtual-machine:~$ sudo /etc/init.d/ssh start
asir@asir-virtual-machine:~$ sudo /etc/init.d/ssh restart
asir@asir-virtual-machine:~$ sudo /etc/init.d/ssh stop
asir@asir-virtual-machine:~$
```

Iniciar SSH **sudo /etc/init.d/ssh start**  
Reiniciar SSH **sudo /etc/init.d/ssh restart**  
Parar SSH **sudo /etc/init.d/ssh stop**

## 3) Configurar servidor SSH



```
# sshd_config
# Package generated configuration file
# See the sshd_config(8) manpage for details
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will
bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
# Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
# Privilege Separation is turned on for security
UsePrivilegeSeparation yes
# Lifetime and size of ephemeral version 1 server key
KeyGenerationInterval 3000
ServerKeyBits 1024
```

```
asir@asir-virtual-machine:~$ cd /etc/ssh/sshd_config
asir@asir-virtual-machine:~$ sudo gedit /etc/ssh/sshd_config
```

Ir a etc/ssh/sshd\_config **cd /etc/ssh/sshd\_config**  
Editar configuración **sudo gedit /etc/ssh/sshd\_config**

## 4) Conectar por terminal a servidor



```
asir@asir-virtual-machine:~$ ssh 192.168.170.133
asir@192.168.170.133:~$
The authenticity of host '192.168.170.133 (192.168.170.133)' can't be established.
ECDSA key fingerprint is 28:e8:2b:99:eb:9b:f0:69:37:82:da:1f:09:93:81:c7.
Are you sure you want to continue connecting (yes/no)? y
Warning: Permanently added '192.168.170.133' (ECDSA) to the list of known hosts.
asir@192.168.170.133:~$
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)
* Documentation:  https://help.ubuntu.com/

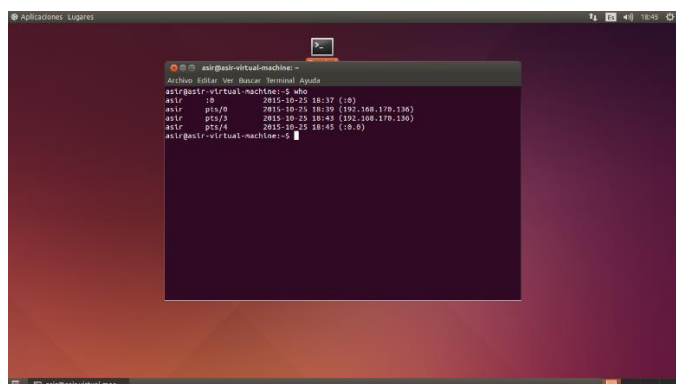
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
aplicable law.
asir@192.168.170.133:~$
```



```
asir@192.168.170.133:~$ ssh asir@192.168.170.133
asir@192.168.170.133:~$
Last login: Sun Oct 25 18:37:17 2015 from 192.168.170.136
asir@192.168.170.133:~$
```

Conectar por terminal **ssh Ipservidor**  
Conectar por terminal a usuario específico **ssh usuario@ipservidor**

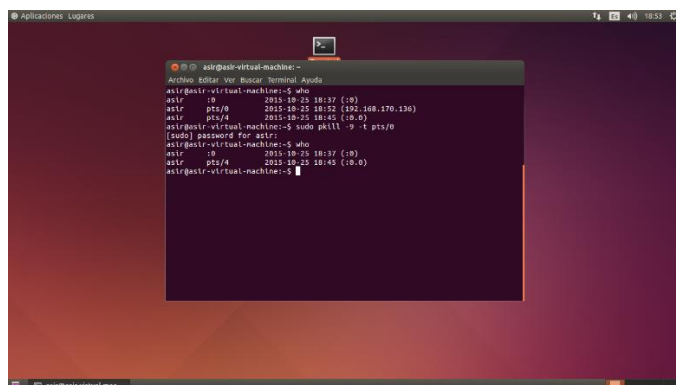
## 5) Ver que usuarios están conectado al servidor



```
asir@192.168.170.133:~$ who
asir    pts/0    2015-10-25 18:37 (10)
asir    pts/2    2015-10-25 18:39 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (10.0)
```

Ver quien hay conectado **who**

## 6) Cerrar conexión a un cliente



```
asir@192.168.170.133:~$ who
asir    pts/0    2015-10-25 18:37 (10)
asir    pts/2    2015-10-25 18:39 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (10.0)
asir@192.168.170.133:~$ sudo kill -9 -t Id
asir@192.168.170.133:~$ who
asir    pts/0    2015-10-25 18:37 (10)
asir    pts/2    2015-10-25 18:39 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (192.168.170.136)
asir    pts/4    2015-10-25 18:45 (10.0)
```



```
asir@192.168.170.133:~$ ssh asir@192.168.170.133
asir@192.168.170.133:~$
Last login: Sun Oct 25 18:37:17 2015 from 192.168.170.133
asir@192.168.170.133:~$
```

Cerrar conexión de cliente **sudo kill -9 -t Id**

## 7) Ver fingerprint

```

ast@ast-virtual-machine: /etc/ssh
$ cd /etc/ssh
$ ls -l
total 284
-rw-r--r-- 1 root root 242891 may 12 2014 moduli
-rw-r--r-- 1 root root 1690 may 12 2014 ssh_config
-rw-r--r-- 1 root root 2541 oct 25 18:11 ssh_config
-rw-r--r-- 1 root root 672 oct 25 18:11 ssh_host_dsa_key
-rw-r--r-- 1 root root 615 oct 25 18:11 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 227 oct 25 18:11 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 187 oct 25 18:11 ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 419 oct 25 18:11 ssh_host_ed25519_key
-rw-r--r-- 1 root root 187 oct 25 18:11 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 1670 oct 25 18:11 ssh_host_rsa_key
-rw-r--r-- 1 root root 487 oct 25 18:11 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root 318 oct 25 18:04 ssh_import_id
ast@ast-virtual-machine: /etc/ssh

```

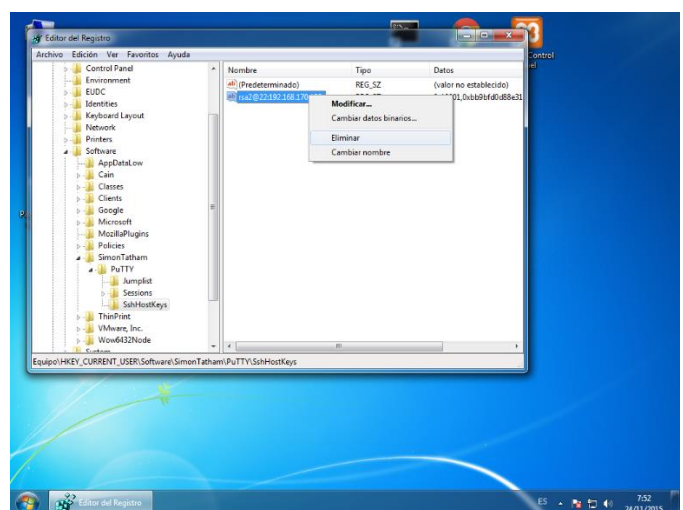
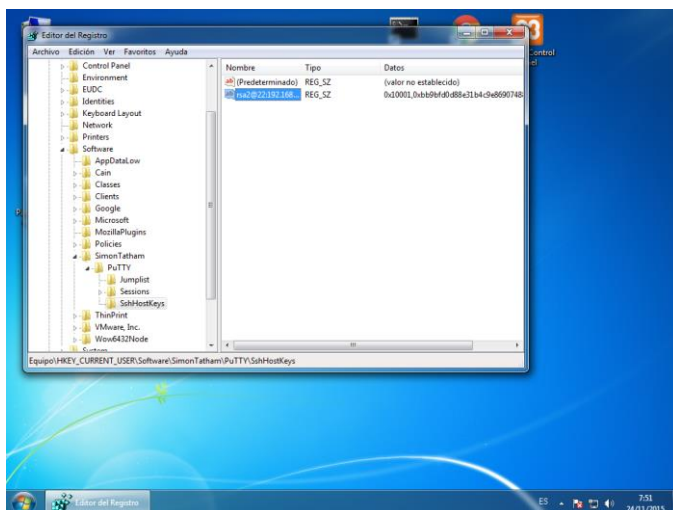
```

ast@ast-virtual-machine: /etc/ssh
$ cd /etc/ssh
$ ls -l
total 284
-rw-r--r-- 1 root root 242891 may 12 2014 moduli
-rw-r--r-- 1 root root 1690 may 12 2014 ssh_config
-rw-r--r-- 1 root root 2541 oct 25 18:11 ssh_config
-rw-r--r-- 1 root root 672 oct 25 18:11 ssh_host_dsa_key
-rw-r--r-- 1 root root 615 oct 25 18:11 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 227 oct 25 18:11 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 187 oct 25 18:11 ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 419 oct 25 18:11 ssh_host_ed25519_key
-rw-r--r-- 1 root root 187 oct 25 18:11 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 1670 oct 25 18:11 ssh_host_rsa_key
-rw-r--r-- 1 root root 487 oct 25 18:11 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root 318 oct 25 18:04 ssh_import_id
ast@ast-virtual-machine: /etc/ssh
$ ssh-keygen -l -f nombre de la clave

```

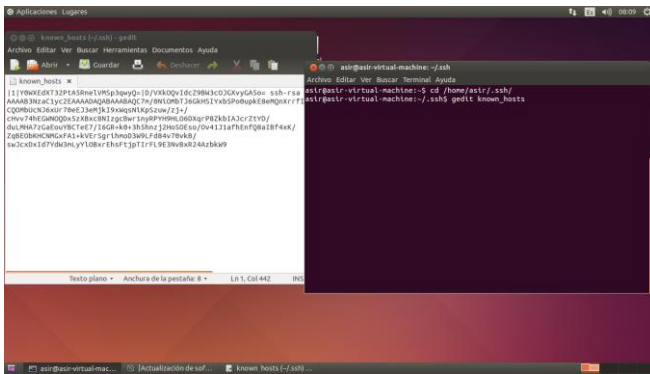
Ir a `cd /etc/ssh`  
 Listar contenido del directorio `ls -l`  
 Ver fingerprint `ssh-keygen -l -f nombre de la clave`

## 8) Borrar fingerprint Windows



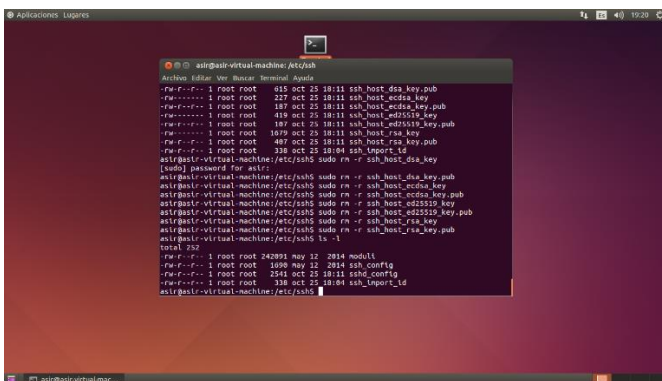
Ejecutar regedit e ir a **HKEY\_CURRENT\_USER\Software\SimonTatham\PuTTY\SshHostKeys**  
 Boton derecho sobre la fingerprint y eliminar.

## 9) Borrar fingerprint Linux



Ir al directorio .ssh del usuario al que se conectan los clientes en el servidor **cd /home/asir/.ssh/**  
 Editar el archivo known\_hosts **gedit known\_hosts**  
 Dejarlo limpio.

## 10) Borrar claves



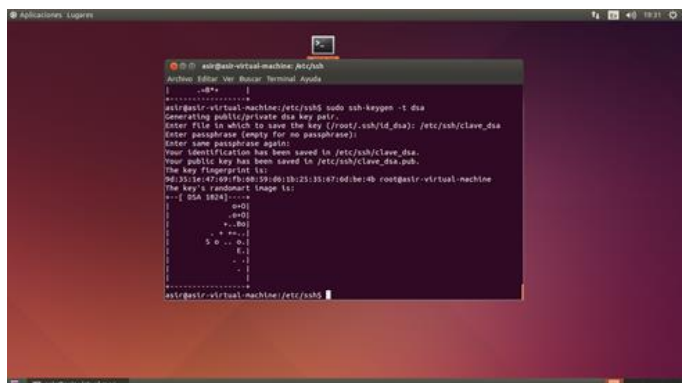
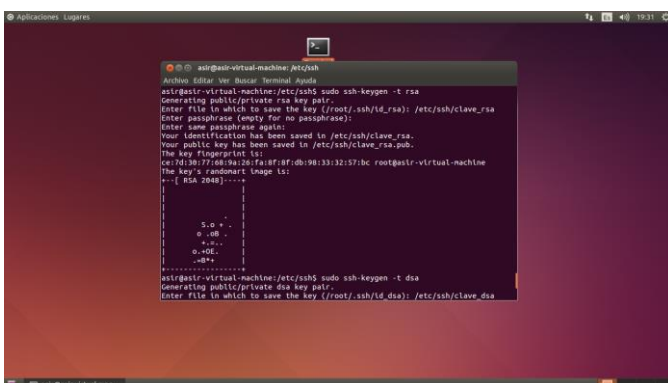
Ir a

Listar contenido del directorio

Borrar claves

```
cd /etc/ssh
ls -l
sudo rm -r nombre de la clave
```

### 11) Crear claves

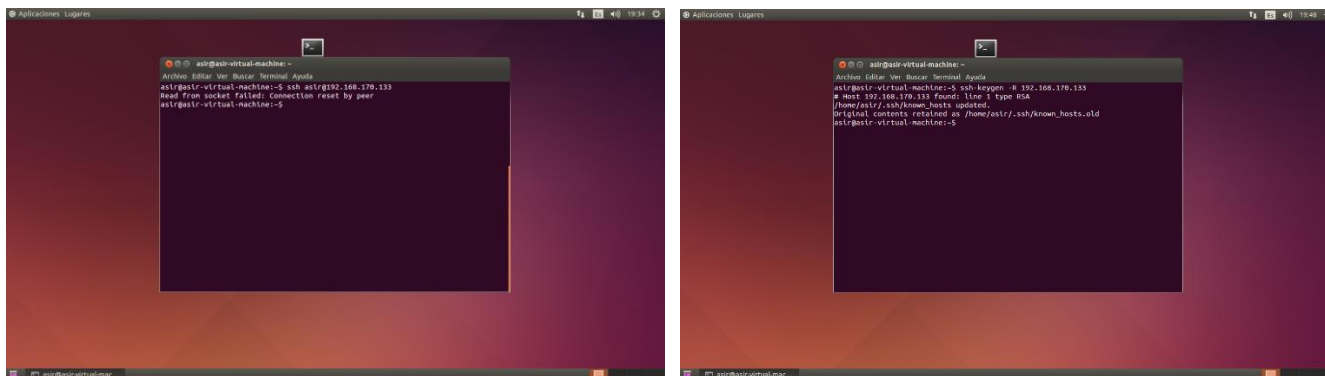


- Crear claves rsa
- Crear claves dsa
- Editar el archivo sshd\_config
- Reiniciar ssh

```
sudo ssh-keygen -t rsa
sudo ssh-keygen -t dsa
sudo gedit /etc/ssh/sshd_config
```



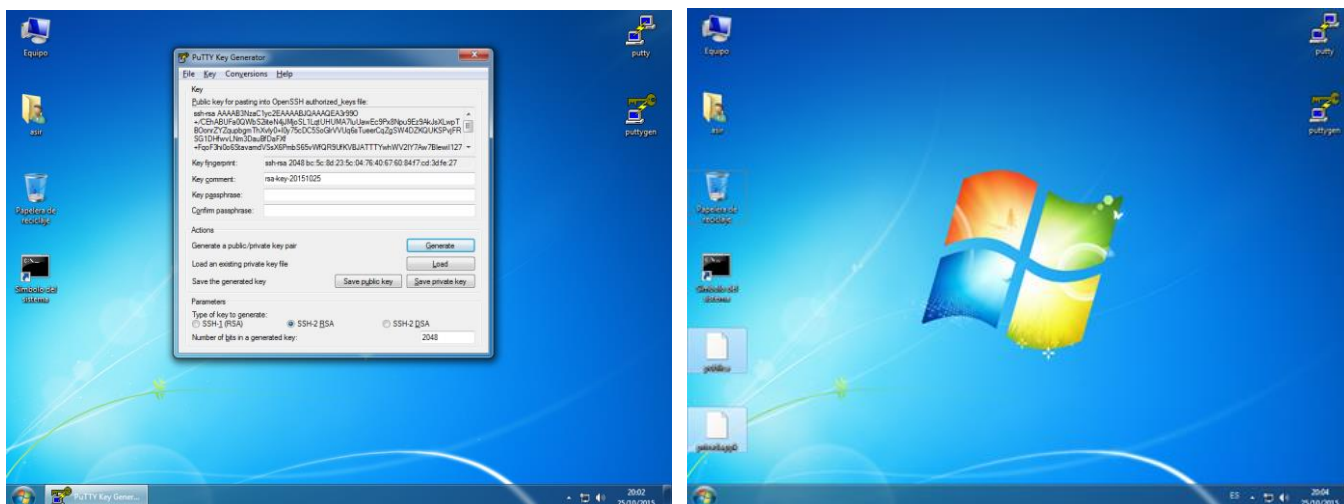
## 12) Error al conectarse al servidor SSH al tener claves nuevas



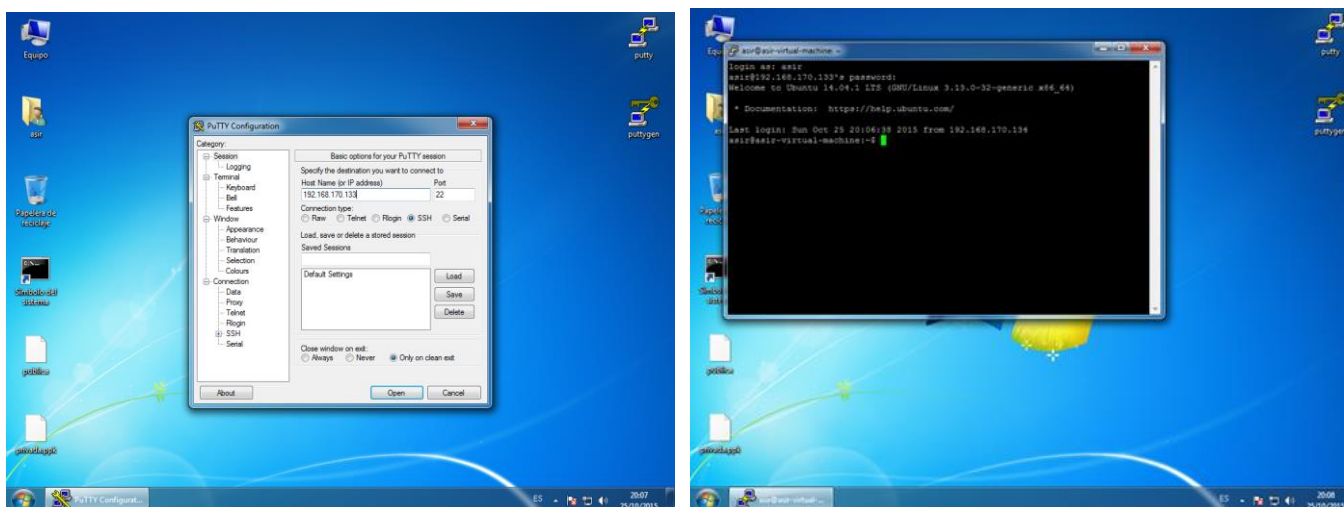
Desde el cliente **ssh-keygen -R ipservidor**

## 13) Validar SSH clave pública Servidor Linux Cliente Windows

Cliente

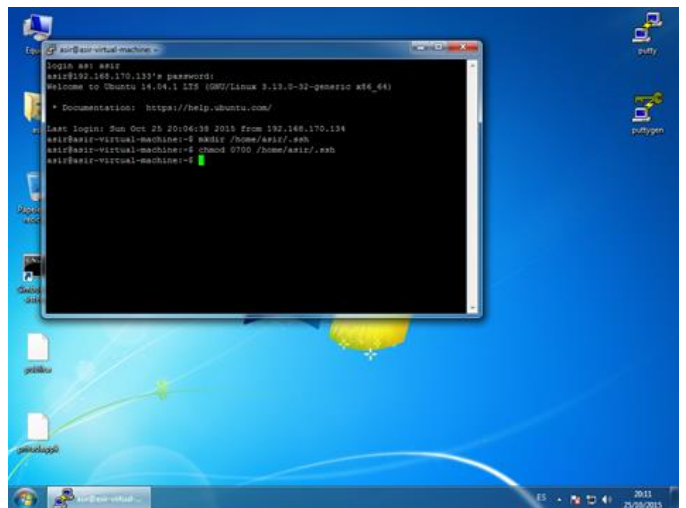
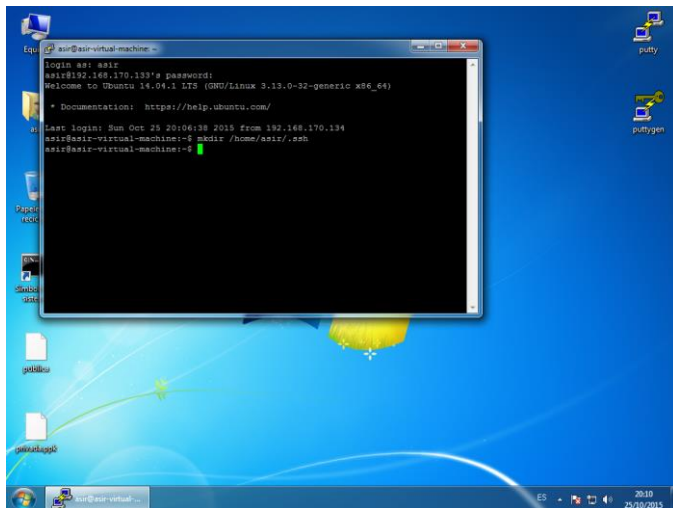


Utilizar Puttygen para generar el par de claves ssh2-rsa.  
Copiar la clave publica en un archivo y guardar la privada.



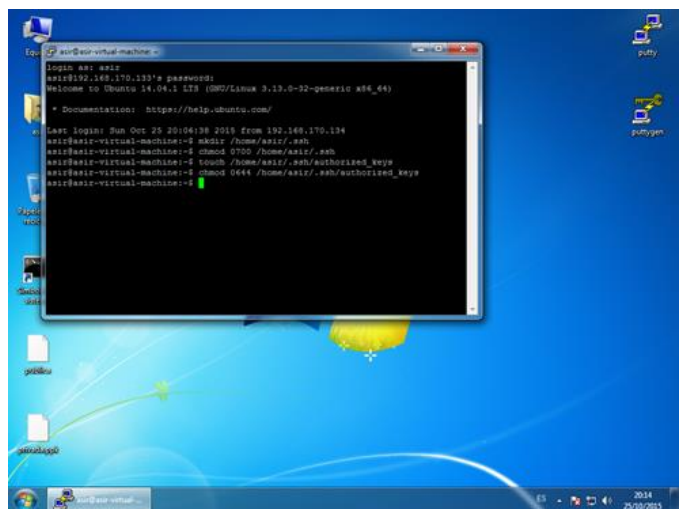
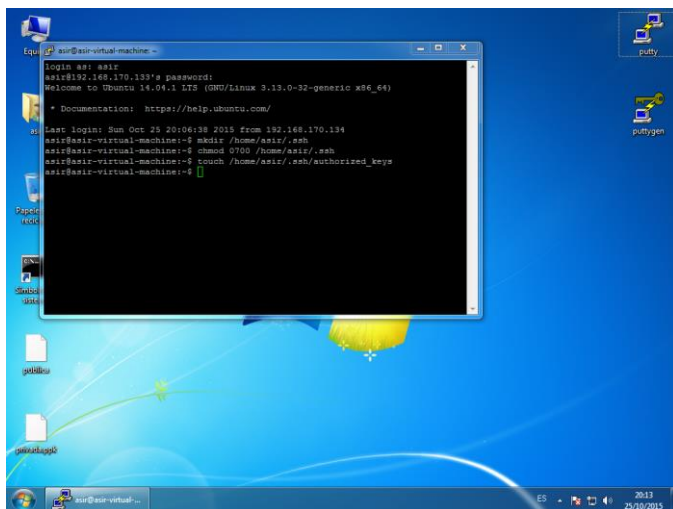
Utilizar Putty para conectar al servidor.  
Conectar al usuario del servidor **usuario: asir contraseña: Patata**.

David González Porras y Julio Arpa Delgado 2ºASIR



Crear el directorio .ssh en el directorio del usuario del servidor al que se va a conectar **mkdir /home/asir/.ssh**

Otorgar permisos al directorio .ssh **chmod 0700 /home/asir/.ssh**



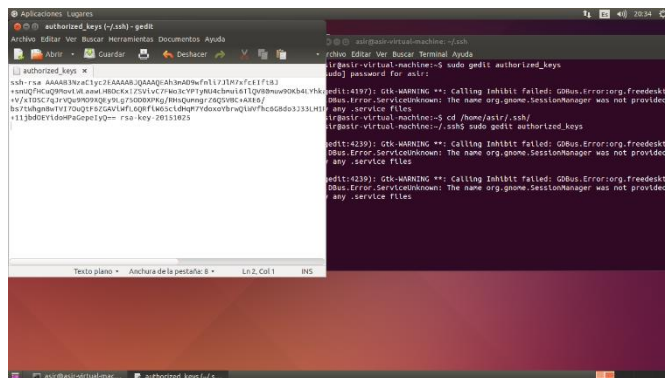
Crear el archivo authorized\_keys **touch /home/asir/.ssh/authorized\_keys**

Otorgar permisos al archivo authorized\_keys **chmod 0644 /home/asir/.ssh/authorized\_keys**

Enviar clave pública al servidor.



## Servidor



A terminal window titled 'Aplicaciones Lugares' with the command 'authorized\_keys - gedit' in the title bar. The terminal shows the contents of the file `/home/asir/.ssh/authorized_keys` being edited. The file contains a single line with a public key. The terminal output shows the file's permissions and ownership: `ls -l /home/asir/.ssh/authorized_keys` returns `-rw-r--r-- 1 asir asir 2013 2013`. The terminal also shows the command `sudo gedit /etc/ssh/sshd_config` being executed, which opens the `/etc/ssh/sshd_config` file in the gedit editor.

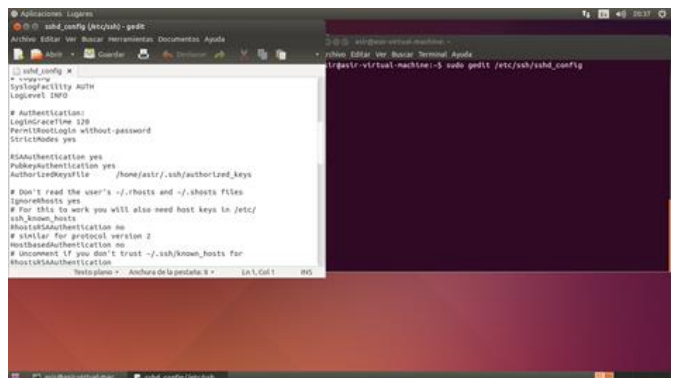
Editar el archivo `authorized_keys` y agregar la clave pública del cliente **sudo gedit /home/asir/.ssh/authorized\_keys**

Editar el archivo `sshd_config` **sudo gedit /etc/ssh/sshd\_config** comprobar que existen las líneas:

RSAAuthentication yes  
PubkeyAuthentication yes  
AuthorizedKeysFile /home/asir/.ssh/authorized\_keys

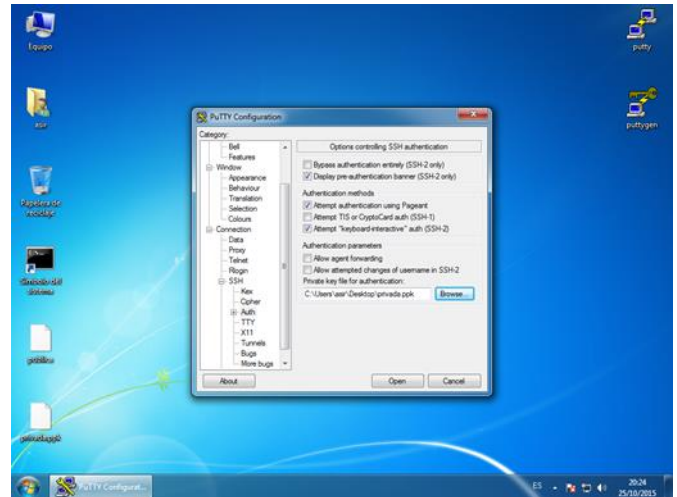
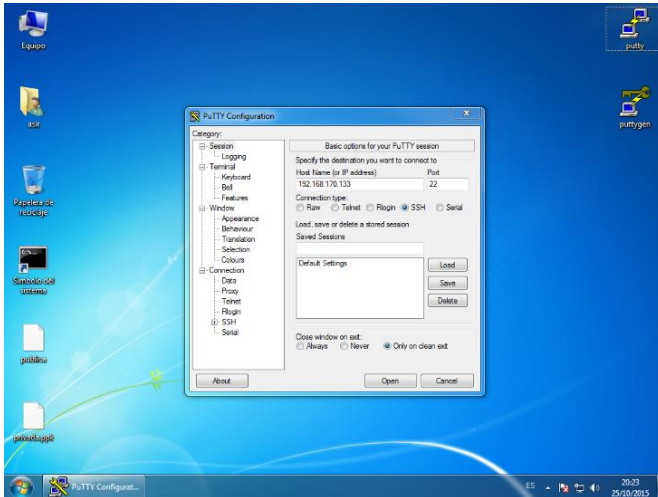
Especificar la ruta de `AuthorizedKeysFile` y quitar # de la línea.

Reiniciar SSH.



A terminal window titled 'Aplicaciones Lugares' with the command 'sshd\_config - gedit' in the title bar. The terminal shows the contents of the file `/etc/ssh/sshd_config` being edited. The file contains configuration options for the SSH daemon. The terminal output shows the file's permissions and ownership: `ls -l /etc/ssh/sshd_config` returns `-rw-r--r-- 1 root root 1024 2013`. The terminal also shows the command `sudo gedit /etc/ssh/sshd_config` being executed, which opens the `/etc/ssh/sshd_config` file in the gedit editor.

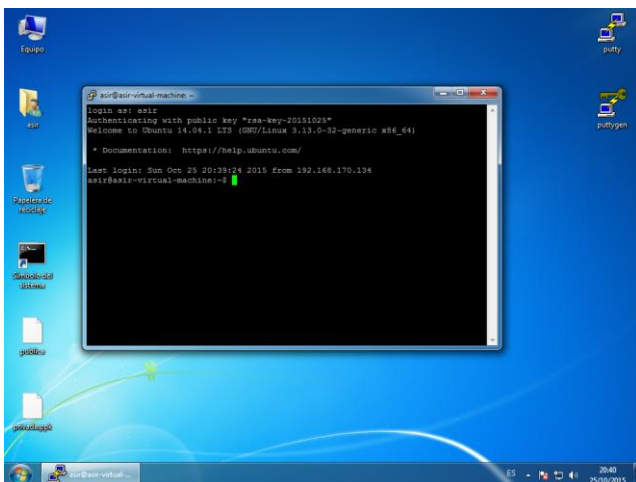
## Cliente



Iniciar Putty.

En la pestaña **Sesión** especificar la IP o el nombre del servidor al que se quiere conectar.

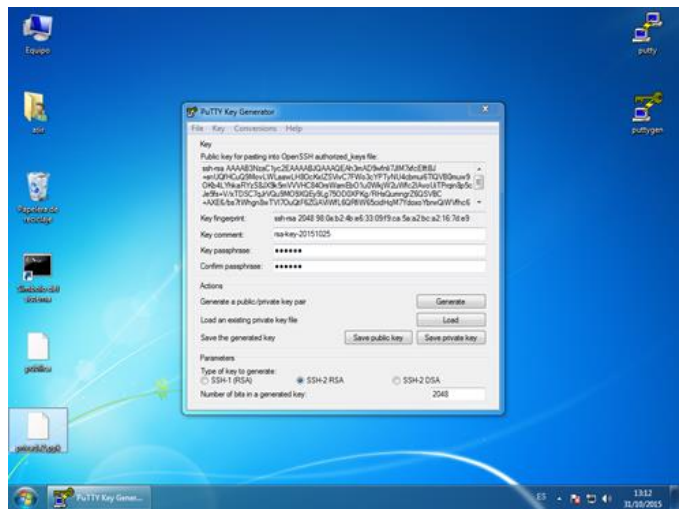
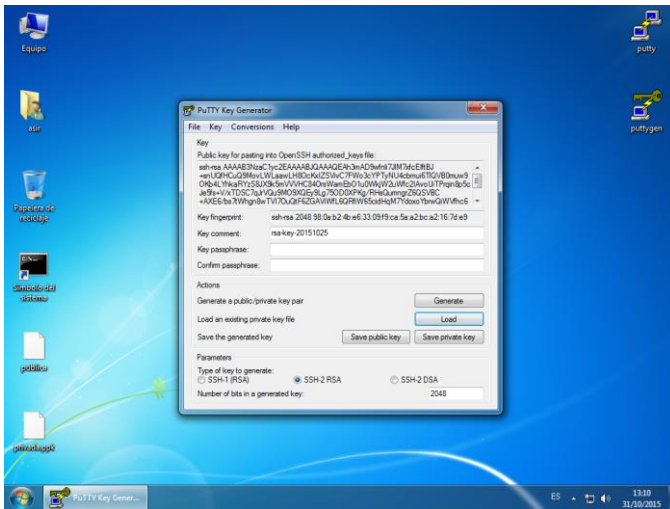
En la pestaña **Connection**, desplegar la pestaña **SSH** en **Auth** seleccionar el .ppk que contiene la clave privada.



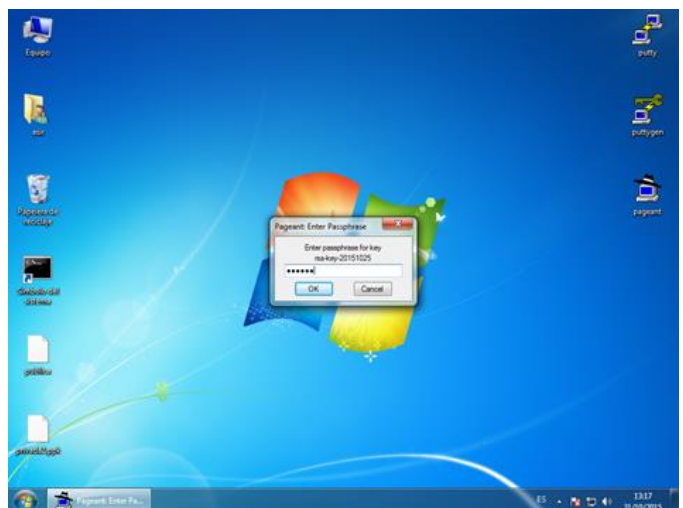
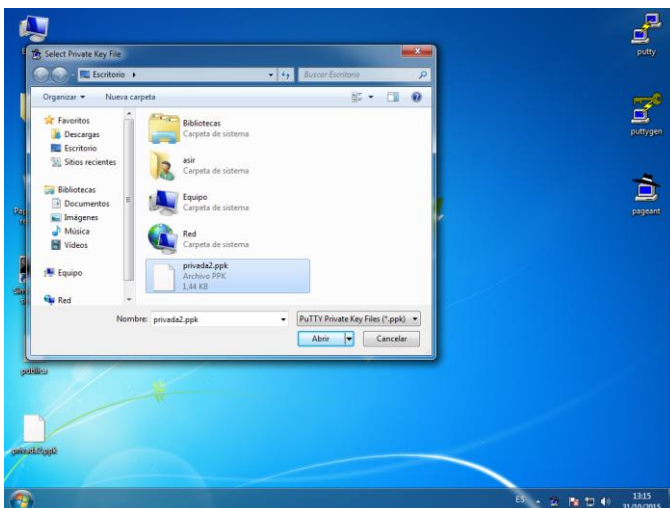
Conexión establecida.

## 14) Agente SSH Servidor Linux Cliente Windows

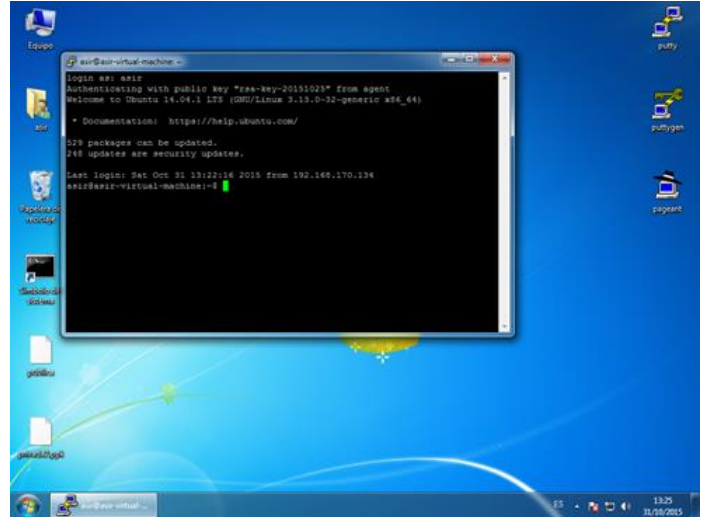
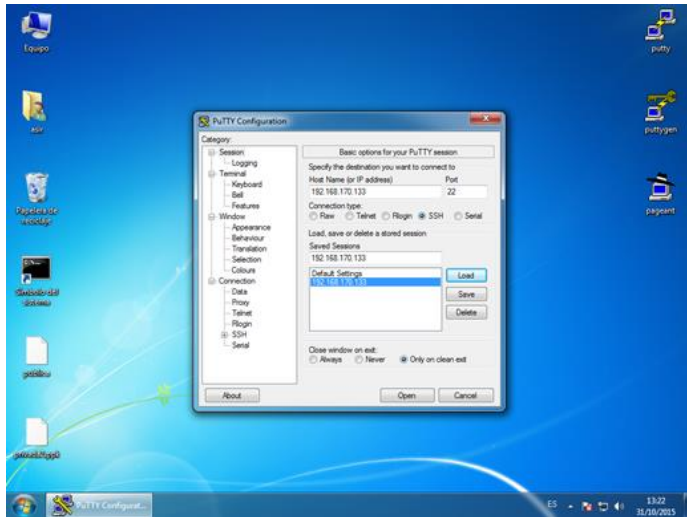
### Cliente



Abrir Puttygen y cargar la clave privada.  
Especificar la passphrase y guardar la clave privada.



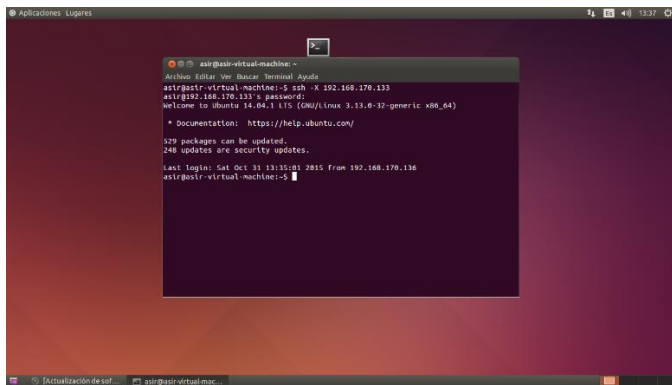
Iniciar Pageant y añadir la clave privada.  
Especificar la passphrase asociada a la clave privada.



Abrir Putty, seleccionar la sesión y conectar.  
Conexión establecida.

## 15) Ejecutar aplicaciones X remotas a través de SSH Servidor Linux Cliente Linux

### Cliente



### Conectar al servidor **ssh -X IP SERVIDOR**



Iniciar xeyes **xeyes**

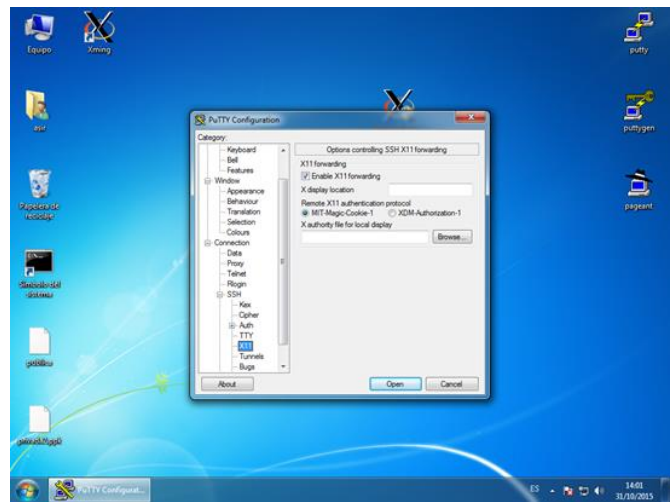
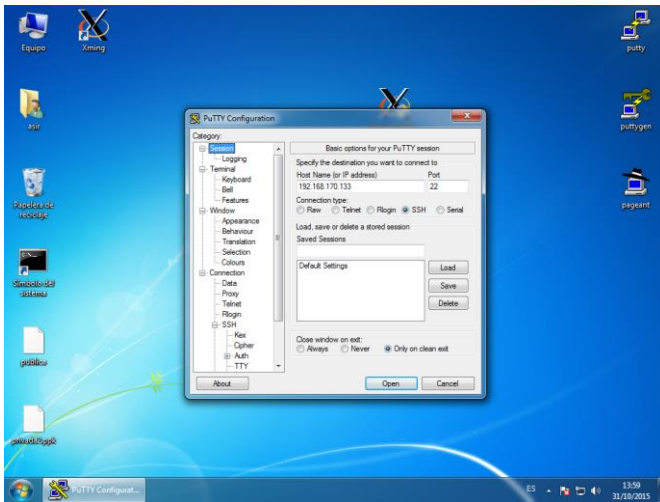
Iniciar xclock **xclock**



## 16) Ejecutar aplicaciones X remotas a través de SSH Servidor Linux Cliente Windows

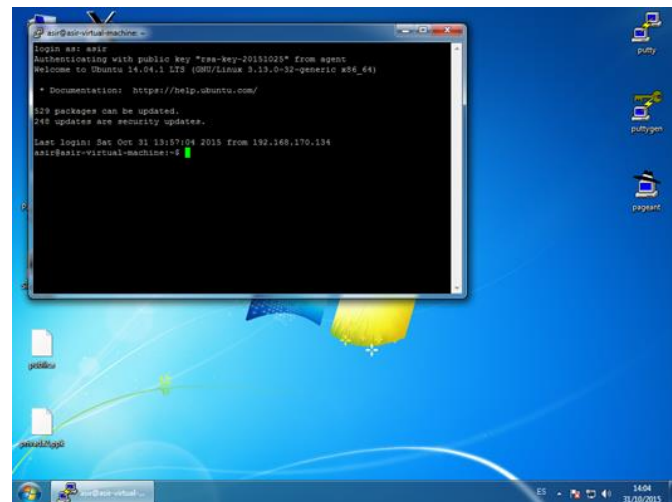
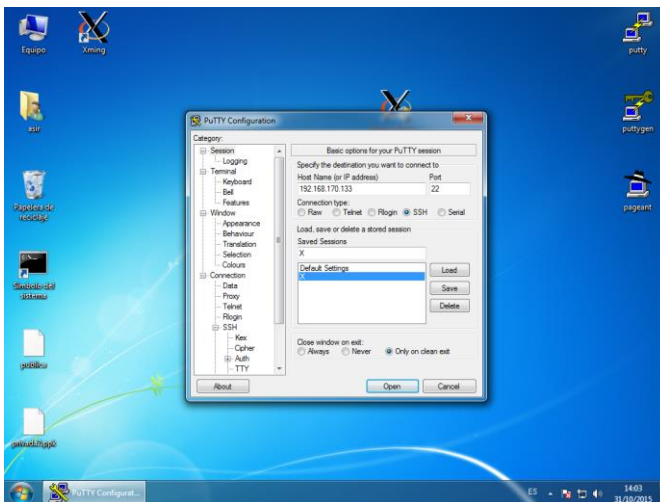
### Cliente

#### Instalar Xming



#### Iniciar Putty.

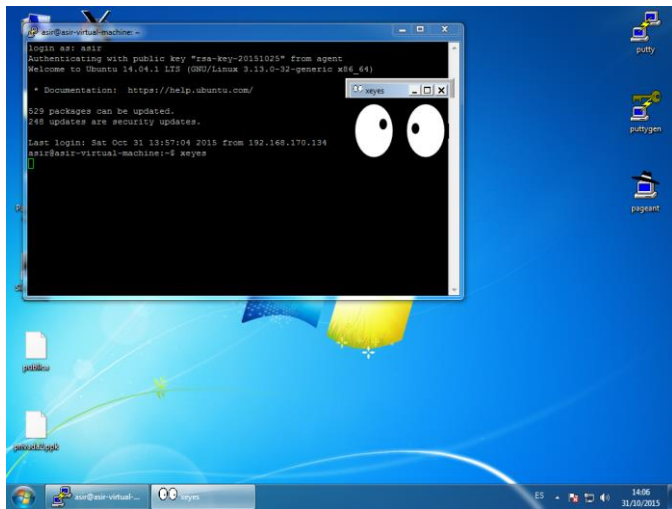
En la pestaña **Connection**, desplegar la pestaña **SSH** en **X11** Enable X11 forwarding



Seleccionar la sesión y conectar.

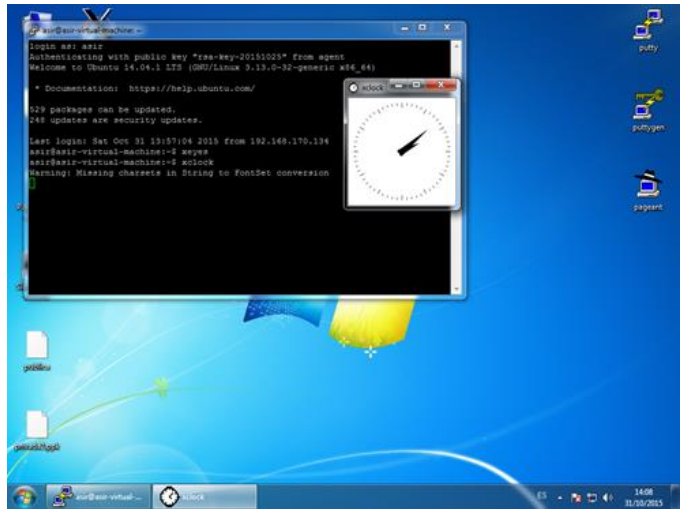
Conexión establecida.





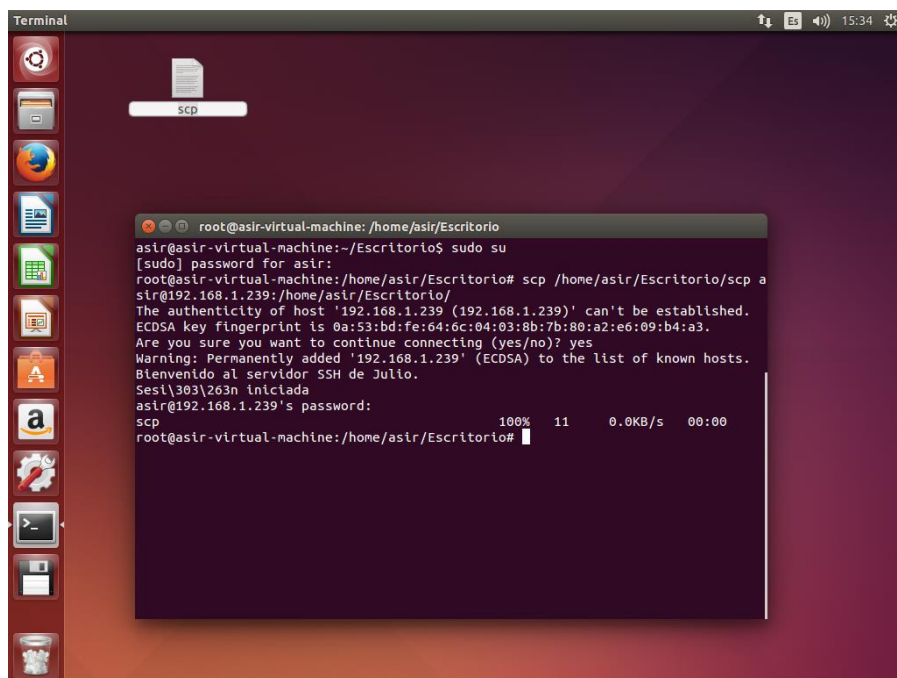
Ejecutar xeyes  
Ejecutar xclock

**xeyes**  
**xclock**



## 17) SCP Enviar archivos Servidor Linux Cliente Linux

### Servidor



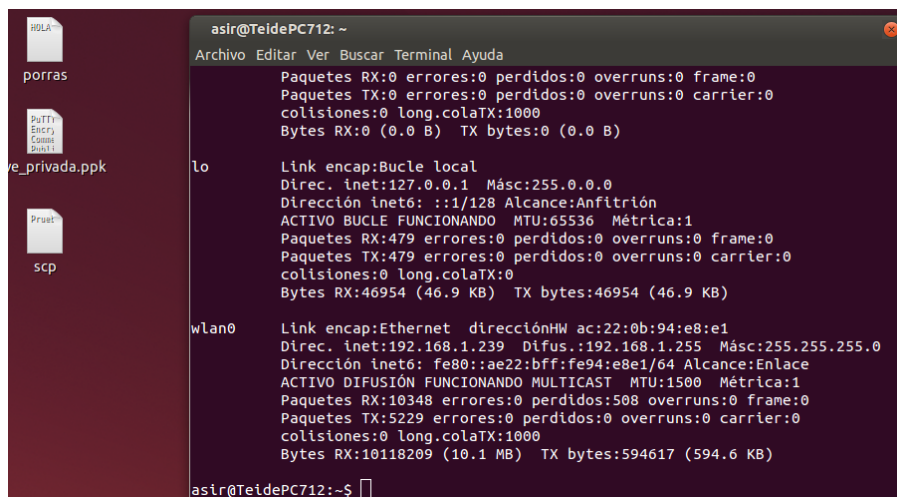
```
Terminal
root@asir-virtual-machine: /home/asir/Escritorio
asir@asir-virtual-machine:~/Escritorio$ sudo su
[sudo] password for asir:
root@asir-virtual-machine: /home/asir/Escritorio# scp /home/asir/Escritorio/scp a
sir@192.168.1.239:/home/asir/Escritorio/
The authenticity of host '192.168.1.239 (192.168.1.239)' can't be established.
ECDSA key fingerprint is 0a:53:bd:fe:64:6c:04:03:8b:7b:80:a2:e6:09:b4:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.239' (ECDSA) to the list of known hosts.
Bienvenido al servidor SSH de Julio.
Ses\303\263n iniciada
asir@192.168.1.239's password:
scp
100% 11 0.0KB/s 00:00
root@asir-virtual-machine: /home/asir/Escritorio#
```

### sudo su

Especificar ruta del archivo en local y la ruta de destino.

scp /home/asir/Escritorio/scp [asir@192.168.1.239:/home/asir/Escritorio/](#)

### Cliente



```
asir@TeidePC712: ~
Archivo Editar Ver Buscar Terminal Ayuda
Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)

lo
Link encap:Bucle local
Direc. inet:127.0.0.1 Másc:255.0.0.0
Dirección inet6: ::1/128 Alcance:Anfitrión
ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
Paquetes RX:479 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:479 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:0
Bytes RX:46954 (46.9 KB) TX bytes:46954 (46.9 KB)

wlan0
Link encap:Ethernet direcciónHW ac:22:0b:94:e8:e1
Direc. inet:192.168.1.239 Difus.:192.168.1.255 Másc:255.255.255.0
Dirección inet6: fe80::ae22:bff:fe94:e8e1/64 Alcance:Enlace
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
Paquetes RX:10348 errores:0 perdidos:508 overruns:0 frame:0
Paquetes TX:5229 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:10118209 (10.1 MB) TX bytes:594617 (594.6 KB)

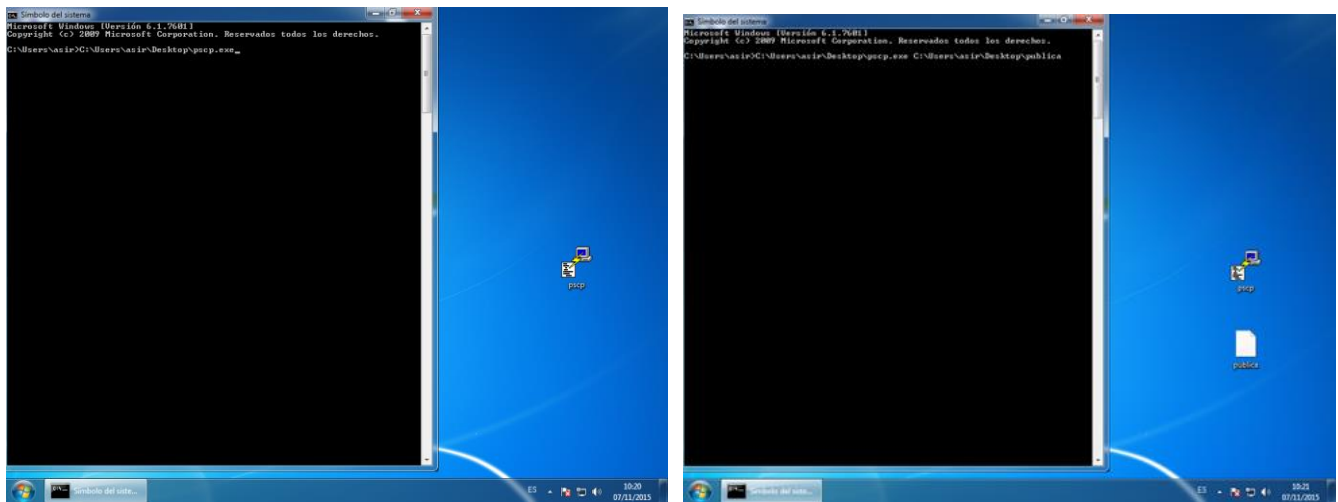
asir@TeidePC712:~$
```

Archivo enviado.

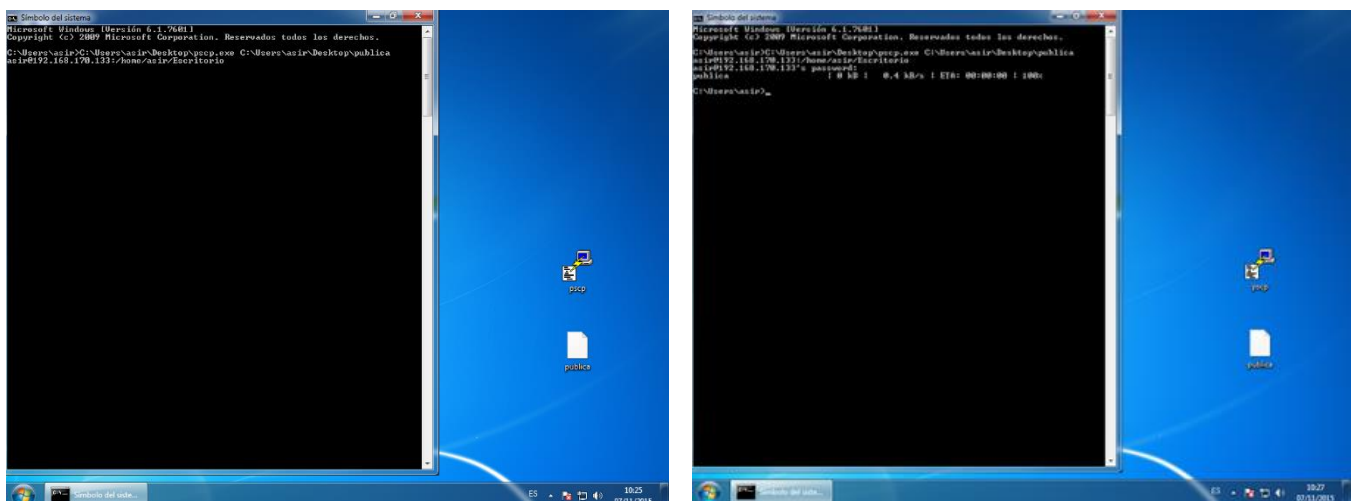
## 18) SCP Enviar archivos Servidor Windows Cliente Linux

### Servidor

Descargar pscp.

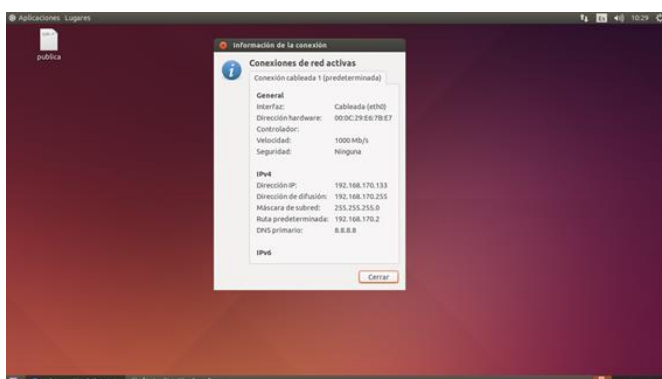


Abrir un cmd y arrastrar el icono de pscp.  
Arrastrar el archivo que se quiere enviar.



Especificar usuario@ IP cliente ruta de destino.

### Cliente

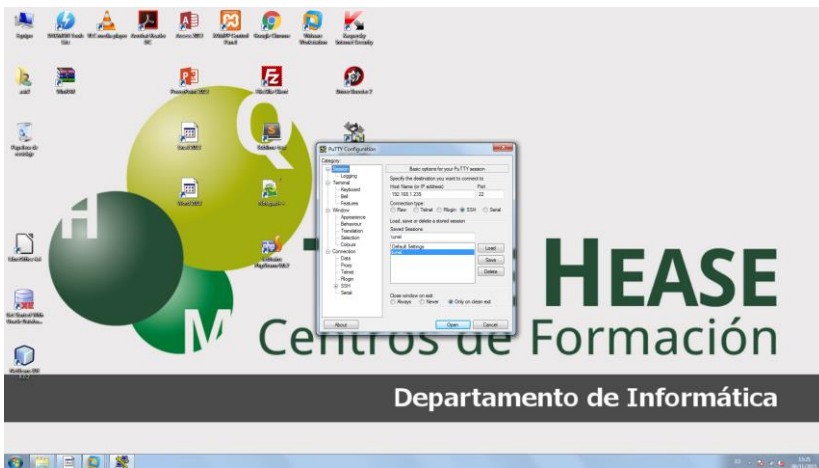


Archivo enviado.

David González Porras y Julio Arpa Delgado 2ºASIR

## 19) Tunel SSH Servicio daytime Servidor Linux Cliente Windows

### Cliente



Iniciar Putty.

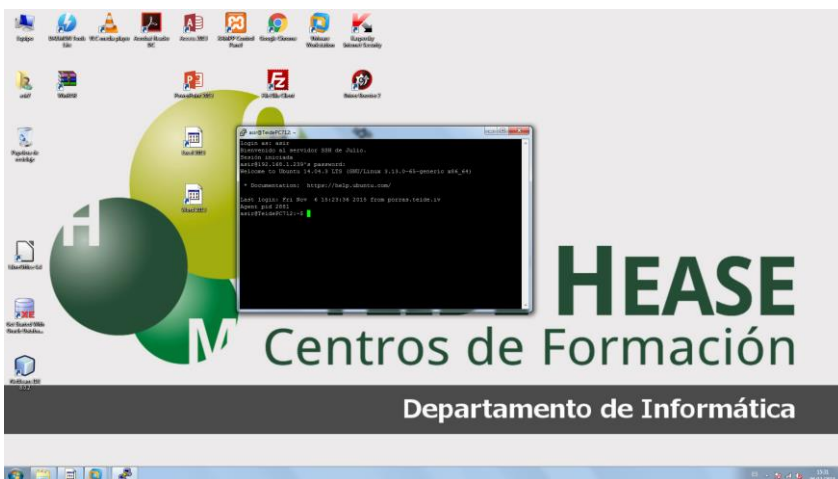
En la Pestaña Session especificar la IP del servidor.



En la Pestaña Connection, SSH, Tunnels

**Source port** Seleccionar un Puerto desocupado.

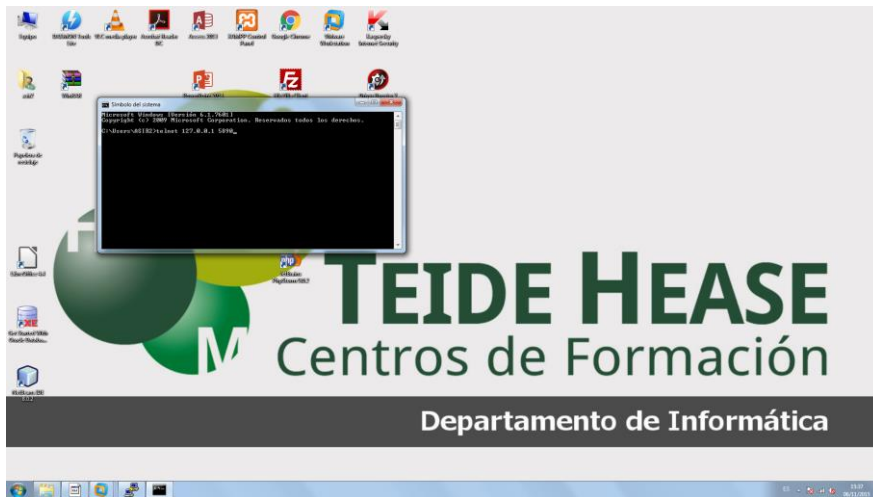
**Destination:** Ip del servidor:Puerto del servicio



Establecer conexión al servidor.

Conexión desde el puerto 5890 del cliente al puerto 13 del servidor.

David González Porras y Julio Arpa Delgado 2ºASIR



Desde la cmd telnet 127.0.0.1 puerto en uso.

El servicio daytime del servidor devuelve la fecha y la hora.