

Análisis forense

Unidad 1. Actividad 1



16 de octubre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Ejercicio 1. 2](#_Toc148985456)

[Ejercicio 2 4](#_Toc148985457)

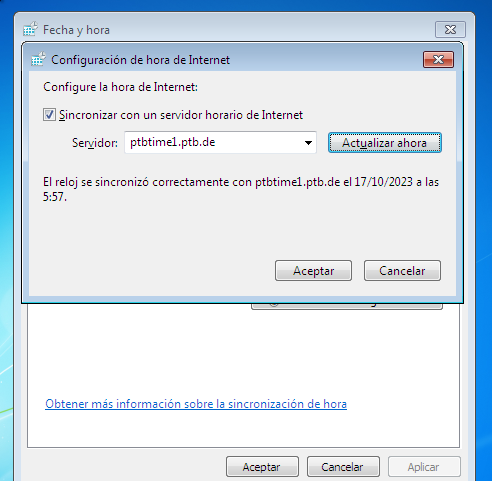
[Ejercicio 3. 8](#_Toc148985458)

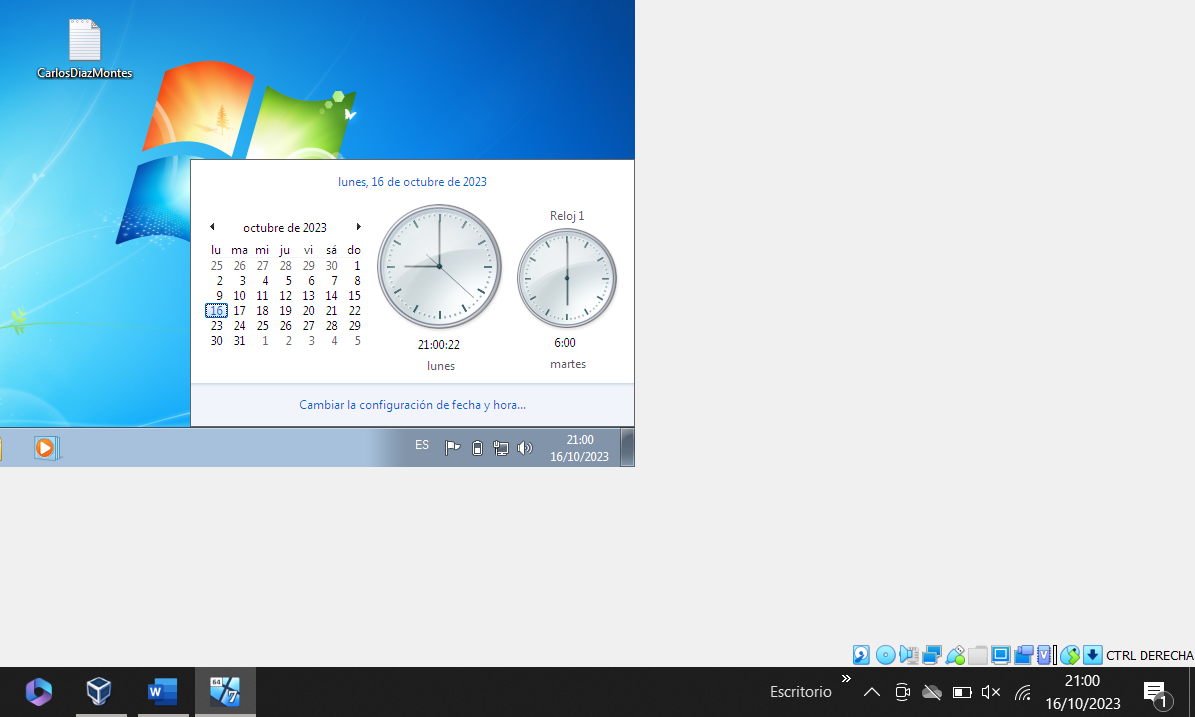
[Ejercicio 4 10](#_Toc148985459)

# Ejercicio 1.

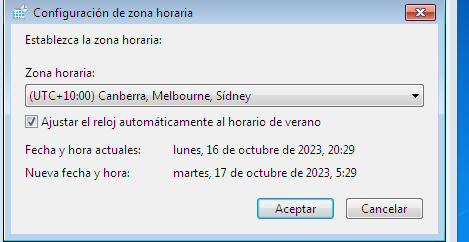
Una vez instalado correctamente el Windows 7, ajustamos la hora y fecha del equipo:

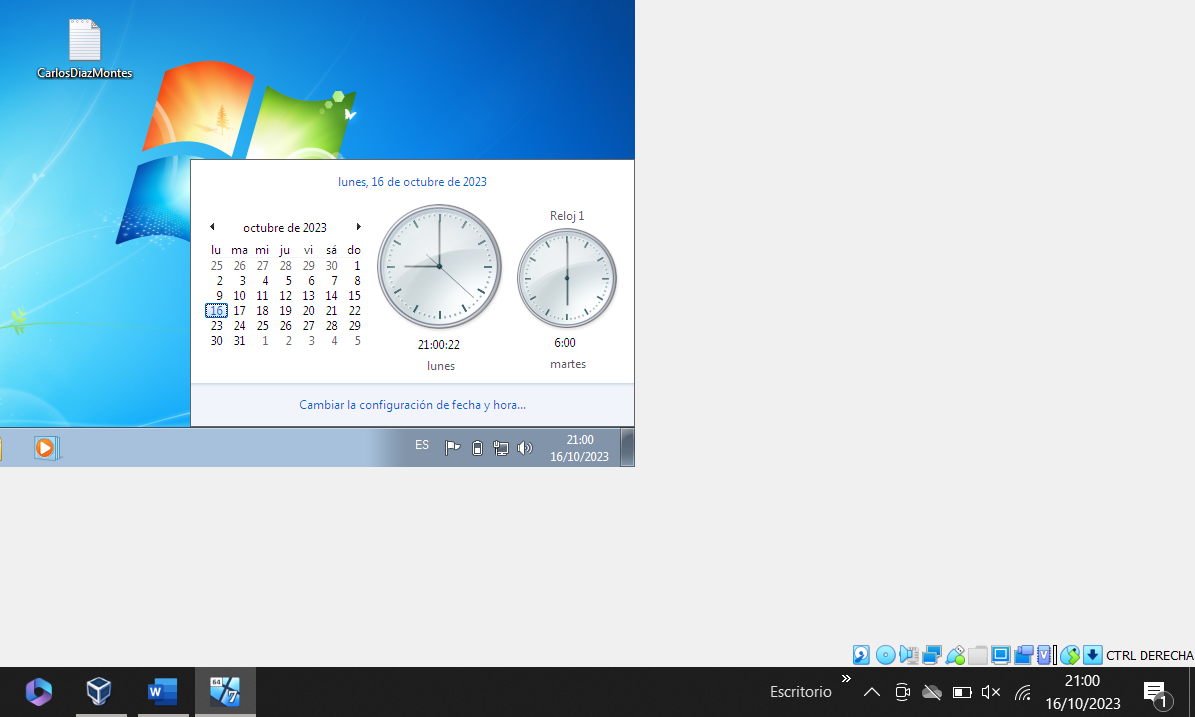
**a)**





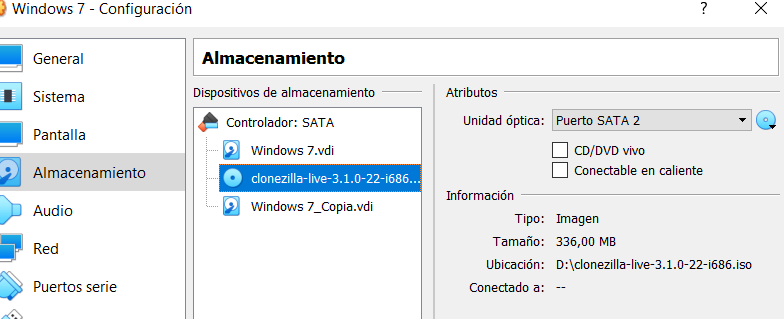
**b)**



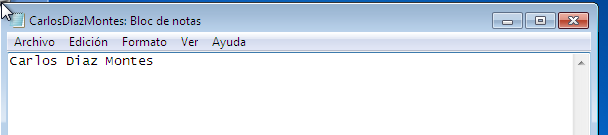


# Ejercicio 2

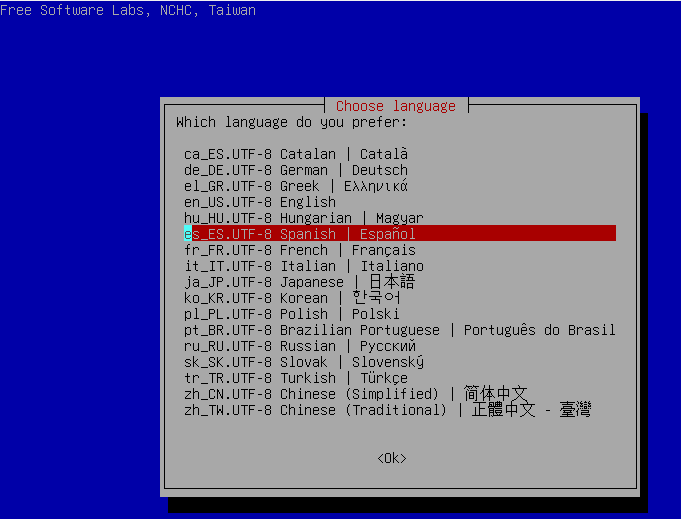
Nos vamos a la configuración de la maquina y en almacenamiento añadimos el disco duro llamado Clonezilla:



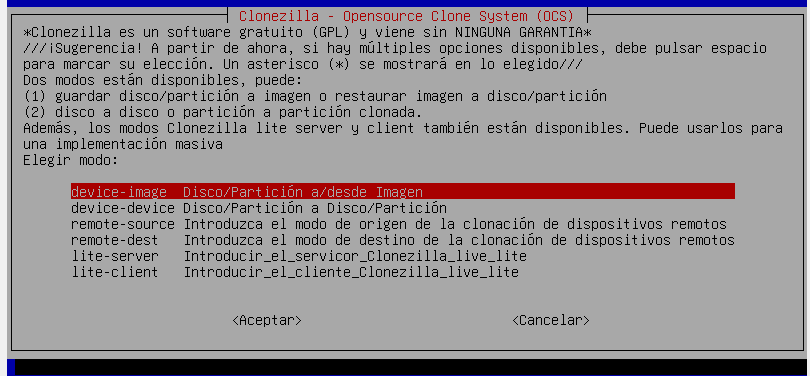
Ahora nos creamos el txt:



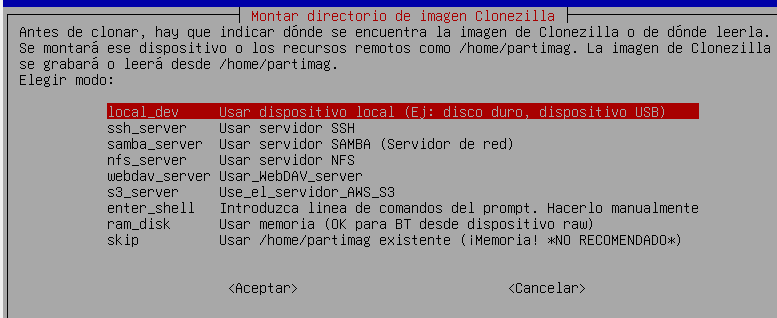
Elegimos el idioma una vez arrancado el clonezilla:



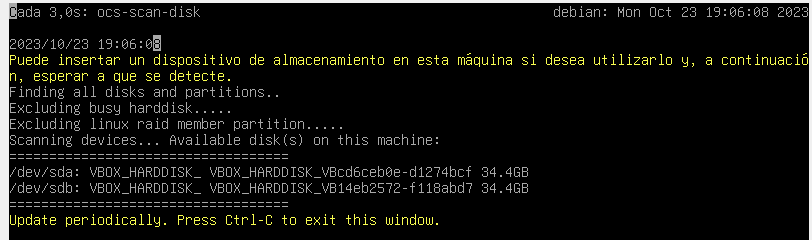
En este menú seleccionamos que queremos trabajar de imagen a dispositivo:



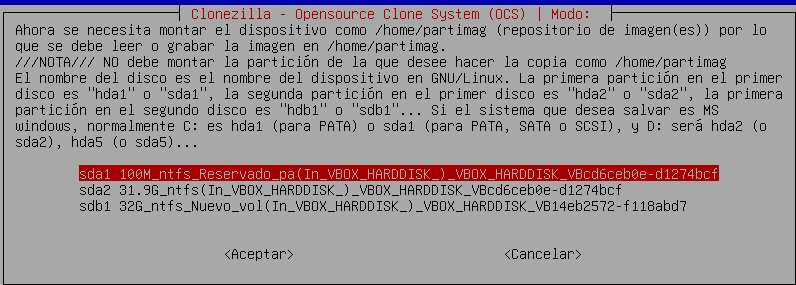
Ahora seleccionamos donde montamos la imagen de clonezilla:



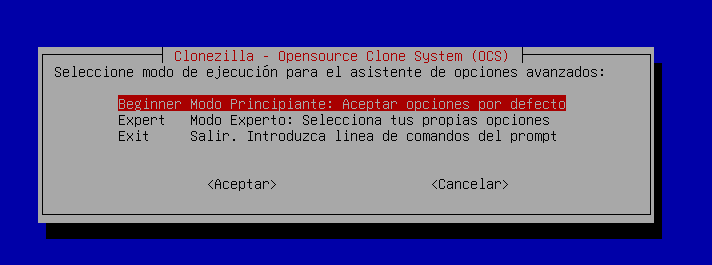
Ahora como vemos esta detectando los dos discos que tenemos en la máquina:



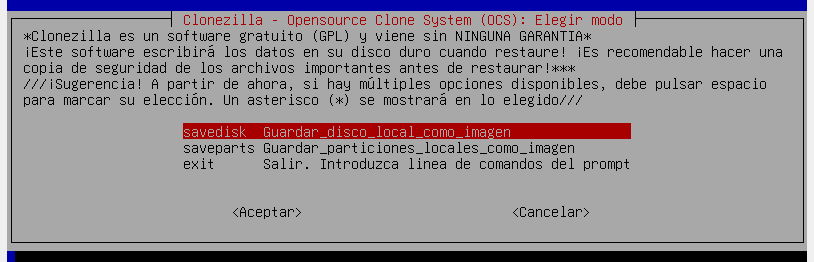
Ahora seleccionamos el disco:



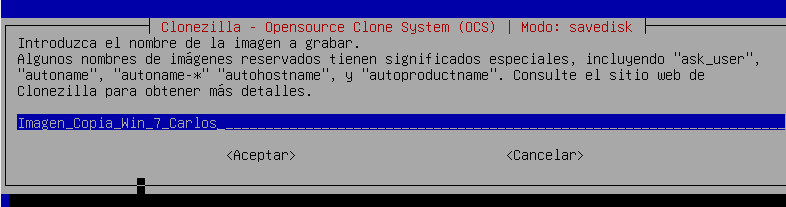
Seleccionamos el tipo de ejecución:

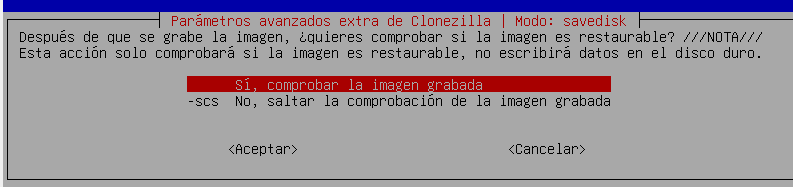


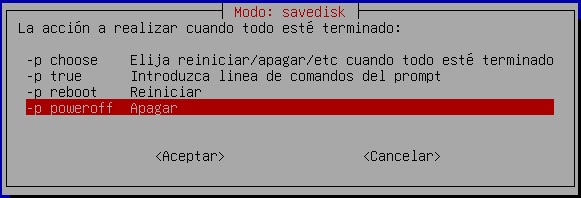
Guardamos el disco local en particiones:



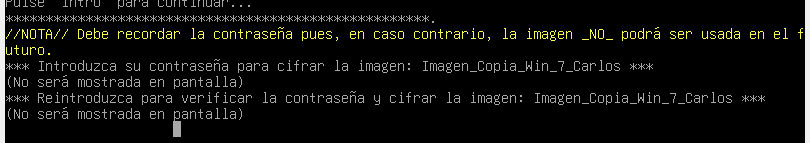
Seleccionamos el nombre de la imagen:



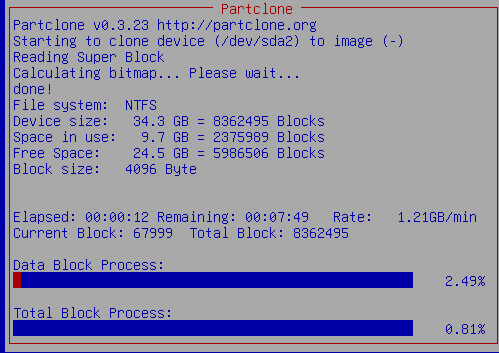
Comprobamos que la imagen sea cifrable: 



Ponemos la contraseña (cdiazm21)

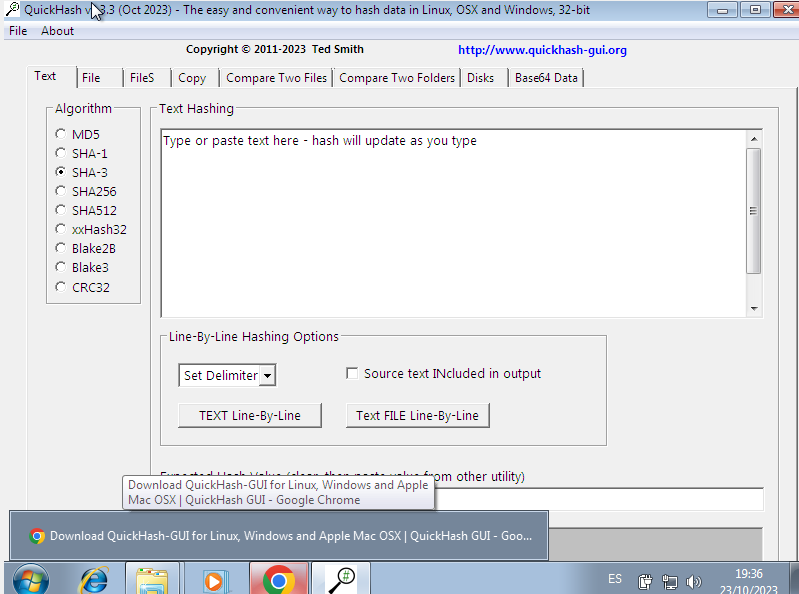


Ahora se hace la partición:

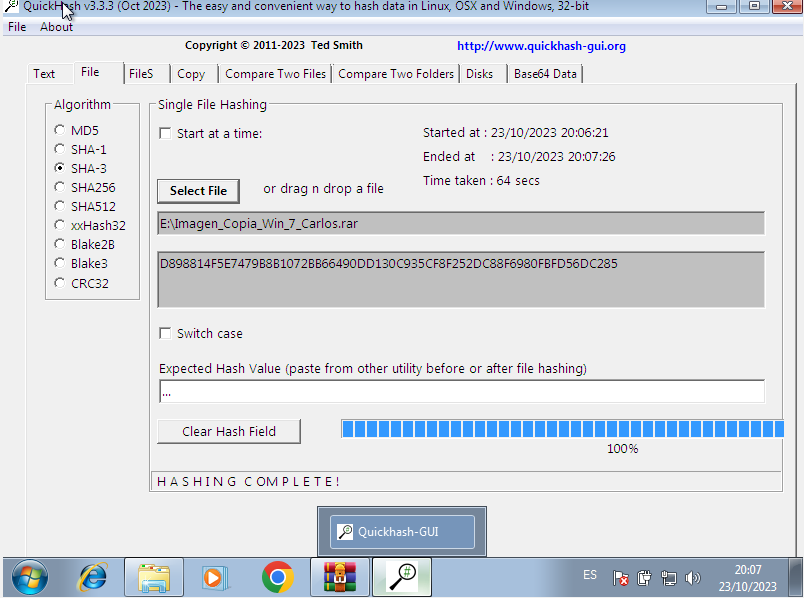


# Ejercicio 3.

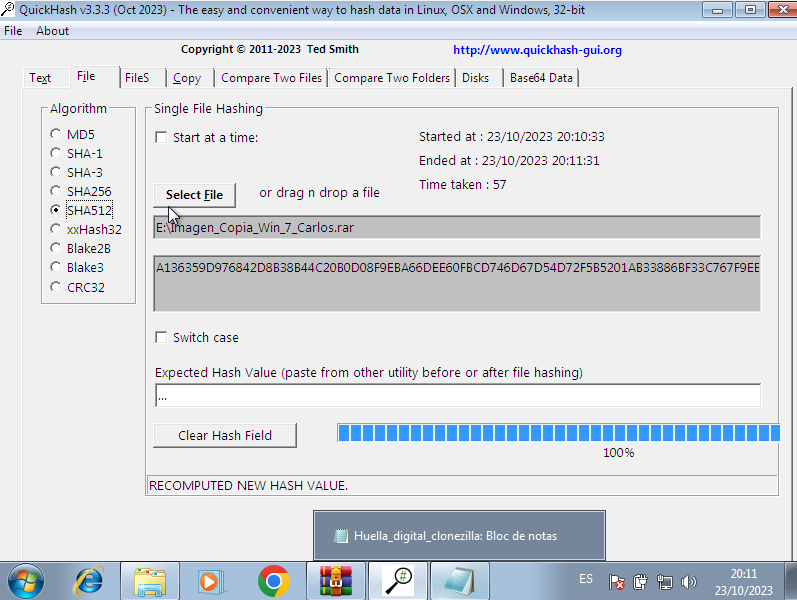
Ahora reiniciamos la maquina y nos decargamos quickhash:



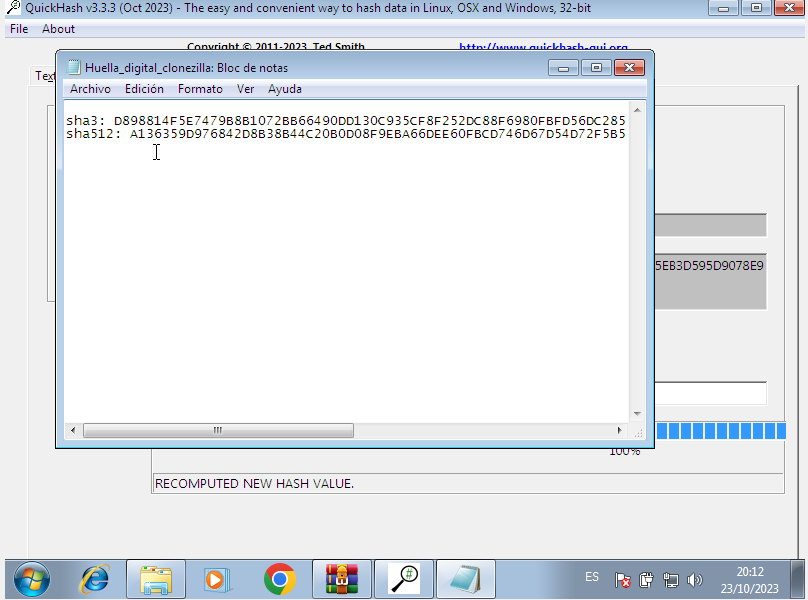
Ahora instalamos el winrar y la carpeta la comprimimos a .rar y con quickhash usamos el sha3:



Y con sha 512:

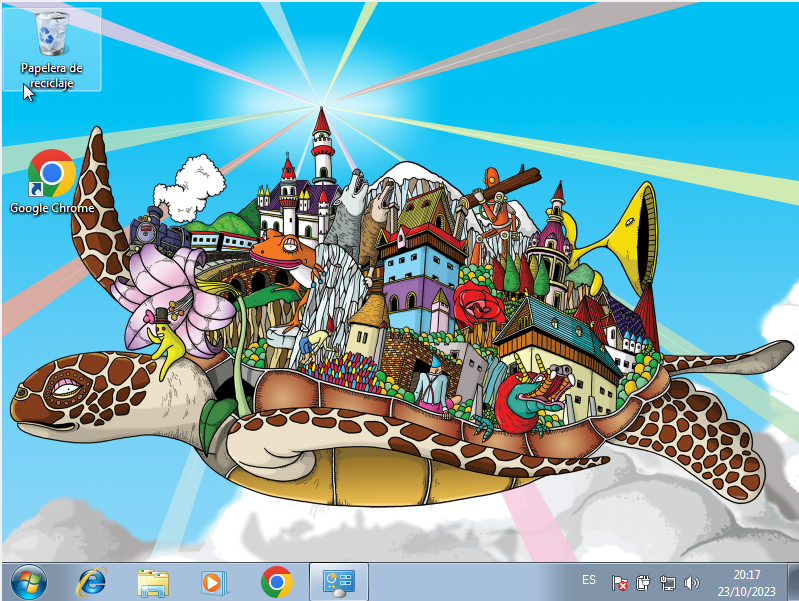


El documento de texto:

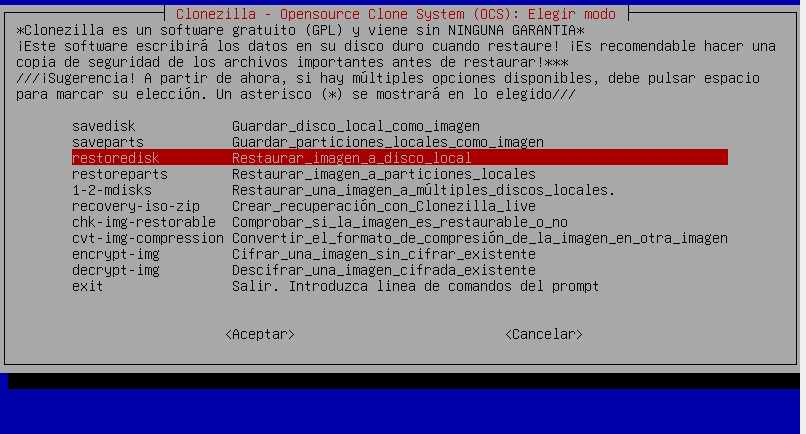


# Ejercicio 4

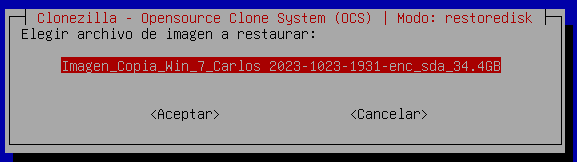
Cambio el fondo de pantalla y borro el archivo txt:



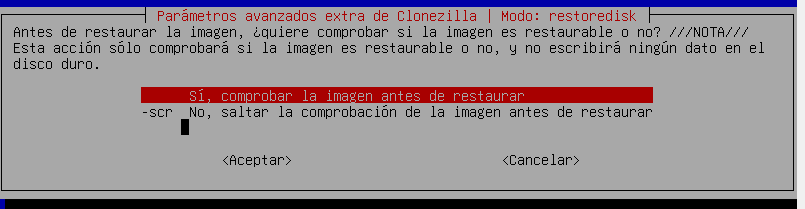
Iniciamos otra vez con el clonezilla y seleccionamos restaurar la imagen:



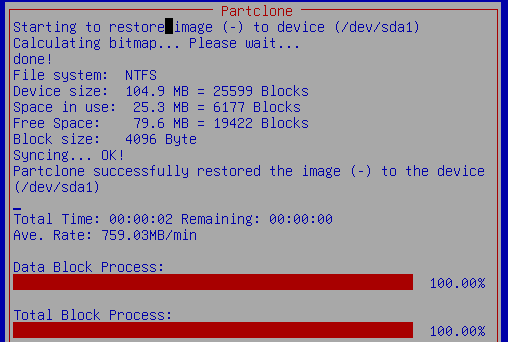
Seleccionamos el disco de antes:



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:

