

ACTIVIDAD 3. UF_5 SISTEMAS INFORMÁTICOS



Miembros del equipo:

- **VESSELIN BONTCHEV STANEV**
- **JOSÉ IGNACIO GUTIÉRREZ CERRATO**
- **DIEGO PAUL LLIVE CARPIO**
- **DANIEL PAVÓN GÓMEZ**

Requerimiento 1

TAREAS:

1. Máscaras de subred y direcciones IP

Calcula las direcciones de red y difusión en las siguientes redes, suponiendo que tu dirección IP y máscara de subred es la que está indicada en cada caso. Especifica también la clase de red de que se trata y el número máximo de “hosts” (equipos con dirección IP asignada) podemos tener en cada una de ellas.

- 192.168.2.119 / 255.255.255.192

Solución:

Lo primero que hacemos es convertir en binario tanto la dirección IP como la máscara de subred:

Dirección IP: 192.168.2.119 = 1100000.10101000.00000010.01110111

Máscara: 255.255.192= 11111111.11111111.11111111.11000000

Cálculo dirección de red:

Para obtener la **dirección de red** hacemos un AND lógico entre la IP y la máscara:

1100000.10101000.00000010.01110111

11111111.11111111.11111111.11000000

1100000.10101000.00000010.01000000 = 192.168.2.64 (dirección de Red)

Calculo dirección de difusión (broadcast):

Para obtener la dirección de red hacemos un OR lógico entre la IP y el inverso de la máscara (negación):

1100000.10101000.00000010.01110111

00000000.00000000.00000000.00111111

1100000.10101000.00000010.01111111 = 192.168.2.127 (broadcast)

En este caso se trata de una dirección de clase C, ya que el número de red empieza por 192 (direcciones IP de clase C: 192-223)

El rango de hosts son todos los valores que existen entre la dirección de red y la dirección broadcast.

Podemos tener 64 direcciones, pero serían máximos **62 hosts disponibles** ya que la primera y la última dirección se reservan para la dirección de red y dirección de difusión respectivamente.

El primer host disponible sería 192.168.2.65
El último host disponible sería 192.168.2.126

- **192.168.2.126/26**

Solución:

Igual que en el caso anterior pasamos a número binario tanto la dirección IP como la máscara de subred (4 octetos):

Dirección IP: 192.168.2.126 = 11000000.10101000.00000010.01111110
Máscara: 255.255.255.192 = 11111111.11111111.11111111.11000000 (el enunciado nos indica que la máscara es de 26 bits)

Cálculo dirección de red:

Para obtener la **dirección de red** hacemos un AND lógico entre la IP y la máscara:

11000000.10101000.00000010.01111110
11111111.11111111.11111111.11000000

11000000.10101000.00000010.01000000 = 192.168.2.64 (dirección de Red)

Calculo dirección de difusión (broadcast):

Para obtener la dirección de red hacemos un OR lógico entre la IP y el inverso de la máscara (negación):

11000000.10101000.00000010.01111110
00000000.00000000.00000000.00111111

11000000.10101000.00000010.01111111 = 192.168.2.127 (broadcast)

La red es de clase C, ya que el número de red empieza por 192 (direcciones IP de clase C: 192-223)

Podemos tener 64 direcciones, pero serían máximo **62 hosts disponibles** ya que la primera y la última dirección se reservan para la dirección de red y dirección de difusión respectivamente.

El primer host disponible sería 192.168.2.65
El último host disponible sería 192.168.2.126

- **192.168.0.190 / 255.255.255.240**

Solución:

Igual que en los casos anteriores pasamos a número binario tanto la dirección IP como la máscara de subred:

Dirección IP: 192.168.0.190 = 11000000.10101000.00000000.10111110
Máscara de subred: 255.255.255.240 = 11111111.11111111.11111111.11110000

Cálculo dirección de red:

Para obtener la **dirección de red** hacemos un AND lógico entre la IP y la máscara:

11000000.10101000.00000000.10111110	
11111111.11111111.11111111.11110000	

11000000.10101000.00000000.10110000 = 192.168.0.176 (dirección de subred)	

Calculo dirección de difusión (broadcast):

Para obtener la dirección de red hacemos un OR lógico entre la IP y el inverso de la máscara (negación):

11000000.10101000.00000000.10111110	
00000000.00000000.00000000.00001111	

11000000.10101000.00000000.10111111 = 192.168.0.191 (dirección de broadcast)	

En este caso se trata de una dirección de clase C, ya que el número de red empieza por 192 (direcciones IP de clase C: 192-223)

Podemos tener 16 direcciones, pero serían máximos **14 hosts disponibles** ya que la primera y la última dirección se reservan para la dirección de red y dirección de difusión respectivamente

El primer host disponible sería 192.168.0.177

El último host disponible sería 192.168.0.190

- **192.168.0.190 / 255.255.240.0**

Solución:

Pasamos a número binario tanto la dirección IP como la máscara de subred:

Dirección IP: 192.168.0.190 = 11000000.10101000.00000000.10111110

Máscara de subred: 255.255.240.0 = 11111111.11111111.11110000.00000000

Cálculo dirección de red:

Hacemos un AND lógico entre la IP y la máscara:

11000000.10101000.00000000.10111110

11111111.11111111.11110000.00000000

11000000.10101000.00000000.00000000 = 192.168.0.0 (dirección de subred)

Calculo dirección de difusión (broadcast):

Hacemos un OR lógico entre la IP y el inverso de la máscara (negación):

11000000.10101000.00000000.10111110

00000000.00000000.00001111.11111111

11000000.10101000.00001111.11111111 = 192.168.15.255 (broadcast)

En este caso se trata de una dirección de clase C

Podemos tener 4096 direcciones, pero serian máximo **4094 hosts disponibles** ya que la primera y la última dirección se reservan para la dirección de red y dirección de difusión respectivamente

El primer host disponible sería 192.168.0.1
El último host disponible sería 192.168.15.254

- **40.168.2.119 / 255.255.0.0**

Solución:

Pasamos a número binario tanto la dirección IP como la máscara de subred:

Dirección IP: 40.168.2.119 = 00101000.10101000.00000010.01110111

Máscara de subred: 255.255.0.0 = 11111111.11111111.00000000.00000000

Cálculo dirección de red:

Hacemos un AND lógico entre la IP y la máscara:

00101000.10101000.00000010.01110111

11111111.11111111.00000000.00000000

00101000.10101000.00000000.00000000 = 40.168.0.0 (dirección de subred)

Calculo dirección de difusión (broadcast):

Hacemos un OR lógico entre la IP y el inverso de la máscara (negación):

00101000.10101000.00000010.01110111

00000000.00000000.11111111.11111111

00101000.10101000.11111111.11111111 = 40.168.255.255 (broadcast)

En este caso se trata de una dirección de clase A

Podemos tener 65536 direcciones, pero serian máximo **65534 hosts disponibles** ya que la primera y la última dirección se reservan para la dirección de red y dirección de difusión respectivamente

El primer host disponible sería 40.168.0.1

El último host disponible sería 40.168.255.254

Si te damos las siguientes máscaras de subred, dinos cuántos hosts puede tener como máximo cada subred:

- **255.255.255.128**
- **255.255.255.255**
- **255.255.255.224**

Solución:

- **255.255.255.128**

En este caso podemos tener 128 direcciones, pero la primera y la última dirección estarían reservadas, por lo tanto, quedan 126 IP para asignar a nuestros equipos de red.

- **255.255.255.255**

No es una mascara de subred válida. Tiene que haber mínimo 4 direcciones: 2 que se reservan para la red y para el broadcast y aparte otras 2 para host.

- **255.255.255.224**

En este caso podemos tener 32 direcciones. La primera y la última dirección estarían reservadas, por lo tanto, quedan 30 IP para asignar a nuestros equipos de red.

Por último, si tienes una red de Clase A con máscara de subred 255.255.255.0...

- **¿Cuántas subredes con máscara 255.255.255.128 podemos tener dentro de ella?**
- **¿Cuántas subredes con máscara 255.255.255.240 podemos tener dentro de ella?**

Solución:

Asumiendo que la Clase es **de tipo C**

1er caso 255.255.255.128:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.255.255.128 = 11111111.11111111.11111111.**100000000**

Podemos tener 2 subredes = $2^1=2$

Host: $2^7-2=126$ host disponibles o efectivos.

2º caso 255.255.255.240:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.255.255.240 = 11111111.11111111.11111111.**11110000**

Podemos tener 16 subredes = $2^4=16$

Host: $2^4-2=14$ host disponibles o efectivos.

Si asumimos que la Clase es de **tipo A**

1er caso **255.255.255.128**:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.255.255.128 = 11111111.11111111.11111111.100000000

Podemos tener 2 subredes = $2^{17}=131072$

Host: $2^7-2=126$ host disponibles o efectivos.

2º caso **255.255.255.240**:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.255.255.240 = 11111111.11111111.11111111.11110000

Podemos tener 16 subredes = $2^{20}=1048576$

Host: $2^4-2=14$ host disponibles o efectivos.

Como podemos observar el número de host no se altera por el tipo de clase, pero si las subredes disponibles.

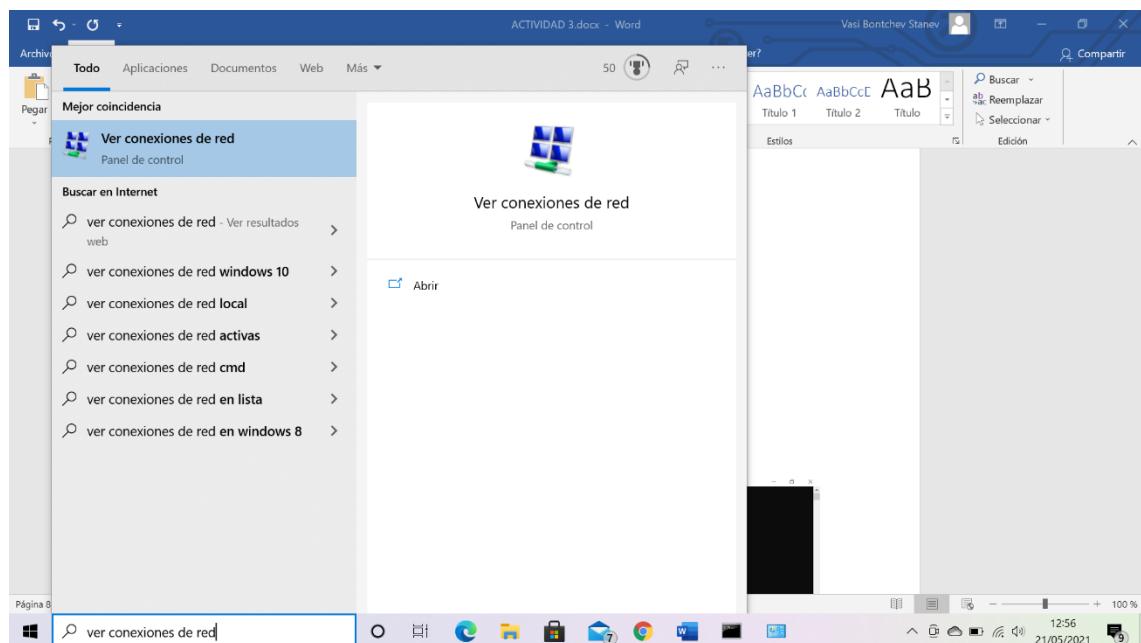
2. Configuración IP

Averigua la dirección IP (estática o dinámica) de tu ordenador personal, de tu máquina virtual de Windows10 y de tu máquina virtual Ubuntu. En la respuesta puedes copiar las pantallas/ventanas de cada sistema, pero incluye también la visualización utilizando comandos de consola/terminal.

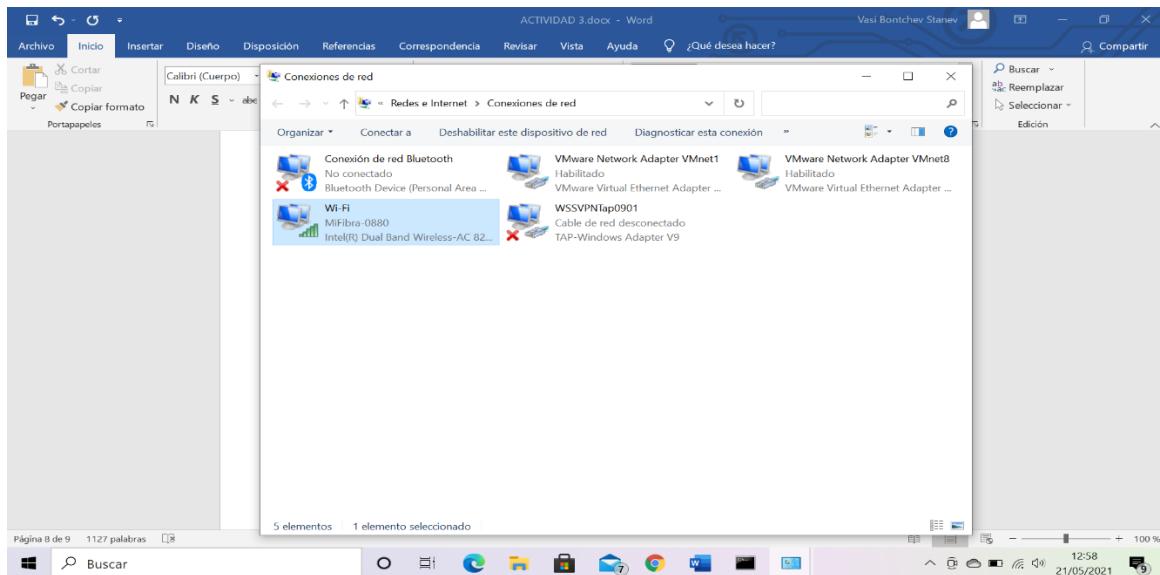
IP ordenador personal:

Visualización de la IP a través del entorno gráfico:

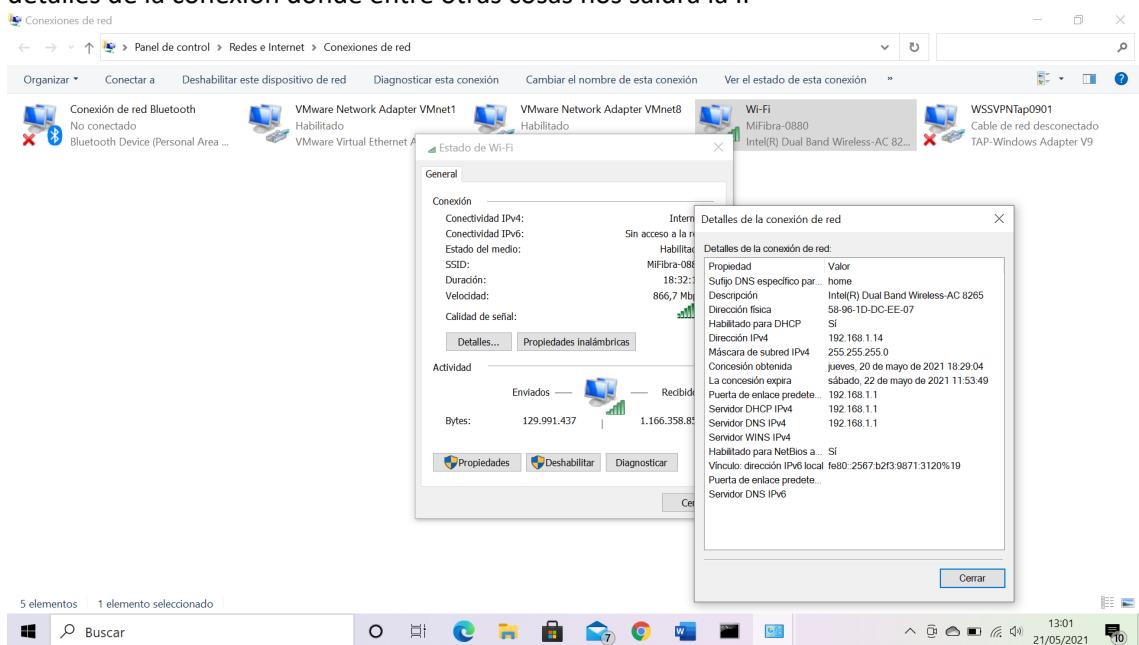
En la barra de búsqueda de Windows escribimos ver conexiones de red:



Seleccionamos la conexión que queremos ver, en este caso WIFI



Al abrirse la ventana seleccionamos “Detalles” y después se abre una nueva ventana con los detalles de la conexión donde entre otras cosas nos saldrá la IP



Visualización de la IP a través de la consola (es la forma más rápida):

Introduciendo el comando “ipconfig” o si queremos tener un informe más detallado “ipconfig/all” en la consola:

```
Selezionare Simbolo del sistema
Microsoft Windows [Versione 10.0.19042.985]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\vasde>ipconfig/all

Configurazione IP di Windows

Nome di host . . . . . : LAPTOP-6FNSHJB9
Sufijo DNS principale . . . . . :
Tipo di nodo . . . . . : ibrido
Enrutamiento IP habilitado . . . . . : no
Proxy WINS habilitado . . . . . : no
Lista di ricerca di suffisso DNS: home

Adattatore non riconosciuto WSSVPTNTap#991:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
Descrizione . . . . . : TAP-Windows Adapter V9
Indirizzo fisico . . . . . : 00-FF-5A-76-5E-33
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si

Adattatore di LAN inalámbrica Connessione di area locale* 3:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Indirizzo fisico . . . . . : 58-96-1D-DC-EE-08
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si

Adattatore di LAN inalámbrica Connessione di area locale* 4:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Indirizzo fisico . . . . . : 5A-96-1D-DC-EE-07
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si

Adattatore di LAN inalámbrica Connessione di area locale* 5:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
Descrizione . . . . . : Intel(R) Dual Band Wireless-AC 8265
Indirizzo fisico . . . . . : 58-96-1D-DC-EE-07
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si
Vinculo: indirizzo IPv6 locale . . . . : fe80::4844:d3d5:13a4:3825%18(Preferito)
Indirizzo IPv4 . . . . . : 192.168.17.1(Preferito)
Máscara di subnet . . . . . : 255.255.255.0
Concesión obtenida . . . . . : viernes, 21 de mayo de 2021 11:53:53
La concesión expira . . . . . : viernes, 21 de mayo de 2021 12:53:50
Puerta de enlace predeterminada . . . . . :
Servidor DHCP . . . . . : 192.168.17.254
IAID DHCPv6 . . . . . : 754995286
DUID del cliente DHCPv6 . . . . . : 00-01-00-01-27-F5-2A-22-58-96-1D-DC-EE-07
Servidores DNS . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
Servidor WINS principal . . . . . : 192.168.17.2
NetBIOS sobre TCP/IP . . . . . : abilitato

Adattatore di LAN inalámbrica Wi-Fi:

Sufijo DNS specifico per la connessione . . . . . : home
Descrizione . . . . . : Intel(R) Dual Band Wireless-AC 8265
Indirizzo fisico . . . . . : 58-96-1D-DC-EE-07
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si
Vinculo: indirizzo IPv6 locale . . . . : fe80::2567:b2f3:9871:3120%19(Preferito)
Indirizzo IPv4 . . . . . : 192.168.1.14(Preferito)
Máscara di subnet . . . . . : 255.255.255.0
Concesión obtenida . . . . . : jueves, 20 de mayo de 2021 18:29:05
La concesión expira . . . . . : sábado, 22 de mayo de 2021 11:53:49
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 156800541
DUID del cliente DHCPv6 . . . . . : 00-01-00-01-27-F5-2A-22-58-96-1D-DC-EE-07
Servidores DNS . . . . . : 192.168.1.1
NetBIOS sobre TCP/IP . . . . . : abilitato

Adattatore di Ethernet Connessione di rete Bluetooth:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
```

```
Selezionare Simbolo del sistema
Microsoft Windows [Versione 10.0.19042.985]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\vasde>ipconfig/all

Configurazione IP di Windows

Indirizzo fisico . . . . . : 00-50-56-C0-00-08
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si
Vinculo: indirizzo IPv6 locale . . . . : fe80::4844:d3d5:13a4:3825%18(Preferito)
Indirizzo IPv4 . . . . . : 192.168.17.1(Preferito)
Máscara di subnet . . . . . : 255.255.255.0
Concesión obtenida . . . . . : viernes, 21 de mayo de 2021 11:53:53
La concesión expira . . . . . : viernes, 21 de mayo de 2021 12:53:50
Puerta di enlace predeterminada . . . . . :
Servidor DHCP . . . . . : 192.168.17.254
IAID DHCPv6 . . . . . : 754995286
DUID del cliente DHCPv6 . . . . . : 00-01-00-01-27-F5-2A-22-58-96-1D-DC-EE-07
Servizi DNS . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
Servizio WINS principale . . . . . : 192.168.17.2
NetBIOS sopra TCP/IP . . . . . : abilitato

Adattatore di LAN inalámbrica Wi-Fi:

Sufijo DNS specifico per la connessione . . . . . : home
Descrizione . . . . . : Intel(R) Dual Band Wireless-AC 8265
Indirizzo fisico . . . . . : 58-96-1D-DC-EE-07
DHCP abilitato . . . . . : si
Configurazione automatica abilitata . . . . . : si
Vinculo: indirizzo IPv6 locale . . . . : fe80::2567:b2f3:9871:3120%19(Preferito)
Indirizzo IPv4 . . . . . : 192.168.1.14(Preferito)
Máscara di subnet . . . . . : 255.255.255.0
Concesión obtenida . . . . . : jueves, 20 de mayo de 2021 18:29:05
La concesión expira . . . . . : sábado, 22 de mayo de 2021 11:53:49
Puerta di enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 156800541
DUID del cliente DHCPv6 . . . . . : 00-01-00-01-27-F5-2A-22-58-96-1D-DC-EE-07
Servizi DNS . . . . . : 192.168.1.1
NetBIOS sopra TCP/IP . . . . . : abilitato

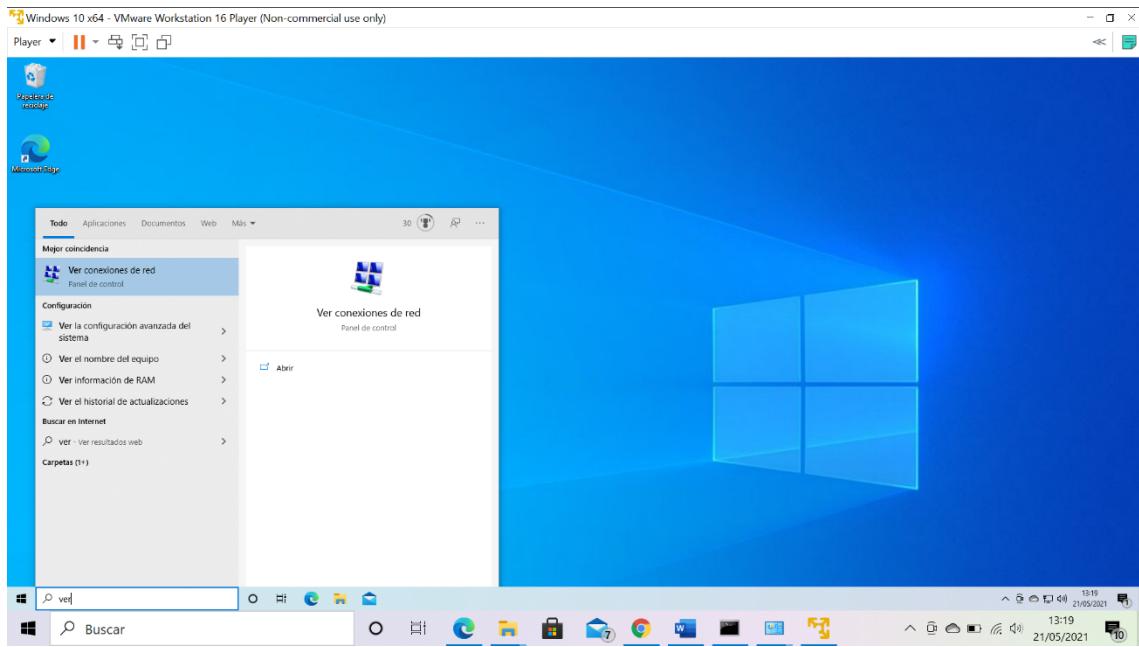
Adattatore di Ethernet Connessione di rete Bluetooth:

Stato dei mezzi . . . . . : mezzi disconnessi
Sufijo DNS specifico per la connessione . . . . . :
```

IP Máquina Virtual Windows 10:

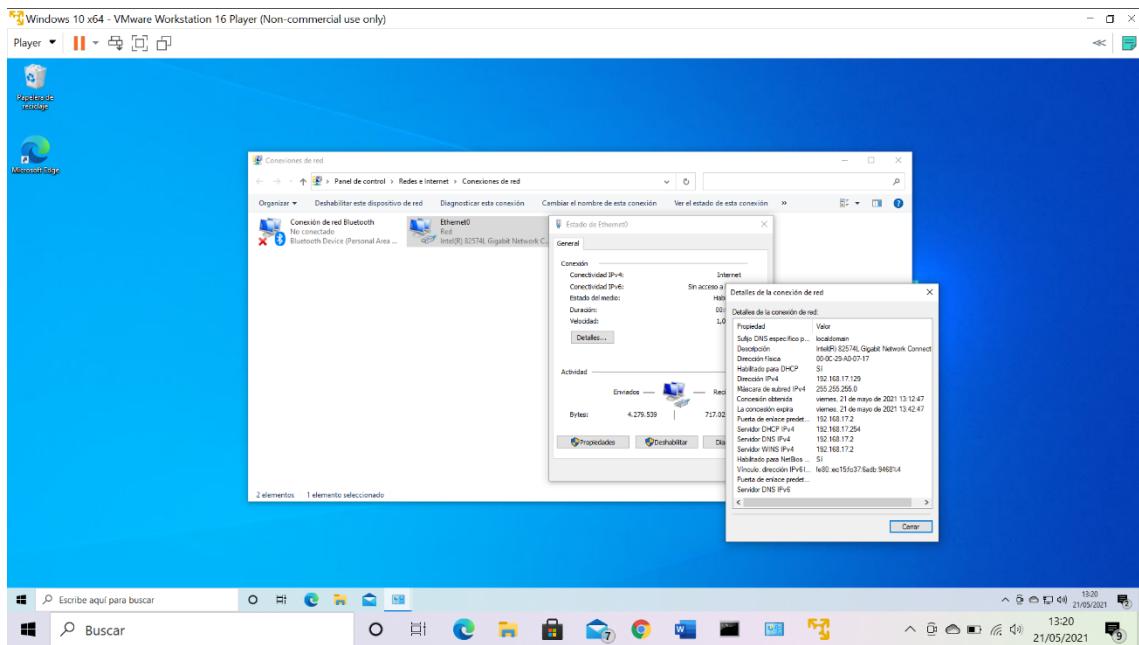
Visualización de la IP a través del entorno gráfico:

De la misma manera que en el caso del ordenador personal, escribimos en la barra de búsqueda de Windows "ver conexiones de red".



Seleccionamos la conexión, en este caso Ethernet

Al abrirse la ventana de "Estado" seleccionamos "Detalles" y después se abre una nueva ventana con los detalles de la conexión donde entre otras cosas nos saldrá la IP



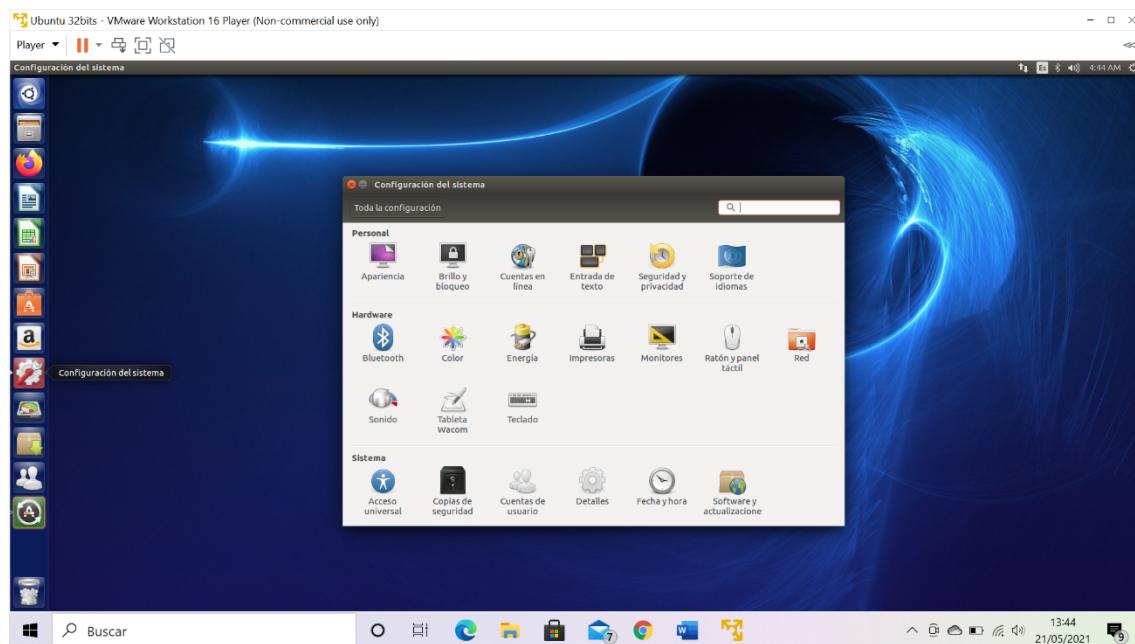
Visualización de la IP a través de la consola (es la forma más rápida):

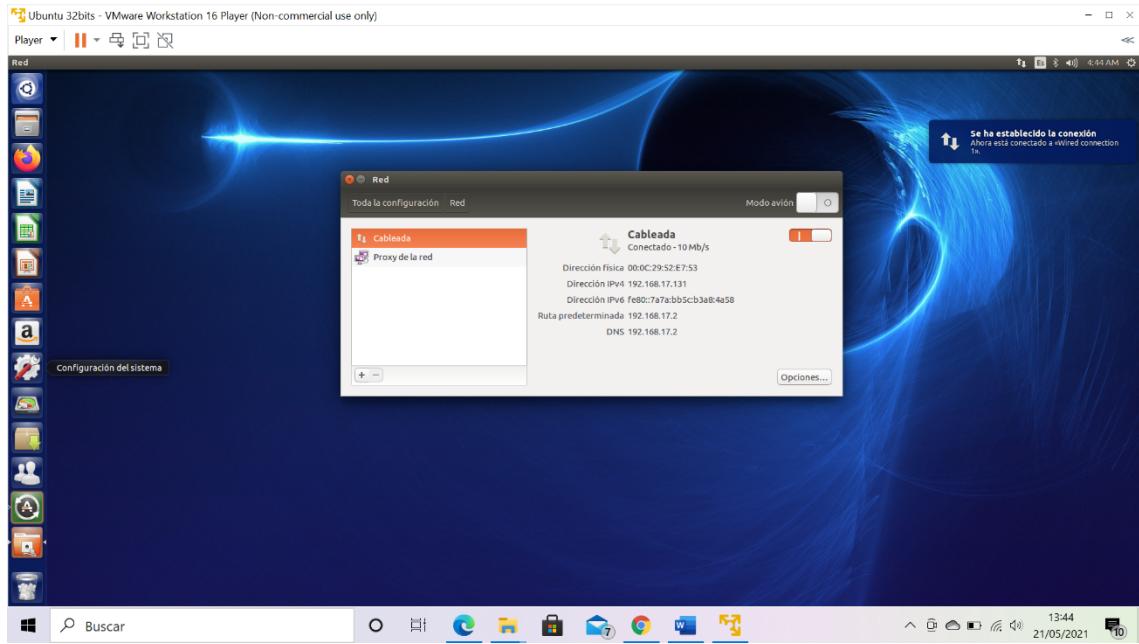
Introduciendo el comando ipconfig o ipconfig/all en la consola:

IP Máquina Virtual Ubuntu:

Visualización de la IP a través del entorno gráfico:

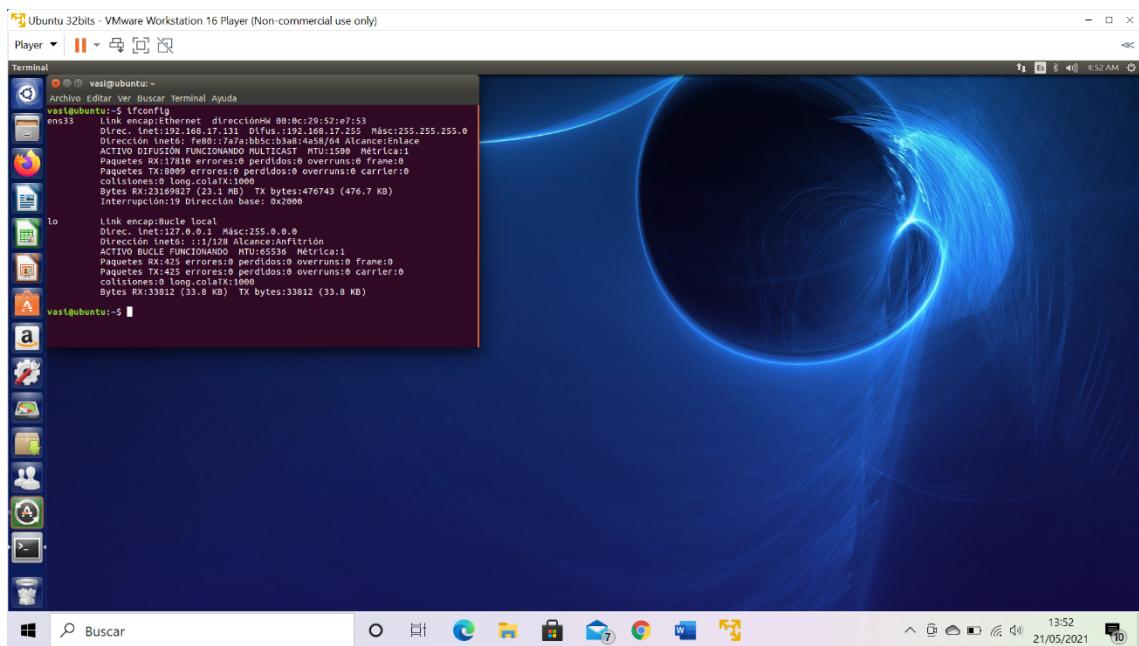
Configuración del sistema > Red





Visualización de la IP a través de la consola:

Abrimos el terminal y después introducimos el comando “ifconfig”.



3. Conexión con Internet

Averigua también la dirección IP pública de tu conexión a Internet. Puedes usar por ejemplo la página <http://www.cualesmiip.com/> o cualquier otra similar.

Utilizamos la página <https://www.cual-es-mi-ip.net/>. Al entrar en la página, se muestra la IP pública automáticamente.

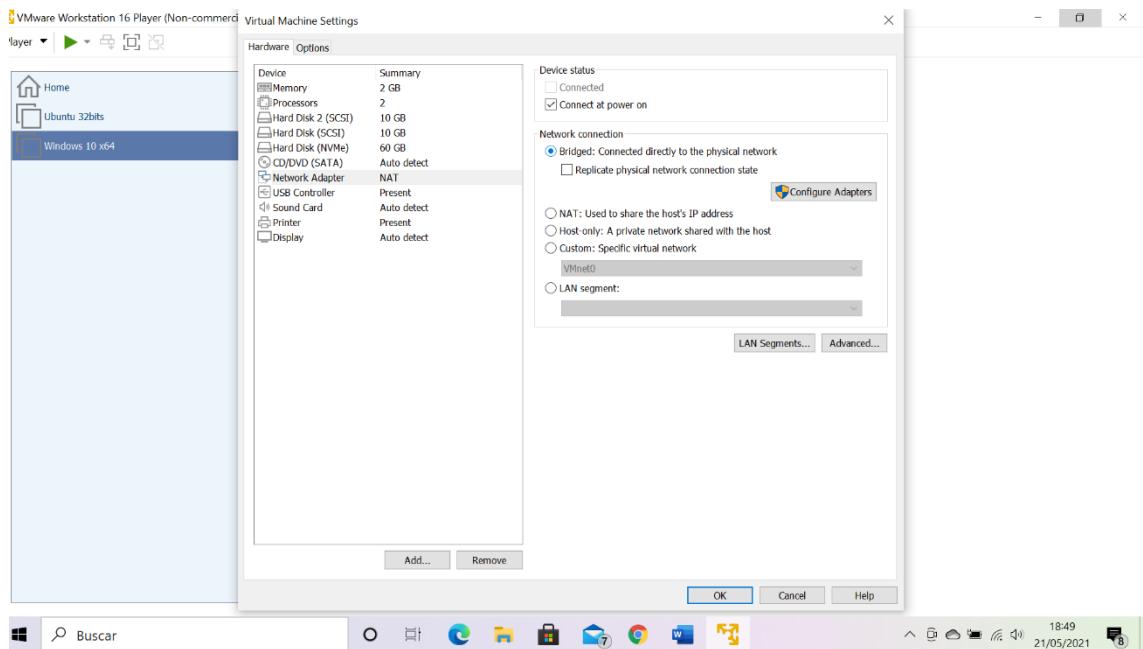
The screenshot shows a web browser window with the URL [cual-es-mi-ip.net](https://www.cual-es-mi-ip.net/) in the address bar. The page title is "CUALESMIIP". The main content area displays the user's IP address as "Tu dirección IP es 146.158.217.169" with a "Geolocalizar IP" button. Below this, it shows the provider as "Jazztel", the country as "Spain", and the proxy status as "no". A sidebar on the right contains a question about the difference between public and private IP addresses, with two checked options: "La dirección IP pública es un número único que identifica nuestra red desde el exterior" and "La dirección IP privada es un número único que identifica a un dispositivo conectado en nuestra red interna". The browser's taskbar at the bottom shows various open tabs and system icons.

4. Practicar con “ping”

Realiza el ejercicio propuesto en el módulo 5.2 con el comando “ping” y comprueba la conexión entre tu máquina física y tus máquinas virtuales. Si tu ordenador lo soporta comprueba también la conexión entre ellas, y si no solamente de cada una con la máquina física.

Antes de realizar el ejercicio configuramos las 2 maquinas virtuales en modo “bridge” para que funcionen como si fueran diferentes equipos conectados a la misma red:

The screenshot shows the VMware Workstation 16 Player interface. A context menu is open over a virtual machine named "Windows 10 x64". The menu options include "Power", "Manage", "Full Screen", "Unity", and "Help". The "Manage" option is currently selected, showing sub-options like "Install VMware Tools...", "Message Log", and "Virtual Machine Settings...". Below the menu, the virtual machine details are listed: "Virtual Machine Name: Windows 10 x64", "State: Powered Off", "OS: Windows 10 x64", "Version: Workstation 16.x virtual machine", and "RAM: 2 GB". At the bottom, there are buttons for "Play virtual machine" and "Edit virtual machine settings". The taskbar at the bottom shows the Windows Start button, a search bar, and various pinned application icons.



También desactivamos el firewall de Windows (en la máquina física y en la máquina virtual) para que los paquetes ICMP que usa "ping" puedan ser recibidos y contestados.

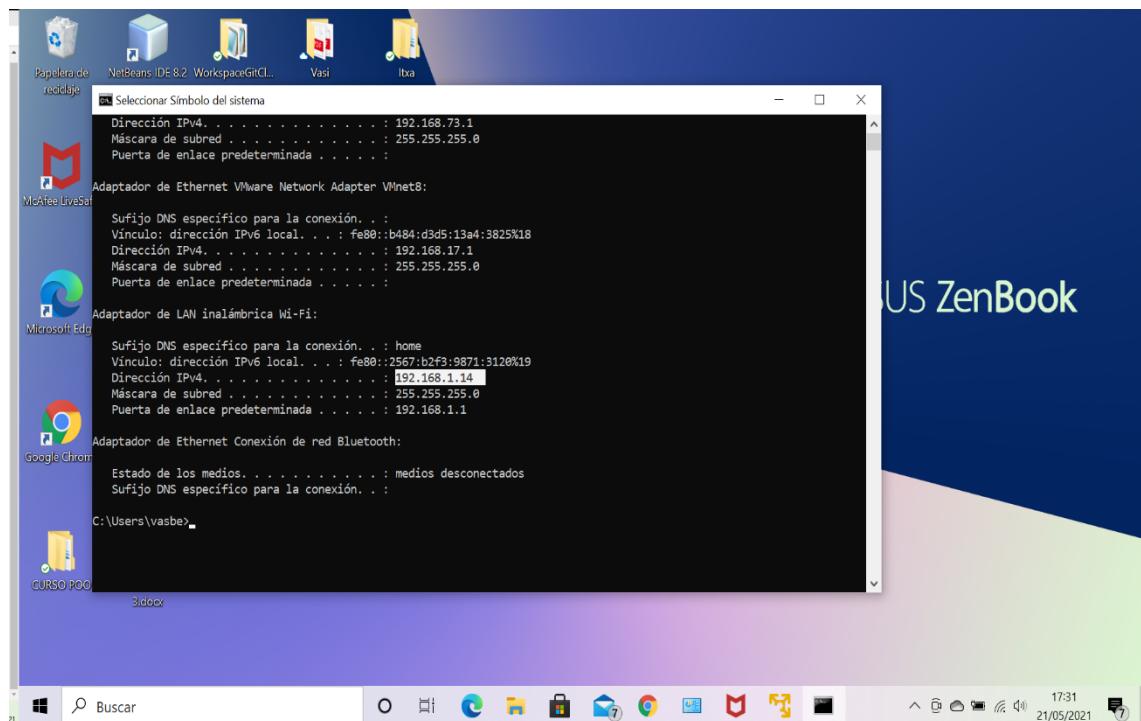
Una vez realizados los pasos previos podemos realizar el ejercicio.

Arrancamos las 2 máquinas virtuales (Windows 10 y Ubuntu) y abrimos consola/terminal de comandos en cada una de ellas y también en el equipo físico anfitrión.

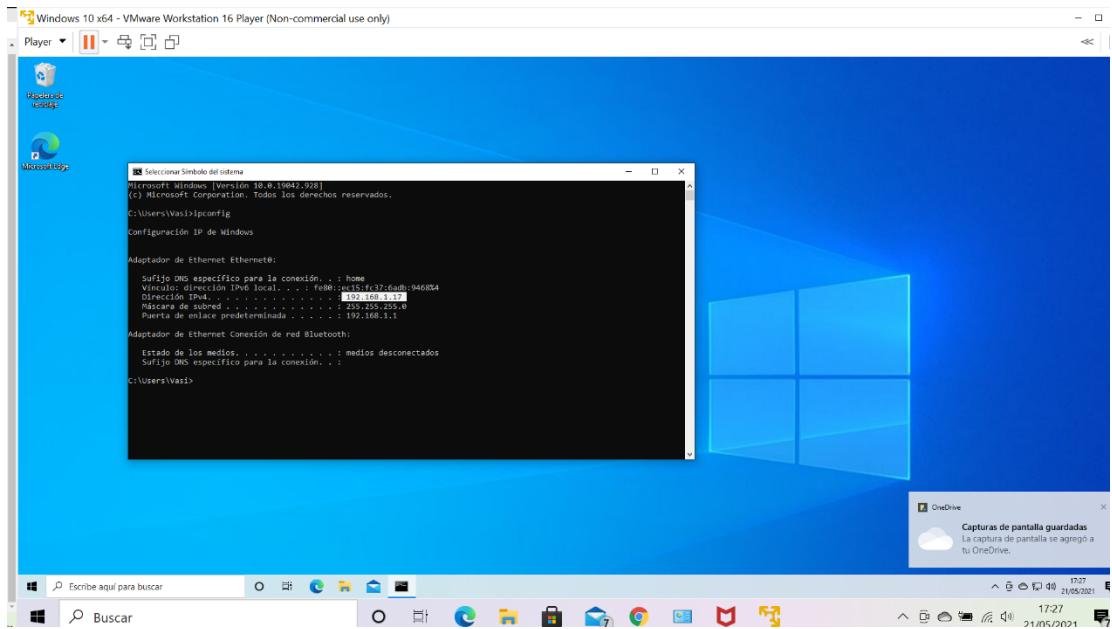
Verificamos cual es la dirección IP en cada uno de los sistemas.

En Windows utilizamos el comando "ipconfig"

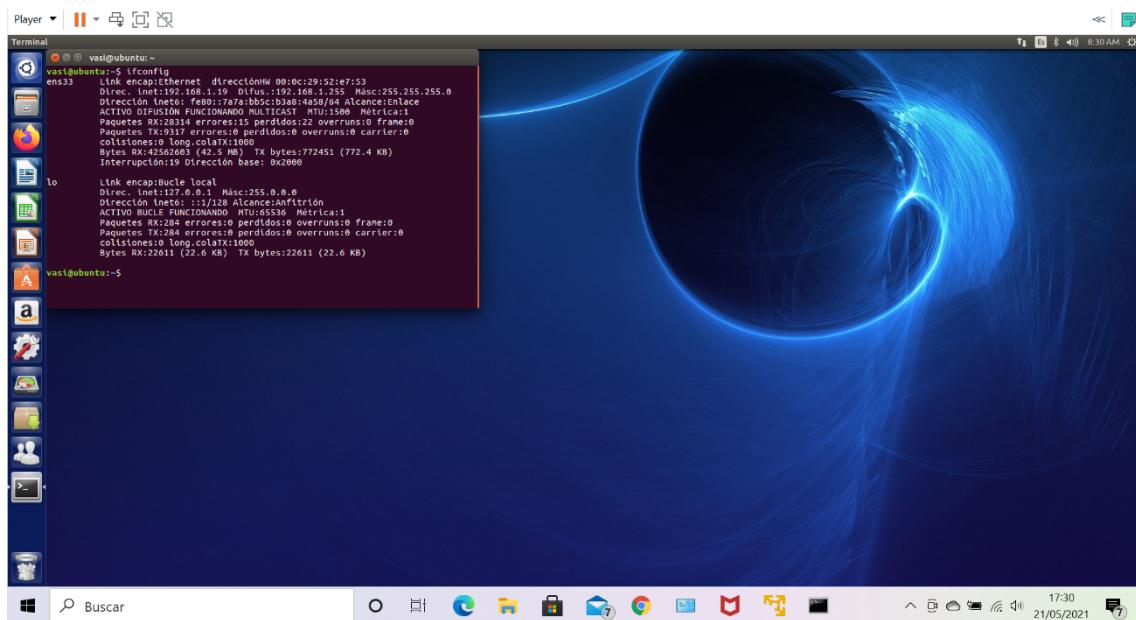
IP del equipo físico: 192.168.1.4



IP de la máquina virtual de Windows 10: 192.168.1.17



IP de la máquina virtual de Ubuntu: 192.168.1.19 (utilizamos el comando “ifconfig”)

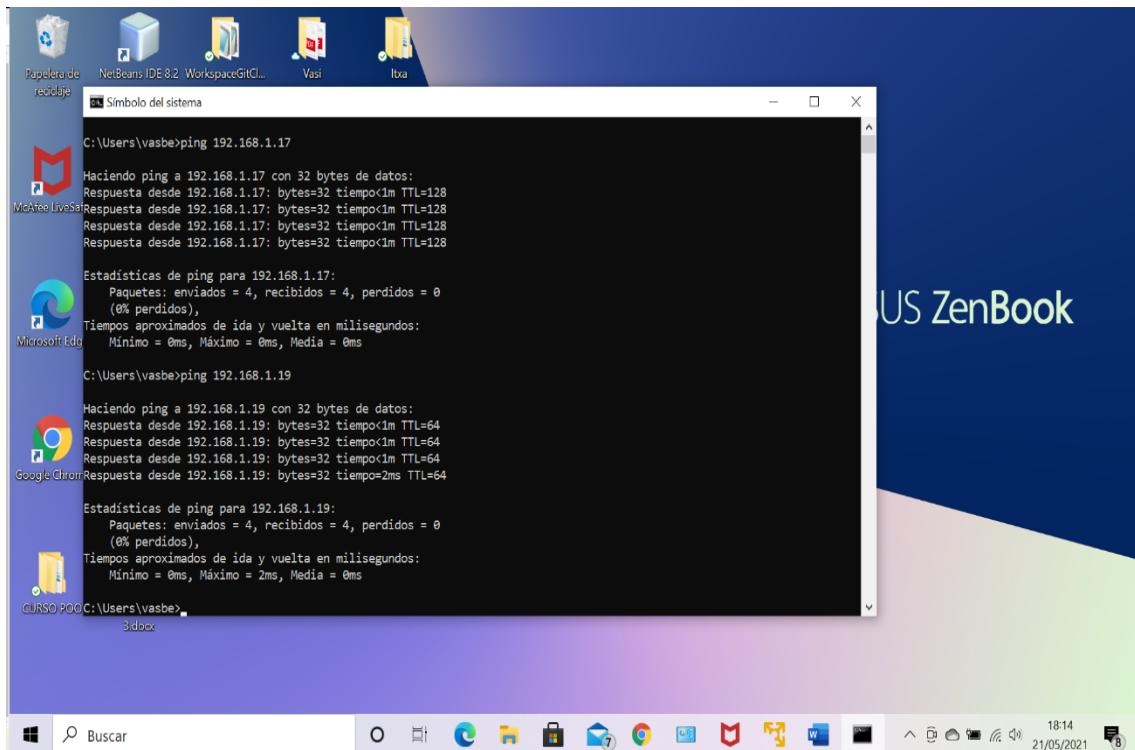


Una vez que tenemos las IP comprobamos que desde la máquina física tenemos conexión con el sistema con dirección IP 192.168.1.17 (MV de Windows 10) y también con el sistema con dirección IP 192.168.1.19 (MV Ubuntu):

Comando ping 192.168.1.17 (para comprobar el envío de paquetes al sistema MV Windows 10)

Comando ping 192.168.1.19 (para comprobar el envío de paquetes al sistema MV Ubuntu)

Vemos que alcanzamos los dos sistemas:

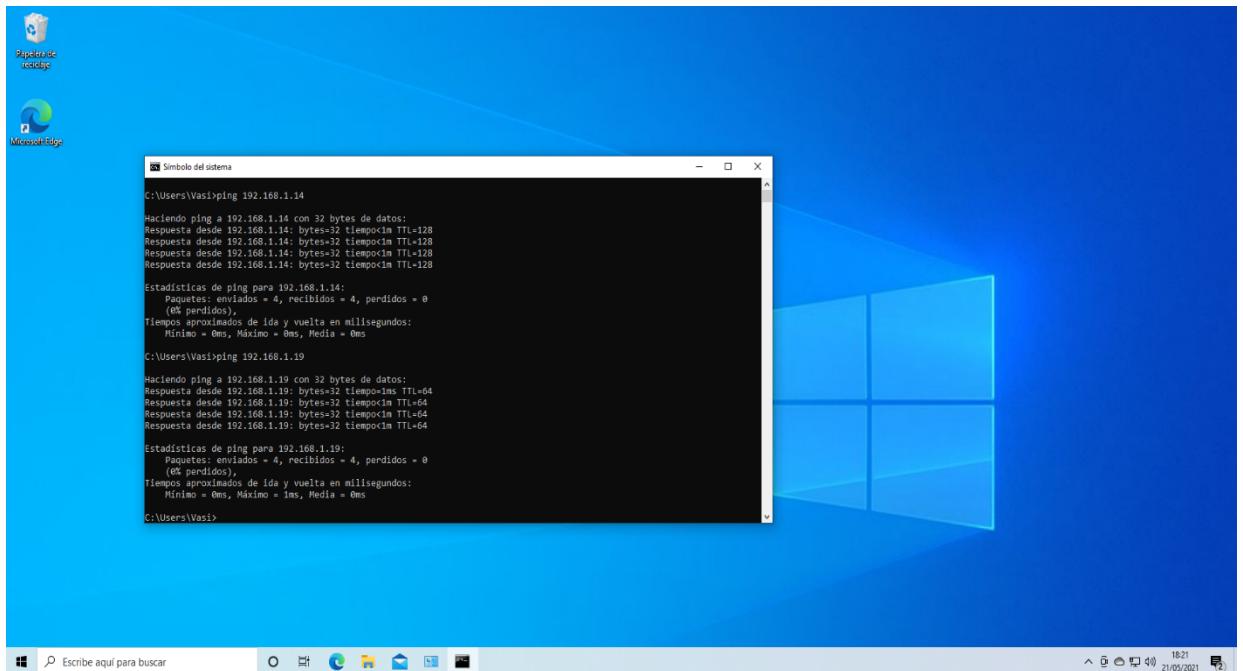


Después comprobamos desde la máquina virtual Windows 10 que tenemos conexión con el sistema con dirección IP 192.168.1.14 (equipo físico anfitrión) y también con el sistema con dirección 192.168.1.19 (MV Ubuntu):

Comando ping 192.168.1.14 (para comprobar el envío de paquetes al equipo físico anfitrión)

Comando ping 192.168.1.19 (para comprobar el envío de paquetes al sistema MV Ubuntu)

Vemos que alcanzamos los dos sistemas:

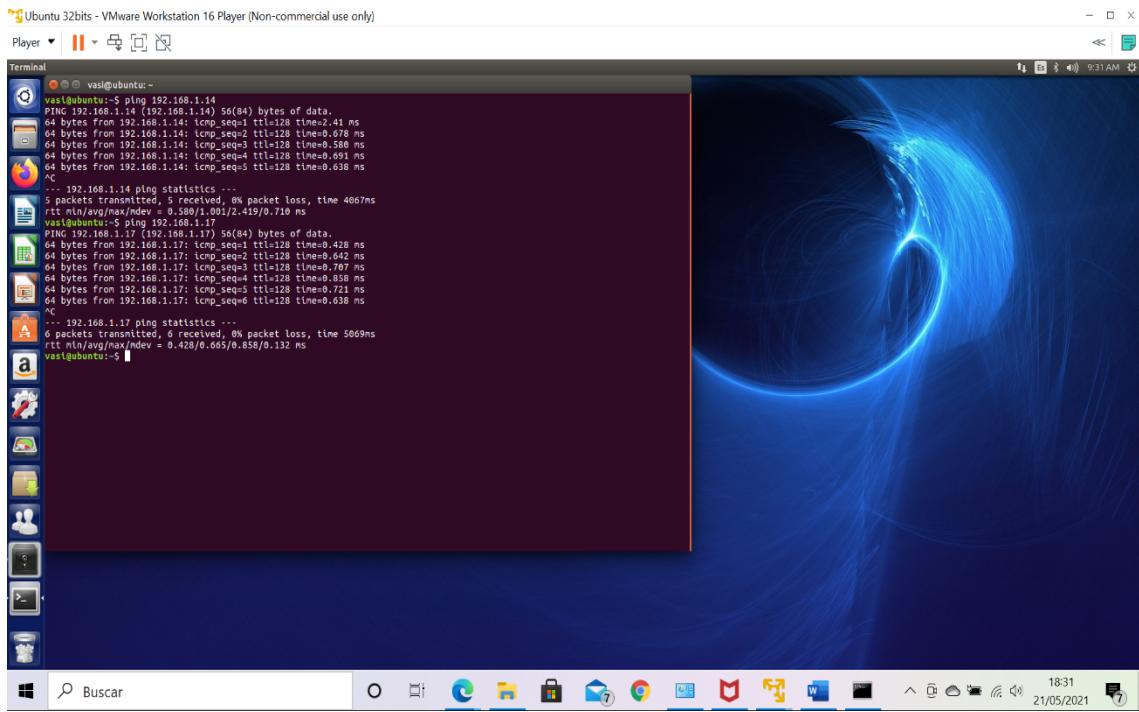


Por último, comprobamos que desde la MV Ubuntu tenemos conexión con el sistema con dirección IP 192.168.1.14 (equipo físico anfitrión) y también con el sistema con dirección IP 192.168.1.17 (MV de Windows 10):

Comando ping 192.168.1.14 (para comprobar el envío de paquetes al equipo físico anfitrión)

Comando ping 192.168.1.17 (para comprobar el envío de paquetes al sistema MV Windows 10)

Vemos que alcanzamos los dos sistemas:



5. Conexión SSH Windows-Ubuntu

Realiza el ejercicio práctico propuesto en la lección 5.3 Seguridad en la red siguiendo los pasos que en él se indican. Aporta como resultado los pantallazos de tus máquinas virtuales.

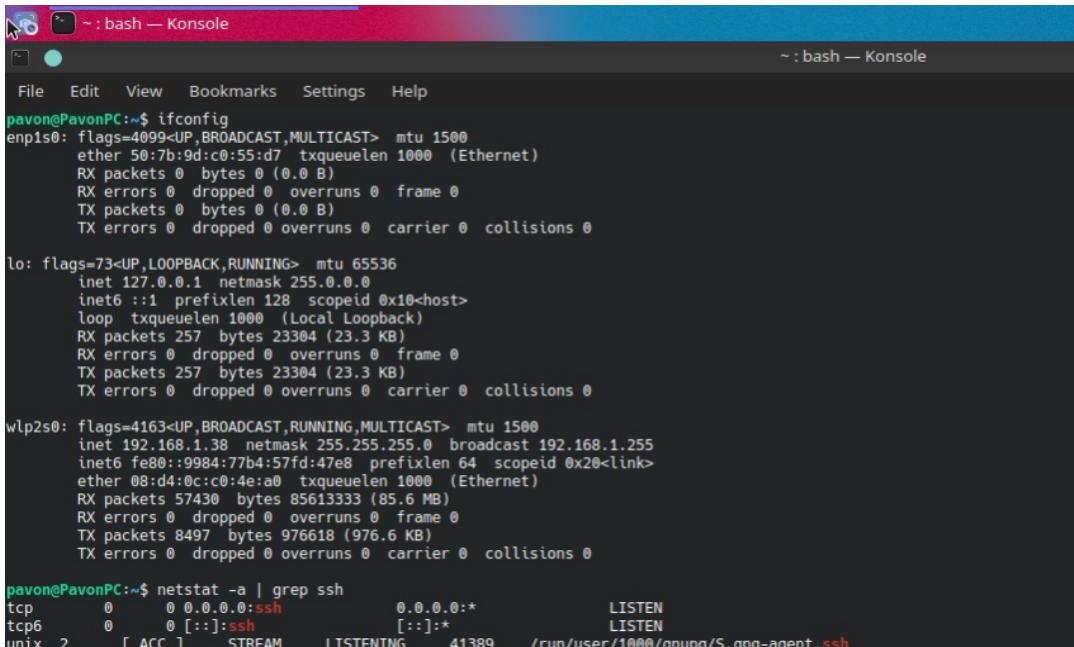
Lo primero que hemos hecho ha sido irnos a una máquina virtual de ubuntu y hemos instalado SSH.

```

dpavon@DESKTOP-7TBMRTP:~$ sudo apt install ssh
[sudo] password for dpavon:
Sorry, try again.
[sudo] password for dpavon:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ssh
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 5084 B of archives.
After this operation, 120 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 ssh all 1:8.2p1-4ubuntu0.2 [5084 B]
Fetched 5084 B in 0s (39.1 kB/s)
Selecting previously unselected package ssh.
(Reading database ... 37880 files and directories currently installed.)
Preparing to unpack .../ssh_1%3a8.2p1-4ubuntu0.2_all.deb ...
Unpacking ssh (1:8.2p1-4ubuntu0.2) ...
Setting up ssh (1:8.2p1-4ubuntu0.2) ...
dpavon@DESKTOP-7TBMRTP:~$ 

```

Una vez tenemos instalado el SSH, vamos a comprobar nuestra dirección IP y de paso comprobar que esté funcionando el servicio SSH.



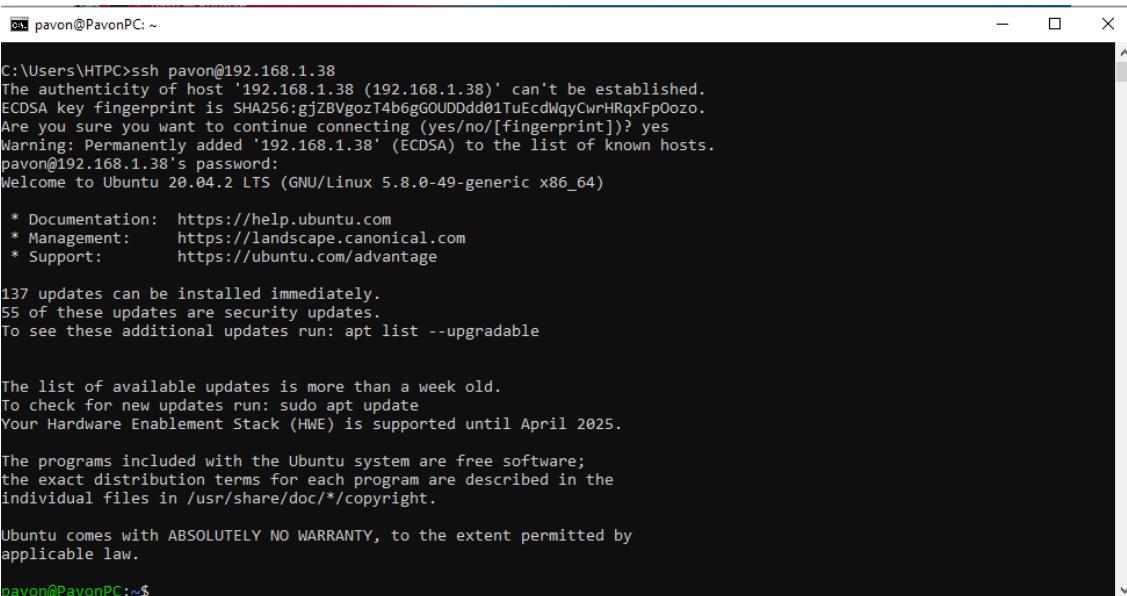
```
pavon@PavonPC:~$ ifconfig
enp1s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 50:7b:9d:c0:55:d7 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 257 bytes 23304 (23.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 257 bytes 23304 (23.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.38 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::9984:77b4:57fd:47e8 prefixlen 64 scopeid 0x20<link>
            ether 08:04:0c:c0:4e:a0 txqueuelen 1000 (Ethernet)
            RX packets 57430 bytes 85613333 (85.6 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8497 bytes 976618 (976.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pavon@PavonPC:~$ netstat -a | grep ssh
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*
                                         LISTEN
tcp6       0      0 [::]:ssh           [::]:*               LISTEN
unix  2      [ ACC ]   STREAM     LISTENING        41389   /run/user/1000/gnupg/S.gpg-agent.ssh
```

Ahora voy a conectarme por ssh a ubuntu desde windows.



```
C:\Users\HTPC>ssh pavon@192.168.1.38
The authenticity of host '192.168.1.38 (192.168.1.38)' can't be established.
ECDSA key fingerprint is SHA256: gjZBVgozT4b6gGOUDDdd01TuEcdWqyCwnHRQxFpOozo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.38' (ECDSA) to the list of known hosts.
pavon@192.168.1.38's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-49-generic x86_64)

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

137 updates can be installed immediately.
55 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

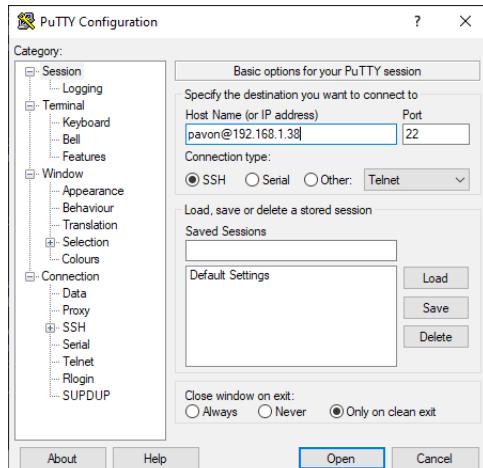
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

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

pavon@PavonPC:~$
```

Como podemos ver ya estamos conectados, el problema es que la práctica nos pide que nos conectemos desde PUTTY y nosotros estamos conectados desde CMD así que nos bajaremos PUTTY.

Una vez instalado PUTTY lo que haremos será abrirlo y escribir el usuario@dirección ip y le daremos a open.



Se nos abrirá y nos pedirá la contraseña de acceso al usuario, la escribimos, pulsamos enter y entramos.

```
pavon@PavonPC: ~
Using username "pavon".
pavon@192.168.1.38's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-49-generic x86_64)

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

173 updates can be installed immediately.
77 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri May 21 19:58:05 2021 from 192.168.1.36
pavon@PavonPC:~$
```

Ahora comprobaremos de nuevo con netstat -a | grep ssh que estamos conectados.

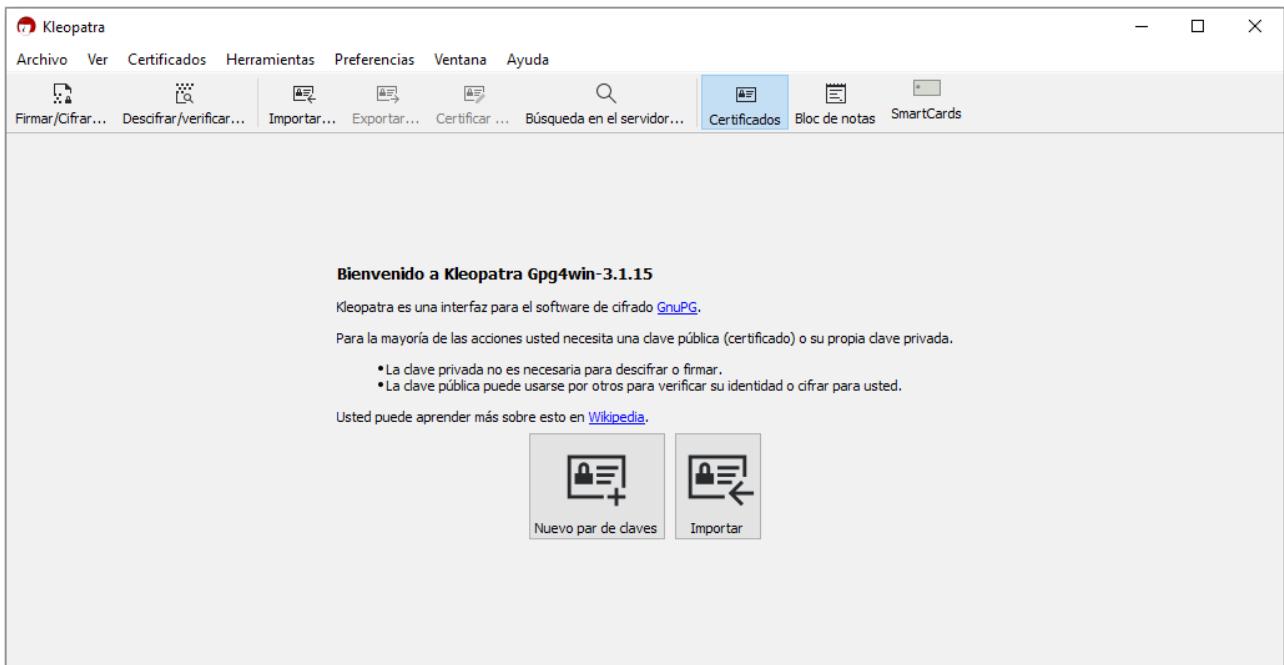
```
pavon@PavonPC:~$ netstat -a | grep ssh
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*          LISTEN
tcp        0      0 PavonPC:ssh          192.168.1.36:59058    ESTABLISHED
tcp6       0      0 [::]:ssh           [::]:*          LISTEN
unix  2      [ ACC ]     STREAM     LISTENING      39925   /run/user/1000/gnupg/S.gpg-agent.s
sh
unix  2      [ ACC ]     STREAM     LISTENING      41718   /tmp/ssh-HkC08wMVRqg/agent.1555
pavon@PavonPC:~$
```

Por último, solo nos queda salirnos de la conexión del ssh escribiendo "logout" o "exit" y validar con netstat que no tenemos la conexión activa y ssh sigue activo.

```
~ : bash — Konsole
File Edit View Bookmarks Settings Help
pavon@PavonPC:~$ netstat -a | grep ssh
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*
tcp6       0      0 [::]:ssh           [::]:*                LISTEN
unix  2      [ ACC ]     STREAM    LISTENING      39925   /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM    LISTENING      41718   /tmp/ssh-HkC08wMVXRqg/agent.1555
pavon@PavonPC:~$
```

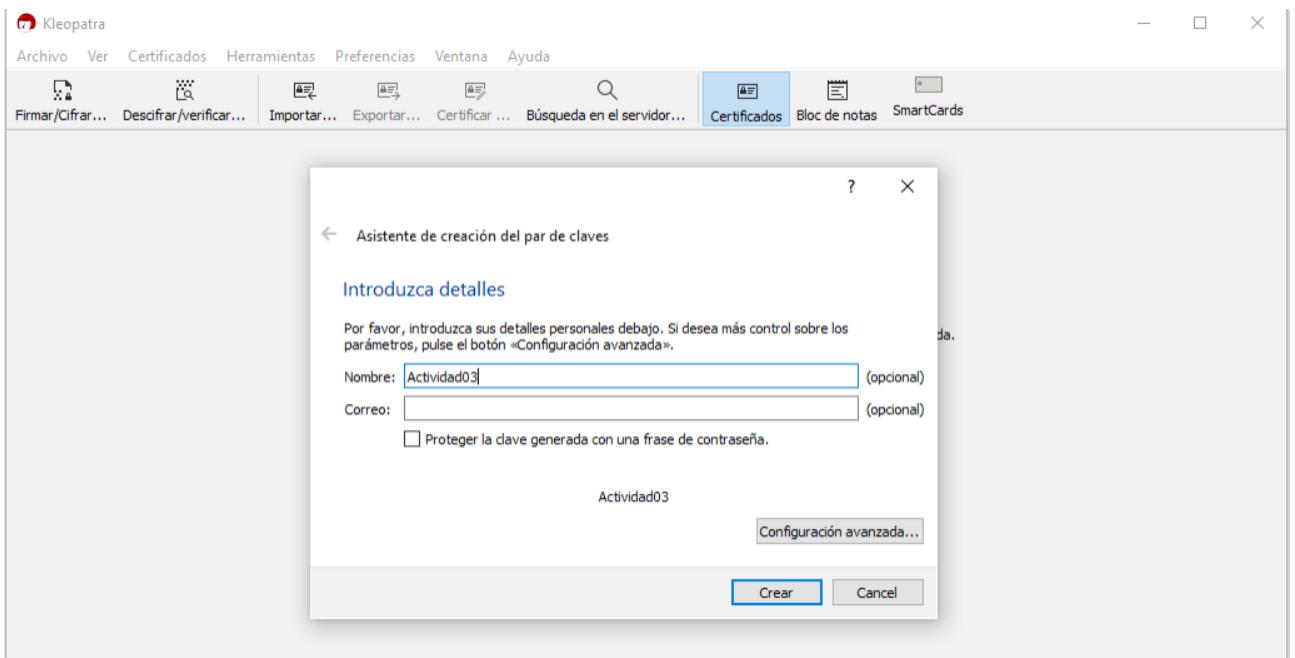
Requerimiento 2

Para esta práctica tenemos que encriptar el fichero pdf creado en la actividad anterior. El primer paso que hemos realizado ha sido instalar “Gpg4win”



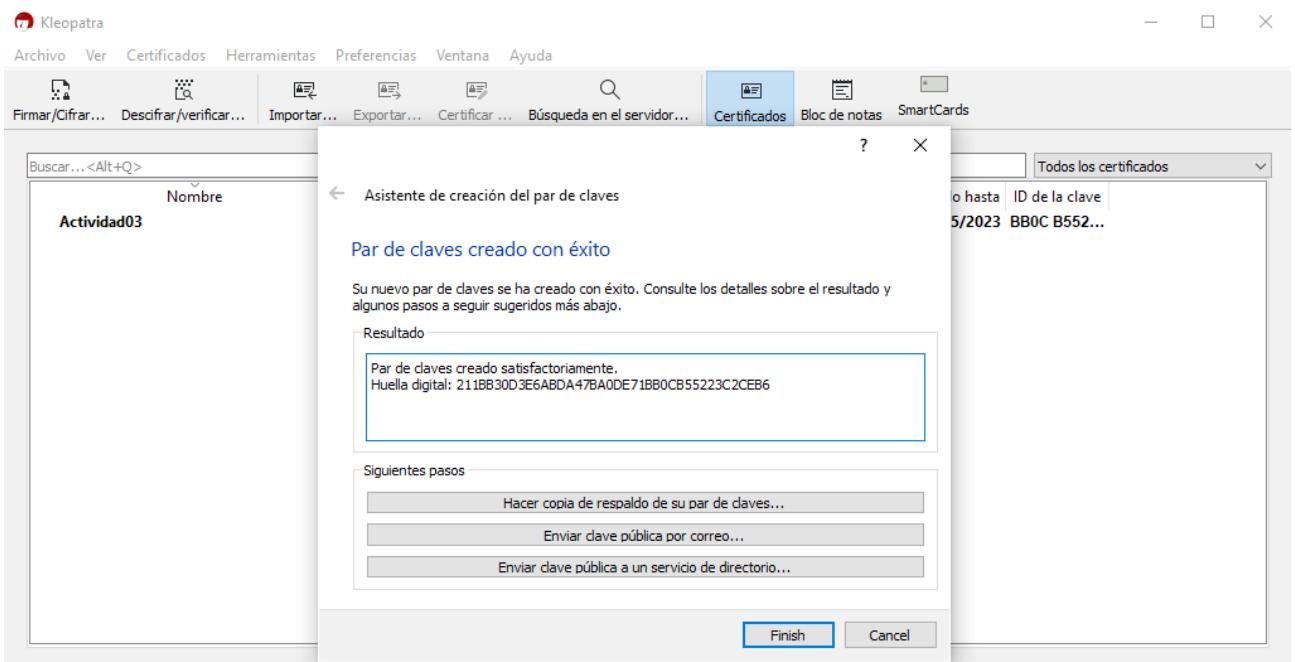
Una vez instalado como dice el ejercicio hemos creado un par de claves dándole al botón de abajo que pone “Nuevo par de claves”.

Nos pedirá que le pongamos un nombre, en nuestro caso va a ser “Actividad03”. También solicita un correo, pero como es opcional no se ha puesto.

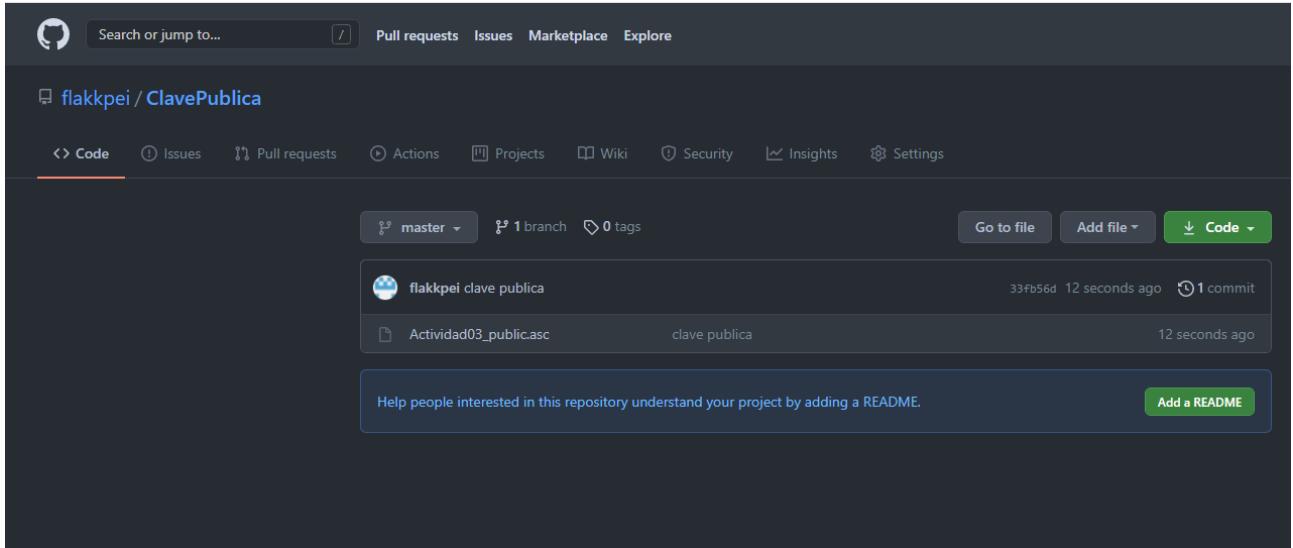


Una vez dado al botón de crear tendremos que esperar unos minutos a que se creen las dos claves “pública y privada”.

Una vez creadas las claves nos aparecerá algo así:

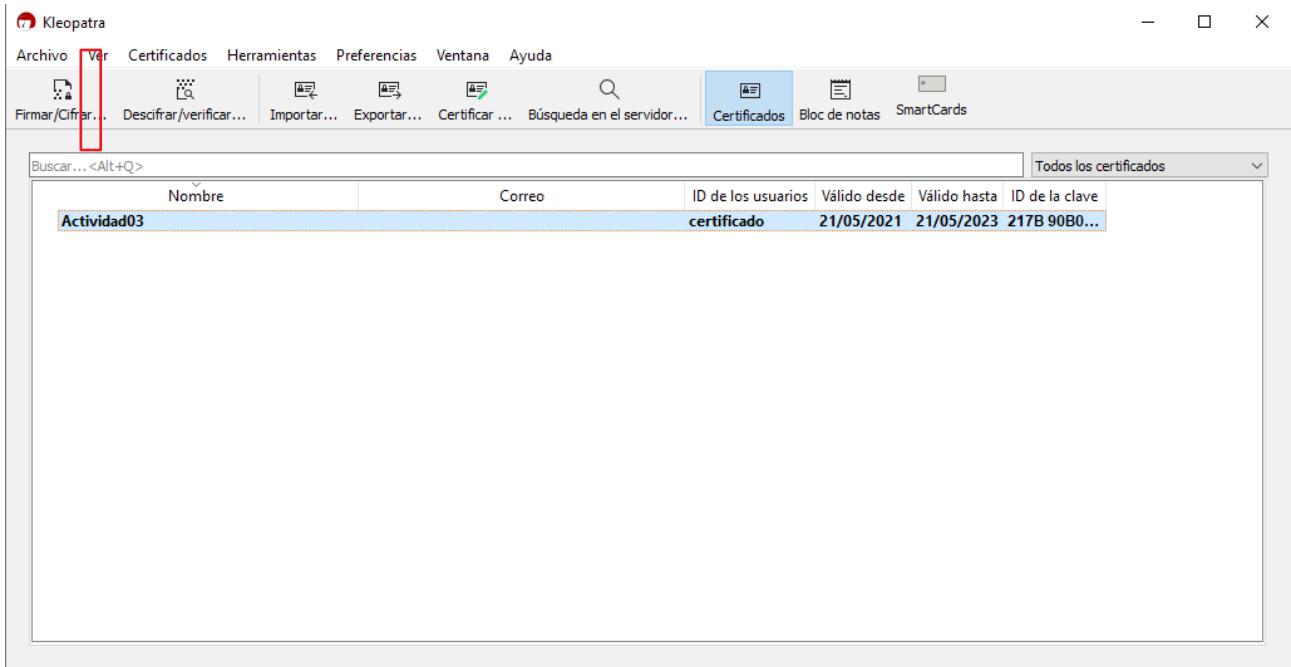


Lo siguiente que hay que hacer es subir la clave pública a un servidor de internet para que cualquiera pueda comprobar que la firma nos corresponde así que lo subiremos por ejemplo a github.



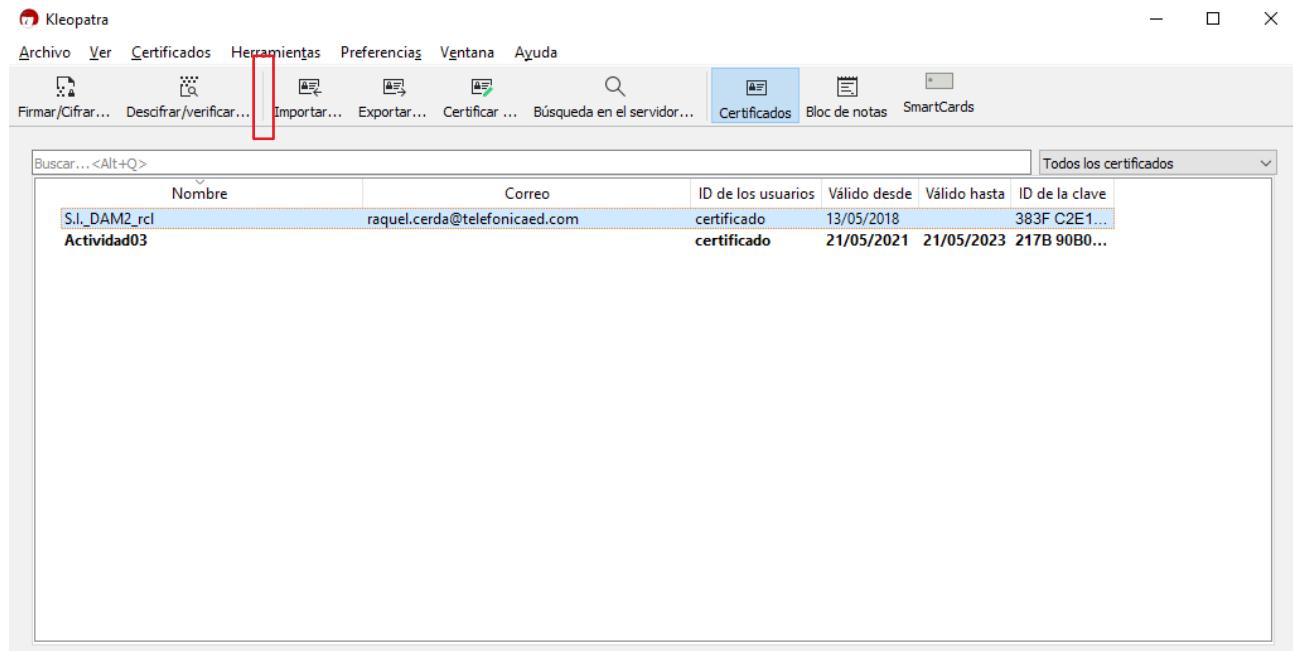
Una vez ya tenemos la clave pública subida, lo siguiente que nos propone el ejercicio es cifrar el un pdf de una actividad anterior para poder pasársela al profesor y que el pueda descifrarla cuando le llegue con su clave privada.

Para eso nos iremos al programa y le daremos a cifrar y seleccionaremos el archivo que queramos cifrar.



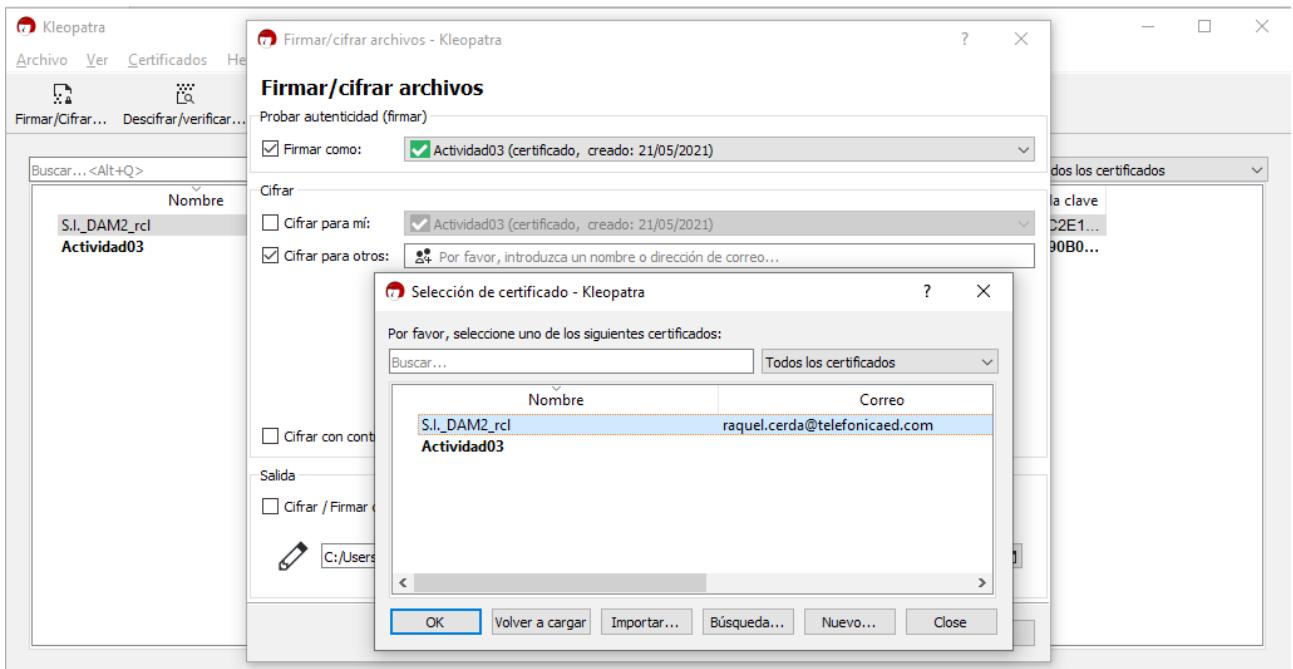
De esta forma solo podemos cifrar para nosotros con nuestro par de claves creado anteriormente. Para poder usar la clave pública del profesor debemos importarla antes.

Debemos darle a importar y una vez dado seleccionaremos la clave pública.

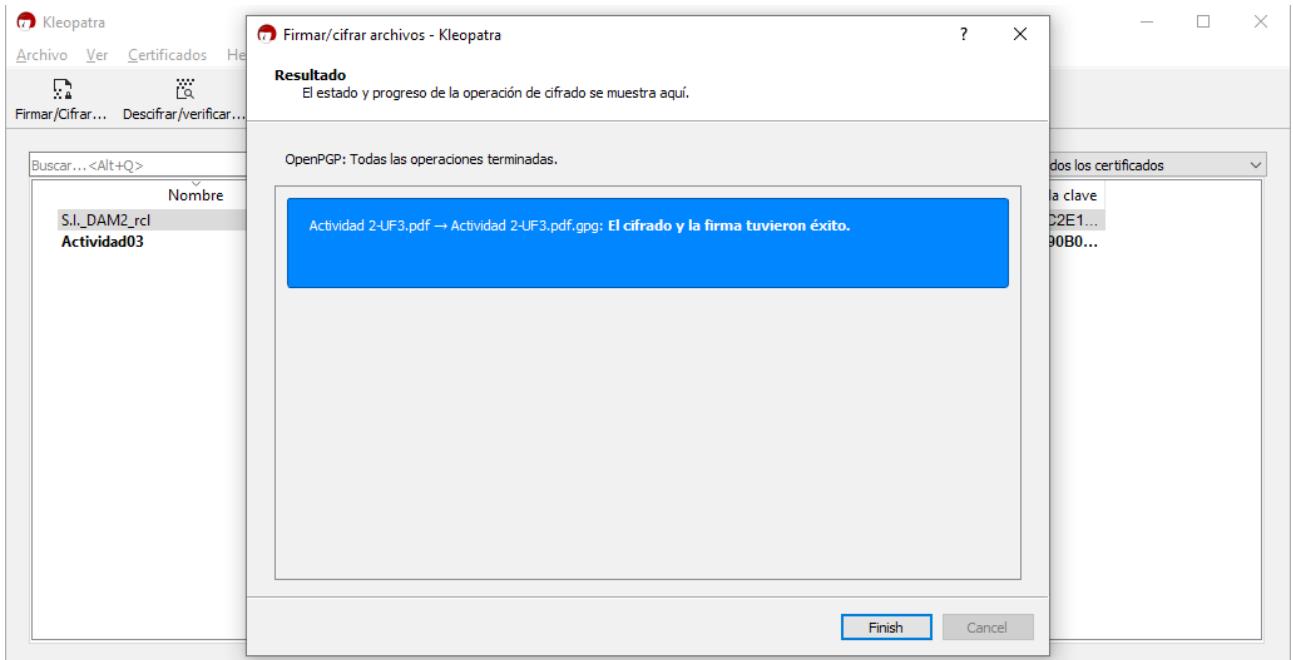


Ahora ya podremos cifrar un archivo seleccionando la clave pública del profesor en este caso.

Le daremos a cifrar, seleccionaremos el archivo que queramos y le daremos a cifrar para otros. Aquí seleccionaremos la clave pública que importamos anteriormente y le daremos a OK.

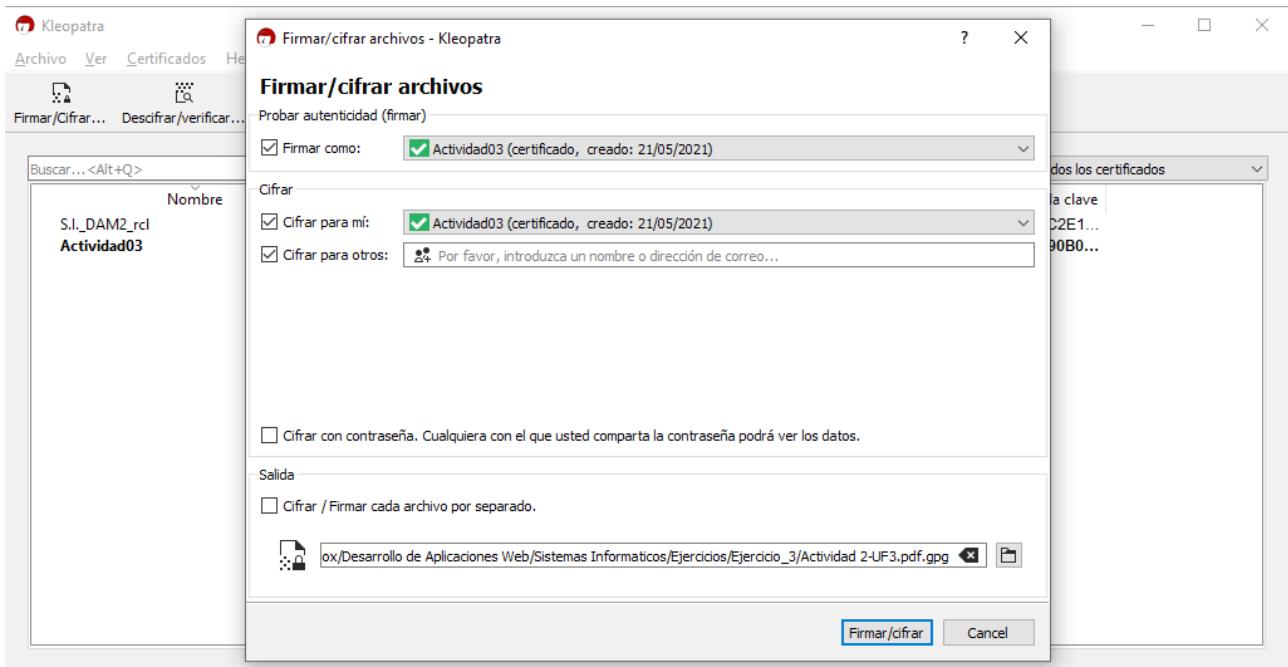


Ya estaría cifrado. Ahora solo queda mandárselo a la persona que tenga la clave privada.

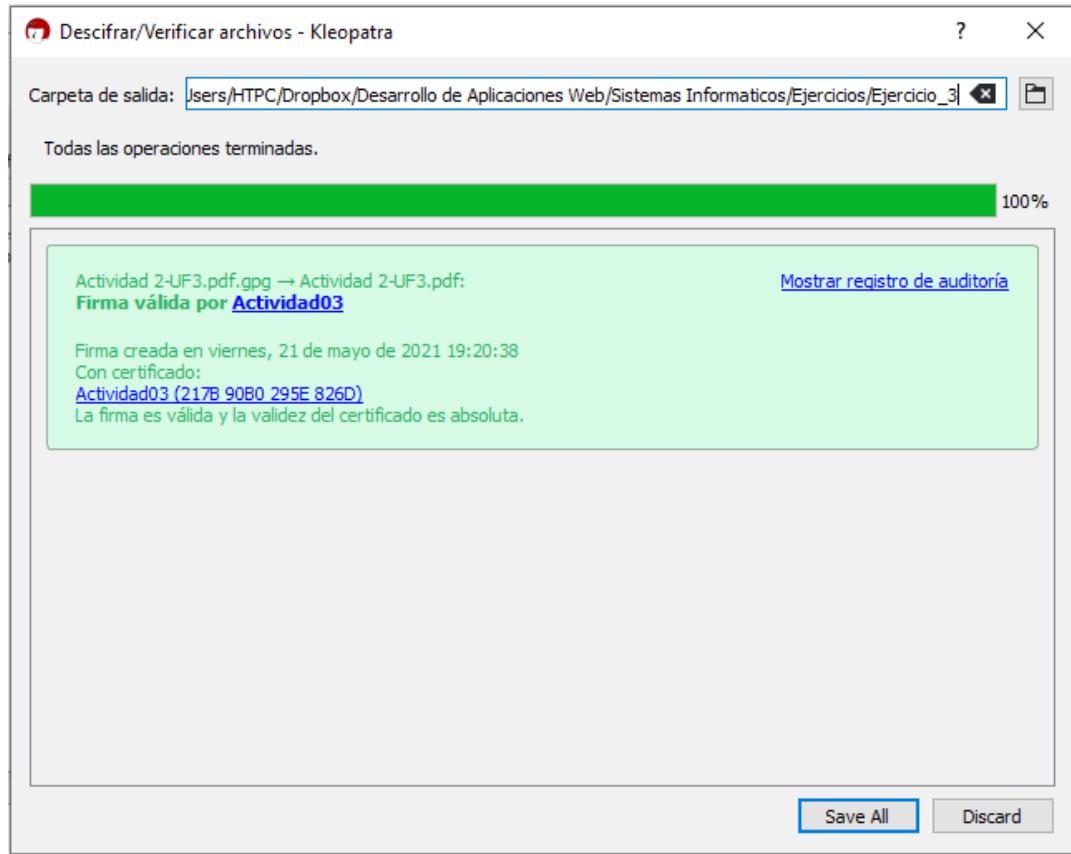


Como no tenemos la clave privada del profesor, no podemos ver si lo que hemos hecho ha funcionado. Así que como extra hemos decidido hacer una prueba con nuestras clave privada y pública y hacer lo que se tendría que hacer para descifrar un archivo.

Hacemos lo mismo, ciframos el archivo pero esta vez con nuestra clave pública.



Una vez cifrado y firmado solo tenemos que darle a descifrar y seleccionar nuestro archivo encriptado. Como podemos ver en lo marcado de rojo, al firmarlo podemos ver por quien ha sido encriptado el archivo.



Y como podemos ver, ya tendríamos nuestro archivo descifrado.

A

Actividad 2-UF3.pdf

Archivo | C:/Users/HTPC/Dropbox/Desarrollo%20de%20Aplicaciones...

1 de 43

Actividad 2.UF3 SISTEMAS INFORMÁTICOS



Miembros del equipo:

- VESSELIN BONTCHEV STANEV
- JOSÉ IGNACIO GUTIÉRREZ CERRATO
- DIEGO PAUL LLIVE CARPIO
- DANIEL PAVÓN GÓMEZ