

PAUTAS DE SEGURIDAD INFORMÁTICA

Raúl Arribas Redondo

Seguridad y Alta disponibilidad

1 Contenido

1.	APARTADO 1: GPG LINUX	2
1.1	Crea en la máquina Linux dos usuarios distintos llamados cidead1 y cidead2 , estableciendo para cada uno de ellos una contraseña segura.....	2
1.2	Para el usuario cidead1, crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, RedIris.	3
1.3	Realiza una copia de seguridad de la pareja de claves que has generado.....	7
1.4	Importa desde RedIris al anillo de claves del usuario cidead2, la clave pública de cidead1. Muestra el anillo de claves resultante de cidead2.	10
1.4.1	Importar la clave del servidor de Ubuntu	11
1.5	Genera un documento de texto y llámalo cifradoLinux_cidead2.txt. Cifralo con la clave pública de cidead1. Envía por algún medio, el documento cifrado al usuario cidead1.	12
1.5.1	Cifrar el documento con la clave publica del usuario cidead1	12
1.6	Descifra usando tu clave privada de cidead1, el documento cifradoLinux_cidead2.txt	13
2	APARTADO 2: GPG WINDOWS.....	15
2.1	Crea en la máquina Windows dos usuarios distintos llamados cidead1 y cidead2 , estableciendo para cada uno de ellos una contraseña segura.....	15
2.2	Para el usuario cidead1, crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, openpgp.....	17
2.2.1	Creamos las claves de los usuarios Cidead1 y Cidead2	22
2.2.2	Publicamos la clave en el servidor keyserver.ubuntu.com.....	25
2.3	Importa desde RedIris al anillo de claves del usuario cidead2, la clave pública de cidead1. Muestra el anillo de claves resultante de cidead2.	28
2.4	Genera un documento de texto cifradoWindows_cidead2.txt. Cifralo con la clave pública de cidead1. Envía por algún medio, el documento cifrado al usuario cidead1.	30
2.5	Descifra usando tu clave privada de cidead1, el documento cifradoWindows_cidead2.txt.	33
3	Apartado 3: Análisis Forense.....	34
3.1	Instala y configura una herramienta para la realización de evidencias digitales(por ejemplo, Access Data Forense Toolkit), sobre una máquina Windows.....	34
3.2	Crea una imagen como evidencia de una unidad USB sobre la que previamente has debido borrar algunos ficheros que deberás recuperar usando la imagen.	38
3.3	Abre una sesión en cualquier sitio web al que debas logarte. Usa la herramienta anterior para capturar toda la información existente en la memoria RAM. Monta dicha captura sobre una imagen y realiza un análisis forense de la imagen creada. Finalmente, captura la pantalla en la que se muestra la sesión abierta en el sitio web junto con las credenciales de acceso.....	51

1. APARTADO 1: GPG LINUX

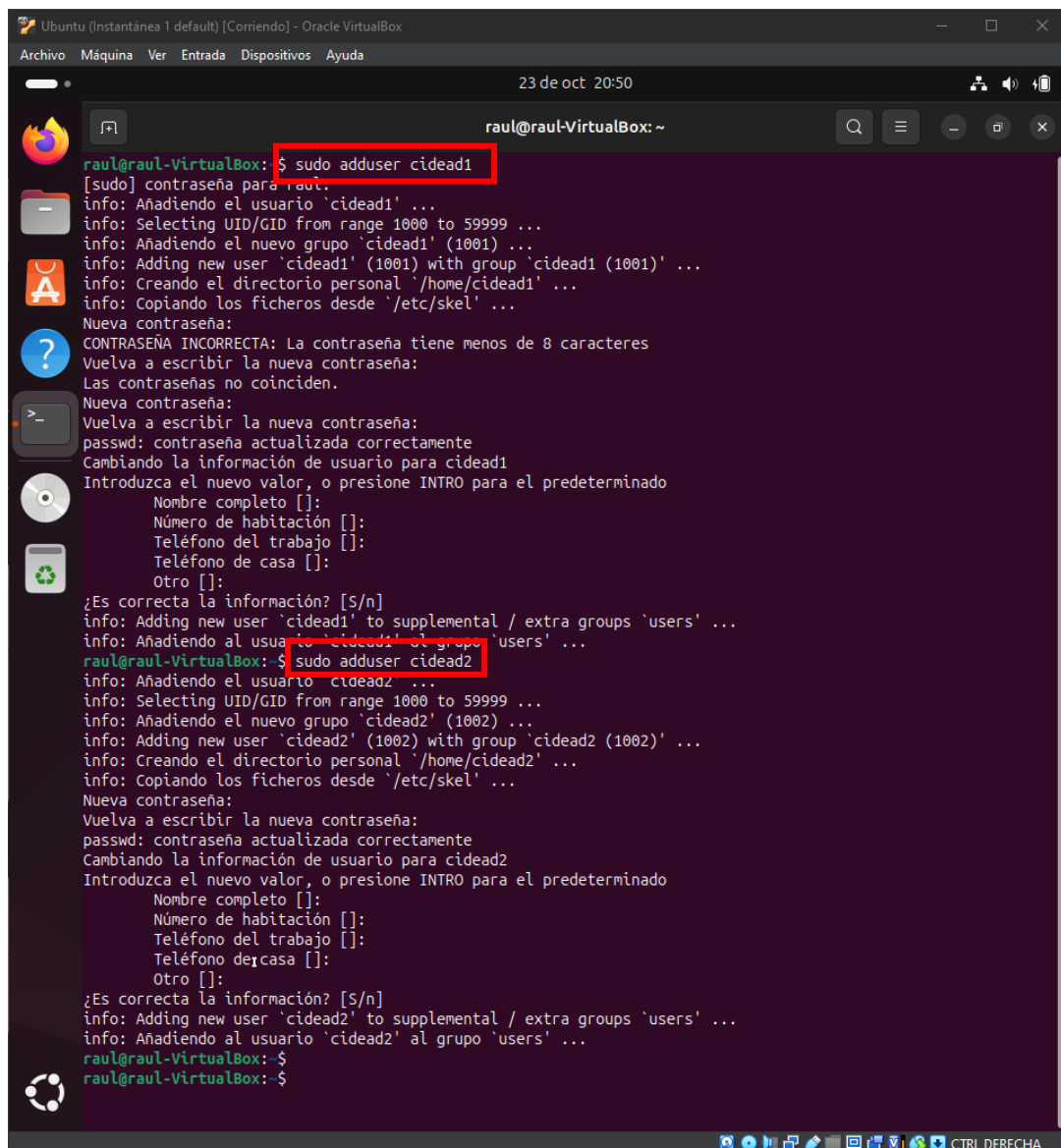
1.1 Crea en la máquina Linux dos usuarios distintos llamados **cidead1** y **cidead2**, estableciendo para cada uno de ellos una contraseña segura.

En primer lugar, vamos a utilizar una máquina virtual en Virtual box con sistema operativo Ubuntu 24.04.1 LTS.

Para crear los usuarios escribimos los siguientes comandos en la terminal, nos pedirá poner una contraseña a cada uno.

```
sudo adduser cidead1
```

```
sudo adduser cidead2
```



```
Ubuntu (Instantánea 1 default) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
23 de oct 20:50
raul@raul-VirtualBox: ~
raul@raul-VirtualBox:~$ sudo adduser cidead1
[sudo] contraseña para raul:
info: Añadiendo el usuario 'cidead1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo 'cidead1' (1001) ...
info: Adding new user 'cidead1' (1001) with group 'cidead1' (1001) ...
info: Creando el directorio personal '/home/cidead1' ...
info: Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
Vuelva a escribir la nueva contraseña:
Las contraseñas no coinciden.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para cidead1
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n]
info: Adding new user 'cidead1' to supplemental / extra groups 'users' ...
info: Añadiendo al usuario 'cidead1' al grupo 'users' ...
raul@raul-VirtualBox:~$ sudo adduser cidead2
info: Añadiendo el usuario 'cidead2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo 'cidead2' (1002) ...
info: Adding new user 'cidead2' (1002) with group 'cidead2' (1002) ...
info: Creando el directorio personal '/home/cidead2' ...
info: Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para cidead2
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n]
info: Adding new user 'cidead2' to supplemental / extra groups 'users' ...
info: Añadiendo al usuario 'cidead2' al grupo 'users' ...
raul@raul-VirtualBox:~$
raul@raul-VirtualBox:~$
```

1.2 Para el usuario cidead1, crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, RedIris.

- Primero agregamos al grupo sudoers a los usuarios que hemos creado para que puedan ejecutar el proceso de creación de la clave.

Sudo usermod -aG sudo cidead1

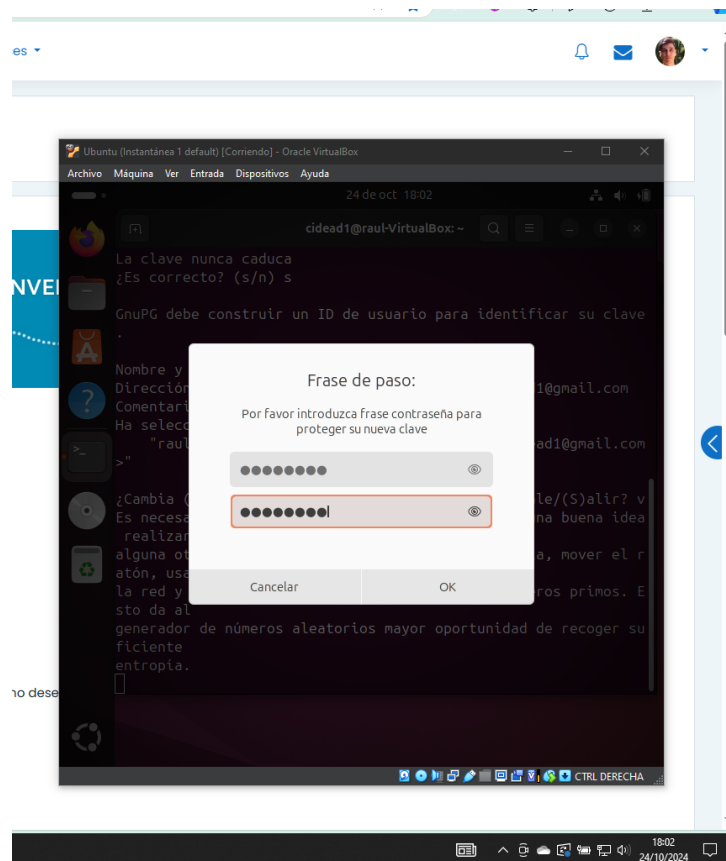
Sudo usermod -aG sudo cidead2

```
raul@raul-VirtualBox:~$ sudo usermod -aG sudo cidead1
raul@raul-VirtualBox:~$ sudo usermod -aG sudo cidead2
raul@raul-VirtualBox:~$
```

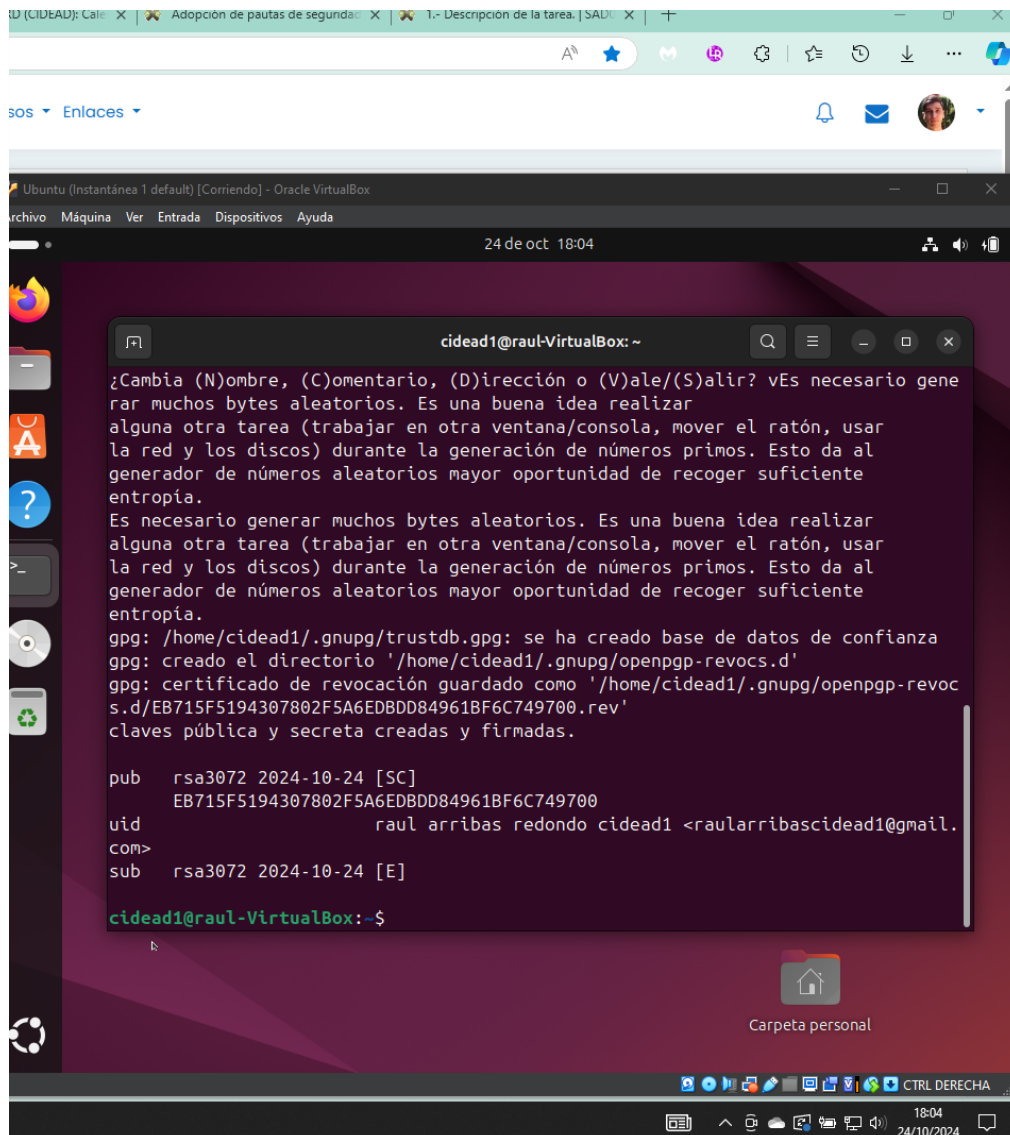
- Ahora generamos la clave para el usuario cidead1, con cidead2 repetimos el mismo paso, nos conectamos al usuario cidead1 cambiando de usuario.

gpg --full-generate-key

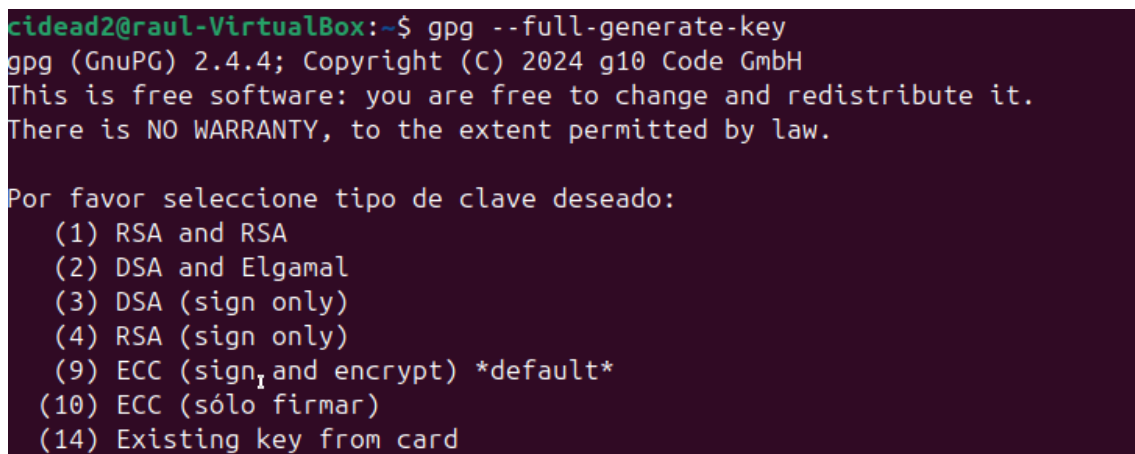
Cuando la generemos nos pedirá la contraseña para protegerla:



Vemos que se nos genera la clave correctamente.



- Creamos la clave de cidead2, para crearla nos pedirá una contraseña para desbloquear la clave privada.



```
pub    rsa3072 2024-10-24 [SC]
       15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
uid          raul arribas redondo cidead2 <raularribascidead2@gmail.
com>
sub      rsa3072 2024-10-24 [E]

cidae2@raul-VirtualBox:~$
```

- Ahora verificamos el proceso para ver las claves se han generado correctamente tanto en cidead1 como en cidead2:

gpg --list-keys

```
cidead1@raul-VirtualBox:~$ gpg --list-keys
gpg: comprobando base de datos de confianza
gpg: marginales needed: 3  completes needed: 1  trust model: pgp
gpg: nivel: 0  validez: 1  firmada: 0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
/home/cidead1/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-10-24 [SC]
      EB715F5194307802F5A6EDBDD84961BF6C749700
uid          [ absoluta ] raul arribas redondo cidead1 <raularribascidead1@gmail.
com>
sub   rsa3072 2024-10-24 [E]
```

```
cidead2@raul-VirtualBox:~$ gpg --list-keys
/home/cidead2/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-10-24 [SC]
      15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
uid           [ absolute ] raul arribas redondo cidead2 <raularribascidead2@gmail.
com>
sub   rsa3072 2024-10-24 [E]
```

- Exportamos la clave publica en un archivo para compartirlo

```
gpg --export -a raularribascidead1@gmail.com > /home/cidead1/cidead1_publica.key
```

```
cidead1@raul-VirtualBox:~$ gpg --export -a raularribascidead1@gmail.com > /home/cidead1/cidead1_publica.key
cidead1@raul-VirtualBox:~$ ls
cidead1_publica.key  Documentos  Imágenes  Plantillas  snap
Descargas            Escritorio  Música    Público     Videos
cidead1@raul-VirtualBox:~$ cat cidead1_publica.key
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGCaGc4BDAC+WWKlK0PaR0ZPnD5hQjsoZBvorOIlHEQM4RhNYkPsO70gvPUZ
JtgHzcsz0rjG0rsED/Y0EMZKhkftooy2f6jNGR0UrFos12rf+MRN7qxZwvTt2VsiB
+m+Z0JoYp25+jHRBMNXXJj5JSQ51HsK2uH8v+9CzPRWG3QNf0Q4bXIjNhcTv2qCQnn
b2ZtDcRtUAgOB4/zgn/fQ418JtM9feSd75ZEz7jz3FB02m2wnusdJw/MsvFMn7yL
lz/w0Sx/mJ5TA+Gumv6i9fykeTSW2AbZG72JrzCQxn33dgkrADJGZc8l0c1bSb4Q
t0YJYtvM3vzlgLALXPHjr7GrHfIXFLzI/qDlxkhSFj8fpl/xCLV51c7xKytvVPLpv
+p3LOvqabWFBfvfqq/XfxBQm+jo8zL0rLq+CUAsqFvKMIrliYmp7p3P0YmTsGv5
PxWTTmbJdDow78eMN9gA7/pvMCI4bY0jXhbKbeETktLrdKV8xYjw7tnAxA8580YeW
TWzs2Njx7XAha4vcAEQEAAQ7cmF1bCBhcnJpYmFzIHJlZG9uZG8gY2lkZWfKMSA8
cmF1bG9ycmlhYXNjaWRlYWQxQGdtYWlsLmNvbT6JAdEEEwEKADSiwIQTrcv9RlDB4
A=
-----
```

gpg --export -a raularribascidead2@gmail.com > /home/cidead2/cidead2_publica.key

```
cidead2@raul-VirtualBox:~$ gpg --export -a raularribascidead2@gmail.com > /home/cidead2/cidead2_publica.key
cidead2@raul-VirtualBox:~$ ls
cidead2_publica.key  Documentos  Imágenes  Plantillas  snap
Descargas           Escritorio  Música    Público     Videos
cidead2@raul-VirtualBox:~$ cat cidead2_publica.key
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGcaFnUBDADK4PvHRnaPhrFHG9y/xf9TCY/VjGWwIgUKqVPn8FQzHIi5AiLR
4S5QOAlNECoxDDuWGJj5cshq5wQ111ZxI2MoYKcA2jpYtT+IEfQqvLHYfoJfJy/m
YvZspTAbOB1C/zqIXHake16CtR3mYLuRrwbipSqWs/rTDzY+UhvI+EVy9vtJ1Nha
aeWn97WDWpPI30yJ4J5np8A7PClKx8KcxJ31bQ9ocvya/RpMmhVWGqUDb2/SU+Ro
```

- Para subir la clave publica al servidor de claves (Ubuntu) hacemos los siguientes pasos:

Cidead1:

**Gpg--keyserver htps://keyserver.ubuntu.com --send-keys
EB715F5194307802F5A6EDBDD84961BF6C749700**

```
cidead1@raul-VirtualBox:~$ gpg --keyserver htps://keyserver.ubuntu.com --send-keys EB715F5194307802F5A6EDBDD84961BF6C749700
gpg: enviando clave D84961BF6C749700 a htps://keyserver.ubuntu.com
```

Cidead2:

**gpg --keyserver htps://keyserver.ubuntu.com --send-keys
15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6**

```
cidead2@raul-VirtualBox:~$ gpg --keyserver htps://keyserver.ubuntu.com --send-keys 15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
gpg: enviando clave 71F0D6E2C6FB21B6 a htps://keyserver.ubuntu.com
```

Nuestro id de claves se muestra al hacer un listado de las claves que tenemos previamente mostrado.

- Verificamos que la clave está en el servidor correctamente:

Cidead1:

gpg --keyserver htps://keyserver.ubuntu.com --search-keys raularribascidead1@gmail.com

```
cidead1@raul-VirtualBox:~$ gpg --keyserver htps://keyserver.ubuntu.com --search-keys raularribascidead1@gmail.com
gpg: data source: https://[2620:2d:4000:1007::d43]:443
(1)      raul arribas redondo cidead1 <raularribascidead1@gmail.com>
        3072 bit RSA key D84961BF6C749700, creado: 2024-10-24
Keys 1-1 of 1 for "raularribascidead1@gmail.com".  Introduzca número(s), 0)tro, o F)in >
```

Cidead2:

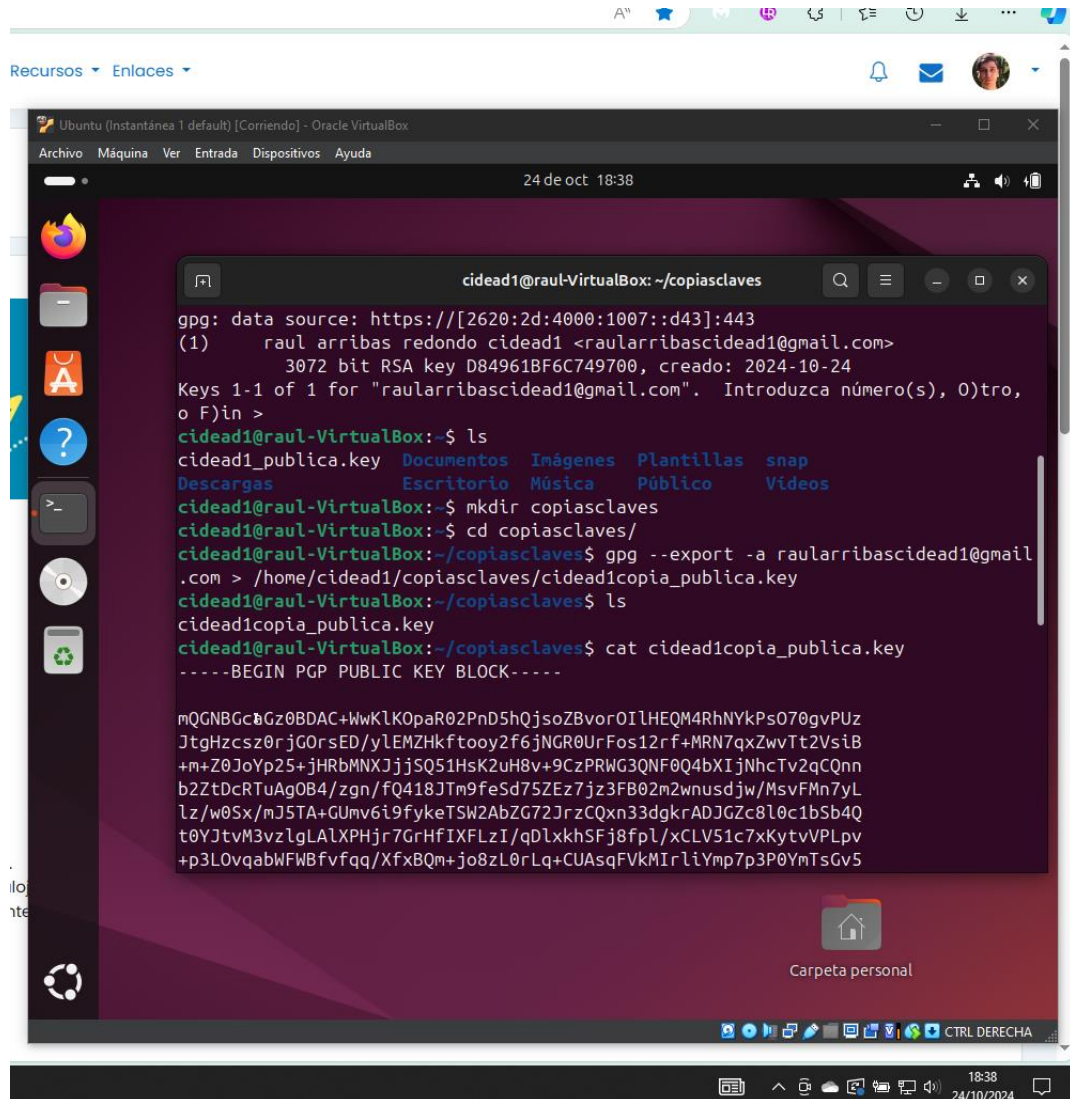
gpg --keyserver htps://keyserver.ubuntu.com --search-keys raularribascidead2@gmail.com

```
cidead2@raul-VirtualBox:~$ gpg --keyserver htps://keyserver.ubuntu.com --search-
keys raularribascidead2@gmail.com
gpg: data source: https://[2620:2d:4000:1007::70c]:443
(1)      raul arribas redondo cidead2 <raularribascidead2@gmail.com>
        3072 bit RSA key 71F0D6E2C6FB21B6, creado: 2024-10-24
Keys 1-1 of 1 for "raularribascidead2@gmail.com".  Introduzca número(s), 0)tro,
o F)in >
```

1.3 Realiza una copia de seguridad de la pareja de claves que has generado.
Vamos a realizar la copia de seguridad de las claves que hemos generado.

Cidead1: Clave Publica

gpg --export -a raularribascidead1@gmail.com >
/home/cidead1/copiasclaves/cidead1copia_publica.key



Cidead2: Clave Publica

```
gpg --export -a raularribascidead2@gmail.com >
/home/cidead2/copiasclaves/cidead2_publica.key
```

```
cidead2@raul-VirtualBox:~$ gpg --export -a raularribascidead2@gmail.com > /home/cidead2/
/copiasclaves/cidead2_publica.key
cidead2@raul-VirtualBox:~$ ls
cidead2_publica.key  Descargas  Escritorio  Música  Público  Videos
copiasclaves        Documentos  Imágenes  Plantillas  snap
cidead2@raul-VirtualBox:~$ cd copiasclaves/
cidead2@raul-VirtualBox:~/copiasclaves$ ls
cidead2_publica.key
cidead2@raul-VirtualBox:~/copiasclaves$ cat cidead2_publica.key
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGCafnUBDADK4PvHRnaPhrFHG9y/xf9TCY/VjGWwIgUKqVPn8FQzHI5AiLR
4S5QOAlNECoxDDuWGJj5cshq5wQ111ZxI2MoYKcA2jpYtT+IEfQqvLHYfoJfJy/m
YvZspTABOB1C/zqIXHake16CtR3mYLuRrbwipSqWs/rTDzY+UhvI+EVy9vtJ1Nha
aeWn97WDWpPI30yJ4J5np8A7PCLKx8KcxJ31bQ9ocvya/RpMmhVWGqUDb2/SU+Ro
ad5nQhigrU7LKBWVxpYWcb4zk57e3WnhZVE3pkf/x+hEJHWA2SVL7vkEmtNQruV
NtlvA0JrfImpdyto3PZPJG60RxnVn7+nX0yfUW0yPTrPMI2SDYOYlBsmv70l4z4s4
zIMA7PMLRT9JHM8p7oWKFYeff+9LmnIR1DbPVX/w0mPSnf/BCbWQDa5tTbbMJHfD
r+ymWgWjQeCv1k/F2Fx/xhd7Lr0SL/FS2VP3ztYmAw0cthSPmL/FONWC0IuegLO1
j85leuIjv11hUjUAEQEAAAbQ7cmF1bCBhcnJpYmFzIHJlZG9uZG8gY2lkZWfkMiA8
cmF1bGFycmliYXNjaWRlYWQyQGdtYWlsLmNvbT6JAdEEwEKADsWlQQV5C8UUQFw
x8U/bg1x8NBixvshtgUCZxoWdQIbAwULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIX
gAAKCRBx8NBixvsht6jC/98afdyRdlid6IQXXzta72d2HhG3ASCL2JjcN0hpLUp
UGcaz/4ofDcA2QTb6UMf0LS/rGJQkaqdFLkKmsJJ2dBq0kSNp0pEL7aPcKsOCLfw
QOIRUg+mRPbUKp1lC9QRwNk0ZuXf/m7mfJriAs4P1Pq/GAg87m1Ui4C6uTY+28it
ir01KREwdLFRHbYvQGO9HuHL44EngHRDuwNxt0uxeFsGryTyj9fPL/jmtvMGYAT
HITcwQcVhVS31s8KwFYLGMY32N07K/FmgLJZuTp8309ERNTMEerMt/4F4EA29v+
qNVddbXIRBWzODFRysEnToe2Mp0un9bDqX67xIgpNt2PSJd0yKgS5Dqdpfk+d8H4
2DilnfcsanSxoXTMotedkJfOR7+vvNcfv/81GT/Ofp/aScxofTLJnH1l9v8n/wt
```

Ahora vamos a realizar la copia de seguridad de nuestra **clave privada**, cambiará un poco la forma de hacerlo ya que esta clave no se puede compartir con nadie:

Cidead1: Clave Privada

Listamos las claves para coger la ID y utilizarlo en el siguiente comando:

```
gpg --list-secret-keys --keyid-format LONG
```

```
cidead1@raul-VirtualBox:~/copiasclaves$ gpg --list-secret-keys --keyid-format LO
NG
/home/cidead1/.gnupg/pubring.kbx
-----
sec  rsa3072/D84961BF6C749700 2024-10-24 [SC]
     EB715F5194507802F5A6ED6DD84961BF6C749700
uid  [ absoluta ] raul arribas redondo cidead1 <raularribascidead1@
gmail.com>
ssb  rsa3072/C4563B81E5EB6213 2024-10-24 [E]
```

Una vez sabemos cuáles es nuestra ID ejecutamos el siguiente comando para hacer una copia de seguridad de nuestra clave privada:

```
gpg --export-secret-keys -a D84961BF6C749700 >
/home/cidead1/copiasclaves/cidead1copia_privada.key
```

-a: lo convierte a un formato legible ASCII

Nos pedirá la contraseña que pusimos cuando generamos:

```
cidead1@raul-VirtualBox:~/copiasclaves$ gpg --export-secret-keys -a D84961BF6C749700 > /home/cidead1/copiasclaves/cidead1copia_privada.key
cidead1@raul-VirtualBox:~/copiasclaves$ ls
cidead1copia_privada.key  cidead1copia_publica.key
```

```
cidead1@raul-VirtualBox:~/copiasclaves$ ls
cidead1copia_privada.key  cidead1copia_publica.key
cidead1@raul-VirtualBox:~/copiasclaves$ cat cidead1copia_privada.key
-----BEGIN PGP PRIVATE KEY BLOCK-----
lQWGBGcaGz0BDAC+UwKlK0naB02PoD5b0iso7BvorOTlHEQM4PBhNYkPs070qvPUz
```

Aquí vemos en la imagen como nos ha generado una copia de nuestra clave privada.

Cidead2: Clave Privada

Hacemos lo mismo con la clave de cidead2:

Listamos la clave para coger el ID y utilizarlo en el siguiente comando:

gpg --list-secret-keys --keyid-format LONG

```
cidead2@raul-VirtualBox:~/copiasclaves$ gpg --list-secret-keys --keyid-format LONG
/home/cidead2/.gnupg/pubring.kbx
-----
sec   rsa3072/71F0D6E2C6FB21B6 2024-10-24 [SC]
      15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
uid           [ absoluta ] raul arribas redondo cidead2 <raularribascidead2@gmail.co
m>
sub   rsa3072/690465473B004506 2024-10-24 [EF]
```

gpg --export-secret-keys -a 71F0D6E2C6FB21B6 > /home/cidead2/copiasclaves/cidead2copia_private.key

-a: lo convierte a un formato legible ASCII

Nos pedirá la contraseña que pusimos cuando la creamos

```
cidead2@raul-VirtualBox:~/copiasclaves$ gpg --export-secret-keys -a 71F0D6E2C6FB21B6 > /home/cidead2/copiasclaves/cidead2copia_private.key
cidead2@raul-VirtualBox:~/copiasclaves$ ls
cidead2copia_private.key  cidead2_publica.key
cidead2@raul-VirtualBox:~/copiasclaves$ cat cidead2copia_private.key
-----BEGIN PGP PRIVATE KEY BLOCK-----
lQWGBGcaFnUBDADK4PvHRnaPhrFHG9y/xf9TCY/VjGwwIgUKqVPn8FQzHIi5AiLR
45500A1NEGcxDPwUKG7iEesbEw01117vIT3MeYKsA2iaV6TzTF50evLUV5e7f67vLm
```

Ya tenemos creadas nuestras copias de las claves públicas y privadas, ahora deberíamos de moverlas a un sitio seguro para tenerlas en caso de perderlas.

1.4 Importa desde RedIris al anillo de claves del usuario cidead2, la clave pública de cidead1. Muestra el anillo de claves resultante de cidead2.

En mi caso lo vamos a realizar con el servidor de Ubuntu ya que con el de RedIris me daba error.

Lo primero que tenemos que comprobar es que el servidor de Ubuntu nos reconoce las claves públicas que subimos anteriormente, podemos buscarla o por ID o por correo electrónico:

```
sudo gpg --keyserver htps://keyserver.ubuntu.com --search-keys 71F0D6E2C6FB21B6
```

```
sudo gpg --keyserver htps://keyserver.ubuntu.com --search-keys  
raularribascidead1@gmail.com
```

```
cidead2@raul-VirtualBox:~/copiasclaves$ sudo gpg --keyserver htps://keyserver.ubuntu.com  
--search-keys 71F0D6E2C6FB21B6  
[sudo] contraseña para cidead2:  
gpg: data source: https://185.125.188.27:443  
(1)      raul arribas redondo cidead2 <raularribascidead2@gmail.com>  
        3072 bit RSA key 71F0D6E2C6FB21B6, creado: 2024-10-24  
Keys 1-1 of 1 for "71F0D6E2C6FB21B6". Introduzca número(s), 0)tro, o F)in > o  
cidead2@raul-VirtualBox:~/copiasclaves$ sudo gpg --keyserver htps://keyserver.ubuntu.com  
--search-keys raularribascidead1@gmail.com  
gpg: data source: https://185.125.188.27:443  
(1)      raul arribas redondo cidead1 <raularribascidead1@gmail.com>  
        3072 bit RSA key D84961BF6C749700, creado: 2024-10-24  
Keys 1-1 of 1 for "raularribascidead1@gmail.com". Introduzca número(s), 0)tro, o F)in >
```

Como vemos las tenemos subidas en el servidor de Ubuntu las claves de los dos usuarios.

1.4.1 Importar la clave del servidor de Ubuntu

Lo siguiente es importar la clave publica del usuario cidead1 a cidead2 desde el servidor de Ubuntu, para eso hacemos lo siguiente:

En la ID tenemos que poner la del usuario de cidead1.

gpg --keyserver htps://keyserver.ubuntu.com --recv-keys D84961BF6C749700

```
cidead2@raul-VirtualBox:~/copiasclaves$ gpg --list-keys
/home/cidead2/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-10-24 [SC]
      15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
uid   [ absoluta ] raul arribas redondo cidead2 <raularribascidead2@gmail.com>
sub   rsa3072 2024-10-24 [E]

cidead2@raul-VirtualBox:~/copiasclaves$ gpg --keyserver htps://keyserver.ubuntu.com --re
cv-keys D84961BF6C749700
gpg: clave D84961BF6C749700: clave pública "raul arribas redondo cidead1 <raularribascid
ead1@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:                importadas: 1

cidead2@raul-VirtualBox:~/copiasclaves$ gpg --list-keys
/home/cidead2/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-10-24 [SC]
      15E42F14510170C7C53F6E0D71F0D6E2C6FB21B6
uid   [ absoluta ] raul arribas redondo cidead2 <raularribascidead2@gmail.com>
sub   rsa3072 2024-10-24 [E]

pub   rsa3072 2024-10-24 [SC]
      EB715F5194307802F5A6EDBDD84961BF6C749700
uid   [desconocida] raul arribas redondo cidead1 <raularribascidead1@gmail.com>
sub   rsa3072 2024-10-24 [E]
```

Para observar que se ha importado bien comprobamos con **gpg --list-keys** vemos que antes solo teníamos 1 y ahora tenemos 2 claves.

- 1.5 Genera un documento de texto y llámalo `cifradoLinux_cidead2.txt`. Cifralo con la clave pública de `cidead1`. Envía por algún medio, el documento cifrado al usuario `cidead1`.

Vamos a crear un documento `cifradoLinux_cidead2.txt`

```
cidead2@raul-VirtualBox:~/copiasclaves$ echo "esto es un documento enviado por cidead2 y esta cifrado raul arribas redondo cidead" > cifradoLinux_cidead2.txt
```

```
cidead2@raul-VirtualBox:~$ cat cifradoLinux_cidead2.txt
esto es un documento enviado por cidead2 y esta cifrado raul arribas redondo cidead
```

- 1.5.1 Cifrar el documento con la clave publica del usuario `cidead1`

Ahora vamos a cifrar el documento que hemos creado con la clave publica de `cidead1`, hacemos lo siguiente:

```
gpg --encrypt --recipient EB715F5194307802F5A6EDBD84961BF6C749700
cifradoLinux_cidead2.txt
```

--encrypt significa que lo vamos a cifrar

--recipient significa a con que id lo vamos a cifrar

```
cidead2@raul-VirtualBox:~$ gpg --encrypt --recipient EB715F5194307802F5A6EDBD84961BF6C749700 cifradoLinux_cidead2.txt
gpg: C4563B81E5EB6213: No hay seguridad de que esta clave pertenezca realmente al usuario que se nombra

sub rsa3072/C4563B81E5EB6213 2024-10-24 raul arribas redondo cidead1 <raularribascidead1@gmail.com>
Huella clave primaria: EB71 5F51 9430 7802 F5A6 EDBD D849 61BF 6C74 9700
Huella de subclave: 88B4 0135 5000 E819 E682 DCE3 C456 3B81 E5EB 6213

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
cidead2@raul-VirtualBox:~$ ls
cidead2_publica.key      copiasclaves  Escritorio    Plantillas    Videos
cifradoLinux_cidead2.txt Descargas     Imágenes     Público
cifradoLinux_cidead2.txt.gpg Documentos    Música        snap
cidead2@raul-VirtualBox:~$
```

Nos genera un fichero nuevo `.gpg` que es el que tenemos encriptado con la clave publica de `cidead1`.

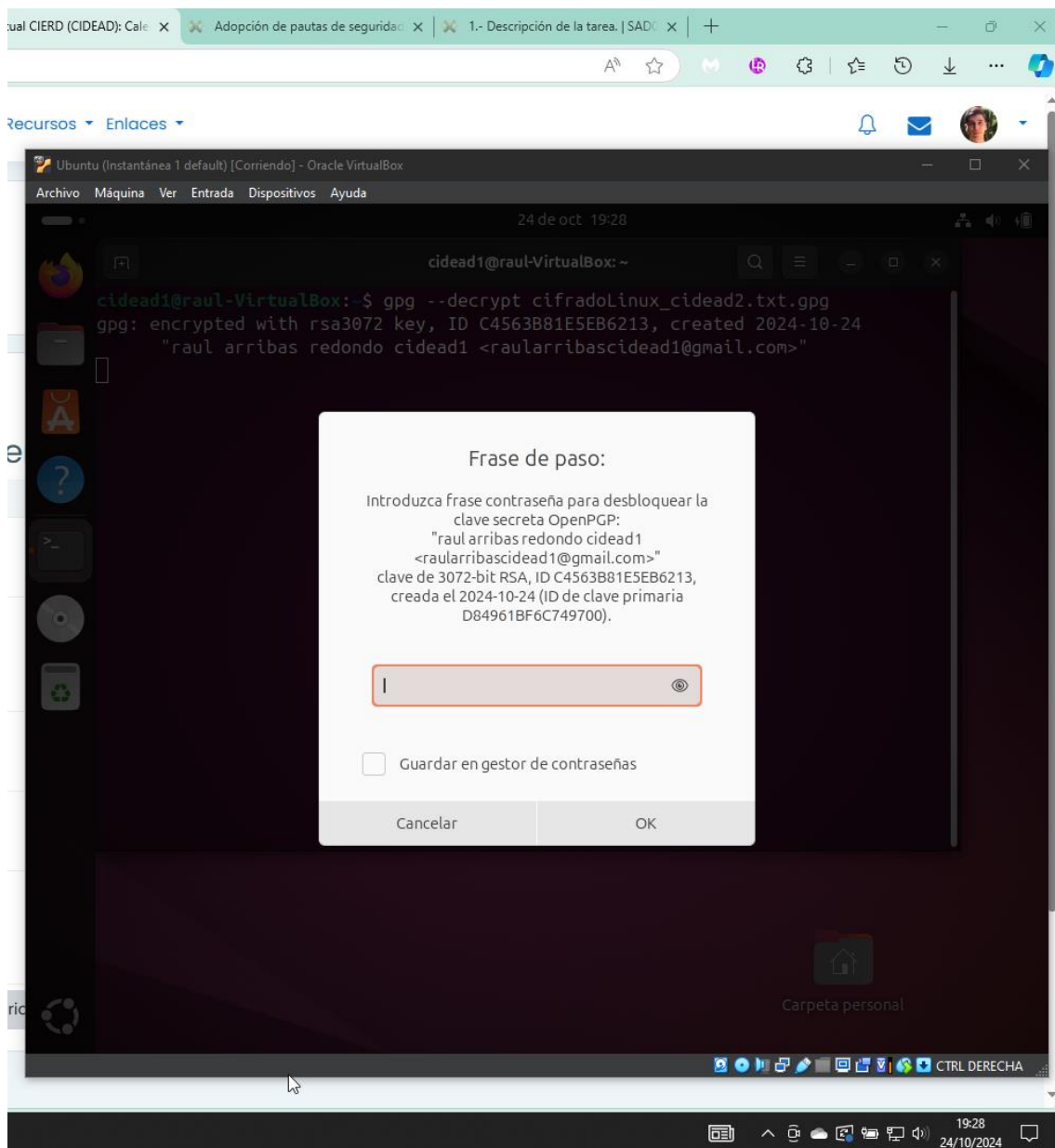
1.6 Descifra usando tu clave privada de cidead1, el documento cifradoLinux_cidead2.txt

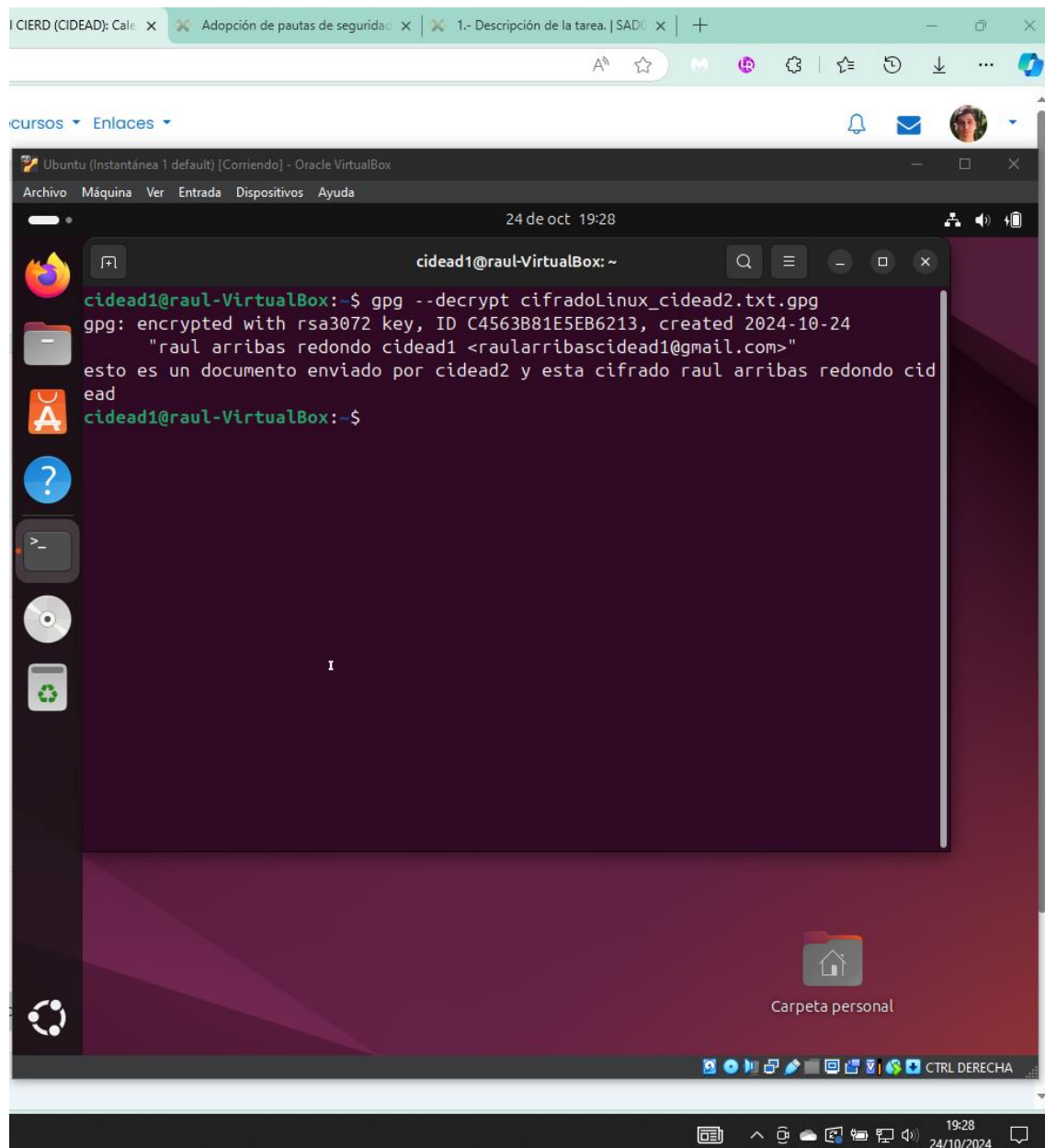
Ahora vamos a descifrar el documento con el usuario cidead1, primero vamos a pasarnos por algún medio el documento generado anteriormente al usuario cidead1.

- PARA COPIAR EL ARCHIVO AL USUARIO CIDEAD1: **sudo cp cifradoLinux_cidead2.txt.gpg /home/cidead1/**

Ahora vamos a descifrar el archivo con nuestra clave privada (la clave privada de cidead1), porque recordemos que para descifrar una clave publica, solo se puede hacer con nuestra privada.

gpg --decrypt cifradoLinux_cidead2.txt.gpg





The screenshot shows a web browser window at the top with several tabs open, including 'CIERD (CIDEAD): Cal...', 'Adopción de pautas de seguridad', and '1.- Descripción de la tarea. | SADO...'. Below the browser is a terminal window titled 'Ubuntu (Instantánea 1 default) [Corriendo] - Oracle VirtualBox'. The terminal shows a user named 'cideal1@raul-VirtualBox' running the command 'gpg --decrypt cifradoLinux_cideal2.txt.gpg'. The output of the command is displayed in green text: 'gpg: encrypted with rsa3072 key, ID C4563B81E5EB6213, created 2024-10-24', followed by a quoted message: '"raul arribas redondo cideal1 <raularribascideal1@gmail.com>"', and then a line of text: 'esto es un documento enviado por cideal2 y esta cifrado raul arribas redondo cideal1'. The terminal prompt is 'cideal1@raul-VirtualBox:~\$'. The background of the terminal window shows the Ubuntu desktop environment with a purple and red gradient, a sidebar with application icons, and a taskbar at the bottom with system icons and the date '24 de oct 19:28'.

```
cideal1@raul-VirtualBox:~$ gpg --decrypt cifradoLinux_cideal2.txt.gpg
gpg: encrypted with rsa3072 key, ID C4563B81E5EB6213, created 2024-10-24
"raul arribas redondo cideal1 <raularribascideal1@gmail.com>"
esto es un documento enviado por cideal2 y esta cifrado raul arribas redondo cideal1
cideal1@raul-VirtualBox:~$
```

Podemos observar cómo nos deja desencriptarlo correctamente y ver el mensaje en texto legible que habíamos puesto antes.

2 APARTADO 2: GPG WINDOWS

Usando la herramienta **GPG4Win** para Windows, lleva a cabo las siguientes acciones relacionadas con la criptografía asimétrica:

2.1 Crea en la máquina Windows dos usuarios distintos llamados **cidead1** y **cidead2**, estableciendo para cada uno de ellos una contraseña segura.

Primero vamos a crear los dos usuarios con sus respectivas contraseñas.

Se puede hacer de varias formas, nosotros lo vamos a realizar mediante la consola de comandos CMD.

Ejecutamos CMD en modo administrador y ponemos lo siguientes comandos:

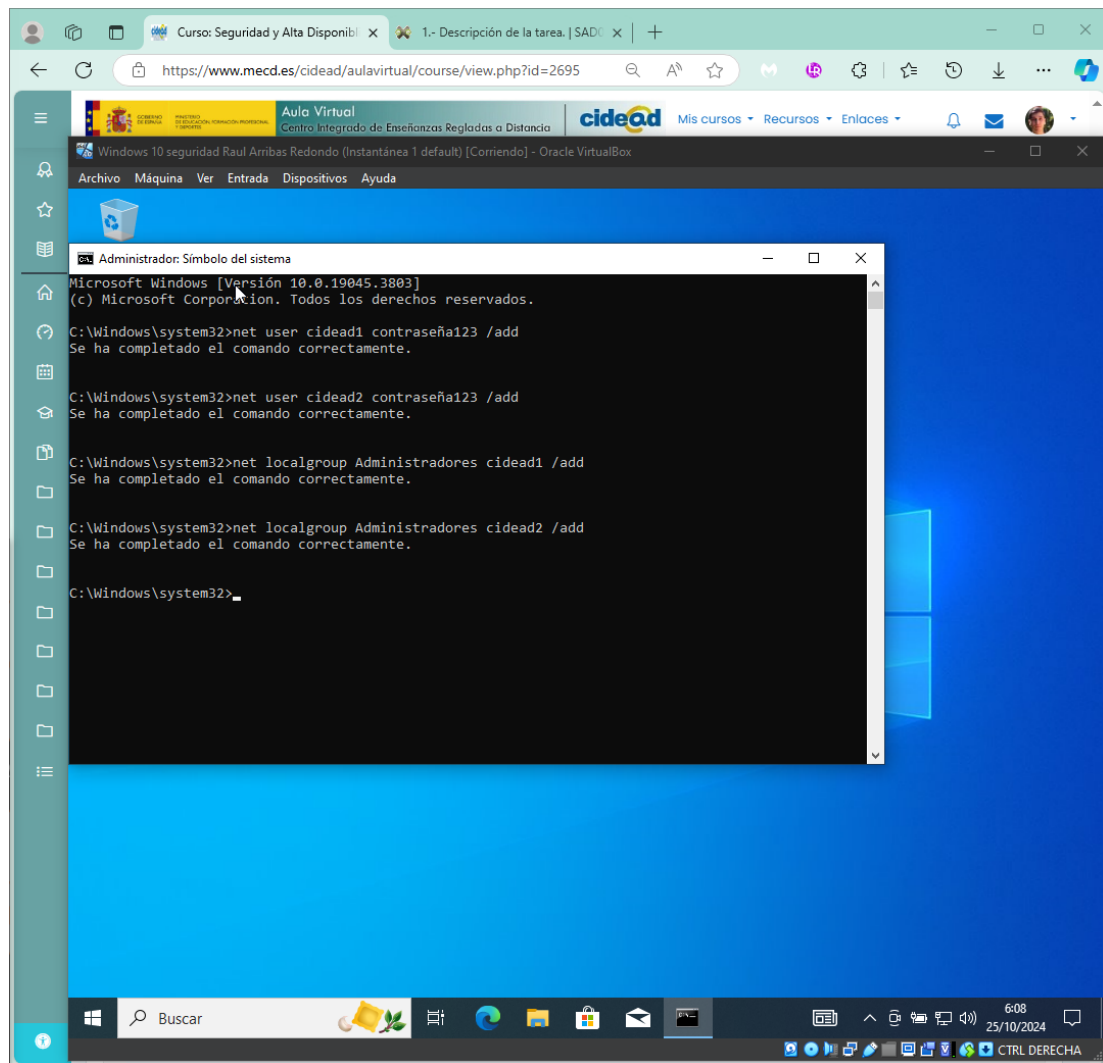
```
Net user cidead1 contraseña123 /add
```

```
Net user cidead2 contraseña123 /add
```

También les agregamos como administradores a los dos usuarios:

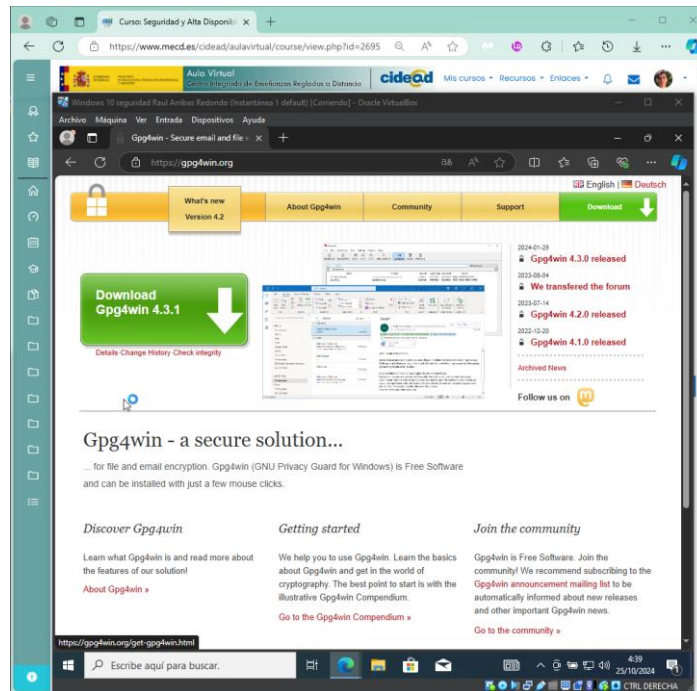
```
Net localgroup Administradores cidead1 /add
```

```
Net localgroup Administradores cidead2 /add
```

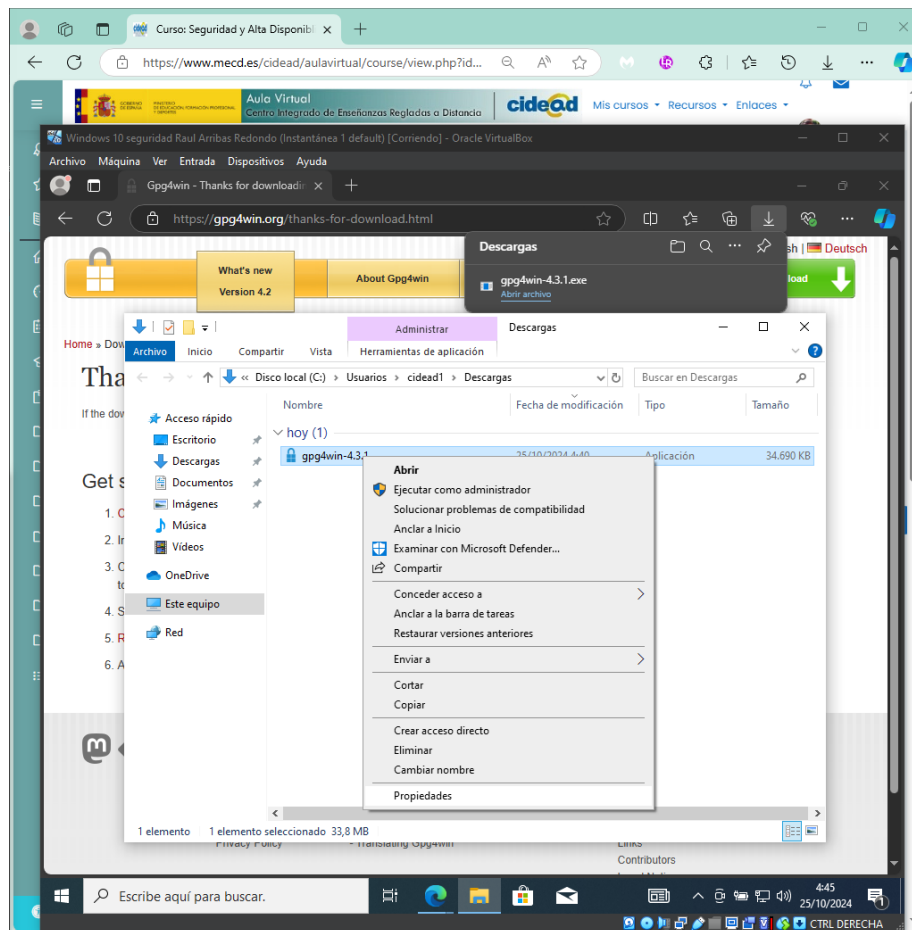


2.2 Para el usuario cidead1, crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, `openpgp`.

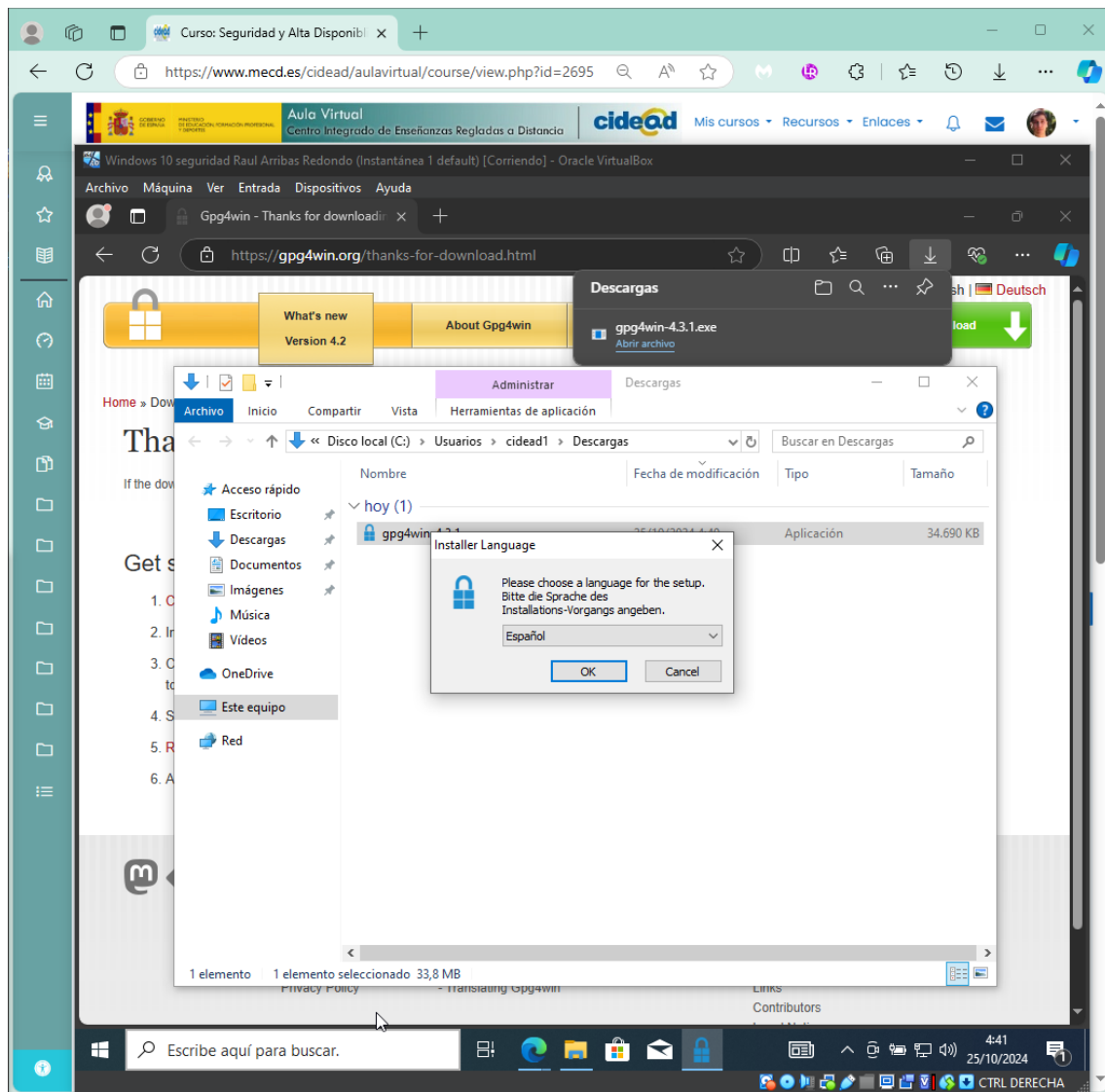
Ahora nos cambiamos de usuario a Cidead1 y nos descargamos e instalamos la aplicación de `gpg4win` (`gpg4win.org`), seguimos los pasos de las imágenes. Esto también hay que hacerlo con el usuario Cidead2.



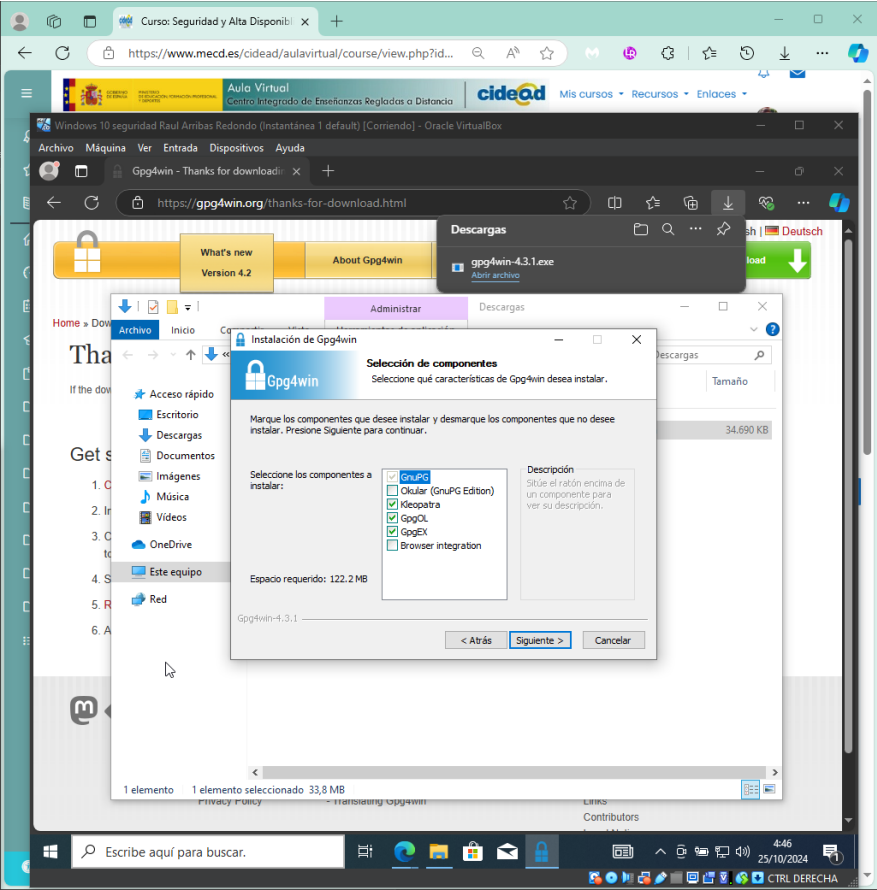
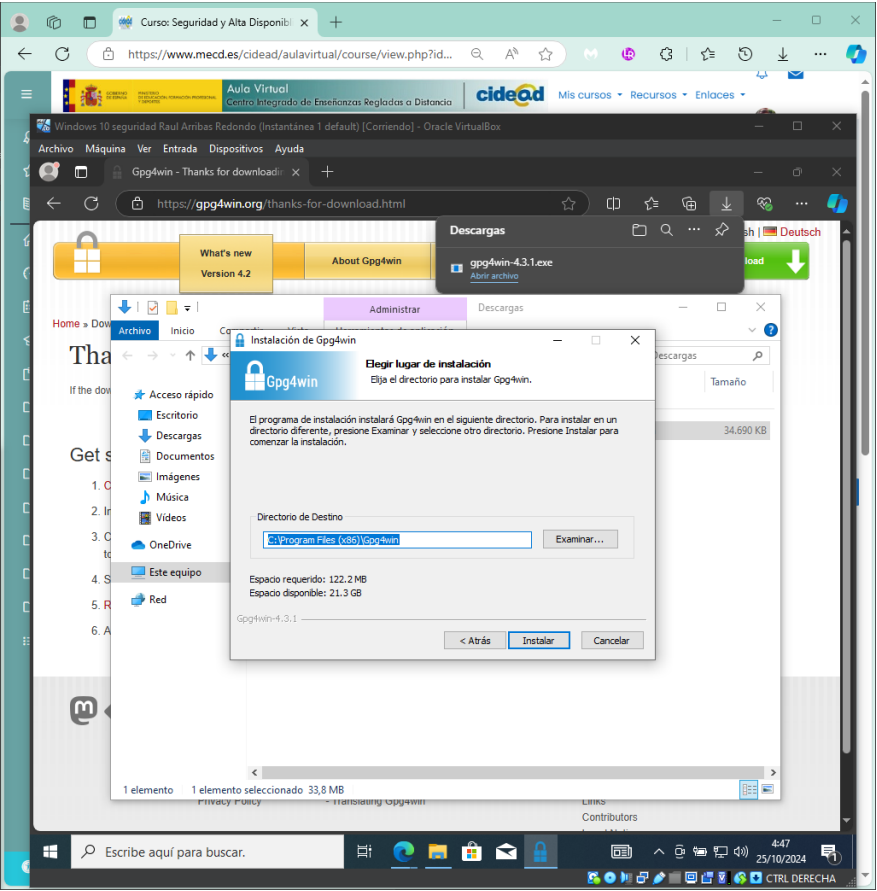
Ejecutamos el instalador y le damos click derecho y abrir



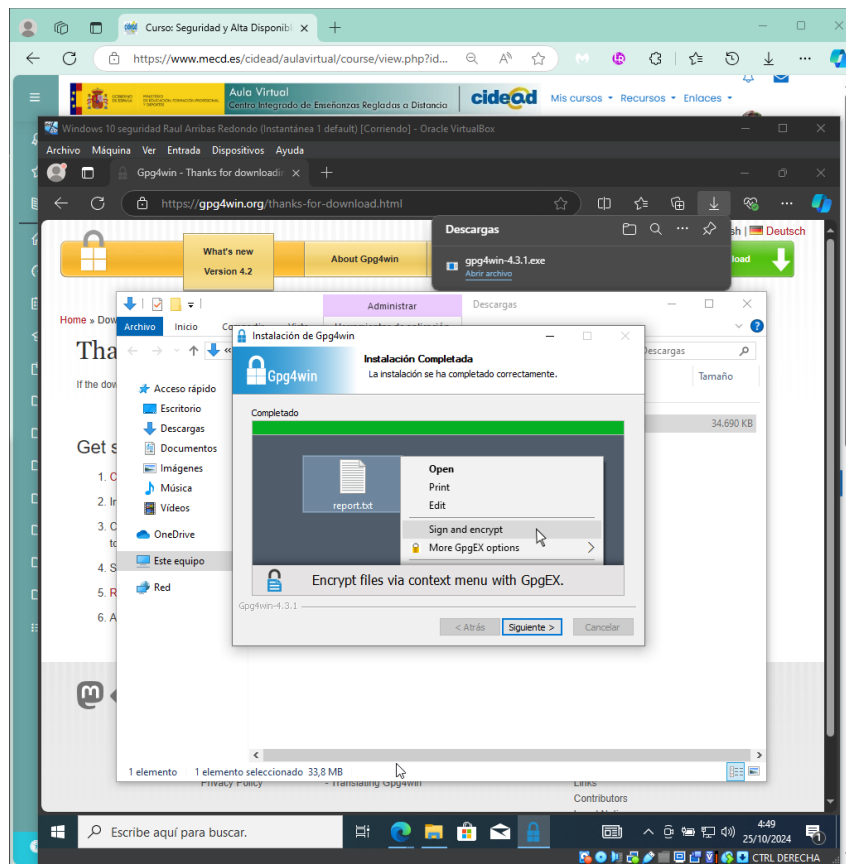
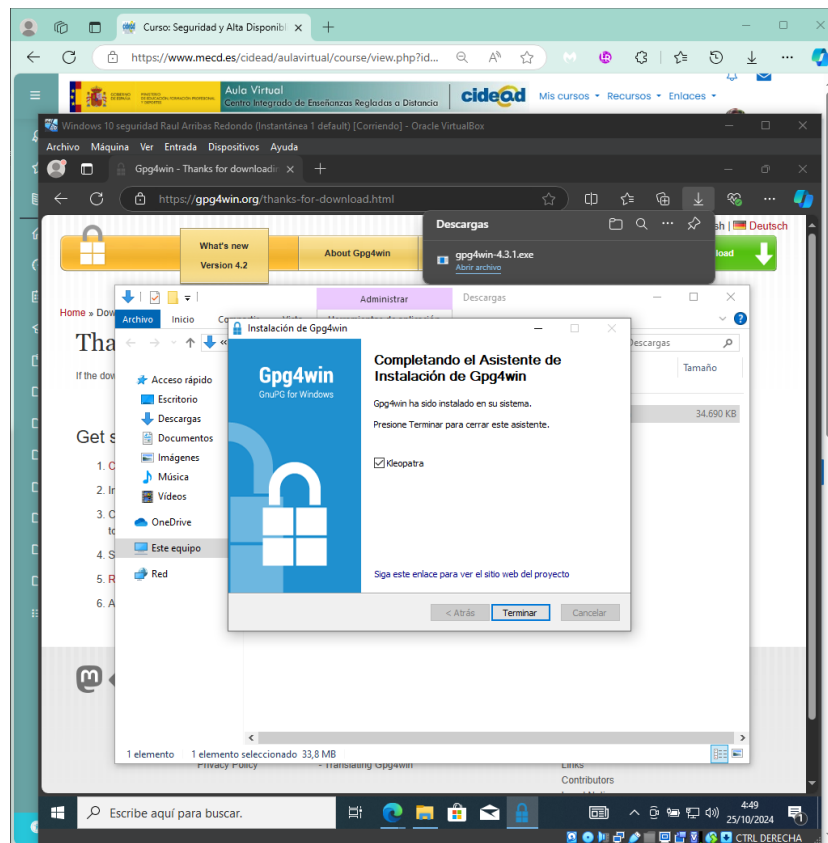
Una vez ejecutado nos saldrá un asistente de instalación en el cual tenemos que escoger idioma y aceptar los términos y condiciones.



Seleccionamos los componentes que vienen por defecto y elegimos la ruta donde lo queremos instalar.



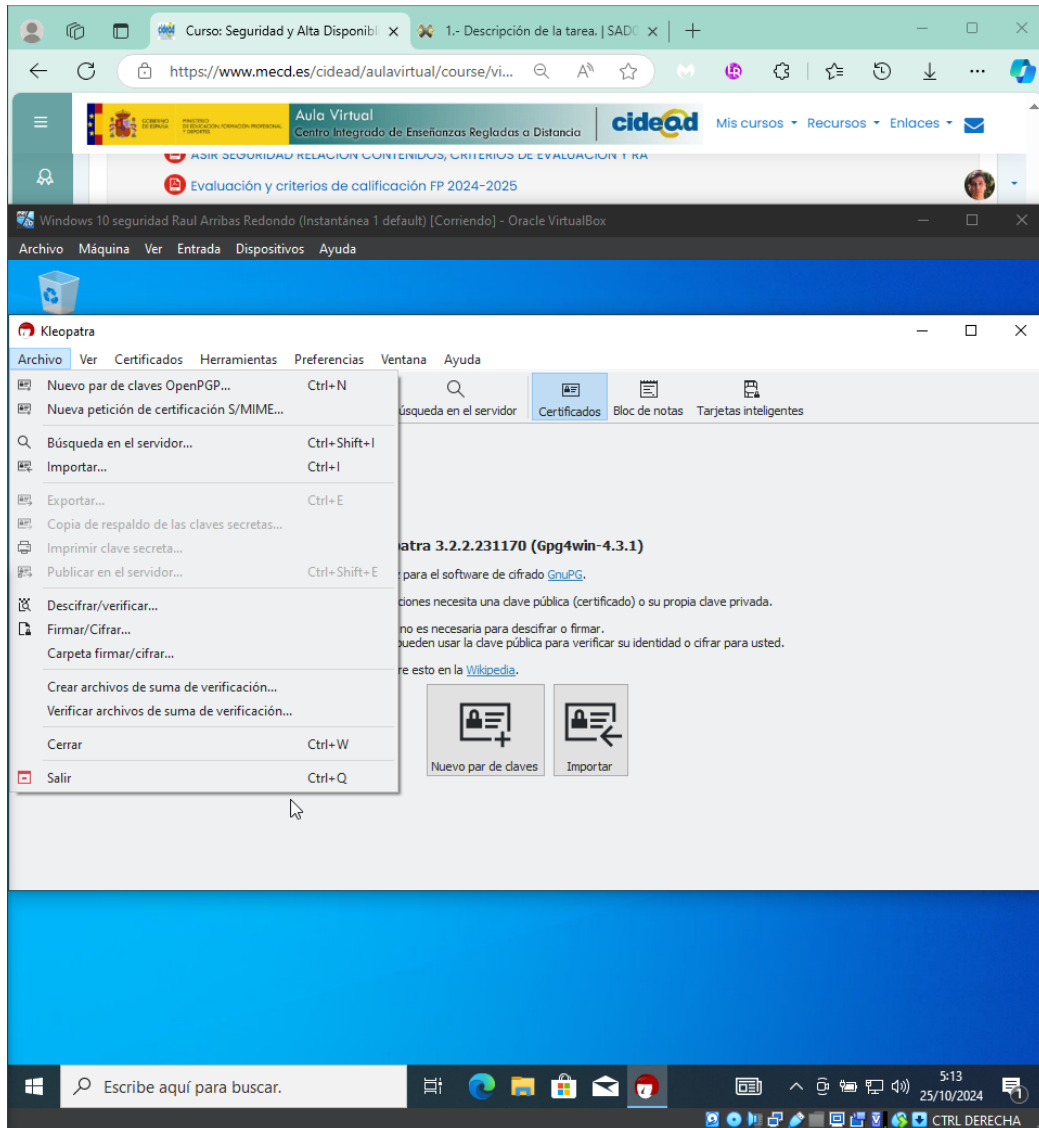
Una vez completado le damos en terminar e iniciamos Kleopatra.



2.2.1 Creamos las claves de los usuarios Cidead1 y Cidead2

El paso anterior lo tenemos que hacer también con el usuario Cidead2, una vez lo hemos hecho con los usuarios creamos las claves abriendo la aplicación de kleopatra.

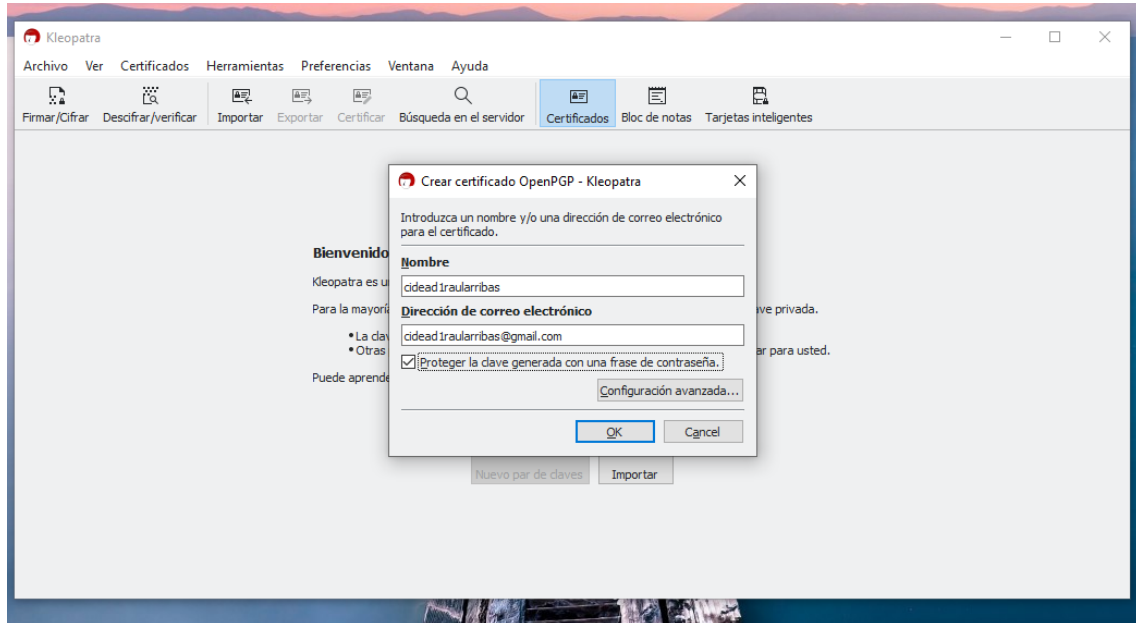
Una vez abierta seleccionamos **Archivo** → **Nuevo par de claves OpenPGP**



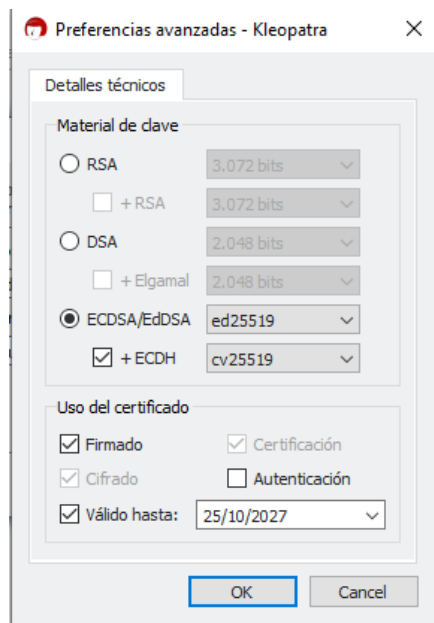
Introducimos los datos que son requeridos, seleccionamos proteger la clave generada con una contraseña:

Nombre: cidead1raularribas

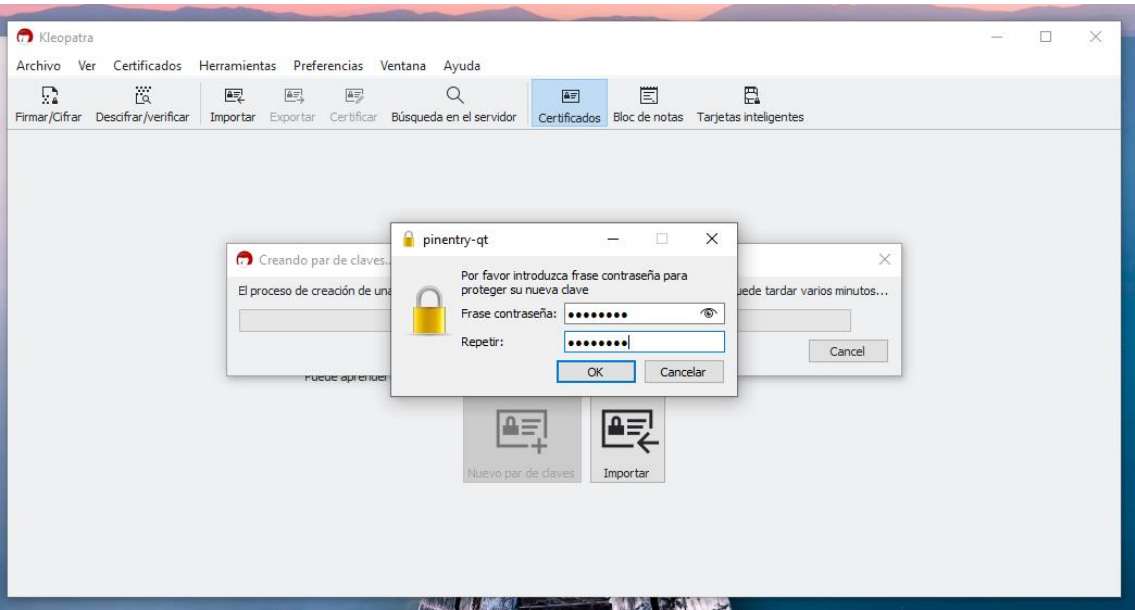
Correo: cidead1raularribas@gmail.com



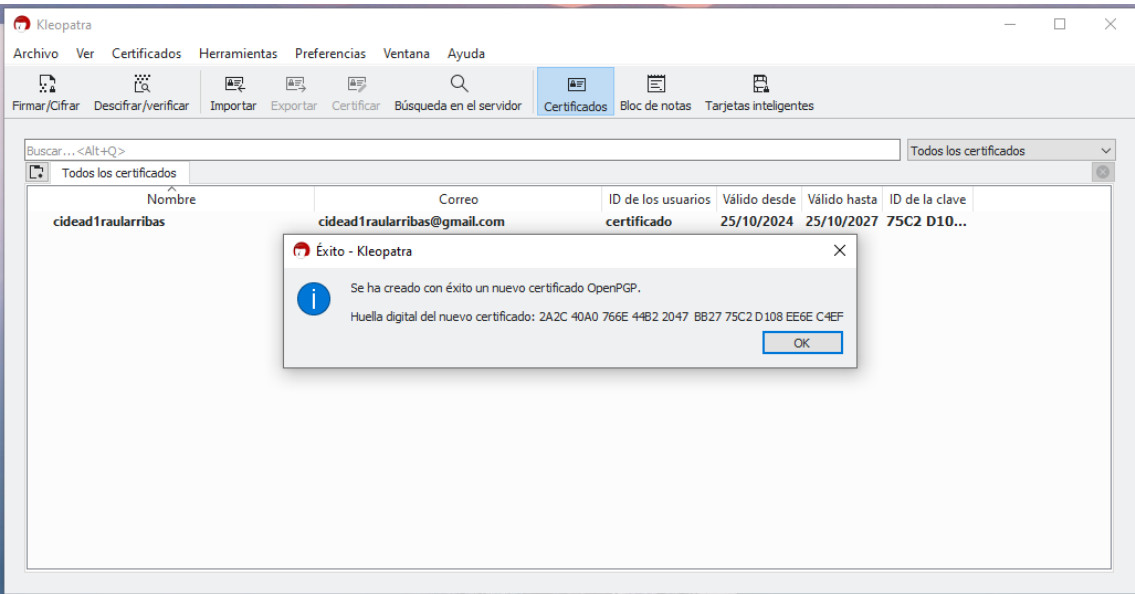
En opciones avanzadas podemos seleccionar si lo queremos cifrar con otro método y la fecha de validez:



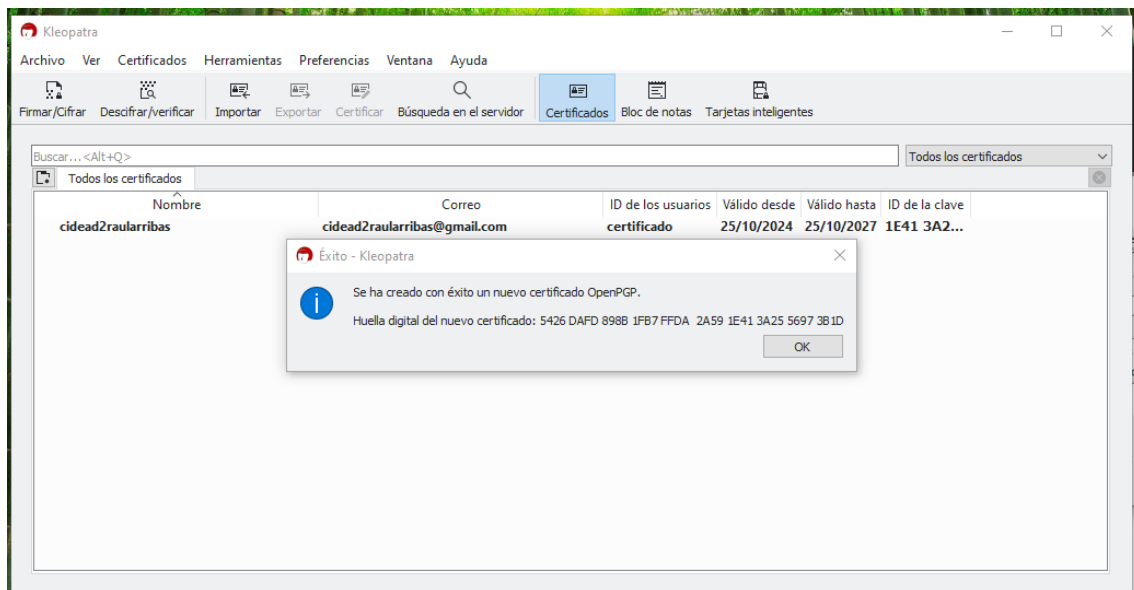
Cuando le demos a crear nos pedirá una contraseña para proteger la nueva clave que hemos creado:



Nos confirma que las claves se han creado correctamente y nos muestra nuestra huella digital, le damos a ok.



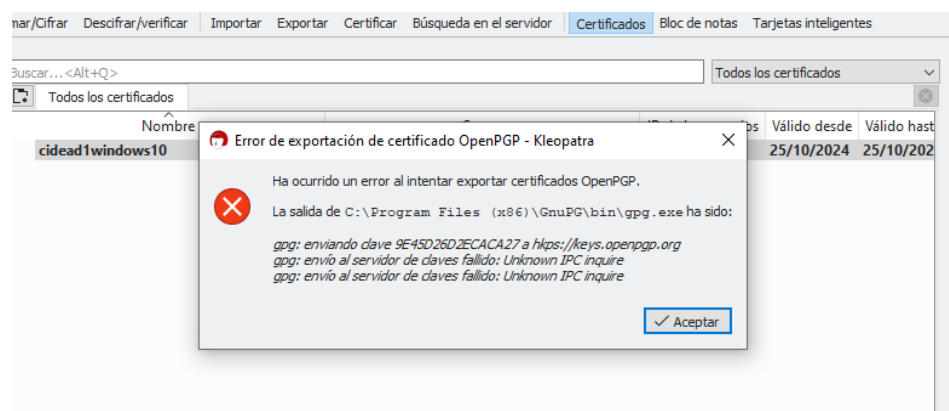
Hacemos los mismos pasos con Cidead2:



2.2.2 Publicamos la clave en el servidor keyserver.ubuntu.com

Una vez creada tenemos que publicarla en el servidor, podemos darle click derecho y publicarla

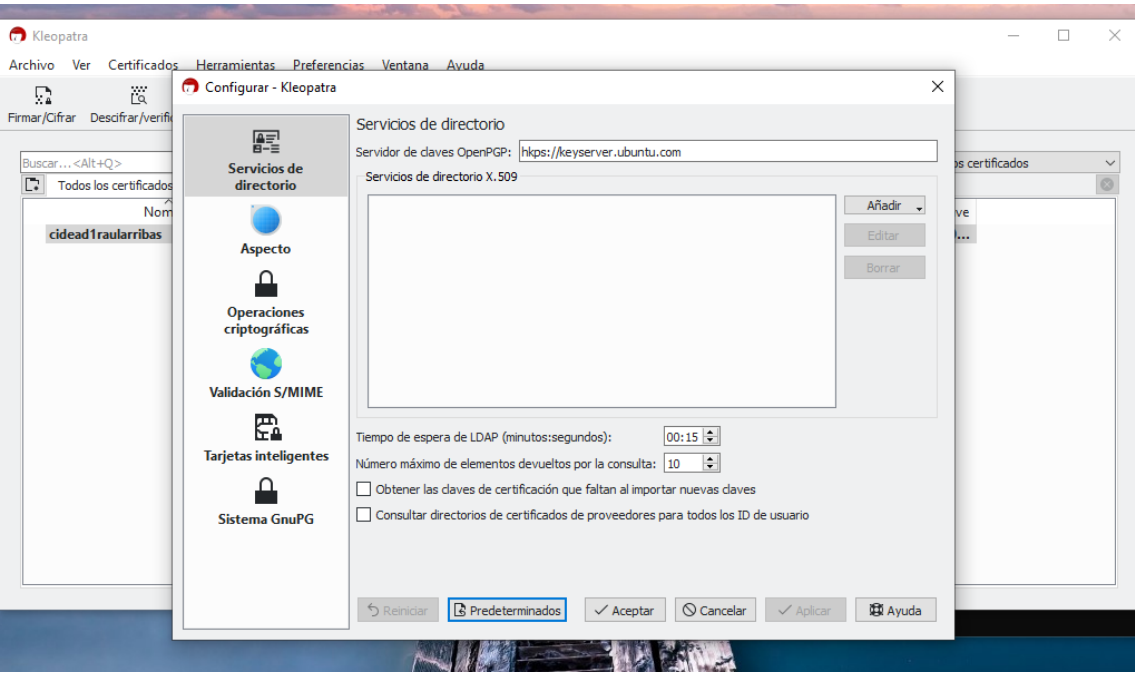
IMPORTANTE: Como no me funciona desde una máquina virtual (desde la maquina real sí que funciona bien) voy a crear 2 usuarios en mi maquina real y voy repetir lo pasos, las huellas digitales no van a coincidir con las capturas anteriores pero el procedimiento es el mismo.



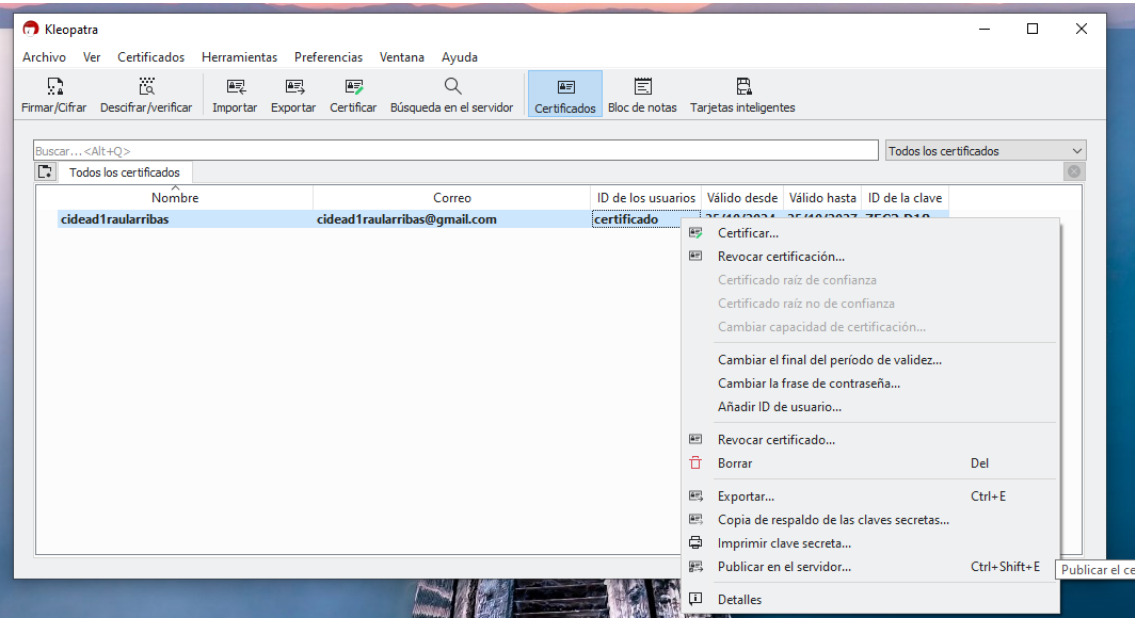
Cidead1:

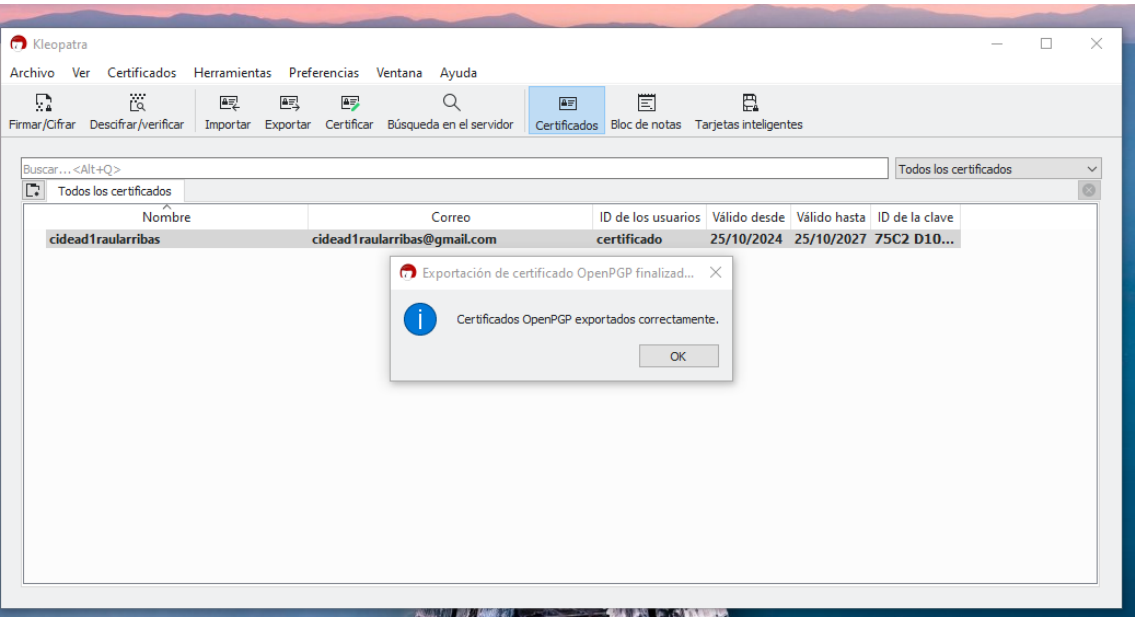
Una vez estamos dentro del usuario cidead1 vamos a preferencias para poner el servidor de Ubuntu donde vamos a subir la clave pública.

Preferencias → Configurar Kleopatra



Una vez tenemos esa configuración, damos click derecho a la clave y Publicar en el servidor:

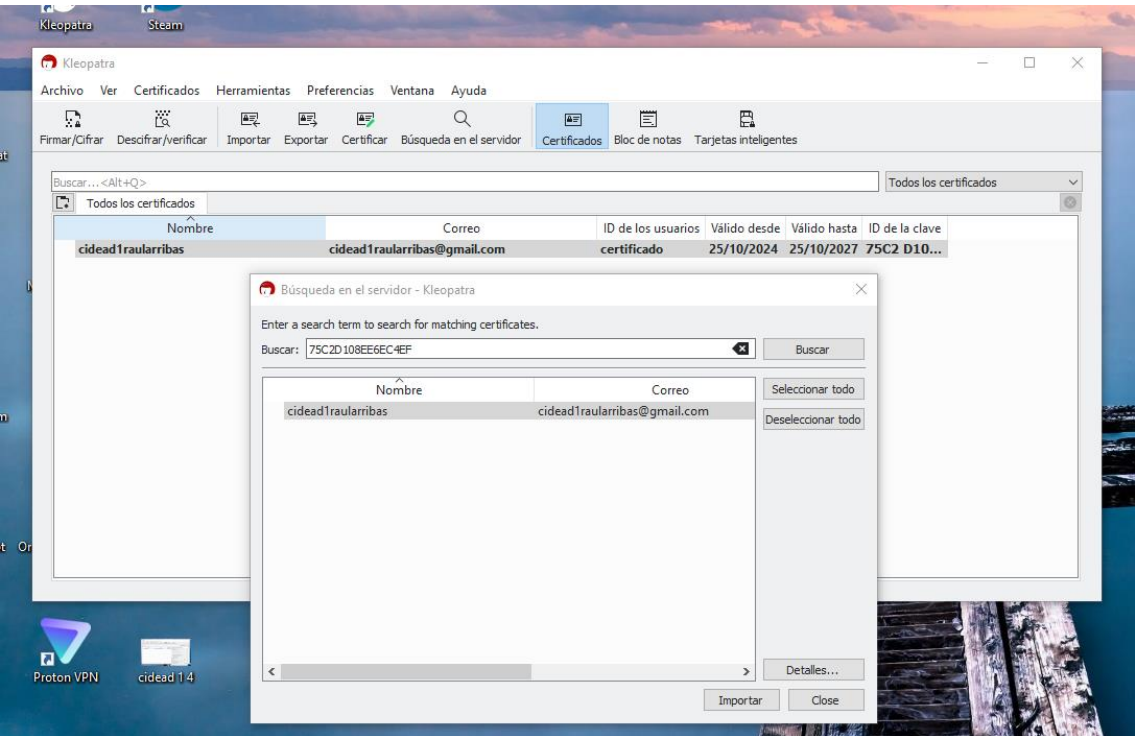




Después comprobamos la clave que está en el servidor correctamente.

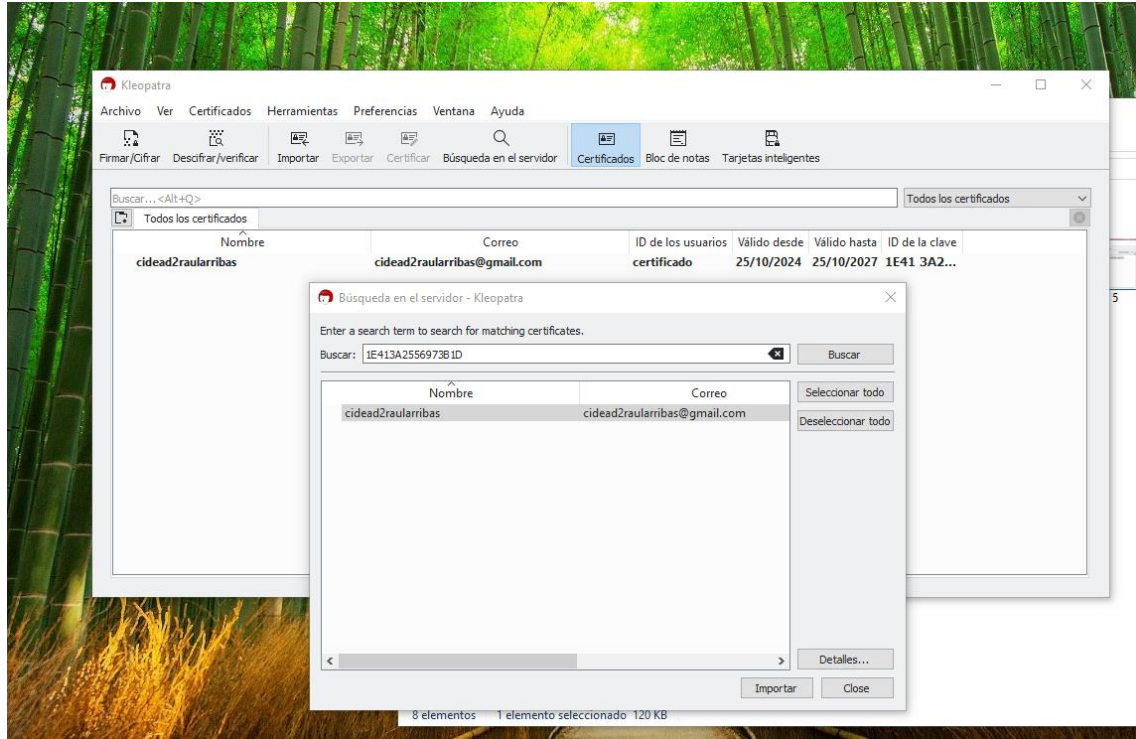
Para comprobar la ID que tenemos para después buscar y verificar que existe podemos abrirnos un CMD y poner los siguientes comandos:

gpg --list-keys --keyid-format LONG



Hacemos los mismos pasos con Cidead 2, configuramos el servidor de Ubuntu desde **preferencias → configurar Kleopatra**

Después publicamos la clave en el servidor y comprobamos que efectivamente se encuentra en el servidor de Ubuntu:



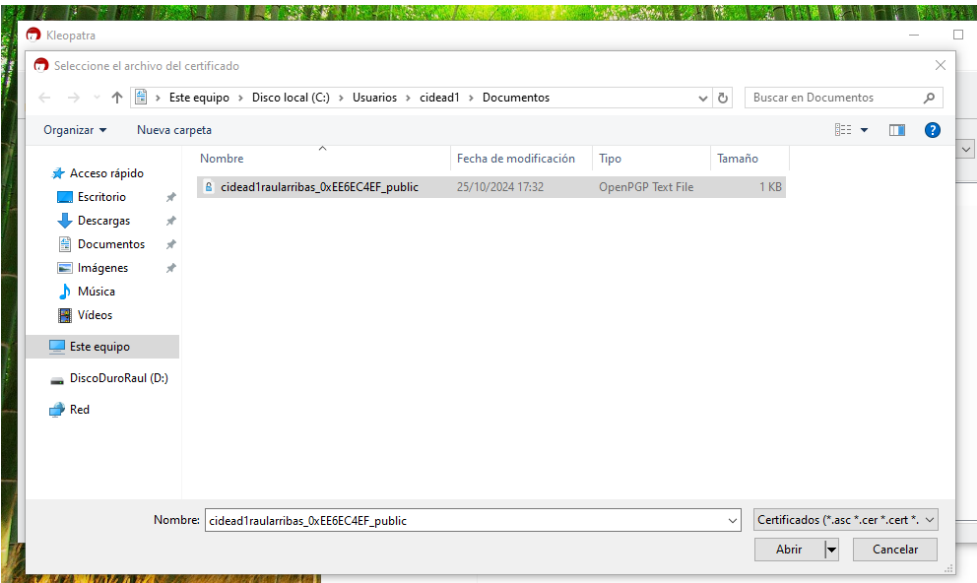
2.3 Importa desde RedIris al anillo de claves del usuario cidead2, la clave pública de cidead1. Muestra el anillo de claves resultante de cidead2. Primero tenemos que exportar la clave pública de **cidead1** para ello nos vamos al usuario **cidead1** y dentro de Kleopatra:

Click derecho en la clave → Exportar

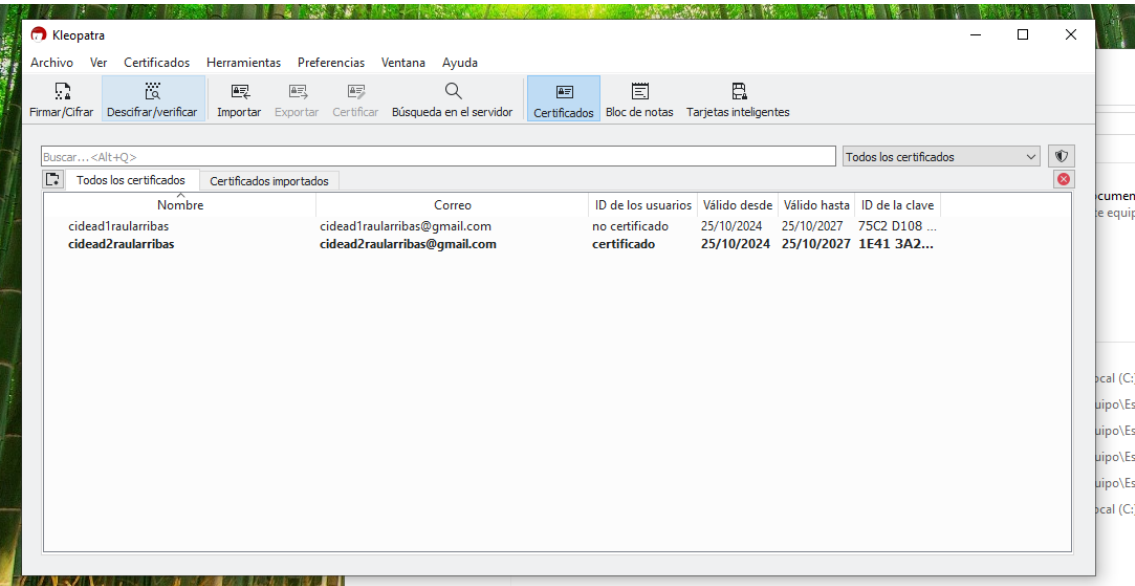
Cuando la tengamos exportada entonces tenemos que importarla desde el usuario **Cidead2**:

Archivo → Importar → seleccionamos la clave que hemos exportado antes (te la puedes pasar por correo o por otro medio).

Le damos a abrir para que se complete la importación:

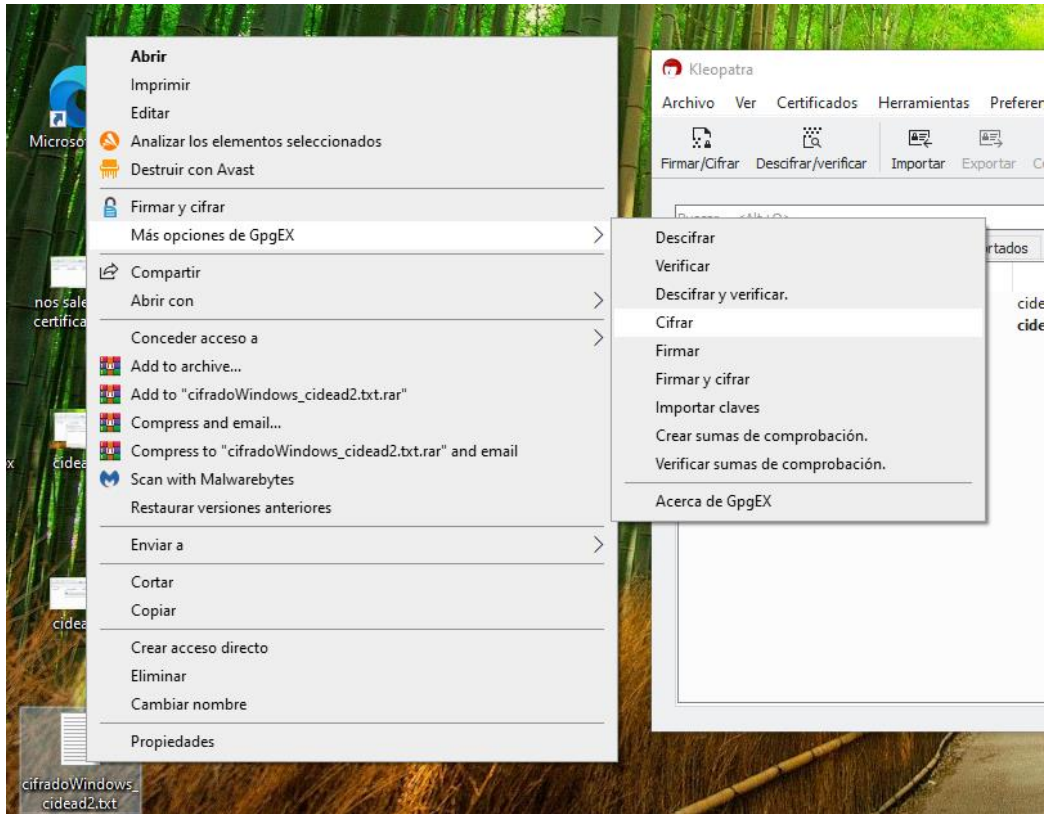


Nos debería de salir así desde el usuario Cidead2:

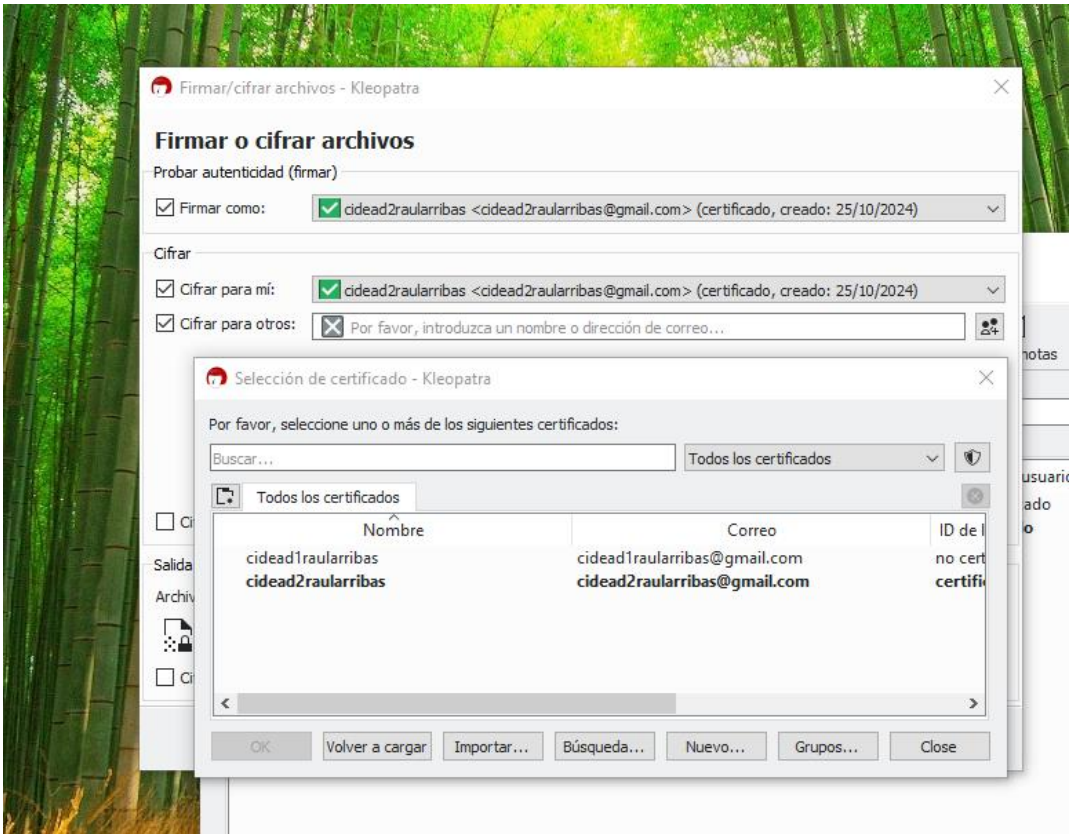
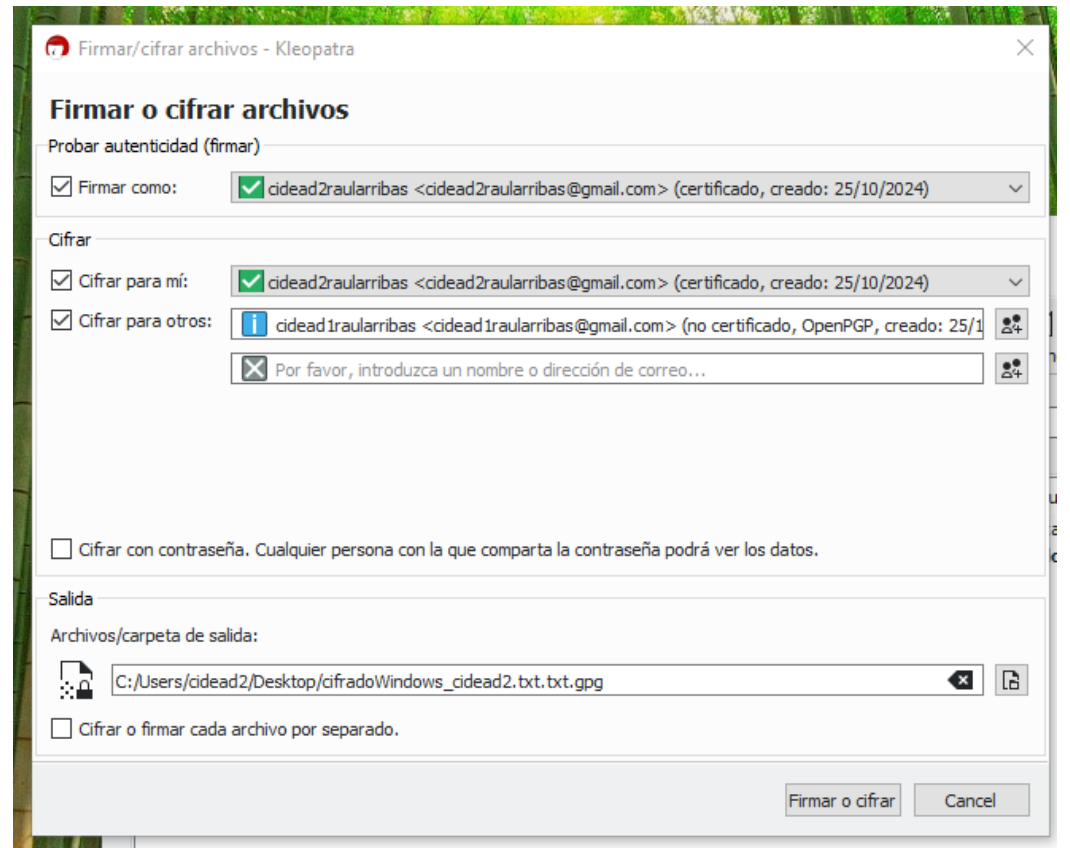


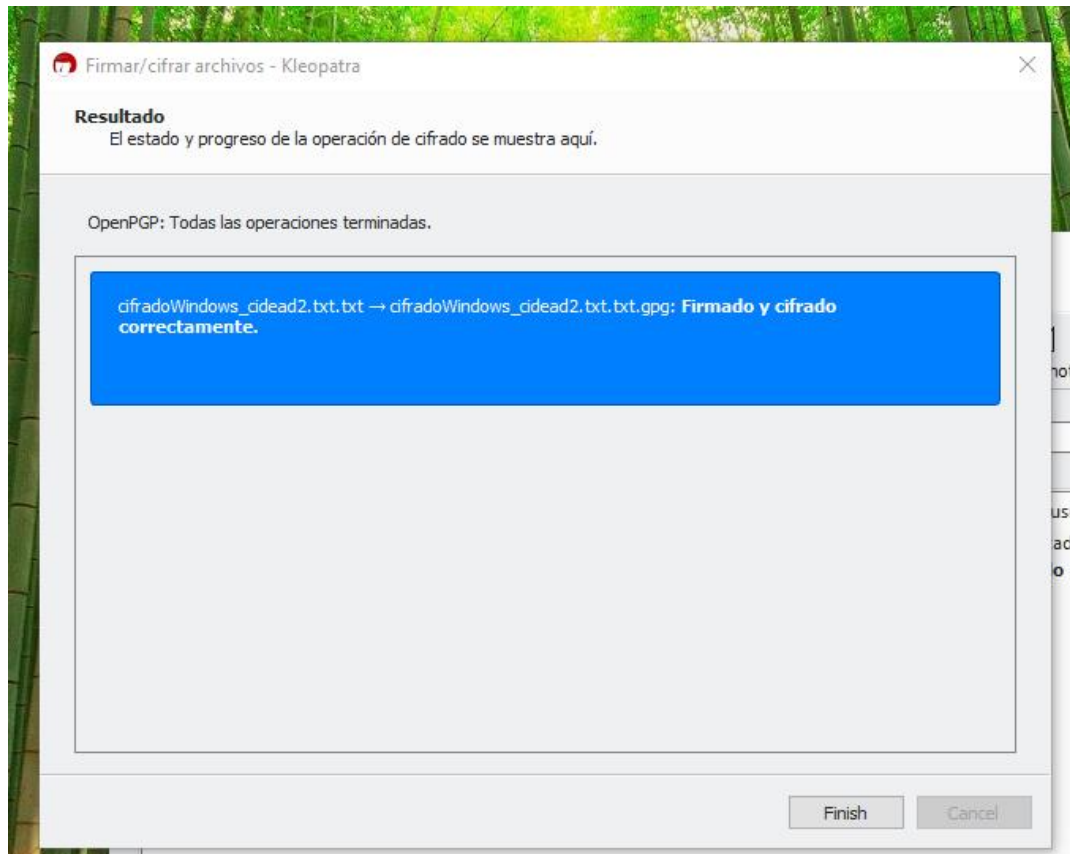
- 2.4 Genera un documento de texto cifradoWindows_cidead2.txt. Cífralo con la clave pública de cidead1. Envía por algún medio, el documento cifrado al usuario cidead1.

Creamos el documento txt y lo ciframos:



Una vez le demos a cifrar nos saldrá esta pantalla, tenemos que agregar la clave publica que previamente hemos importado de Cidead1:



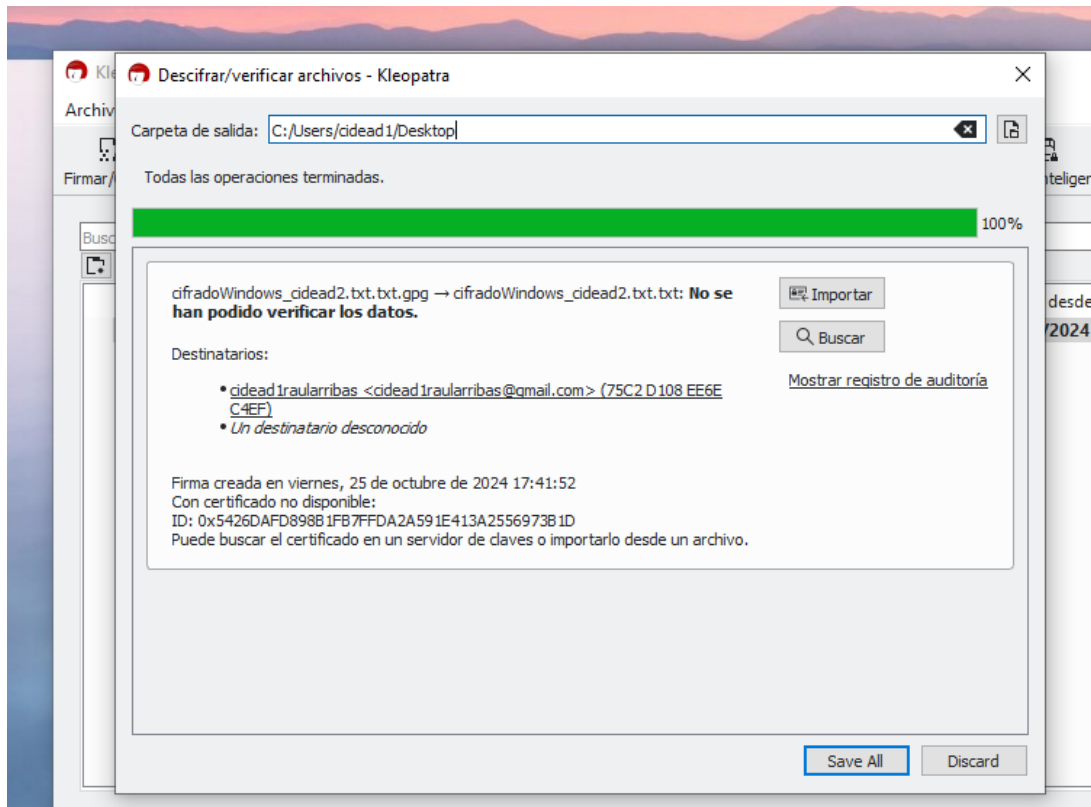


Una vez cifrado, se nos generará un nuevo archivo, lo enviamos por algún medio al usuario Cidead1, si lo hemos hecho bien solamente Cicead1 podrá descifrar el archivo con su clave privada.

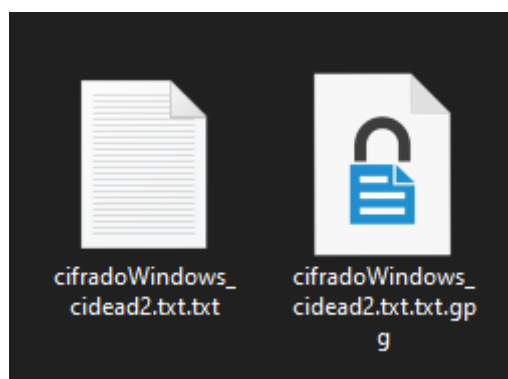
2.5 Descifra usando tu clave privada de cidead1, el documento cifradoWindows_cidead2.txt.

Ahora que ya tenemos el documento de texto que generó cidead2, para descifrarlo tenemos que darle click derecho y darle a Descifrar.

Le damos en Save all para que nos guarde el fichero original y lo podamos leer.



Cuando lo descifremos tendremos el fichero cifrado y el fichero ya en texto plano:

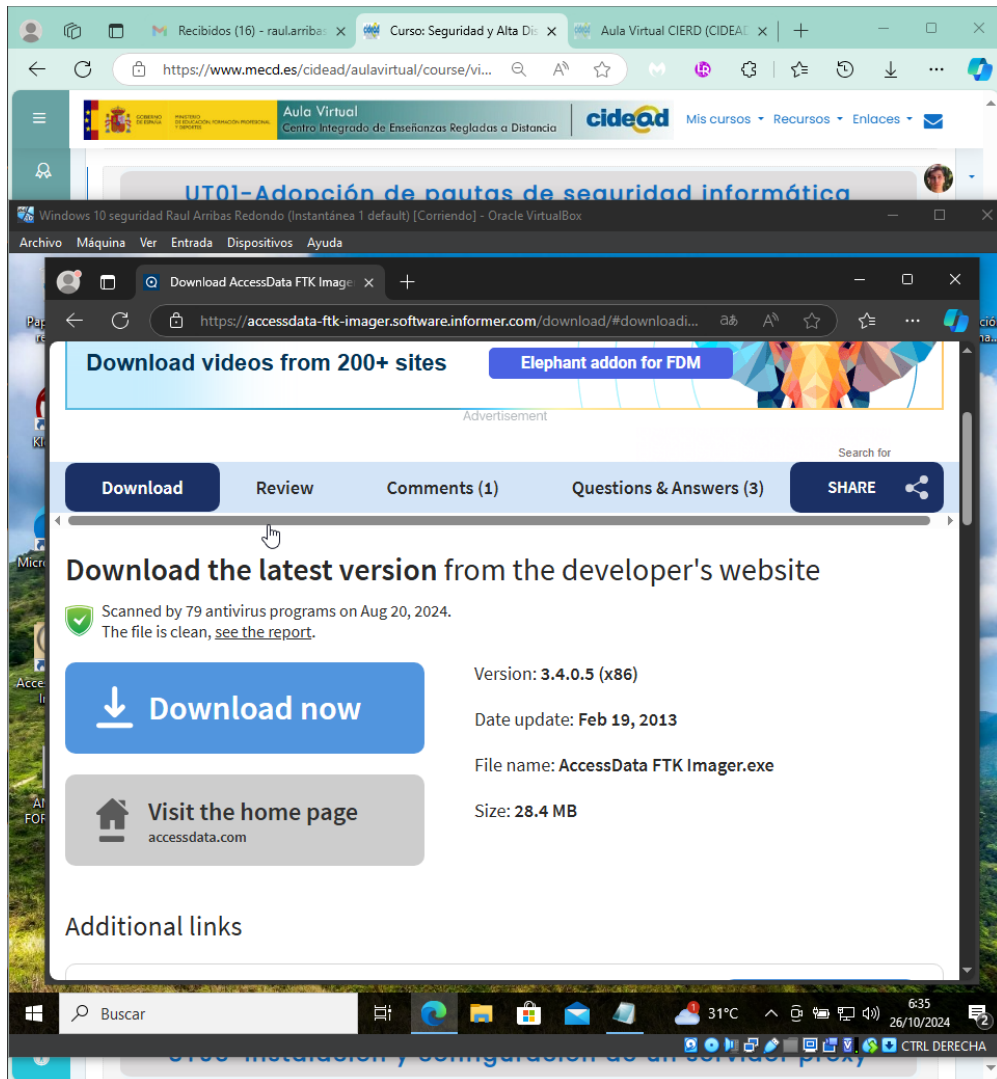


3 Apartado 3: Análisis Forense.

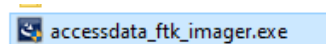
3.1 Instala y configura una herramienta para la realización de evidencias digitales (por ejemplo, Access Data Forense Toolkit), sobre una máquina Windows.

En primer lugar, nos vamos a descargar la herramienta que vamos a utilizar desde este enlace:

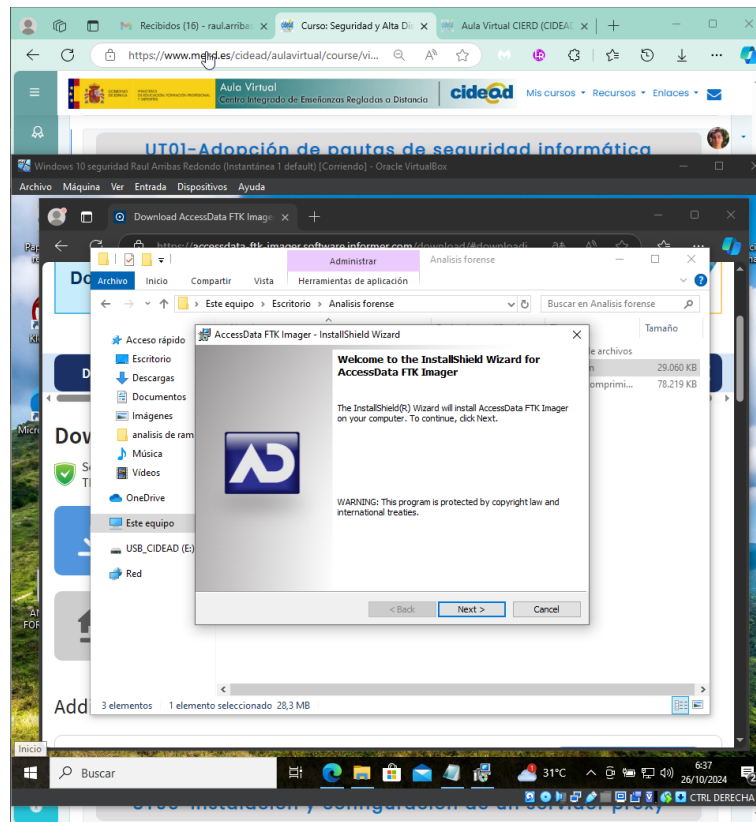
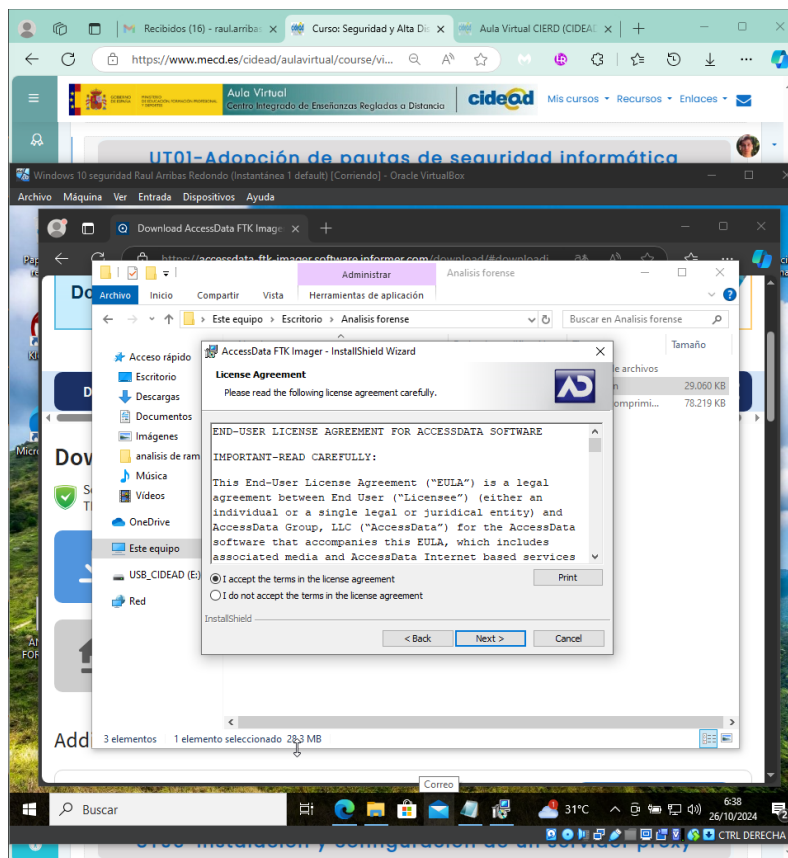
<https://accessdata-ftp-imager.software.informer.com/download/#downloading>

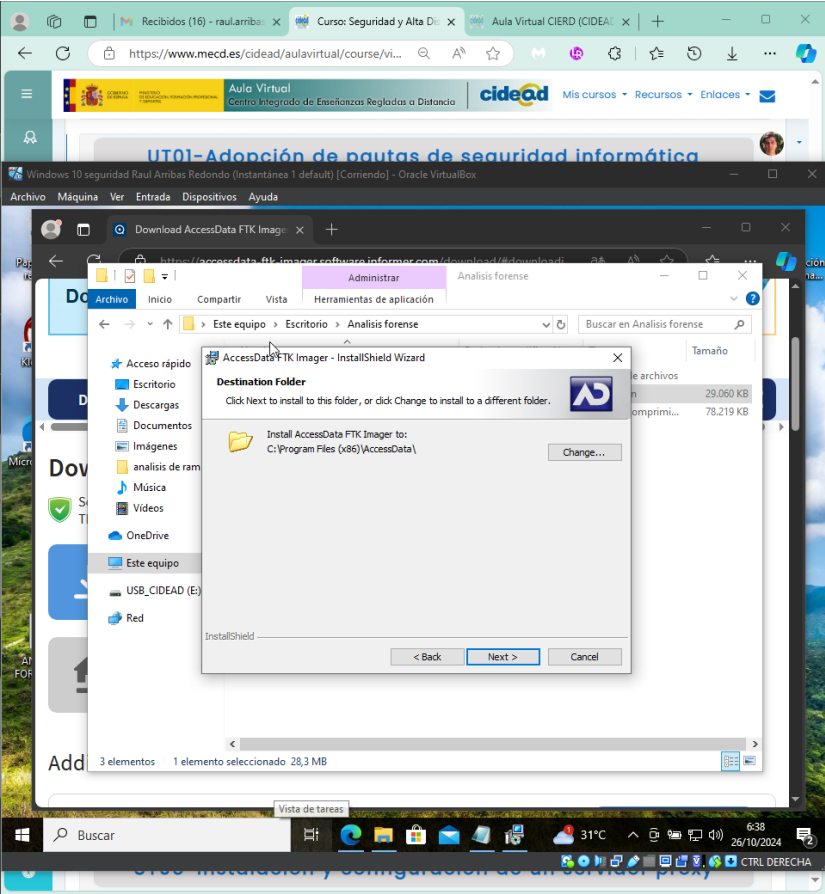
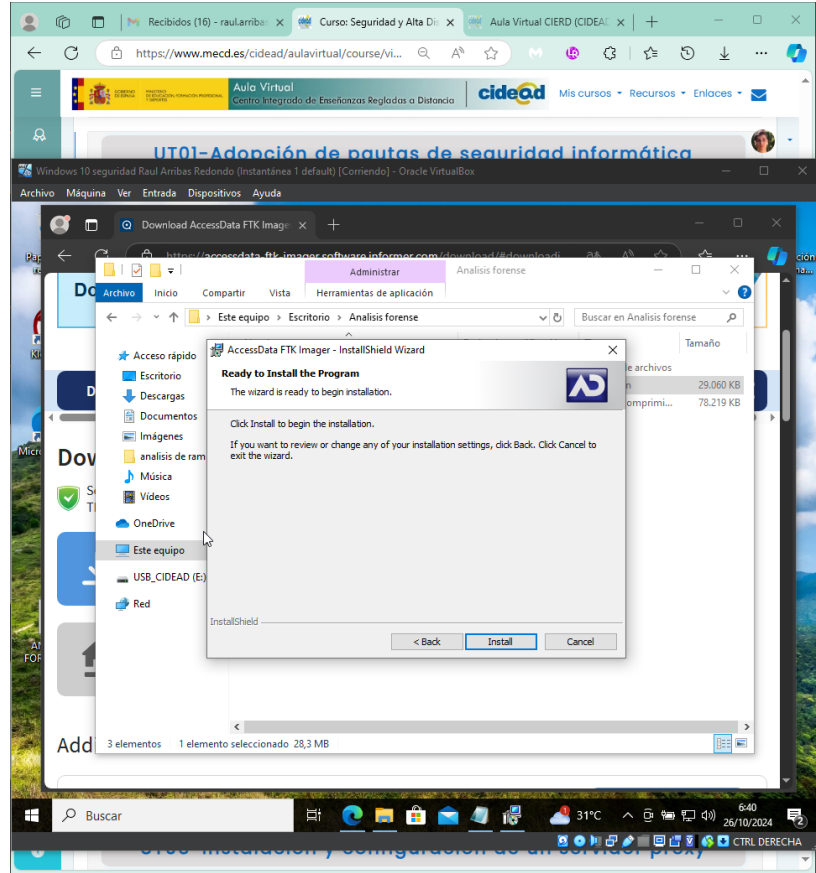


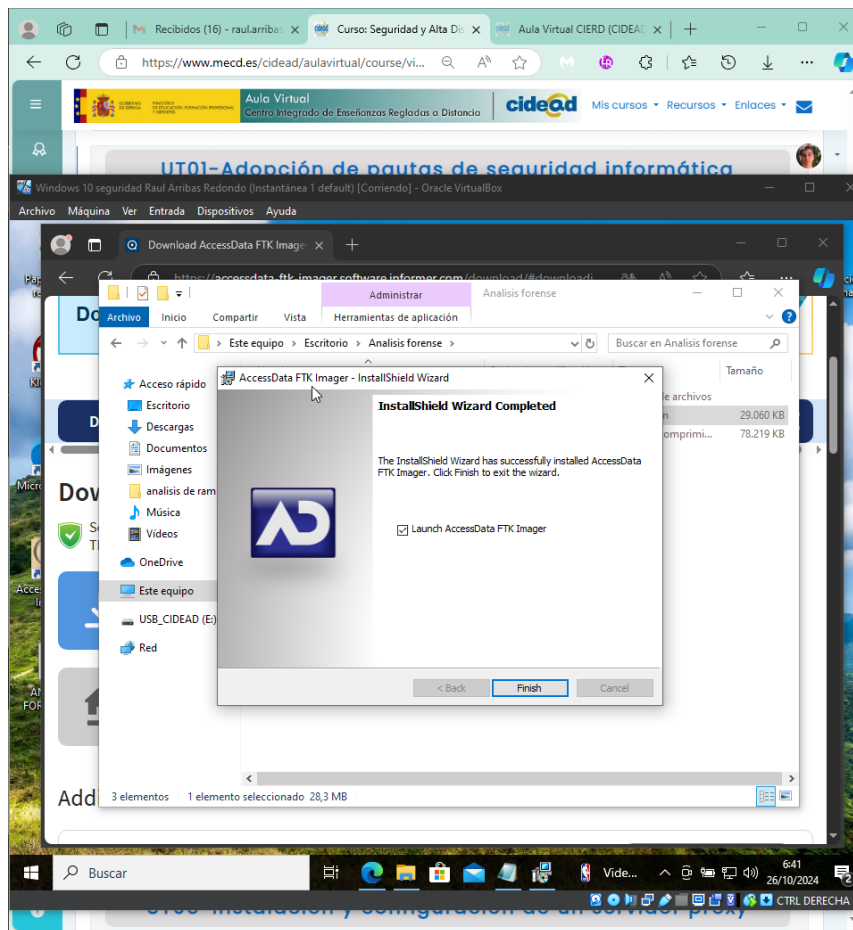
Una vez la tenemos descargada la ejecutamos como administrador:



Le damos siguiente y aceptamos los términos y condiciones y elegimos la ruta donde queremos instalarlo:



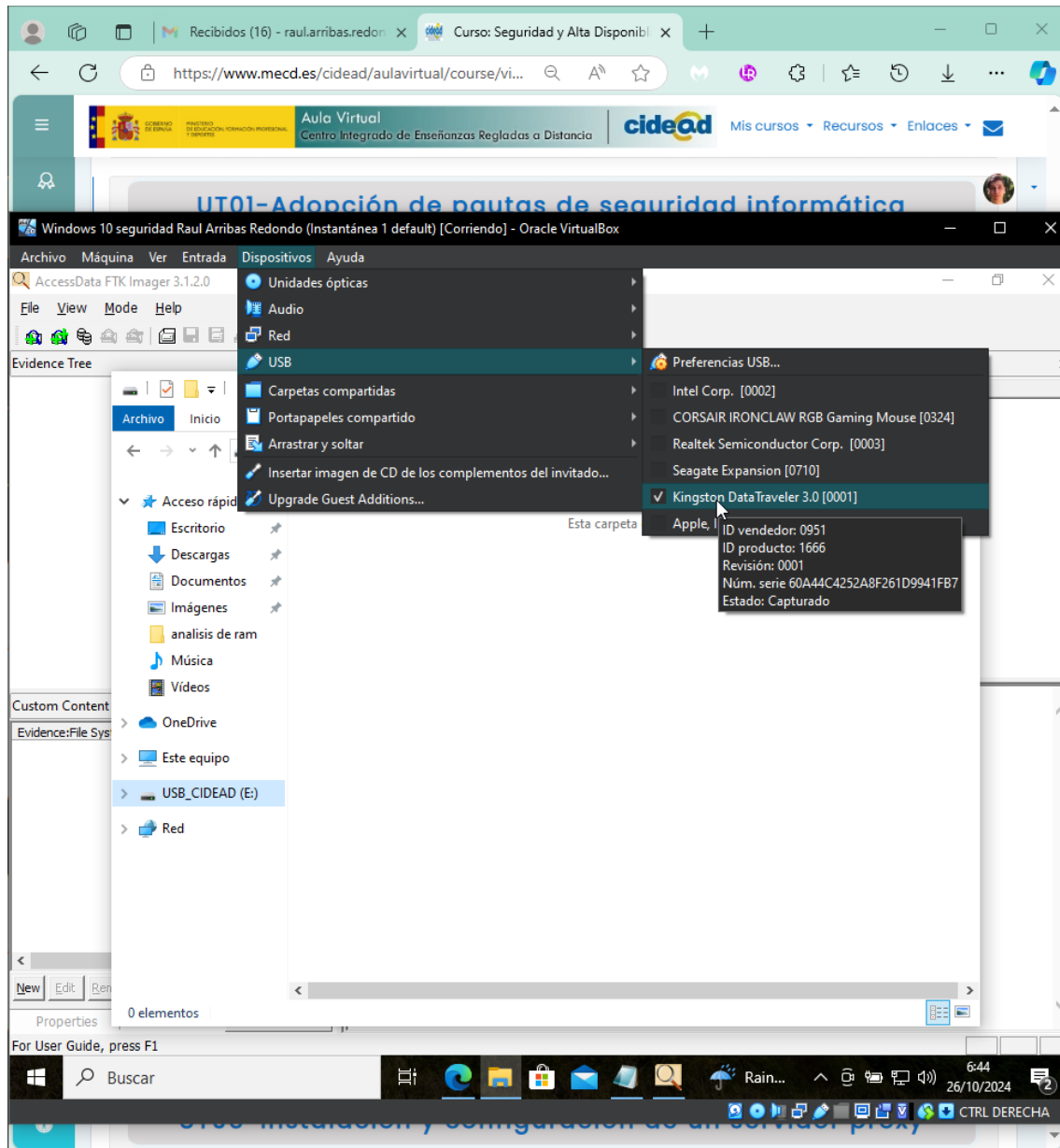




3.2 Crea una imagen como evidencia de una unidad USB sobre la que previamente has debido borrar algunos ficheros que deberás recuperar usando la imagen.

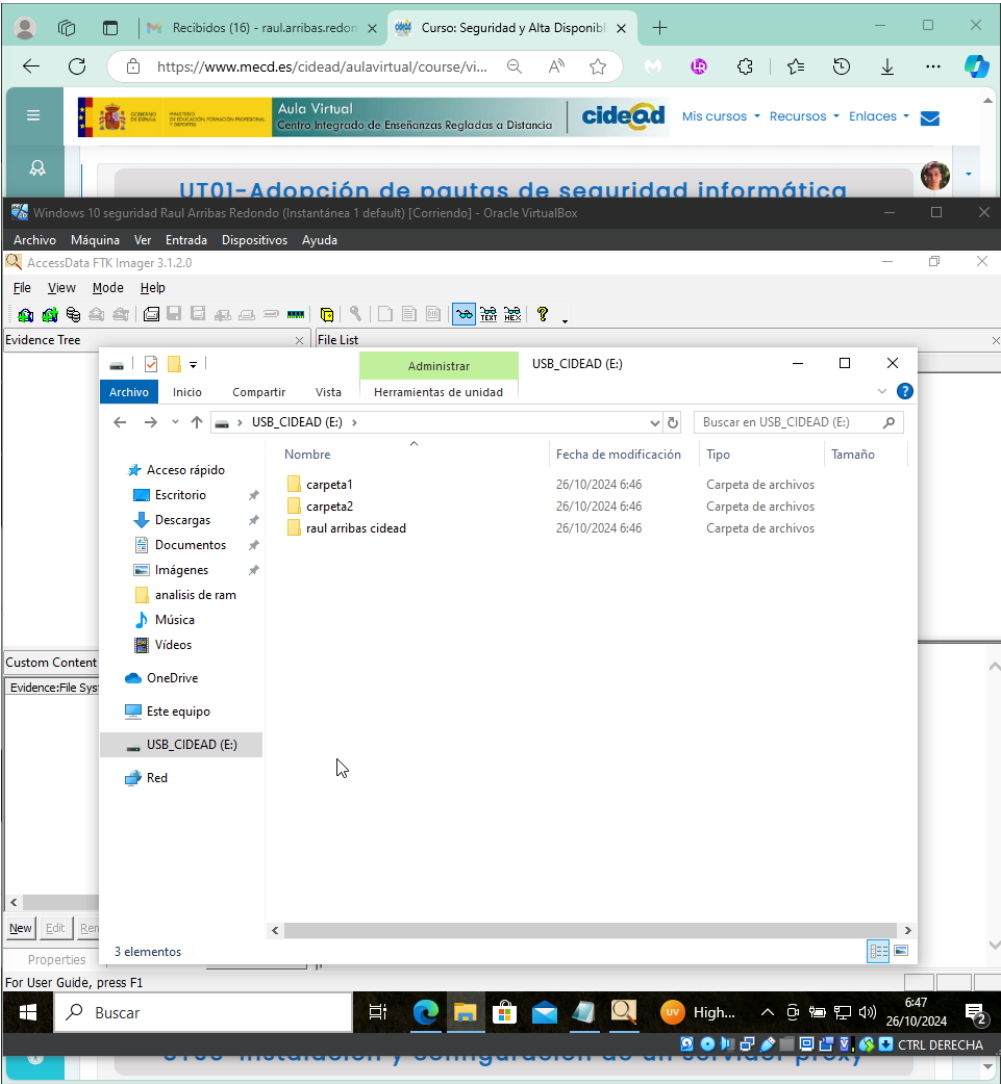
Ahora insertamos un USB en nuestra maquina Host que vamos a utilizar para crear algunos ficheros y eliminar algunos de estos posteriormente.

Dispositivos → USB → NUESTRO USB

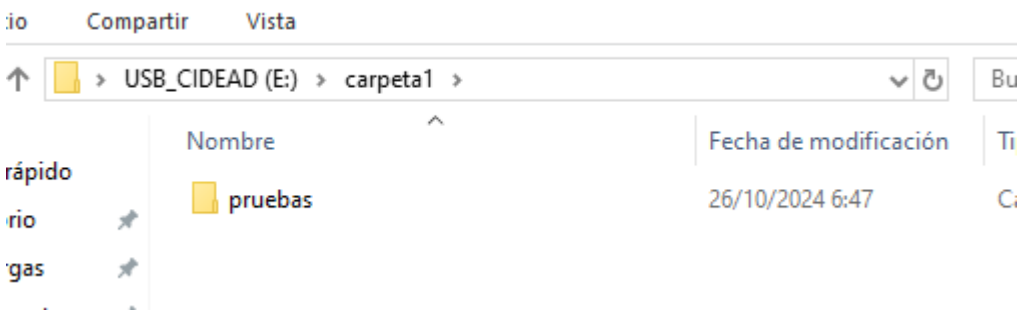


CREAMOS LAS CARPETAS EN EL USB

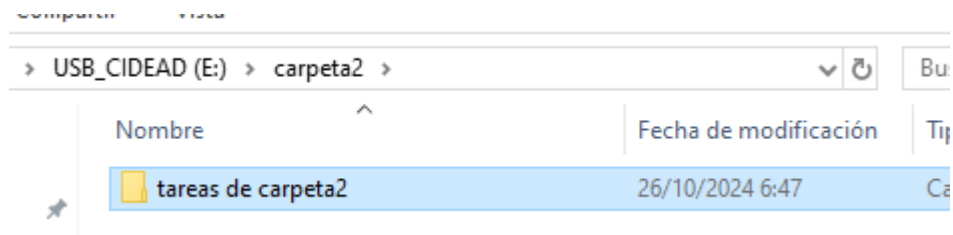
Ahora vamos a crear algunas carpetas y subcarpetas para hacer las pruebas:



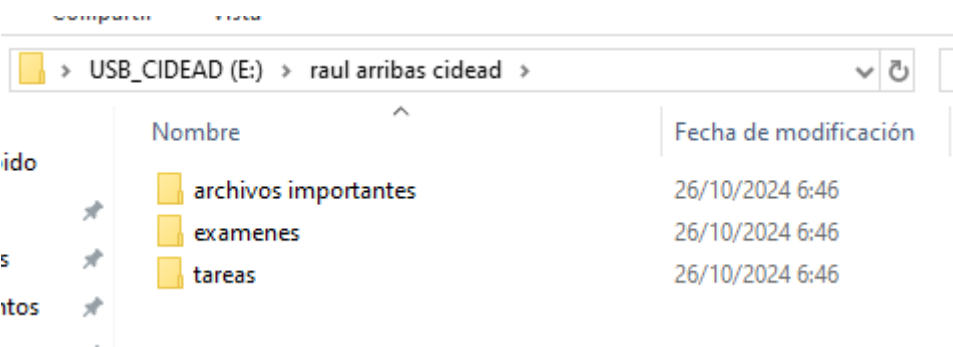
Dentro de carpeta1 tenemos: pruebas



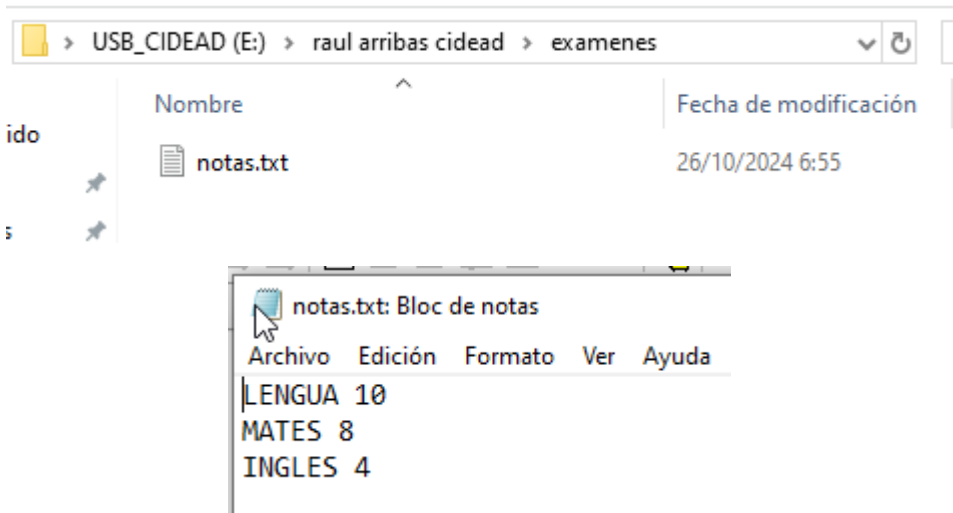
Dentro de carpeta2 tenemos: tarea de carpeta2



Dentro de la carpeta raul arribas Cidead tenemos:



Dentro de exámenes hemos creado un documento de texto con lo siguiente:



ELMINAMOS LAS CARPETAS DEL USB:

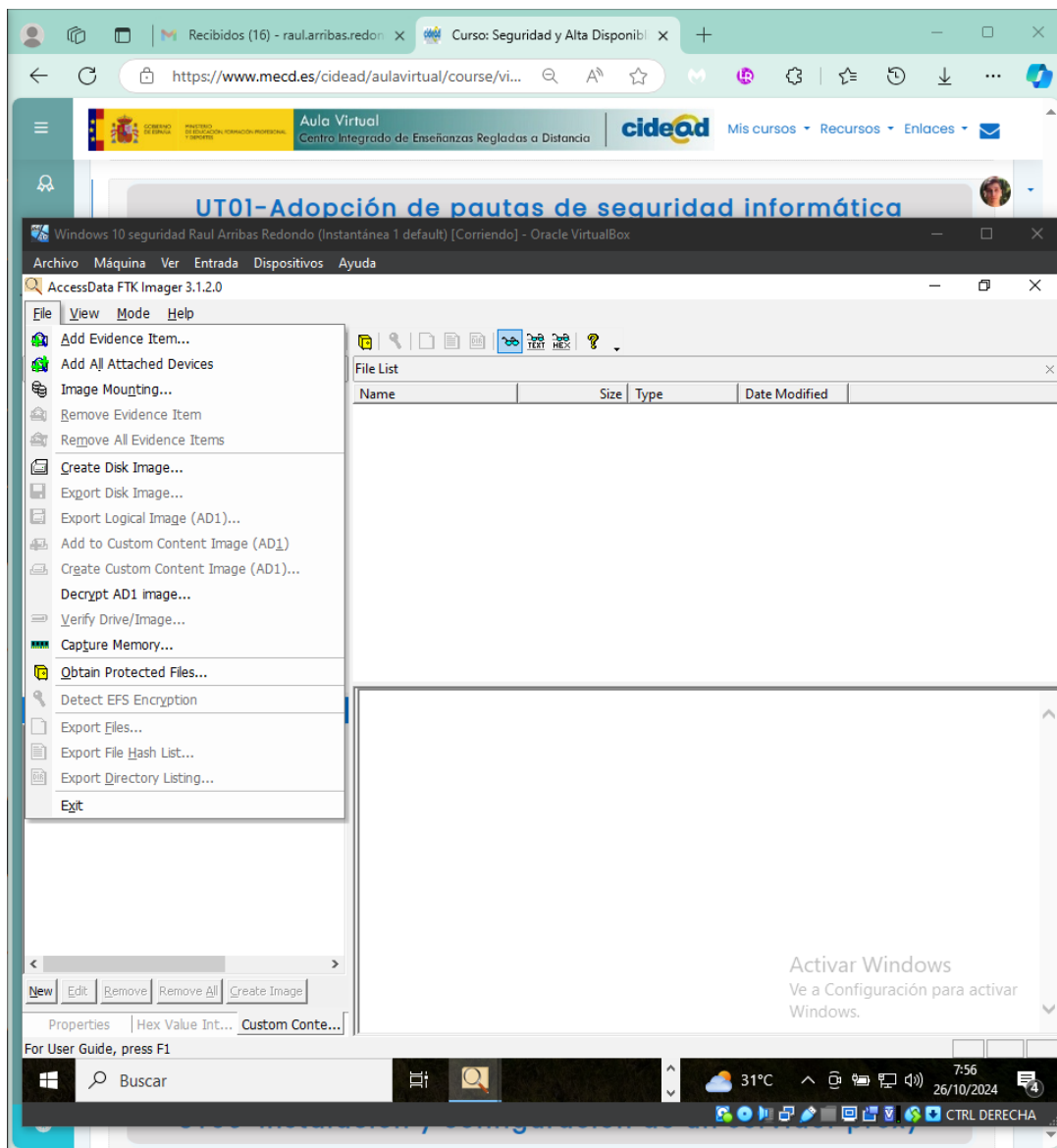
Ahora vamos a eliminar las carpetas con shift + supr: “pruebas” que se encuentra en la carpeta1, la carpeta2 completa y la carpeta de “exámenes” que se encuentra en la carpeta raul arribas Cidead.

Una vez las tengamos eliminadas nos vamos a la aplicación de AccessData FTK Imager.

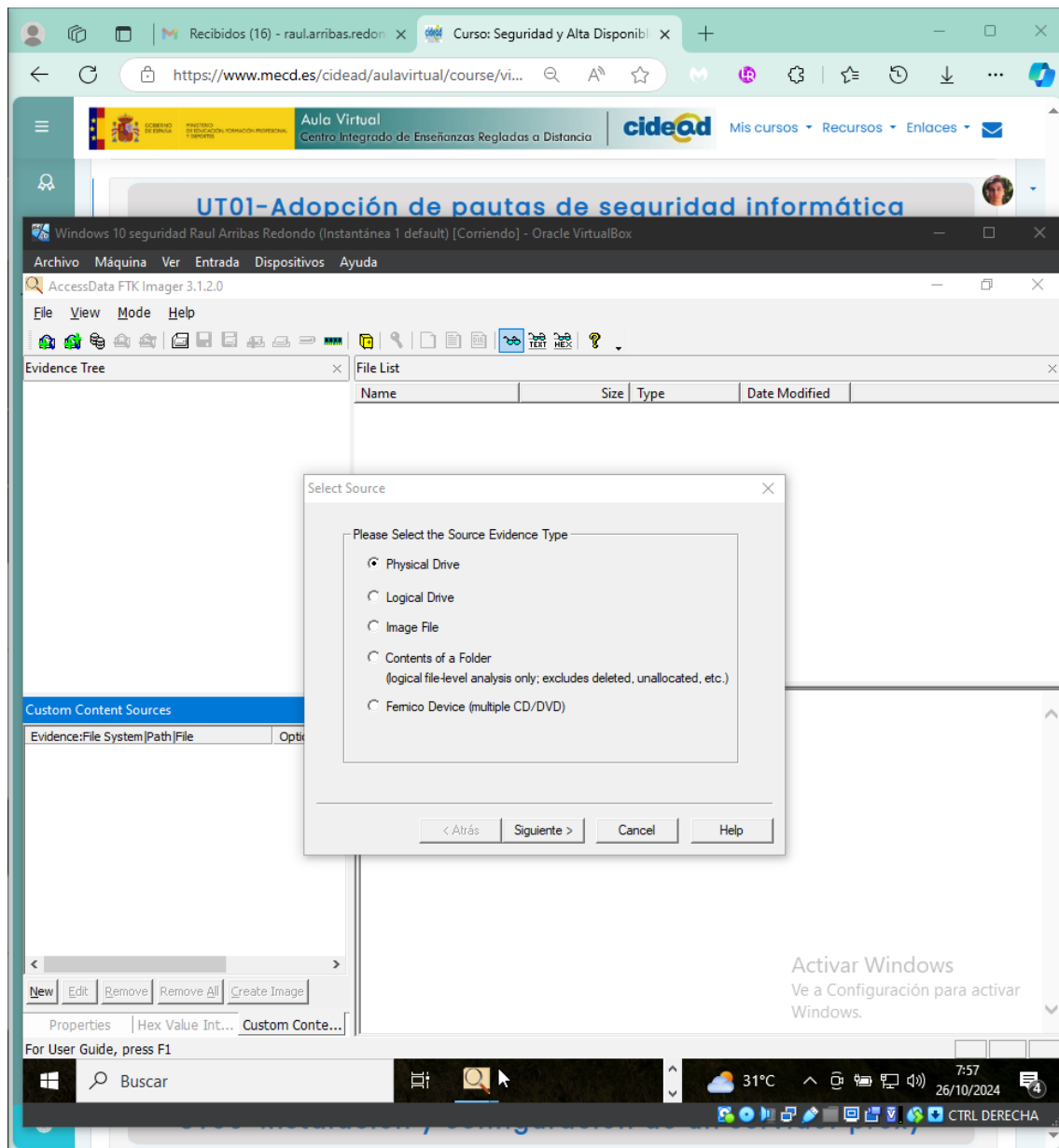
CREAR DISCO DE IMAGEN:

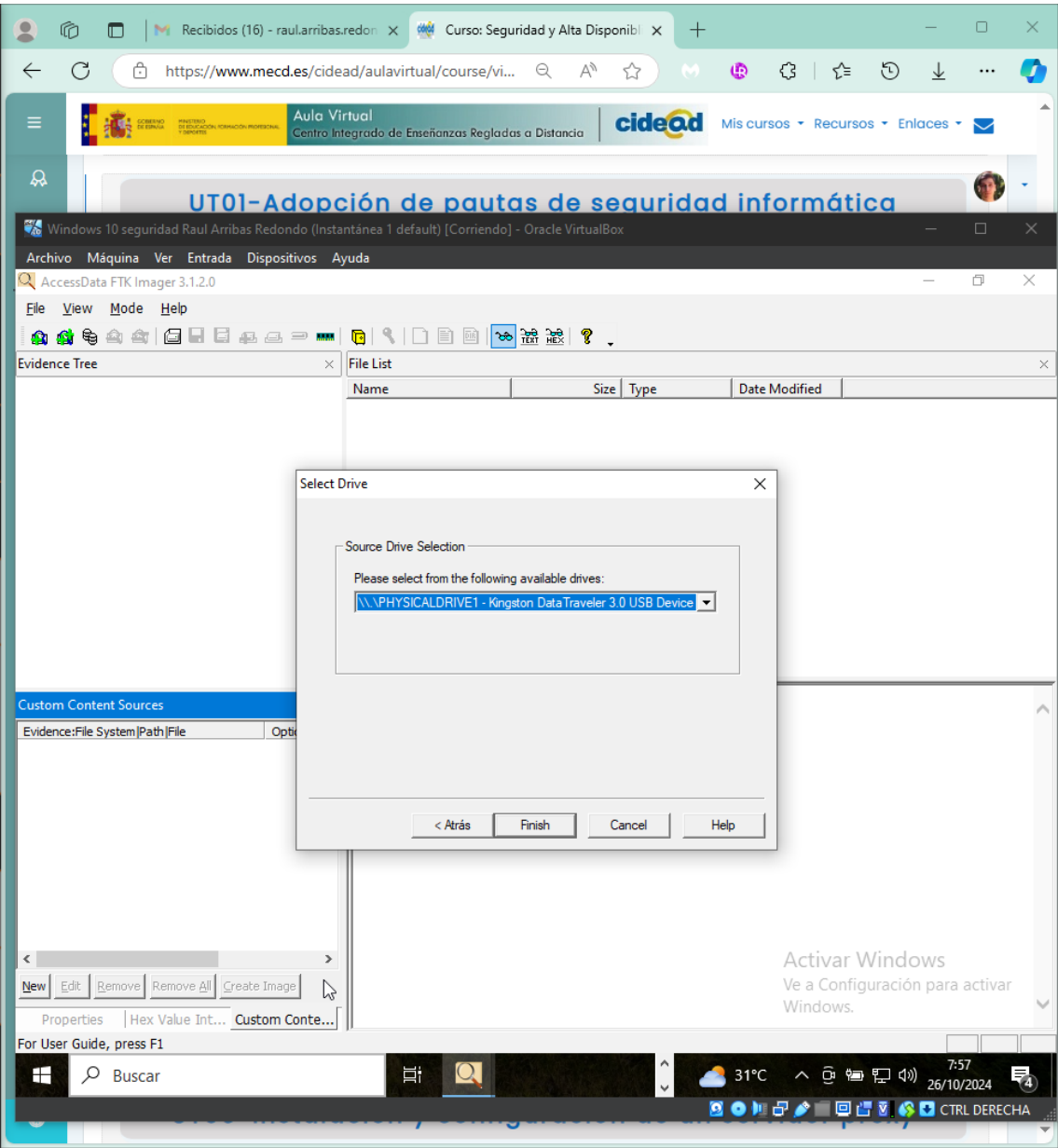
Cuando tengamos la aplicación abierta AccessData FTK Imager hacer lo siguiente,

File → Create Disk Image..

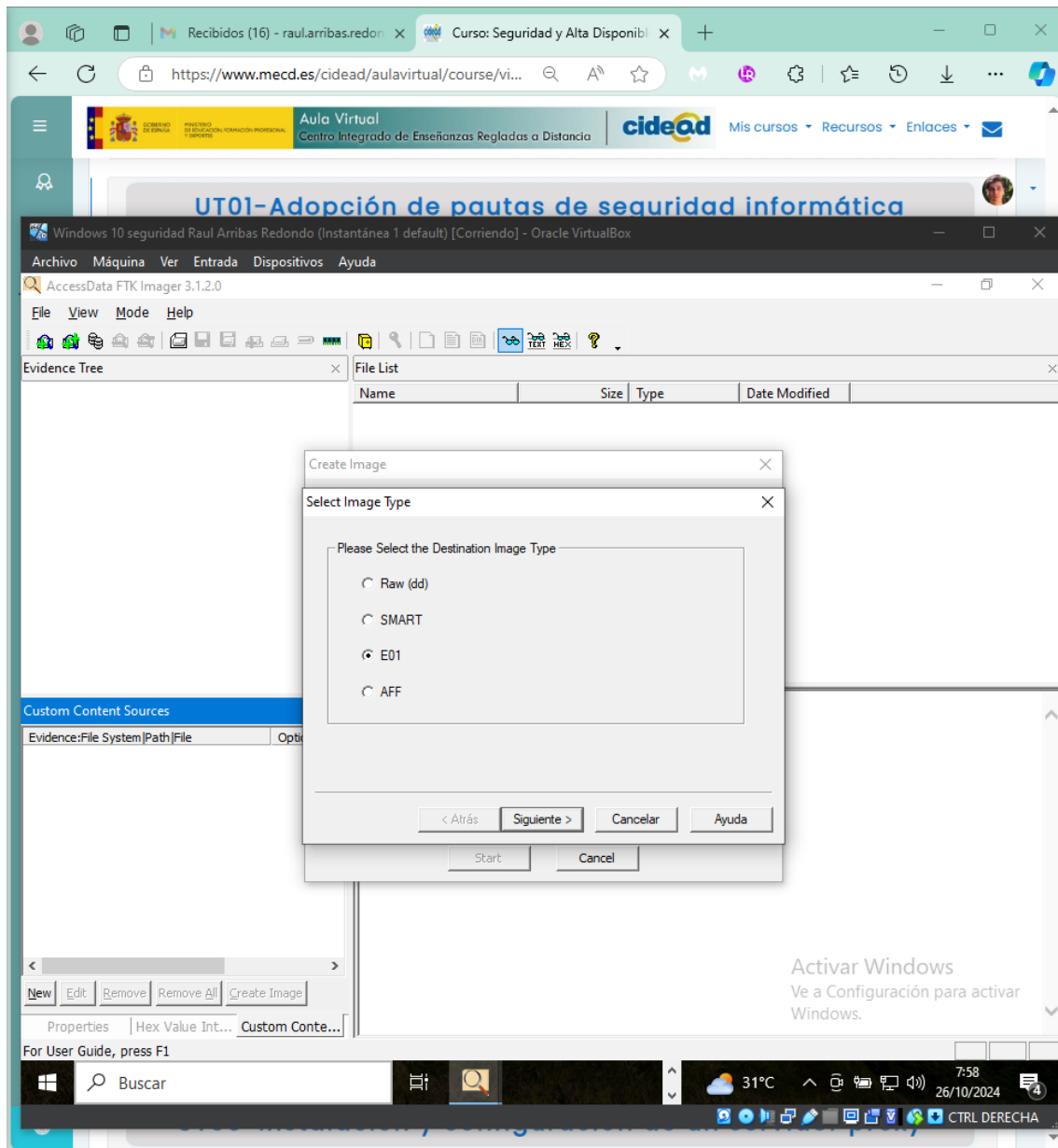
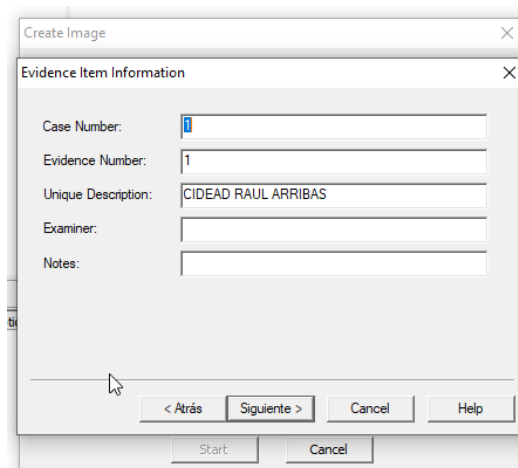


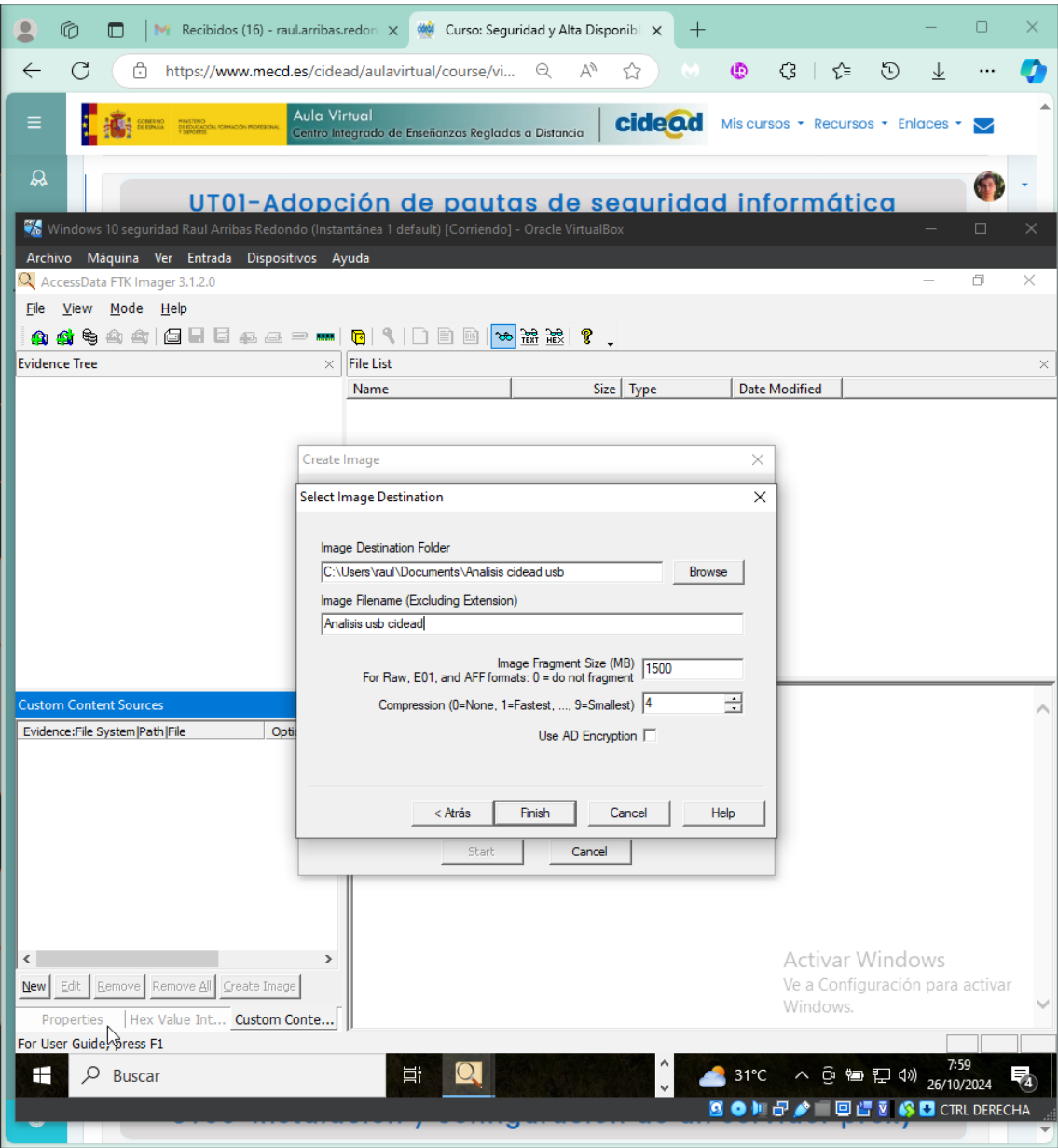
Escogemos la opción de **Physicaldrive** para seleccionar nuestro USB.



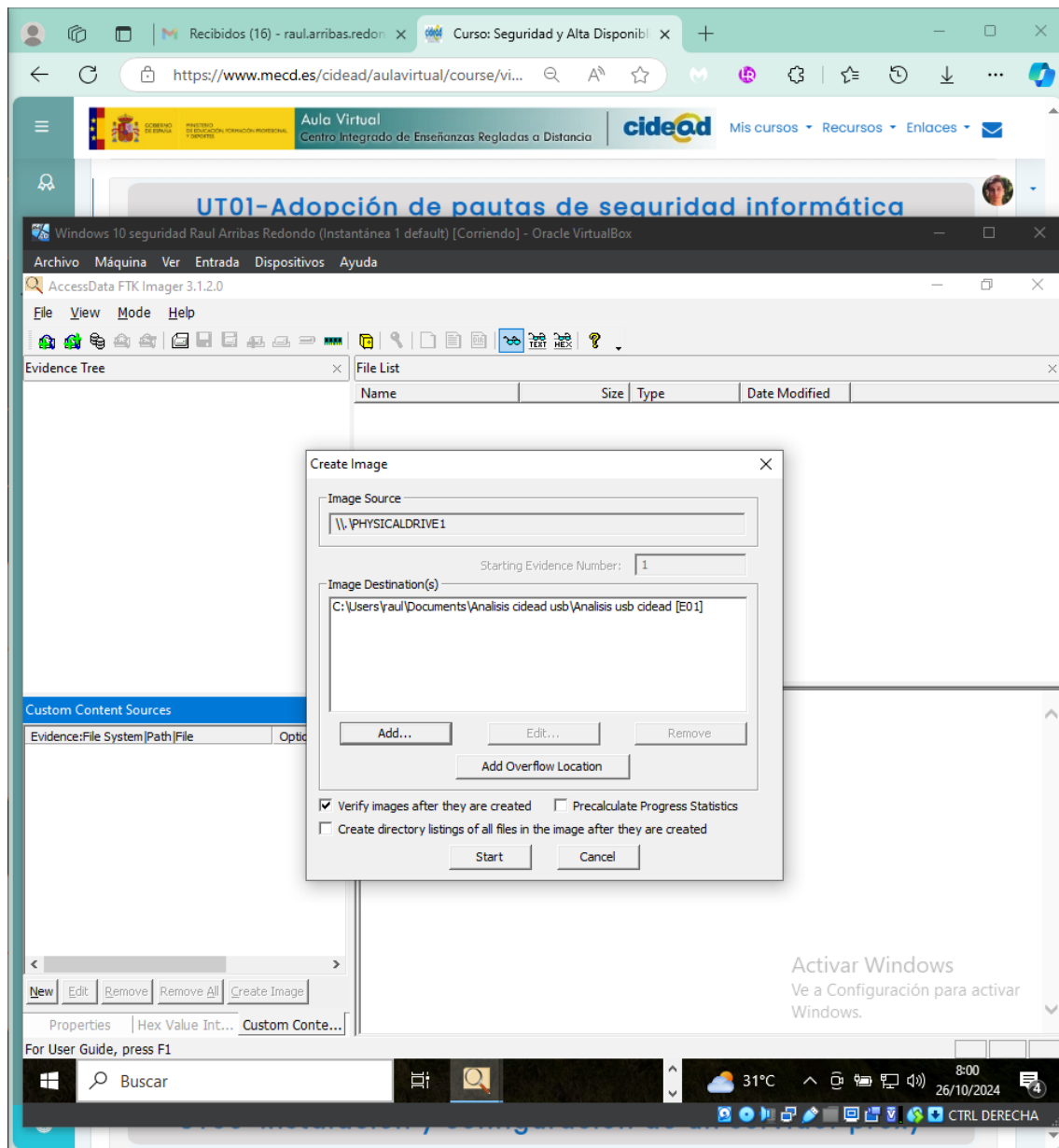


Escogemos el formato de salida **E01** clicando en **Add..** Y seguimos los pasos hasta que nos pida donde guardar la imagen de destino y clicamos en finish:

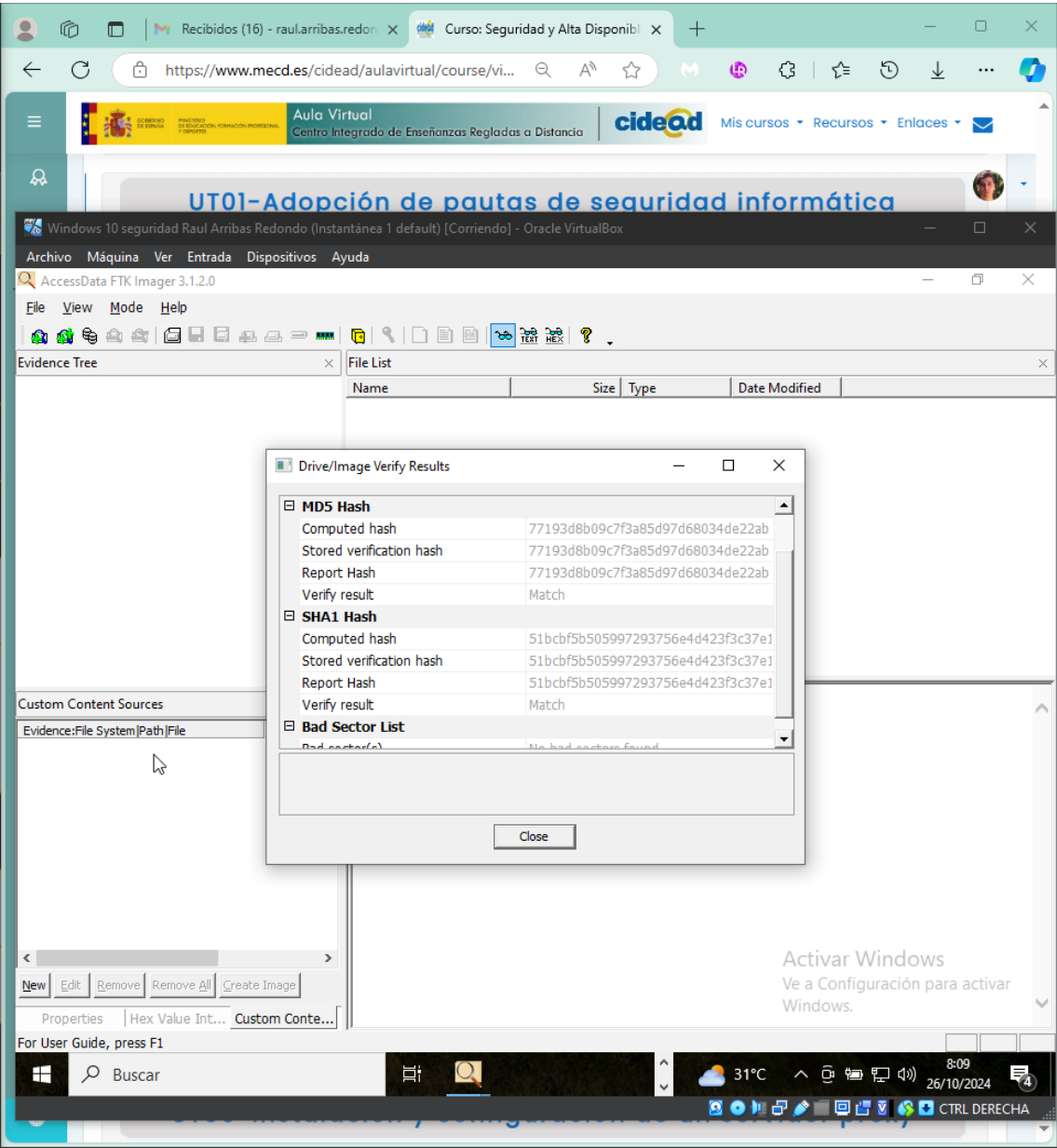




Una vez tengamos la imagen de destino, vamos a darle a Start:



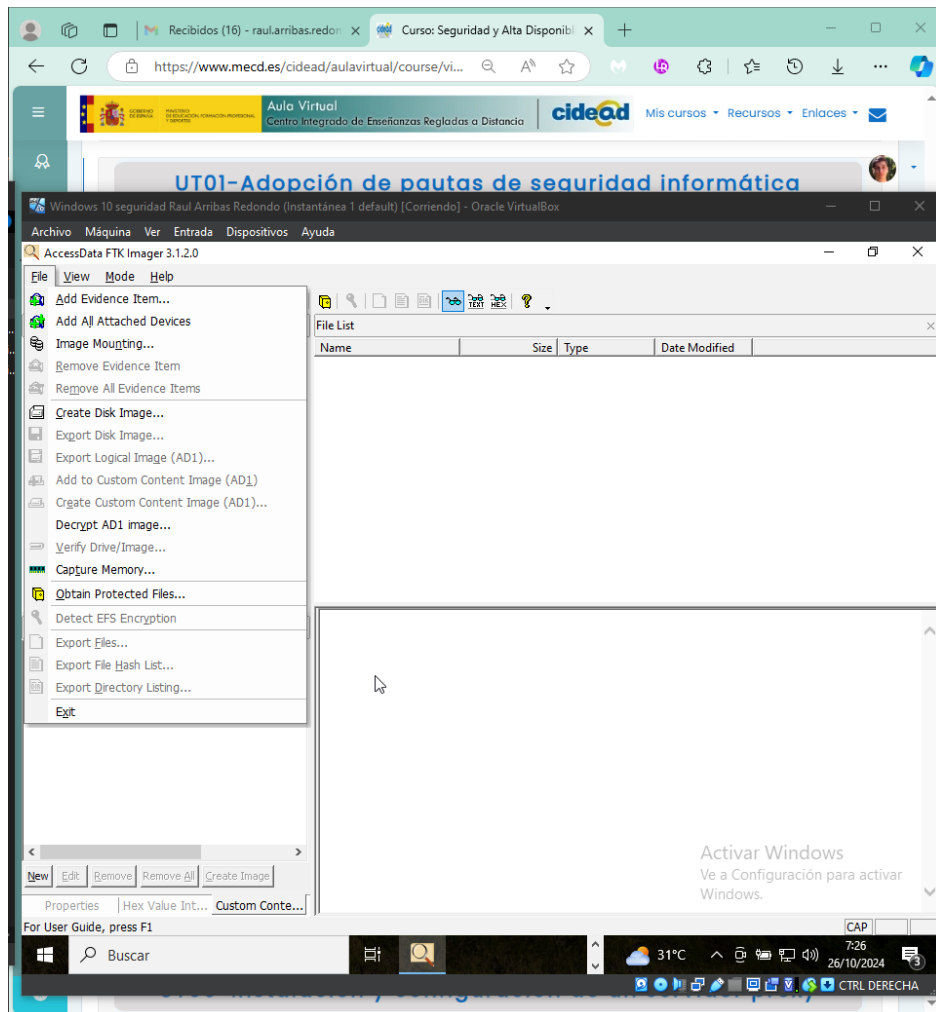
Cuando termine veremos que nos ha guardado una imagen en la ruta que hemos especificado antes, para recuperar los datos tenemos que seguir los siguientes pasos.



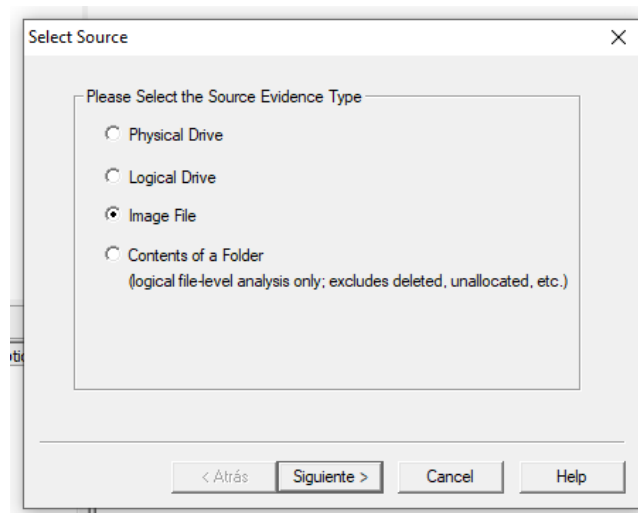
RECUPERAR LOS DATOS ELIMINADOS:

Nos vamos a la aplicación AccessData FKT,

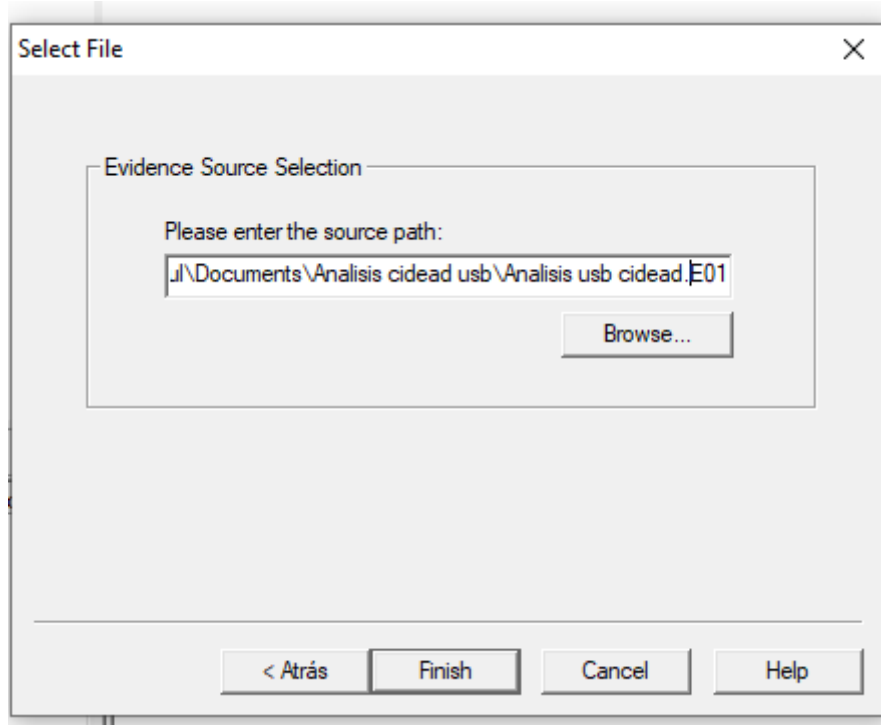
File → Add Evidence Item



Escogemos la opción de Imagen File:

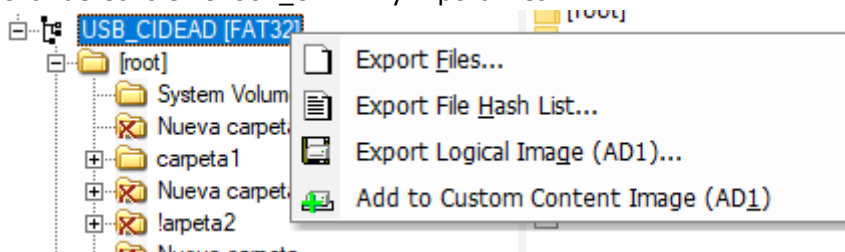


Elegimos la ruta donde tenemos la imagen guardada y tenemos que elegir la primera que nos ha creado, porque una vez detecte la primera detectará las siguientes de forma automática:

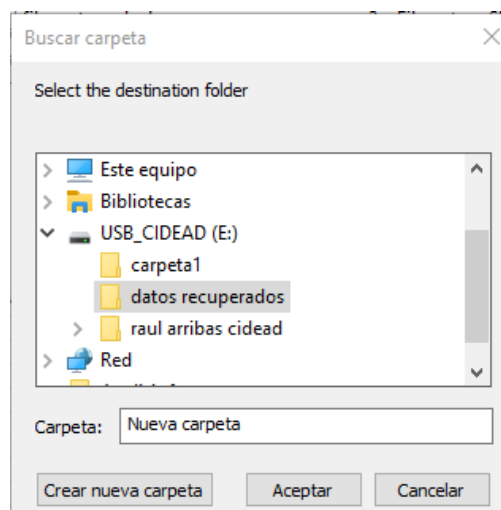


Nos agrega la imagen y podemos ver con una X la que se han eliminado o cambiado de nombre, para recuperar las carpetas:

Click derecho en el USB_CIDEAD y Export Files:

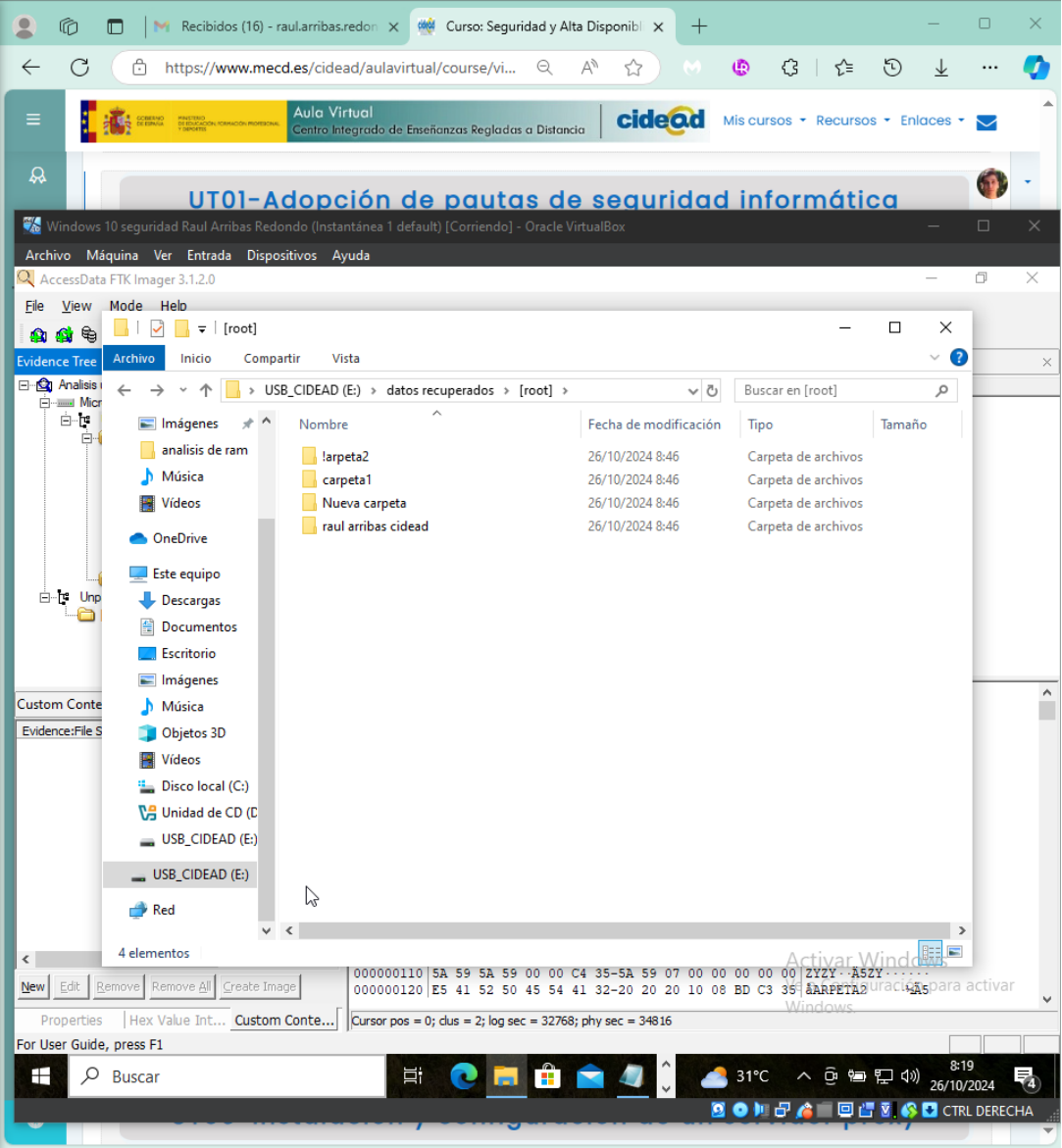
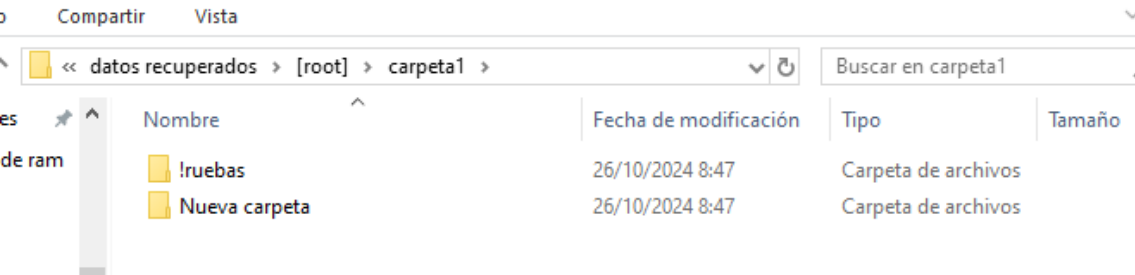


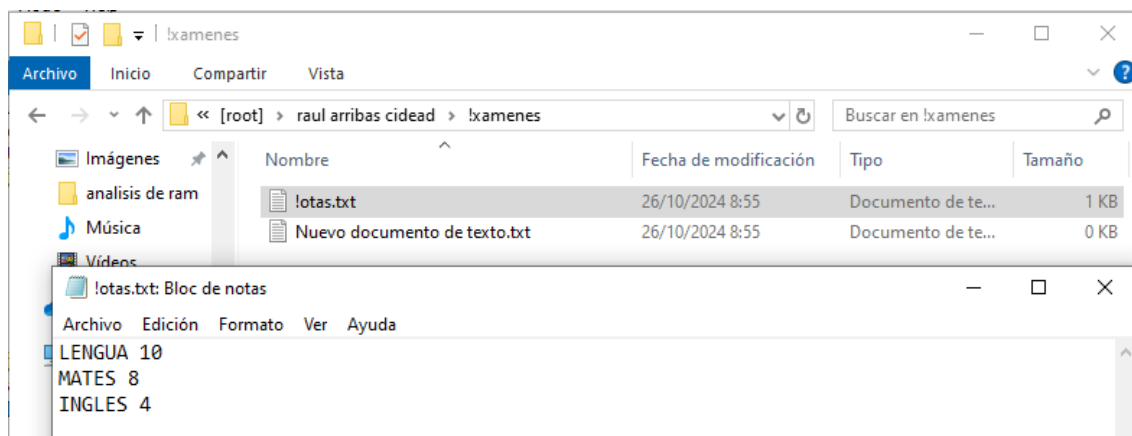
Creamos una carpeta que se llama datos recuperados:



Cuando termine de exportar los archivos comprobamos que efectivamente los archivos están todos, los eliminados y los que ya estaban previamente sin eliminar.

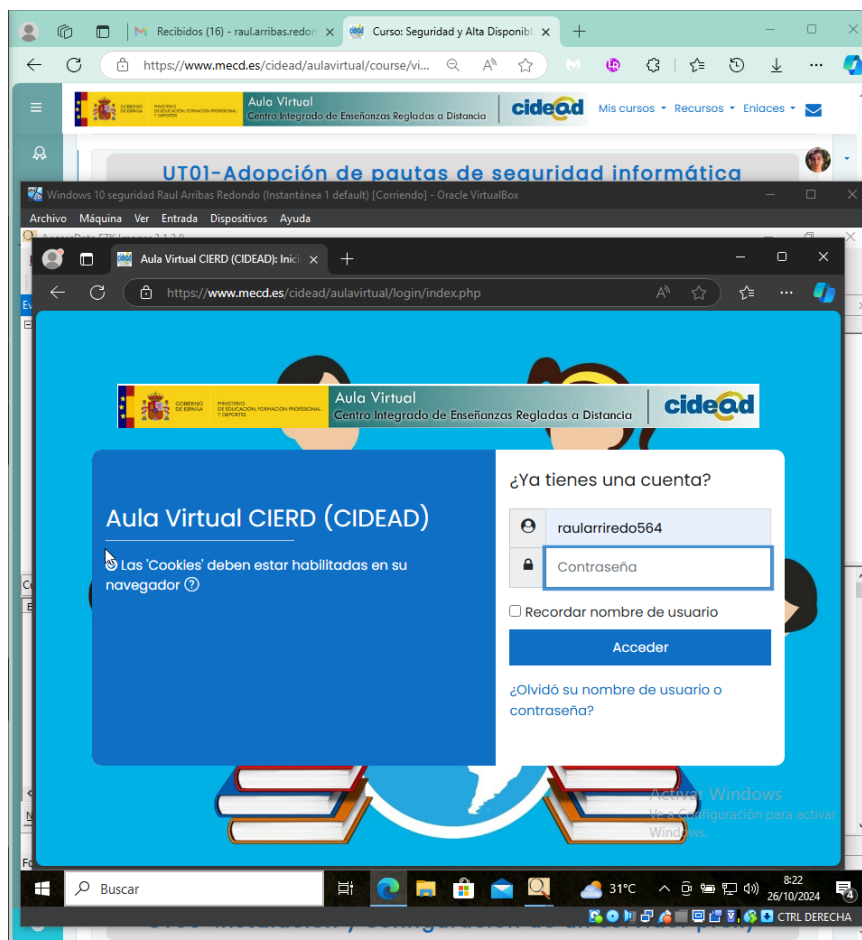
La carpeta 2 esta recuperada, el archivo de exámenes también está recuperado y la carpeta de pruebas también.





3.3 Abre una sesión en cualquier sitio web al que debas logarte. Usa la herramienta anterior para capturar toda la información existente en la memoria RAM. Monta dicha captura sobre una imagen y realiza un análisis forense de la imagen creada. Finalmente, captura la pantalla en la que se muestra la sesión abierta en el sitio web junto con las credenciales de acceso.

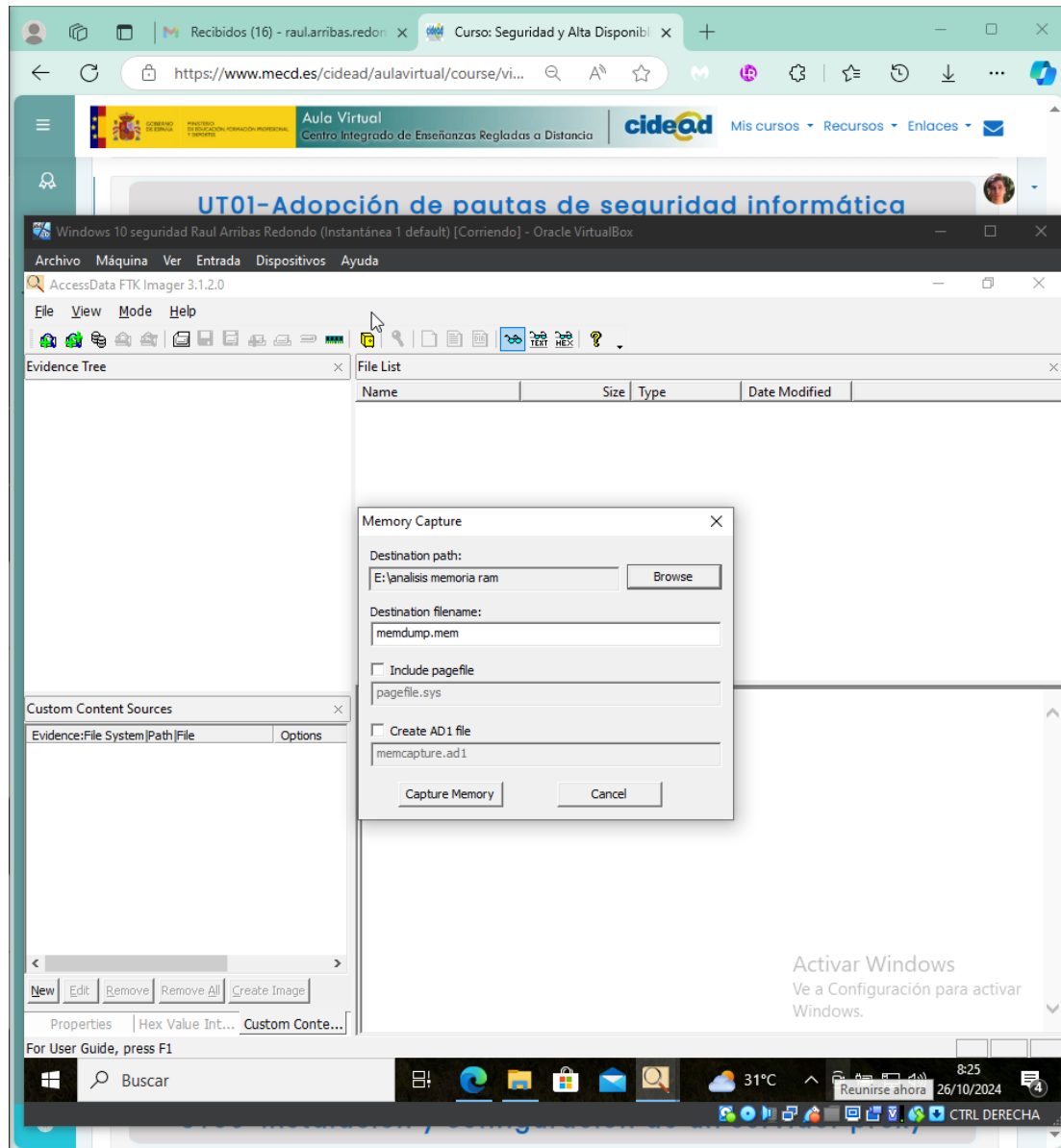
Primero abrimos una pagina web en la cual nos vamos a logar, en nuestro caso será el aula virtual:

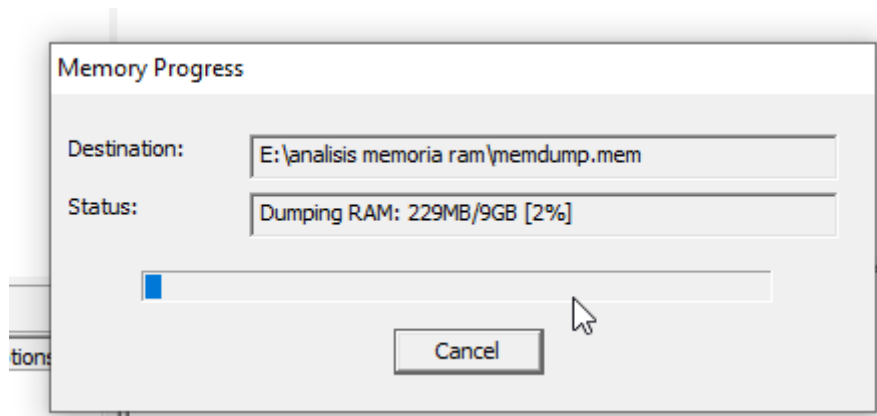


Una vez no loguemos tenemos que abrir nuestra aplicación AccessData FTK Imager y hacer una grabación de nuestra memoria RAM:

File → Capture Memory

Escogemos la ruta donde queremos guardar la evidencia para después utilizarla y analizarla.

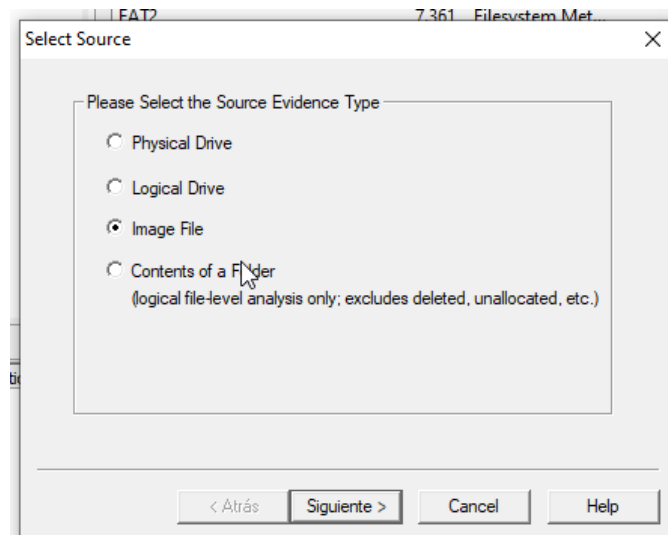




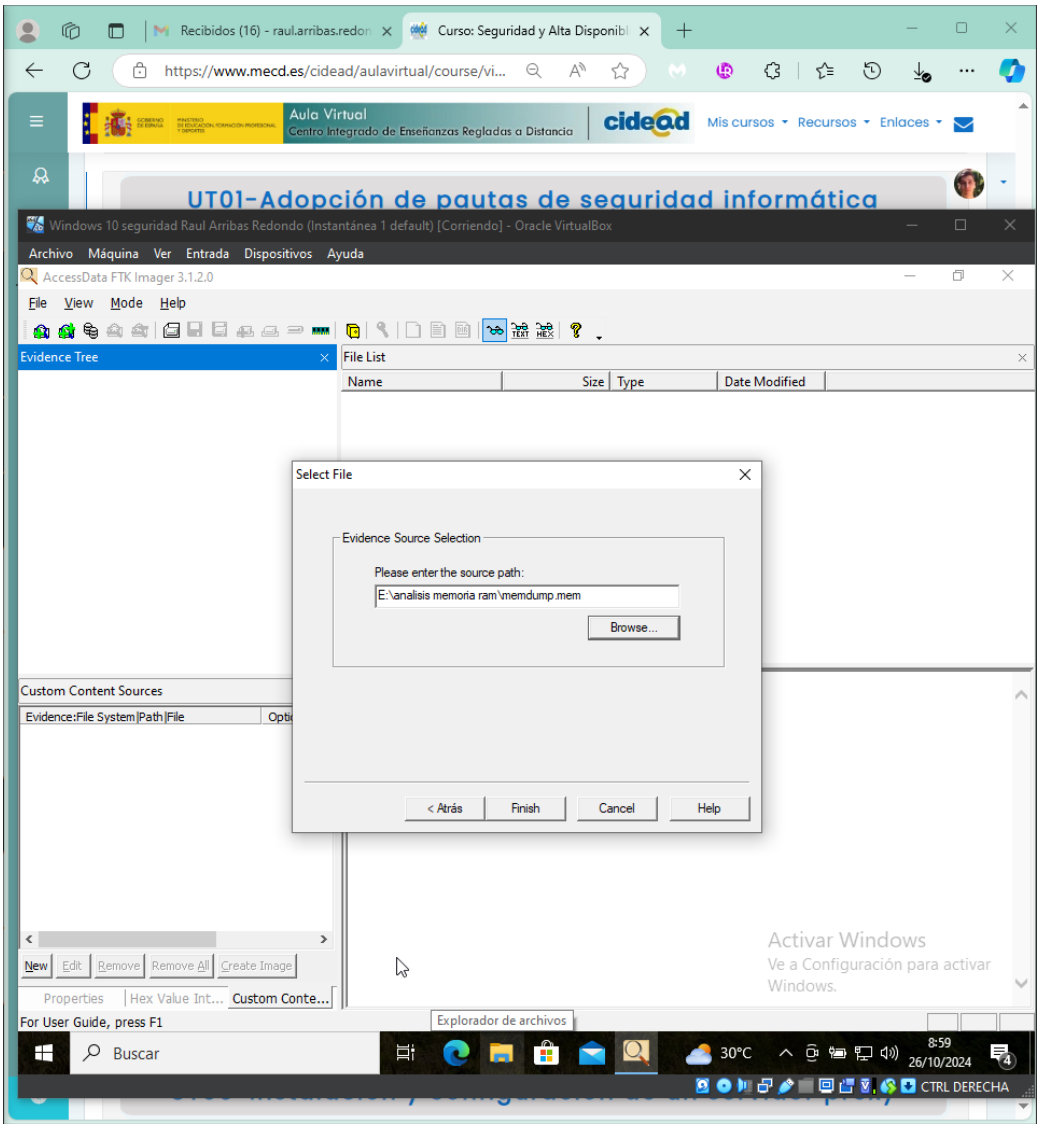
Cuando llegue al límite de memoria que tengamos ocupada nos dará un error, pero aun así comprobamos el archivo generado

Cuando haya terminado de completarse, tenemos que abrir la evidencia y efectivamente, veremos que se puede ver la contraseña en texto claro que hemos puesto en el aula virtual.

File → Add Evidence Item



Insertamos el archivo de memoria que nos ha generado y hacemos una búsqueda de nuestra contraseña que hemos puesto:



6e98f8a0	A0 11 58 01 A4 59 00 00-9A C0 9D CD 6B 76 B1 34	·X··Y···À·íkv±4
6e98f8b0	9A C0 9D CD 6B 76 B1 34-90 CC A7 02 A4 59 00 00	·À·íkv±4·î\$··Y··
6e98f900	6D 73 45 64 67 65 41 75-74 6F 66 69 6C 6C 53 73	msEdgeAutofillSs
6e98f910	50 72 6F 66 69 6C 65 53-75 67 67 65 73 74 69 6F	ProfileSuggestio

Una vez busquemos un poco por los valores que nos salen encontraremos la contraseña.

