



---

# ANÁLISIS FORENSE

---

Unidad 1. Actividad 1



16 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

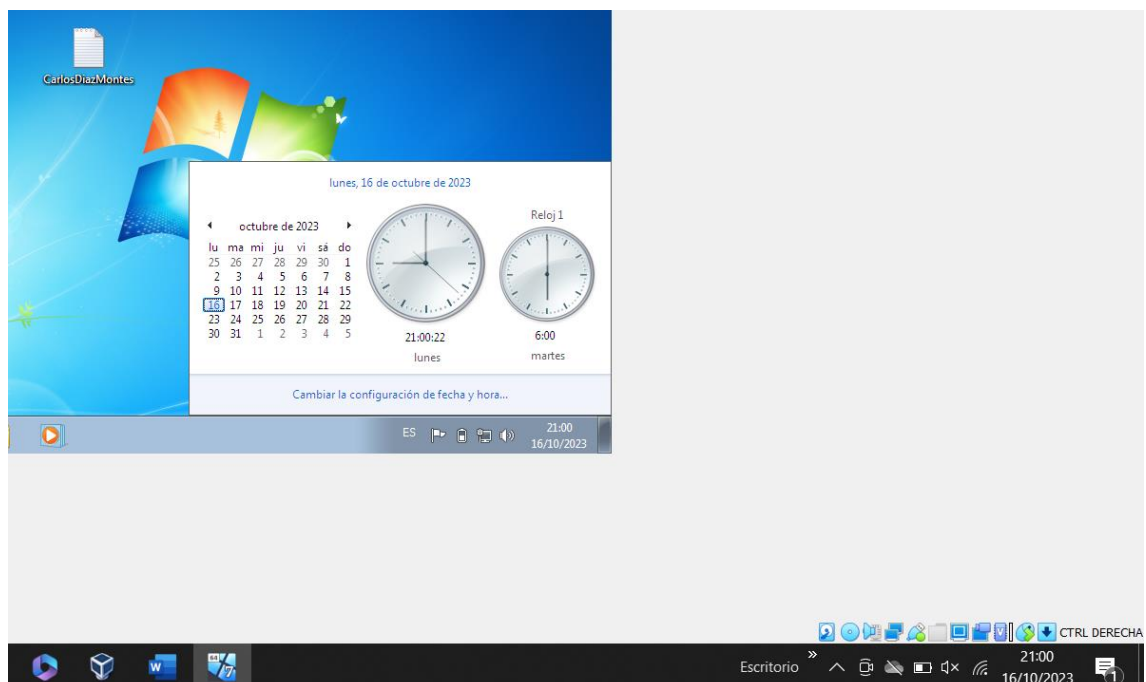
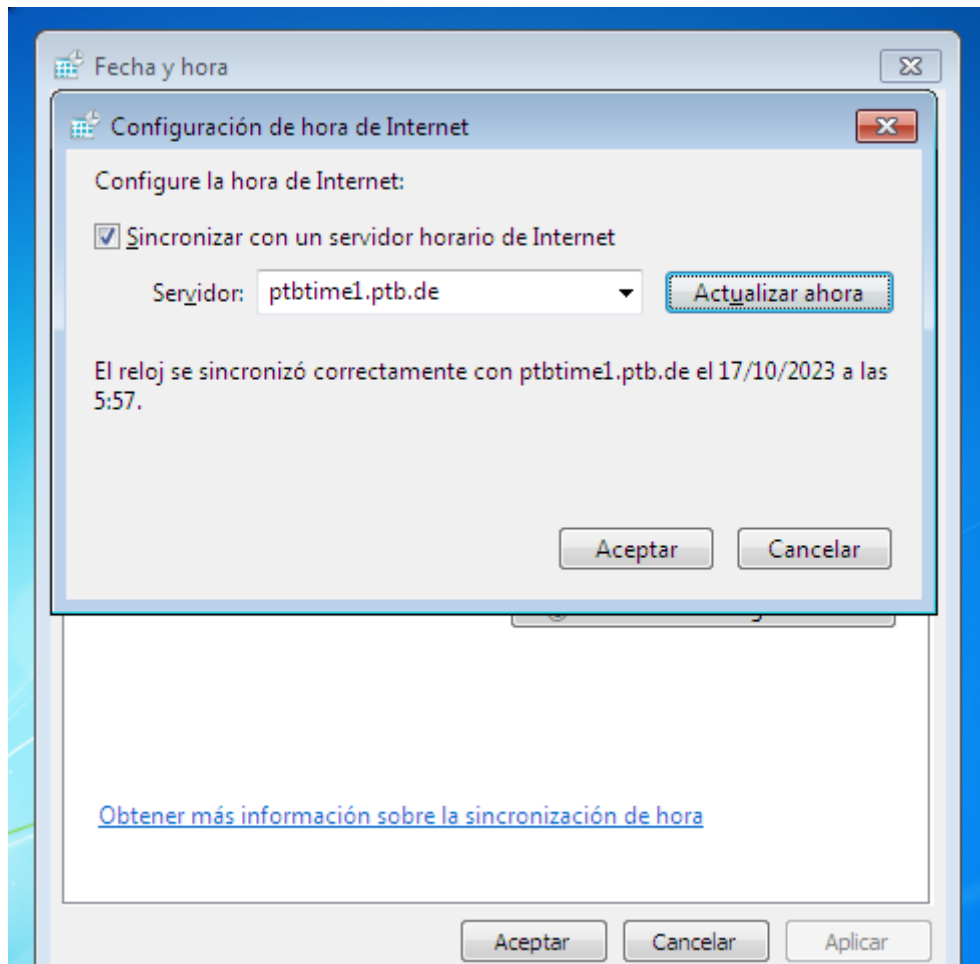
## Índice

Ejercicio 1 .....	2
Ejercicio 2 .....	4
Ejercicio 3 .....	8
Ejercicio 4 .....	10

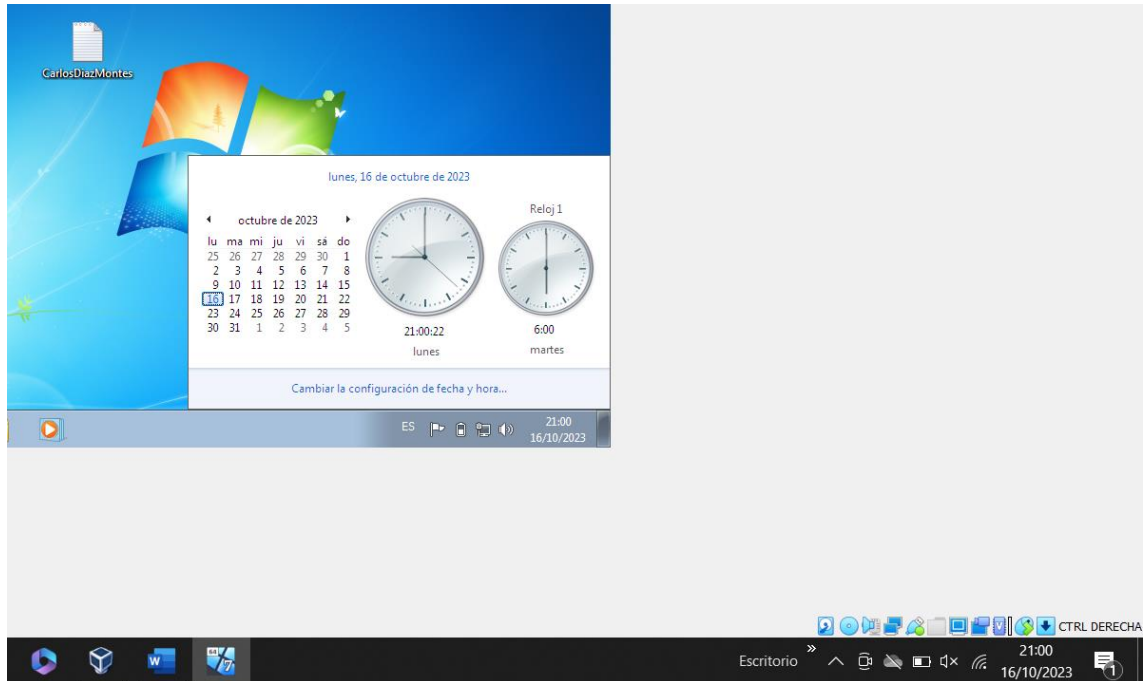
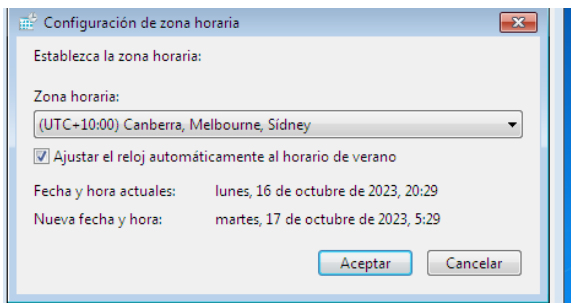
## Ejercicio 1.

Una vez instalado correctamente el Windows 7, ajustamos la hora y fecha del equipo:

a)

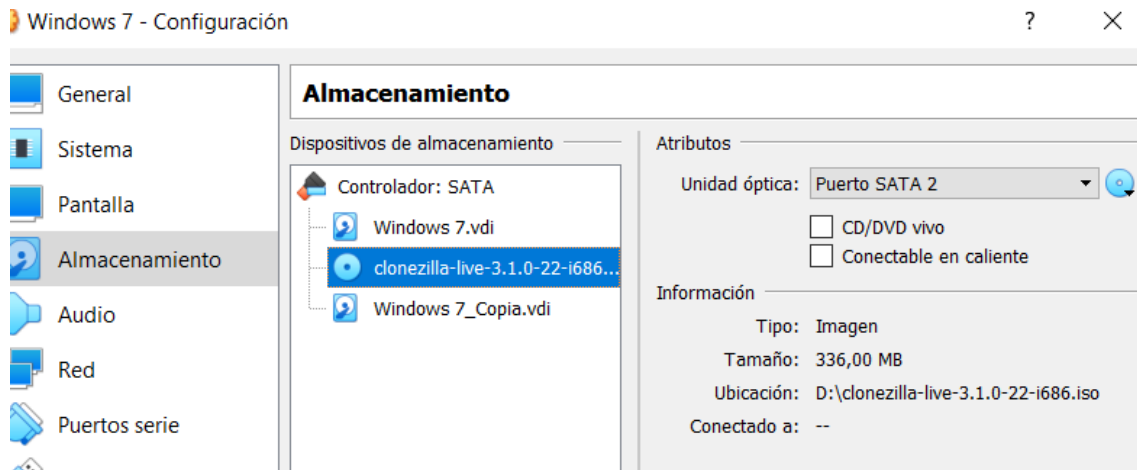


b)

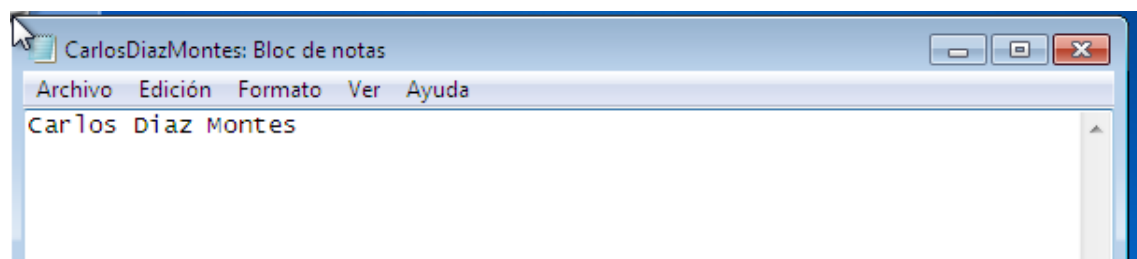


## Ejercicio 2

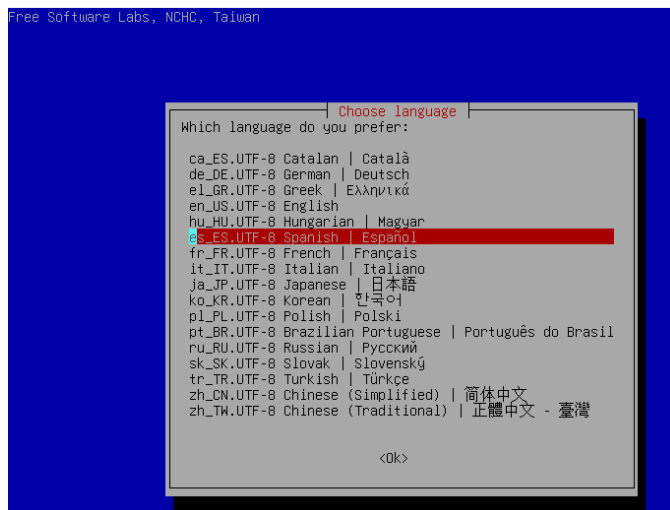
Nos vamos a la configuración de la maquina y en almacenamiento añadimos el disco duro llamado Clonezilla:



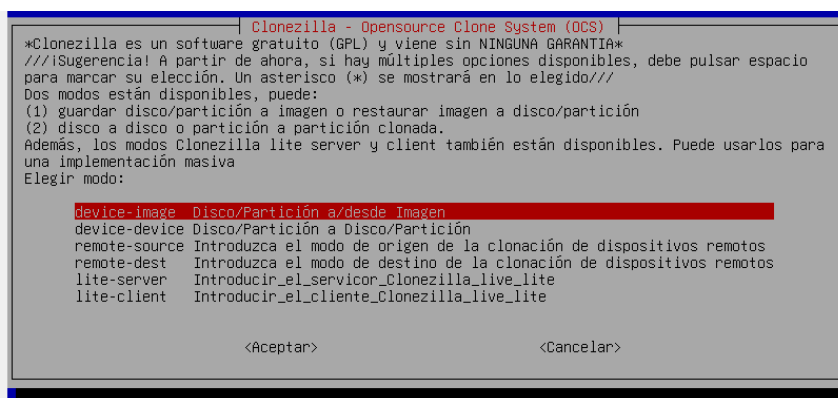
Ahora nos creamos el txt:



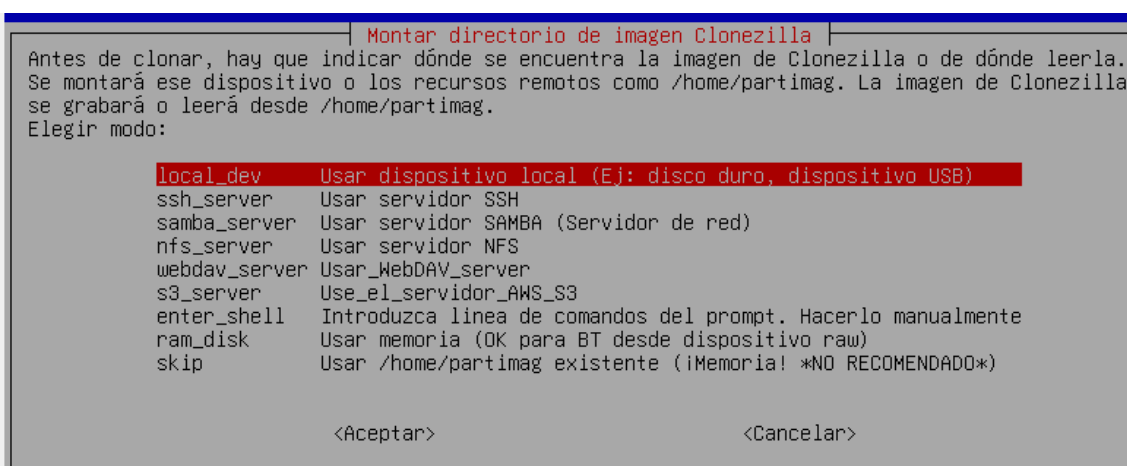
Elegimos el idioma una vez arrancado el clonezilla:



En este menú seleccionamos que queremos trabajar de imagen a dispositivo:



Ahora seleccionamos donde montamos la imagen de clonezilla:



Ahora como vemos esta detectando los dos discos que tenemos en la máquina:

```
Cada 3,0s: ocs-scan-disk debian: Mon Oct 23 19:06:08 2023
2023/10/23 19:06:08
Puede insertar un dispositivo de almacenamiento en esta máquina si desea utilizarlo y, a continuación, esperar a que se detecte.
Finding all disks and partitions..
Excluding busy harddisk.....
Excluding linux raid member partition.....
Scanning devices... Available disk(s) on this machine:
=====
/dev/sda: VBOX_HARDDISK_ VBOX_HARDDISK_VBcd6ceb0e-d1274bcf 34.4GB
/dev/sdb: VBOX_HARDDISK_ VBOX_HARDDISK_VB14eb2572-f118abd7 34.4GB
=====
Update periodically. Press Ctrl-C to exit this window.
```

Ahora seleccionamos el disco:

```
Clonezilla - Opensource Clone System (OCS) | Modo:
Ahora se necesita montar el dispositivo como /home/partimag (repositorio de imagen(es)) por lo
que se debe leer o grabar la imagen en /home/partimag.
///NOTA/// NO debe montar la partición de la que desea hacer la copia como /home/partimag
El nombre del disco es el nombre del dispositivo en GNU/Linux. La primera partición en el primer
disco es "hda1" o "sda1", la segunda partición en el primer disco es "hda2" o "sda2", la primera
partición en el segundo disco es "hdb1" o "sdb1"... Si el sistema que desea salvar es MS
windows, normalmente C: es hda1 (para PATA) o sda1 (para PATA, SATA o SCSI), y D: será hda2 (o
sda2), hda5 (o sda5)...
```

sda1	100M_ntfs_Reservado_pa(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VBcd6ceb0e-d1274bcf
sda2	31.9G_ntfs(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VBcd6ceb0e-d1274bcf
sdb1	32G_ntfs_Nuevo_vol(In_VBOX_HARDDISK_)_VBOX_HARDDISK_VB14eb2572-f118abd7

<Aceptar> <Cancelar>

Seleccionamos el tipo de ejecución:

```
Clonezilla - Opensource Clone System (OCS)
Seleccione modo de ejecución para el asistente de opciones avanzadas:
```

Beginner	Modo Principiante: Aceptar opciones por defecto
Expert	Modo Experto: Selecciona tus propias opciones
Exit	Salir. Introduzca línea de comandos del prompt

<Aceptar> <Cancelar>

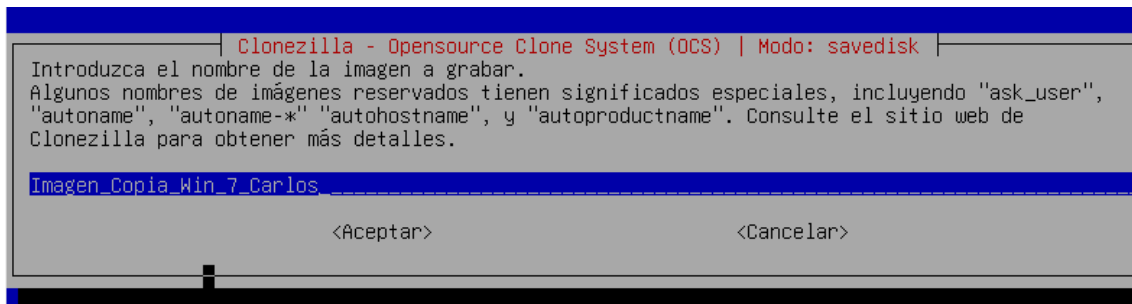
Guardamos el disco local en particiones:

```
Clonezilla - Opensource Clone System (OCS): Elegir modo
*Clonezilla es un software gratuito (GPL) y viene sin NINGUNA GARANTIA*
¡Este software escribirá los datos en su disco duro cuando restaure! ¡Es recomendable hacer una
copia de seguridad de los archivos importantes antes de restaurar!***
///¡Sugerencia! A partir de ahora, si hay múltiples opciones disponibles, debe pulsar espacio
para marcar su elección. Un asterisco (*) se mostrará en lo elegido///
```

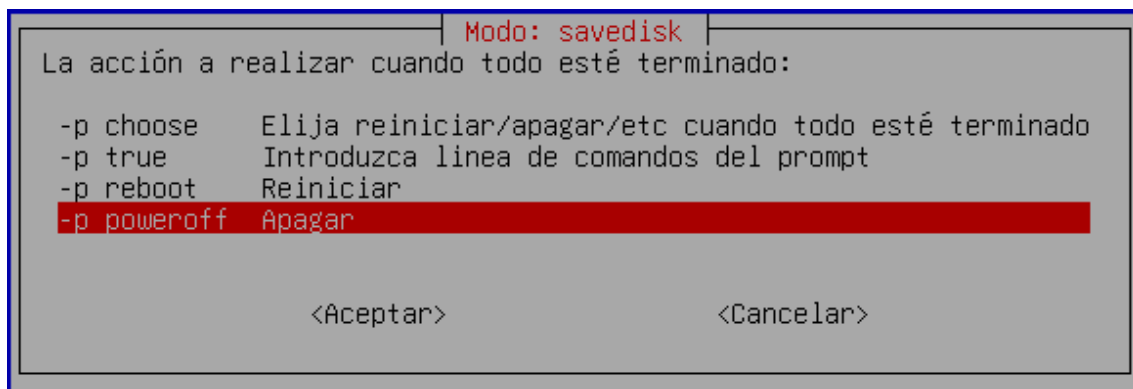
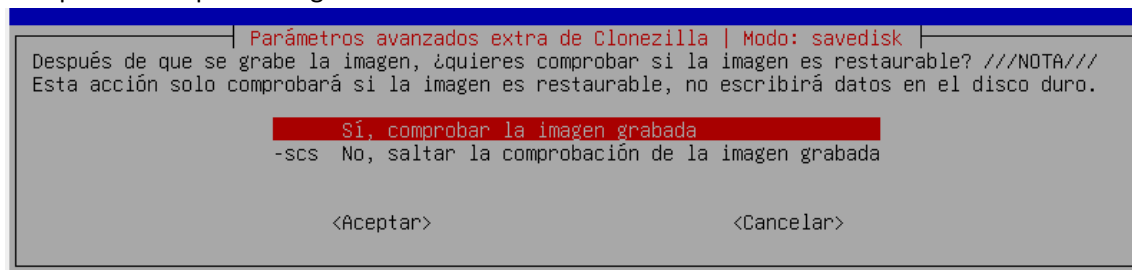
savedisk	Guardar_disco_local_como_imagen
saveparts	Guardar_particiones_locales_como_imagen
exit	Salir. Introduzca línea de comandos del prompt

<Aceptar> <Cancelar>

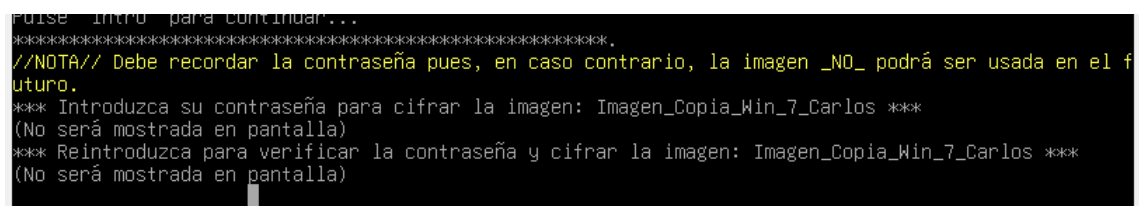
Seleccionamos el nombre de la imagen:



Comprobamos que la imagen sea cifrable:



Ponemos la contraseña (cdiazm21)



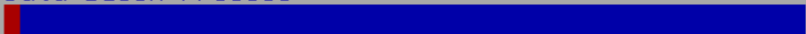
Ahora se hace la partición:




```

Partclone v0.3.23 http://partclone.org
Starting to clone device (/dev/sda2) to image (-)
Reading Super Block
Calculating bitmap... Please wait...
done!
File system:      NTFS
Device size:      34.3 GB = 8362495 Blocks
Space in use:     9.7 GB = 2375989 Blocks
Free Space:       24.5 GB = 5986506 Blocks
Block size:       4096 Byte

Elapsed: 00:00:12 Remaining: 00:07:49   Rate:   1.21GB/min
Current Block: 67999   Total Block: 8362495

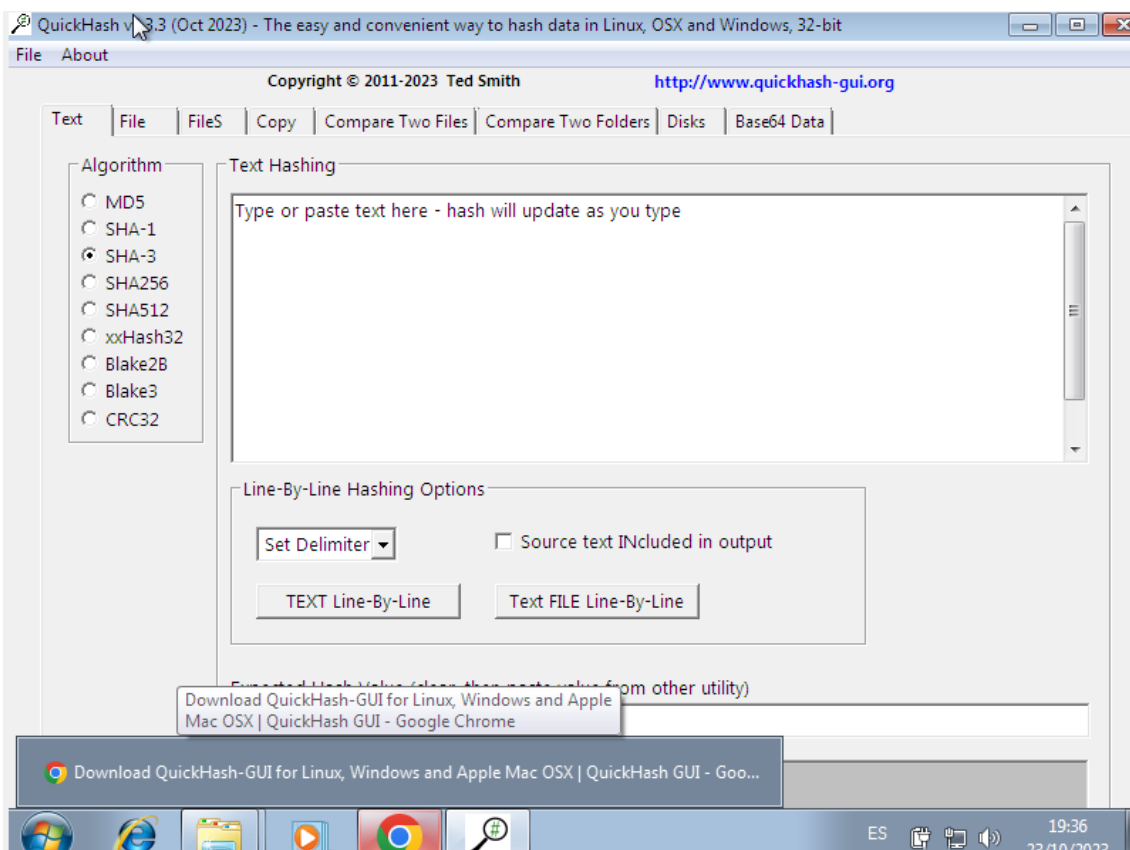
Data Block Process:
 2.49%

Total Block Process:
 0.81%

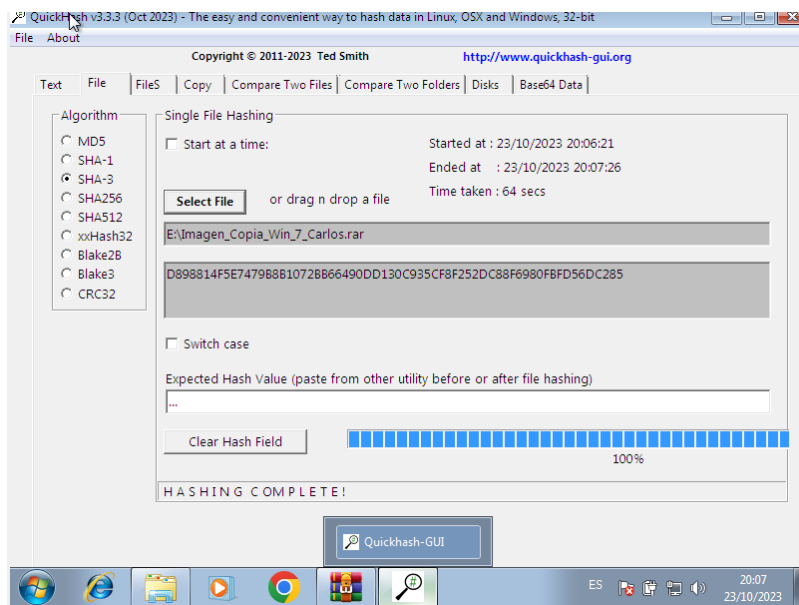
```

### Ejercicio 3.

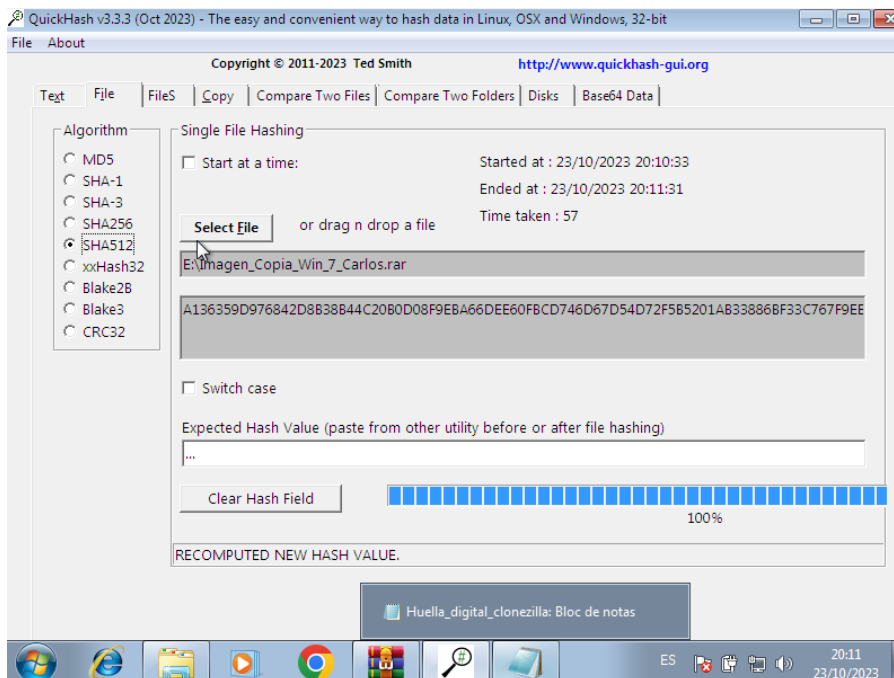
Ahora reiniciamos la maquina y nos decargamos quickhash:



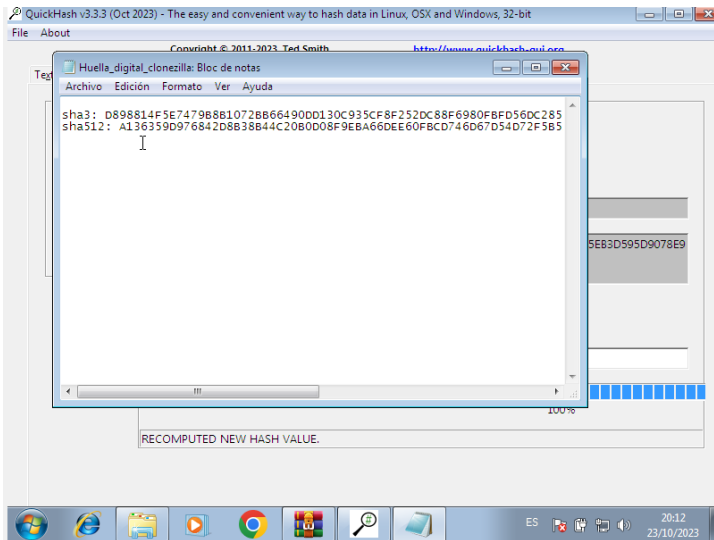
Ahora instalamos el winrar y la carpeta la comprimimos a .rar y con quickhash usamos el sha3:



Y con sha 512:



El documento de texto:

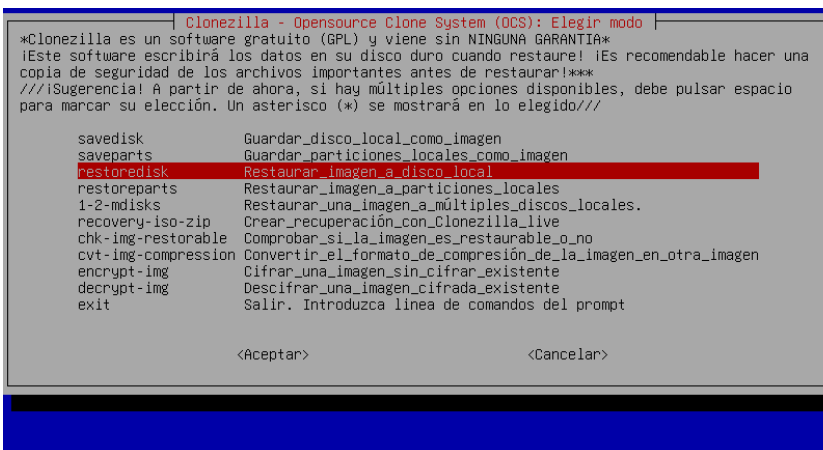


## Ejercicio 4

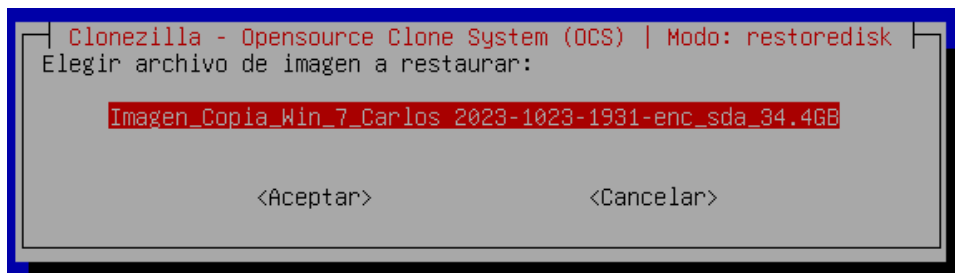
Cambio el fondo de pantalla y borro el archivo txt:



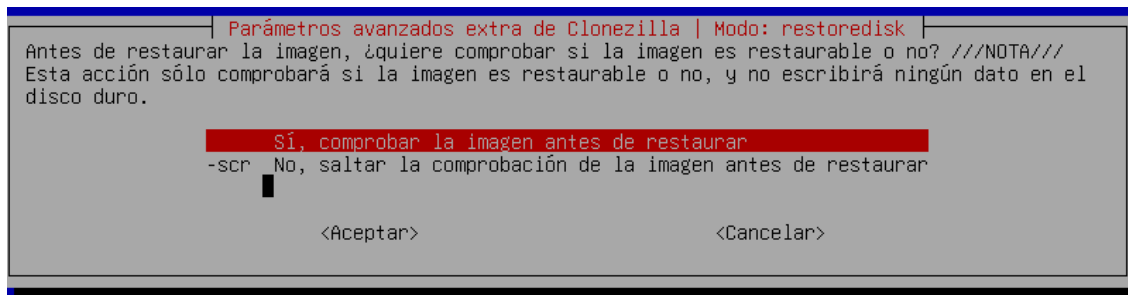
Iniciamos otra vez con el clonezilla y seleccionamos restaurar la imagen:



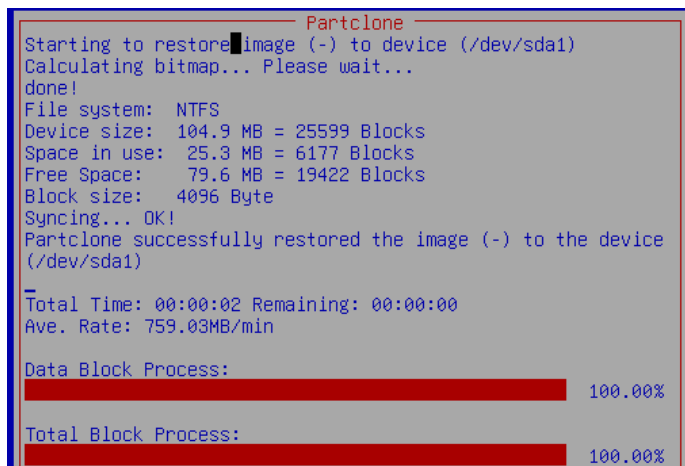
Seleccionamos el disco de antes:



Seleccionamos que queremos comprobar la imagen antes de restaurarla:



Ahora nos pedirá la contraseña y simplemente esperamos la partición:



Y ahora como vemos se nos ha restaurado como lo teníamos antes:

