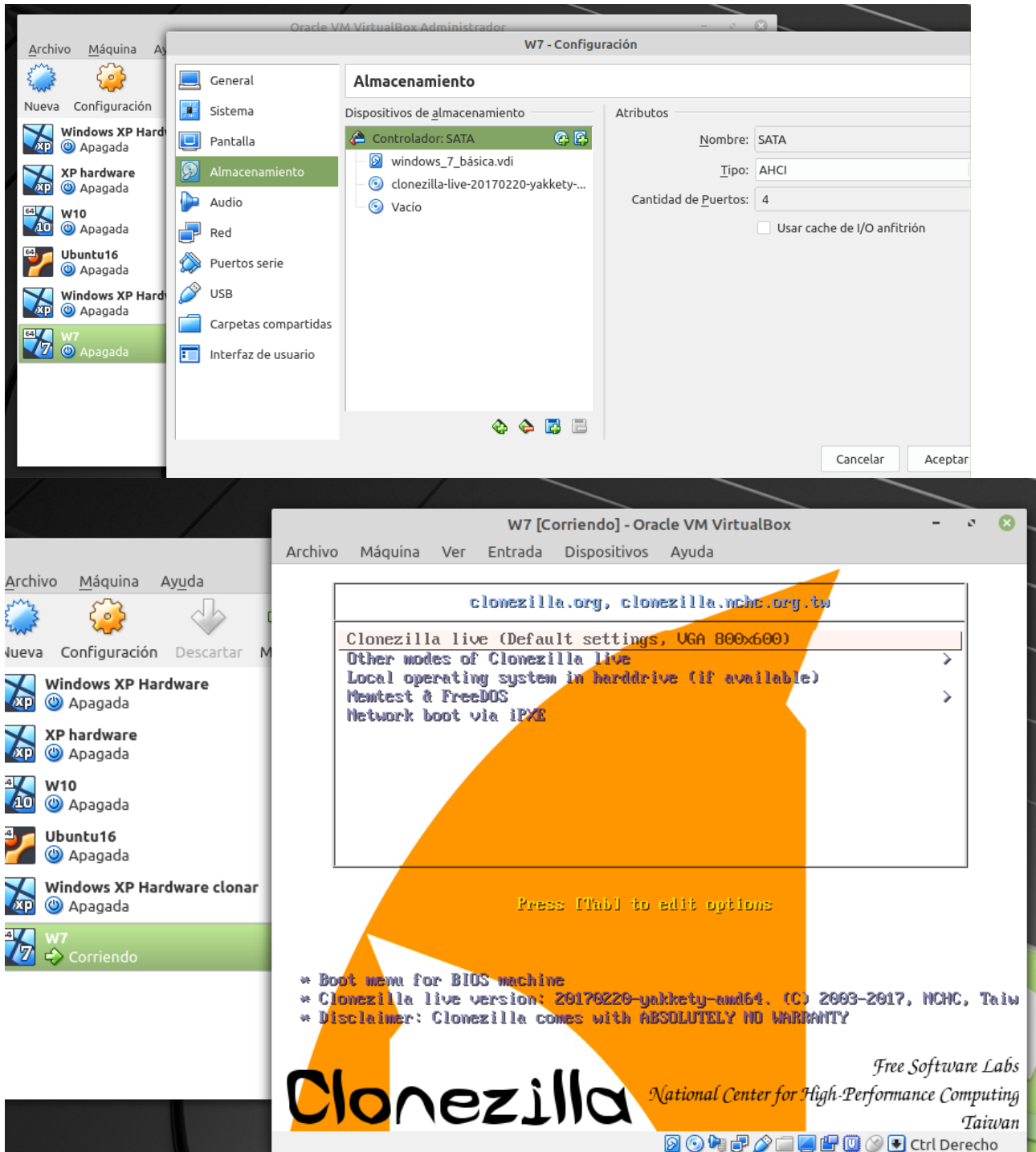


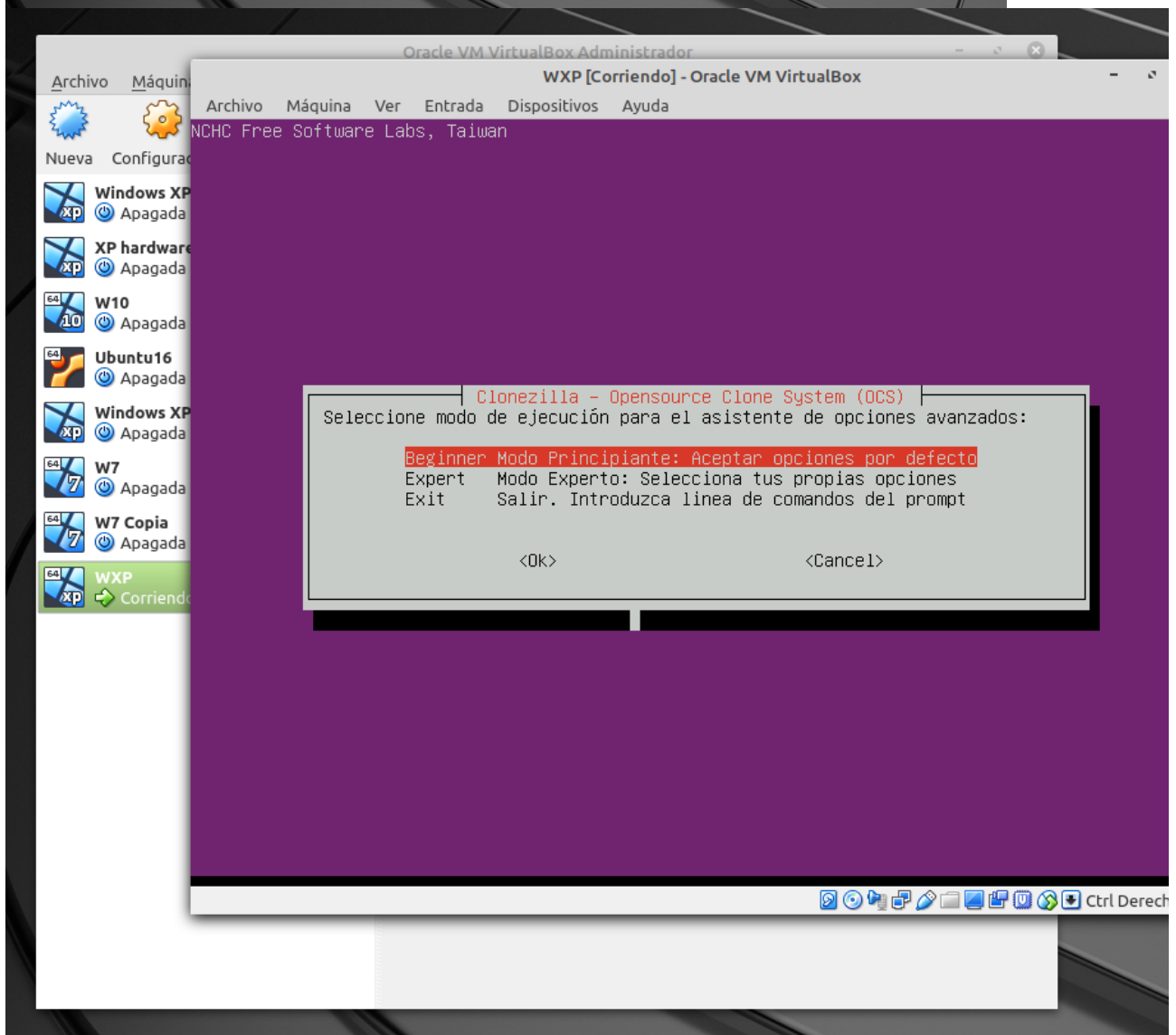
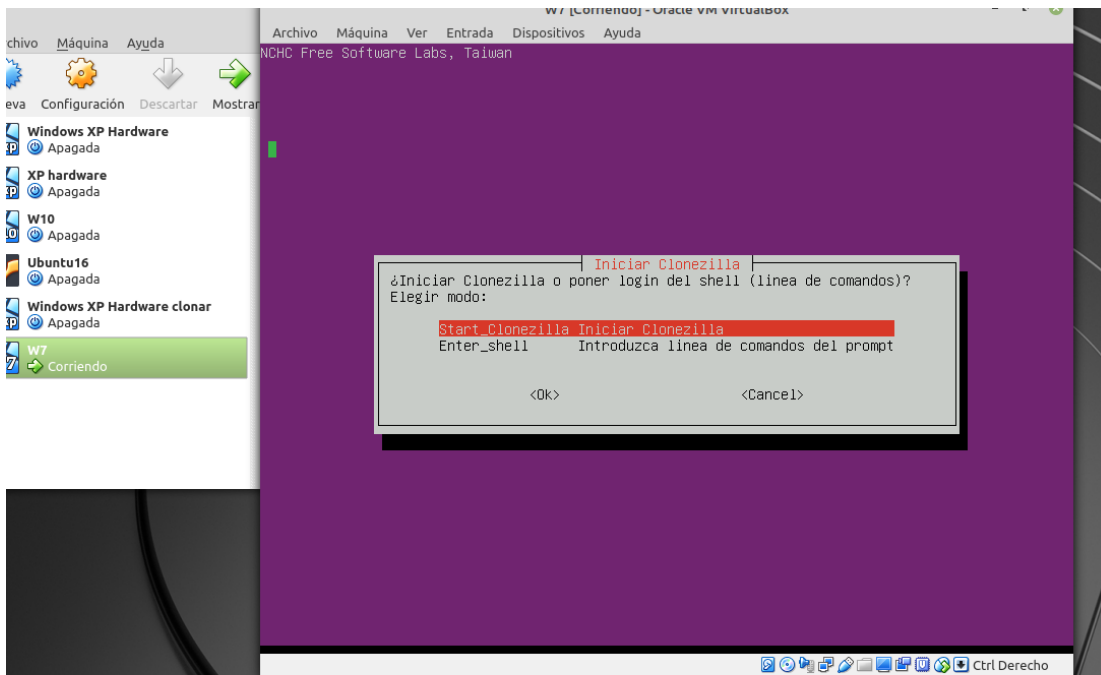
Práctica Clonezilla Imagen – Contraseñas

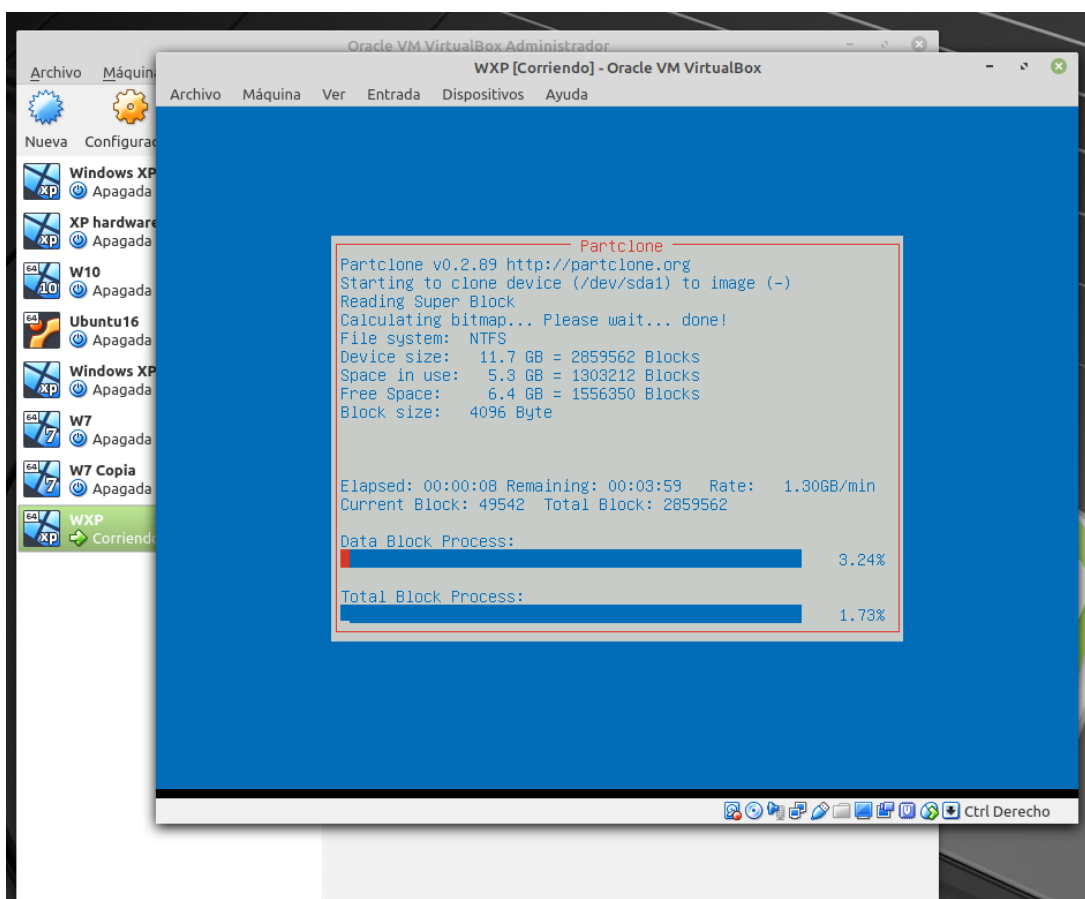
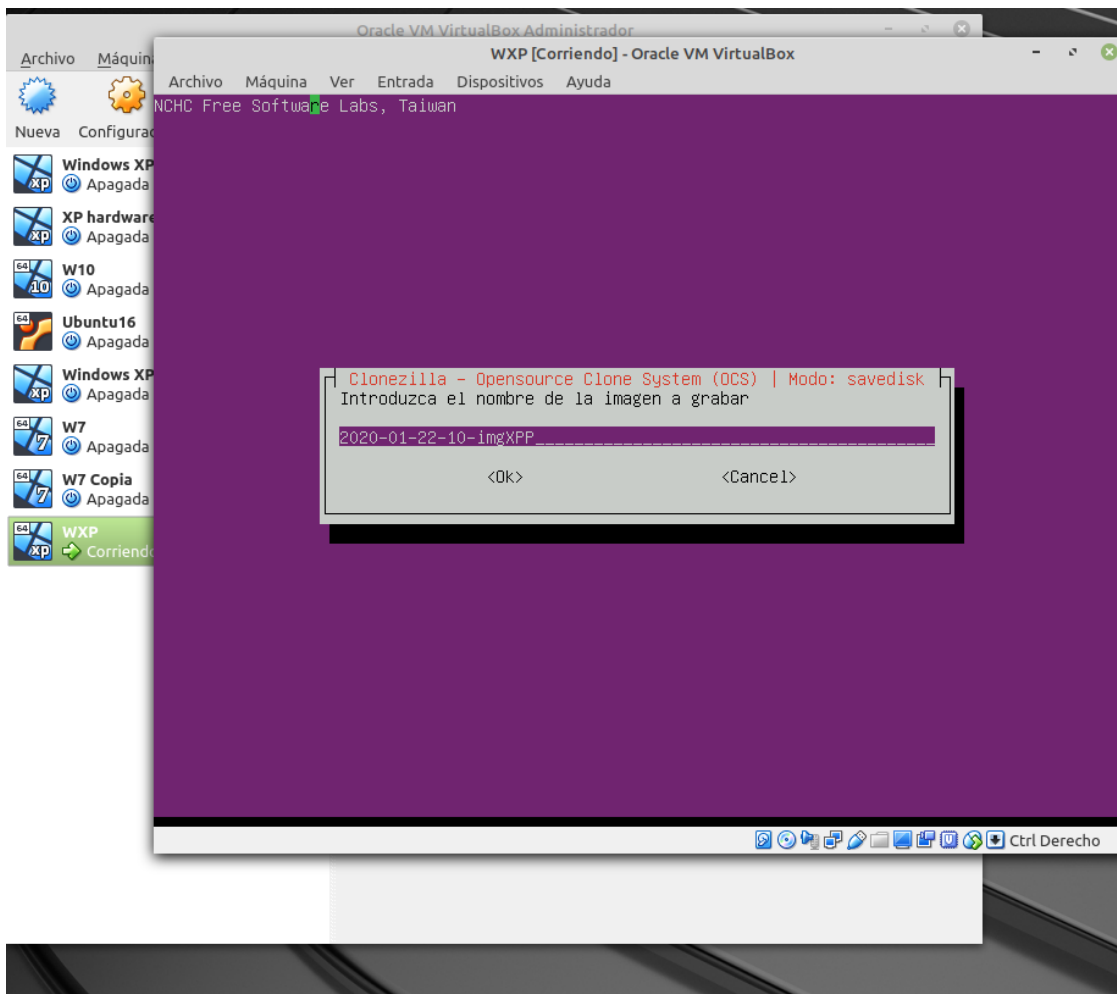
Nombre: José Manuel Monteagudo Sánchez

Fecha: 22/01/2020

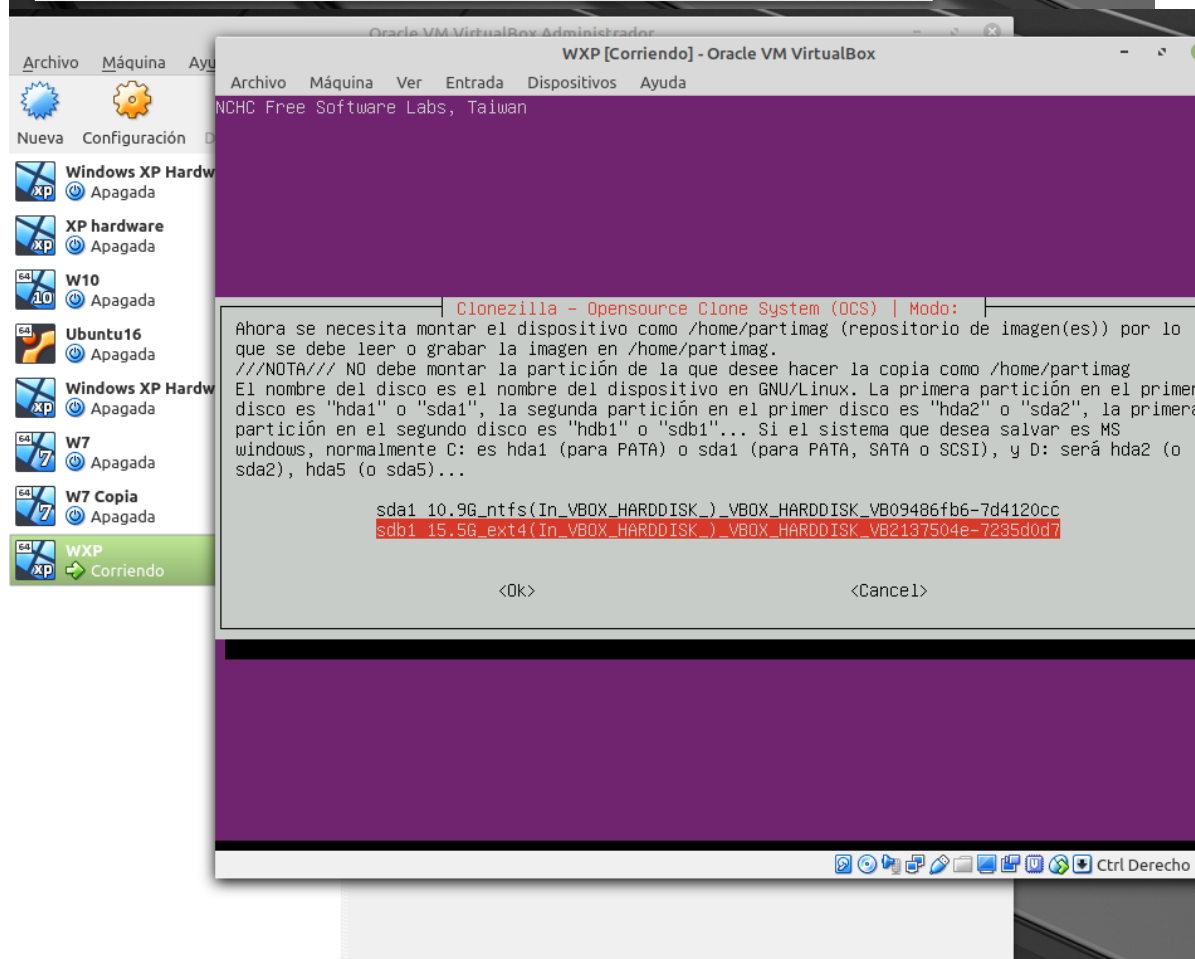
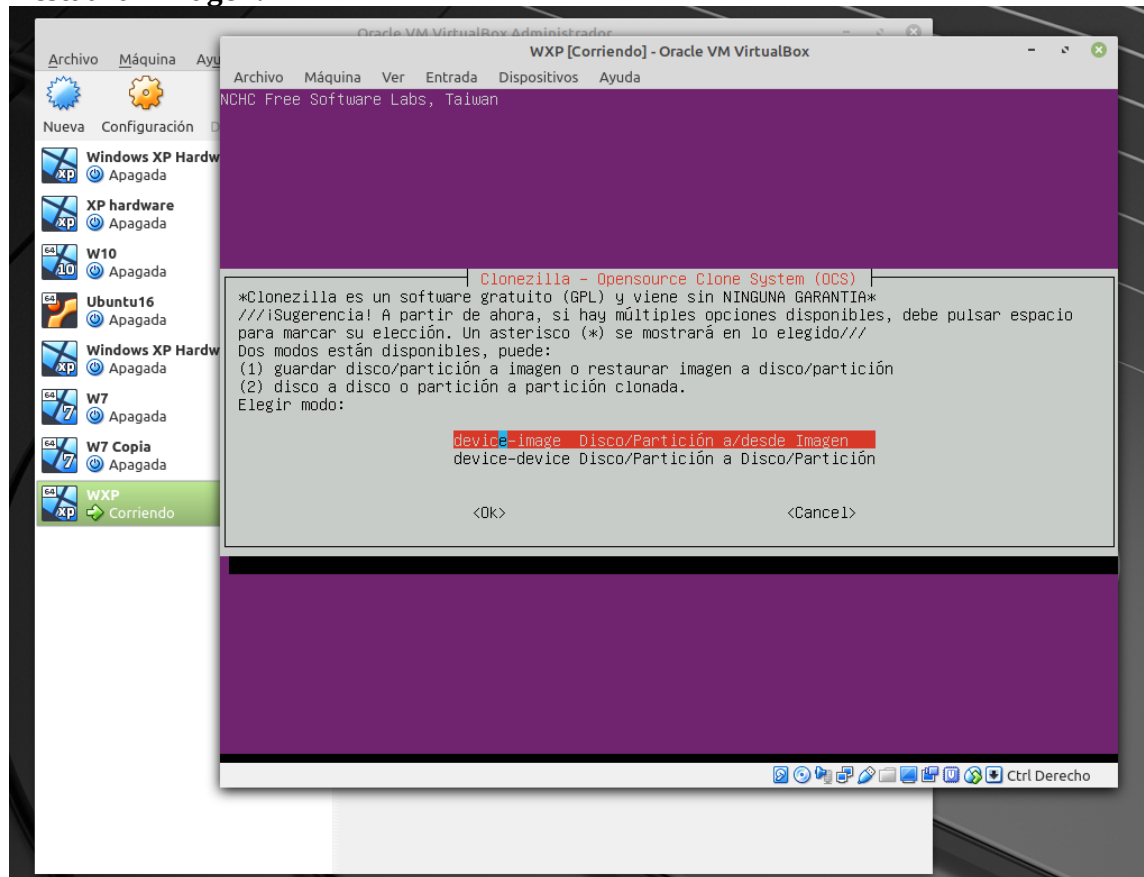
Clonezilla Imagen:

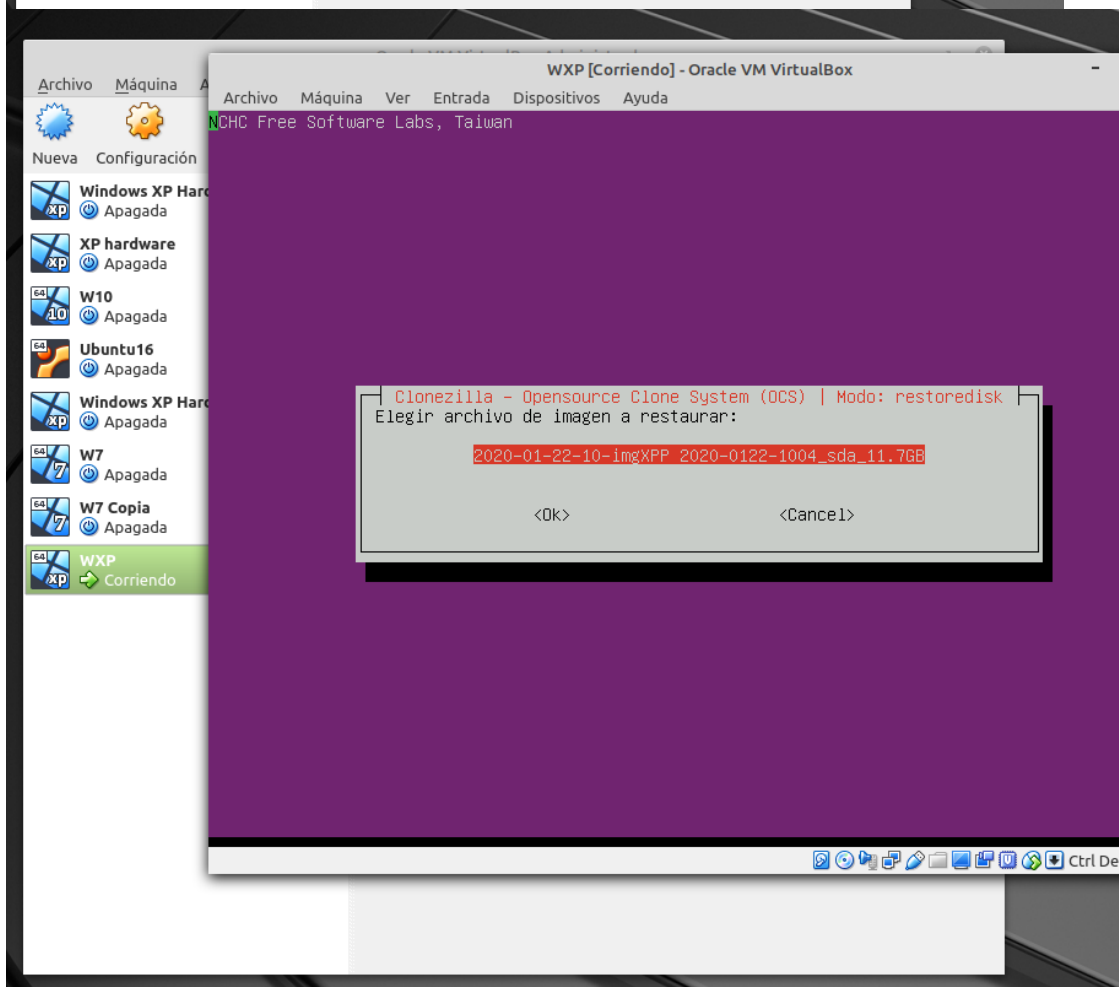
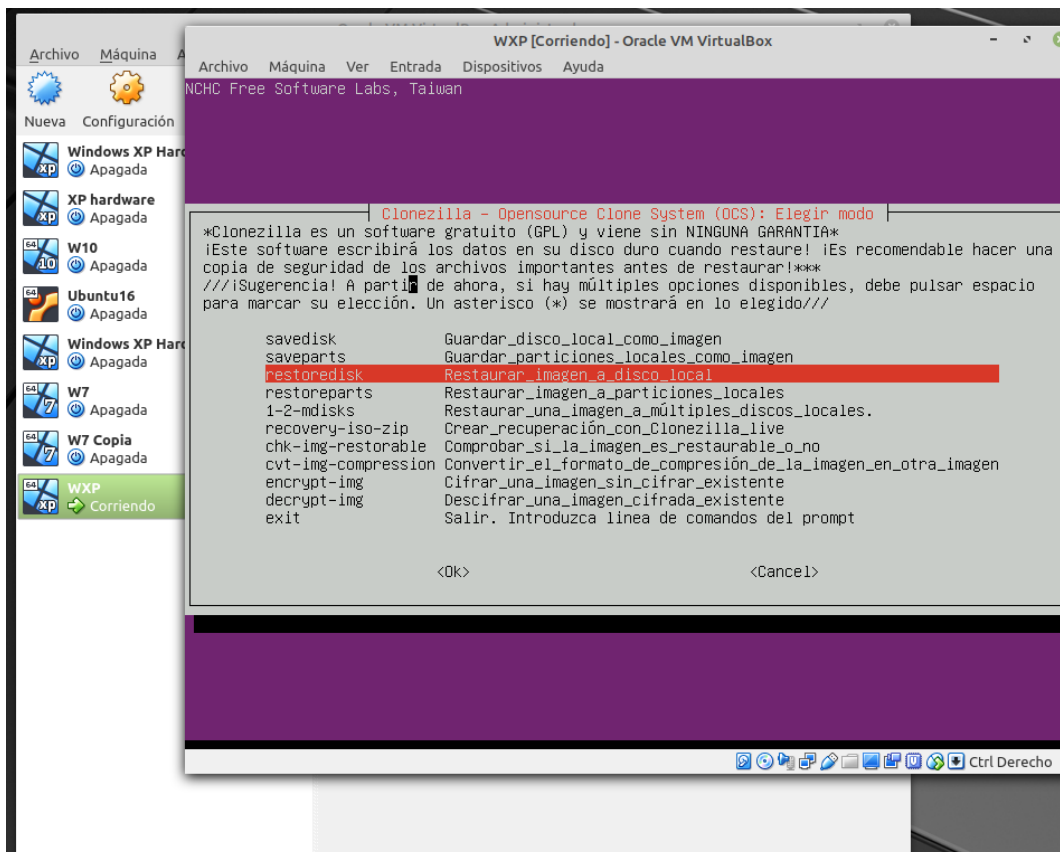


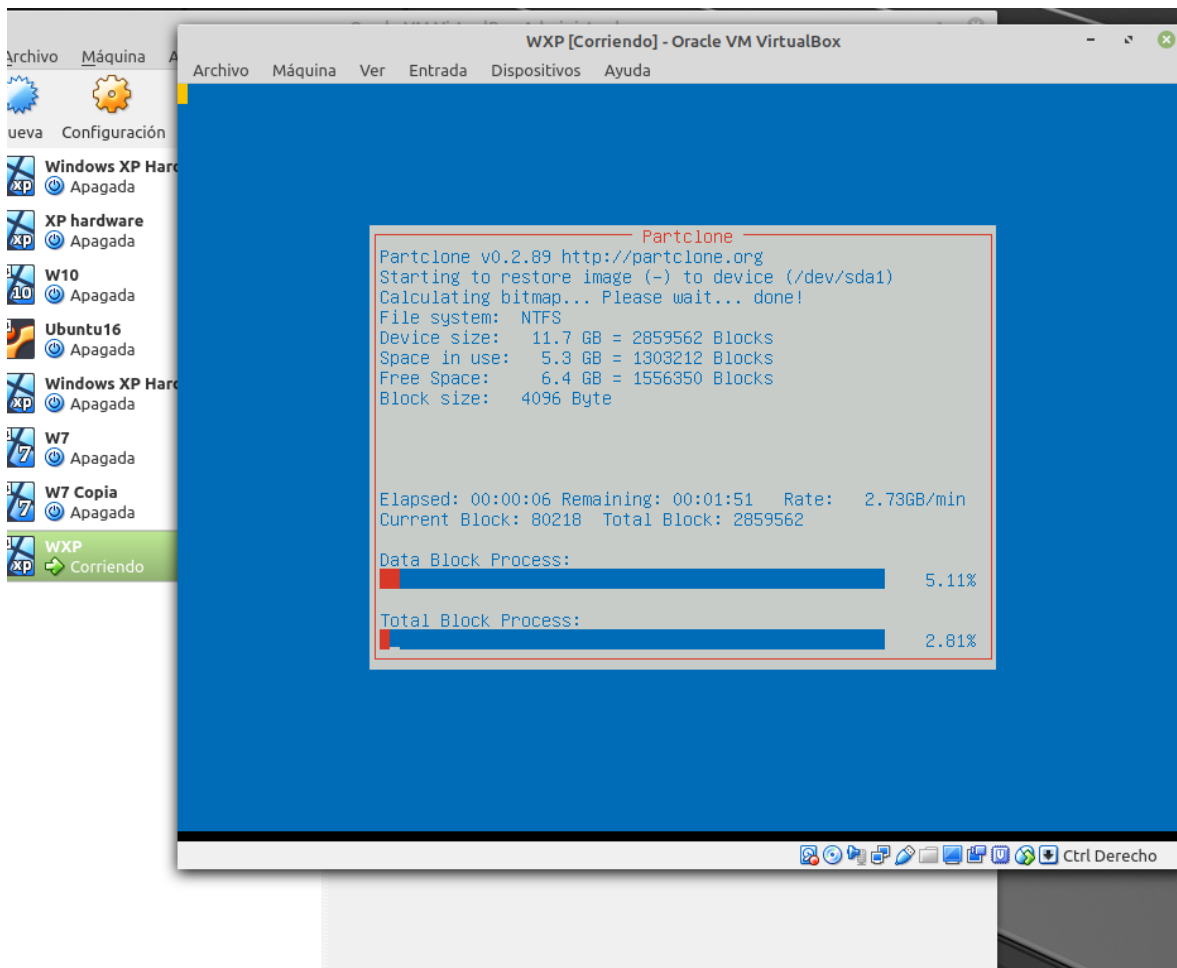




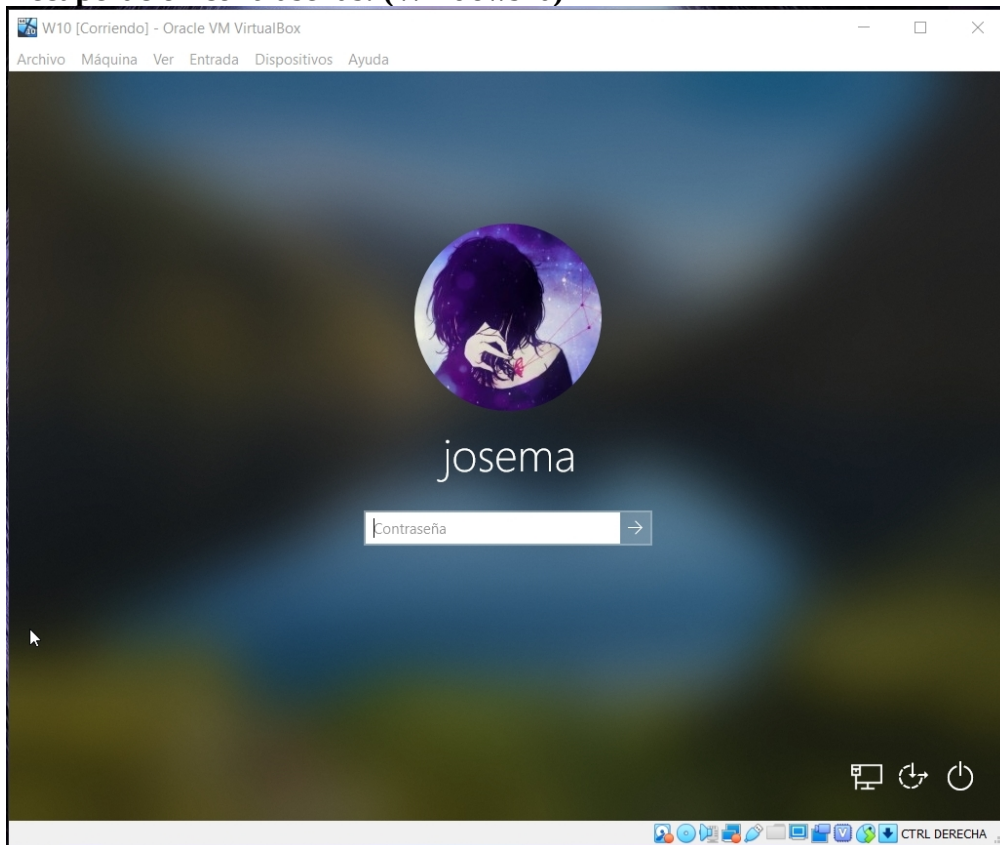
Restaurar imagen:



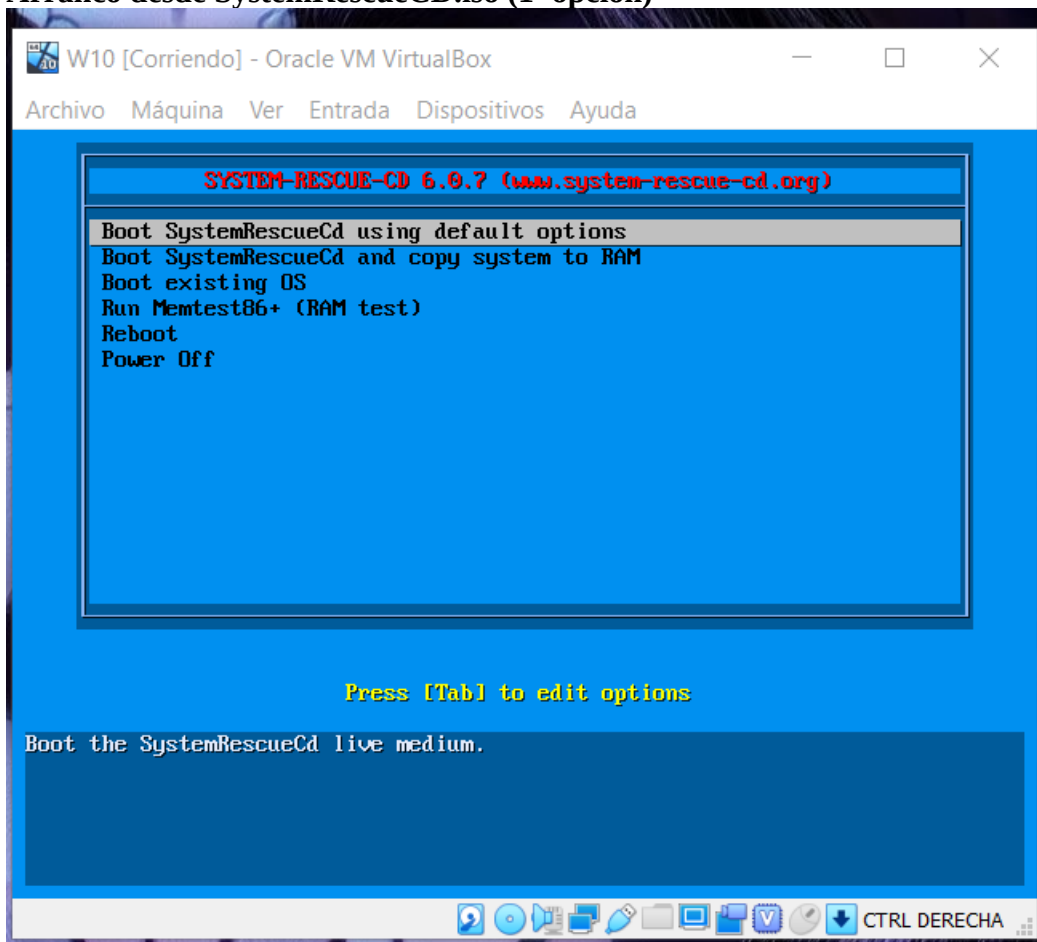




Recuperación contraseñas: (Windows10)

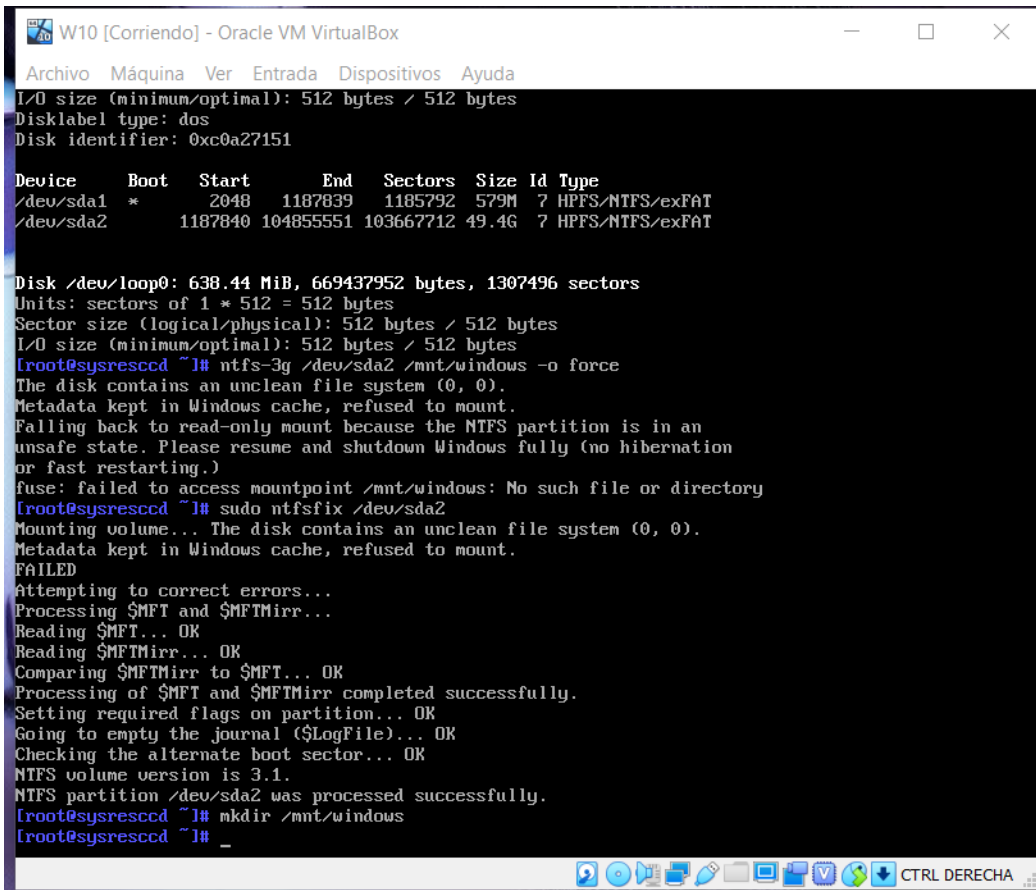


Arranco desde SystemRescueCD.iso (1ª opción)



Miro las particiones con **fdisk -l**

Intento **ntfs-3 /dev/sda2 mnt/windows -o force** pero antes hay que **sudo ntfsfix /dev/sda2** para que pueda montarlo
tampoco encontraba el directorio **mnt/windows** así que **mkdir /mnt/windows**

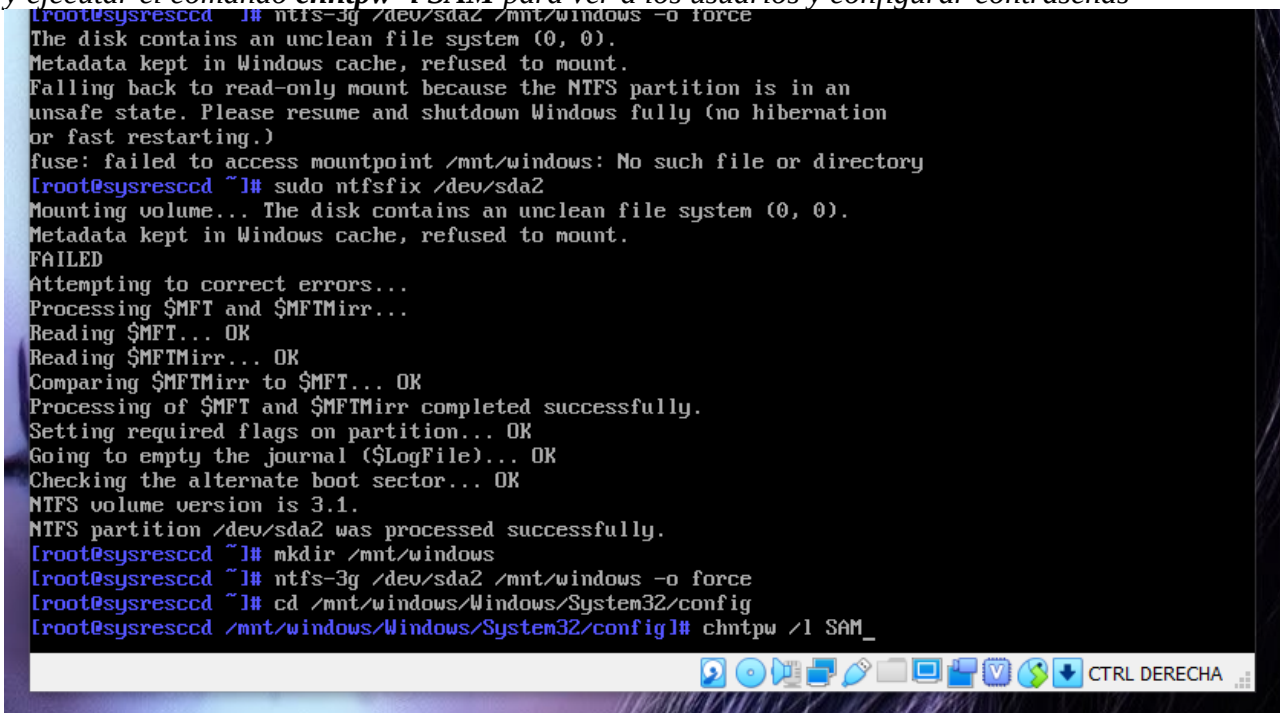


```
W10 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc0a27151

Device      Boot   Start      End  Sectors  Size Id Type
/dev/sda1   *        2048    1187839   1185792   579M  7 HPFS/NTFS/exFAT
/dev/sda2             1187840 104855551 103667712 49.4G  7 HPFS/NTFS/exFAT

Disk /dev/loop0: 638.44 MiB, 669437952 bytes, 1307496 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
[root@sysresccd ~]# ntfs-3g /dev/sda2 /mnt/windows -o force
The disk contains an unclean file system (0, 0).
Metadata kept in Windows cache, refused to mount.
Falling back to read-only mount because the NTFS partition is in an
unsafe state. Please resume and shutdown Windows fully (no hibernation
or fast restarting.)
fuse: failed to access mountpoint /mnt/windows: No such file or directory
[root@sysresccd ~]# sudo ntfsfix /dev/sda2
Mounting volume... The disk contains an unclean file system (0, 0).
Metadata kept in Windows cache, refused to mount.
FAILED
Attempting to correct errors...
Processing $MFT and $MFTMirr...
Reading $MFT... OK
Reading $MFTMirr... OK
Comparing $MFTMirr to $MFT... OK
Processing of $MFT and $MFTMirr completed successfully.
Setting required flags on partition... OK
Going to empty the journal ($LogFile)... OK
Checking the alternate boot sector... OK
NTFS volume version is 3.1.
NTFS partition /dev/sda2 was processed successfully.
[root@sysresccd ~]# mkdir /mnt/windows
[root@sysresccd ~]#
```

Ya se puede hacer **ntfs-3 /dev/sda2 mnt/windows -o force** ,
entrar en el directorio **mnt/windows/Windows/System32/config**
y ejecutar el comando **chntpw -l SAM** para ver a los usuarios y configurar contraseñas



```
[root@sysresccd ~]# ntfs-3g /dev/sda2 /mnt/windows -o force
The disk contains an unclean file system (0, 0).
Metadata kept in Windows cache, refused to mount.
Falling back to read-only mount because the NTFS partition is in an
unsafe state. Please resume and shutdown Windows fully (no hibernation
or fast restarting.)
fuse: failed to access mountpoint /mnt/windows: No such file or directory
[root@sysresccd ~]# sudo ntfsfix /dev/sda2
Mounting volume... The disk contains an unclean file system (0, 0).
Metadata kept in Windows cache, refused to mount.
FAILED
Attempting to correct errors...
Processing $MFT and $MFTMirr...
Reading $MFT... OK
Reading $MFTMirr... OK
Comparing $MFTMirr to $MFT... OK
Processing of $MFT and $MFTMirr completed successfully.
Setting required flags on partition... OK
Going to empty the journal ($LogFile)... OK
Checking the alternate boot sector... OK
NTFS volume version is 3.1.
NTFS partition /dev/sda2 was processed successfully.
[root@sysresccd ~]# mkdir /mnt/windows
[root@sysresccd ~]# ntfs-3g /dev/sda2 /mnt/windows -o force
[root@sysresccd ~]# cd /mnt/windows/Windows/System32/config
[root@sysresccd /mnt/windows/Windows/System32/config]# chntpw -l SAM_
```


Con **chntpw -u "nombre usuario"** selecciono el usuario al que le quiero configurar la contraseña

```
[root@sysresccd /mnt/windows/Windows/System32/config]# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 131072 [20000] bytes, containing 9 pages (+ 1 headerpage)
Used for data: 287/60200 blocks/bytes, unused: 23/13240 blocks/bytes.
```

RID	Username	Admin?	Lock?
01f4	Administrador	ADMIN	dis/lock
01f7	DefaultAccount		dis/lock
01f5	Invitado		dis/lock
03e9	josema	ADMIN	
01f8	WDAGUtilityAccount		dis/lock

```
[root@sysresccd /mnt/windows/Windows/System32/config]# chntpw -u josema_
```

O con **chntpw -i SAM** accedo al archivo SAM de windows y selecciono la opción 1

```
[root@sysresccd /mnt/windows/Windows/System32/config]# chntpw -i SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 131072 [20000] bytes, containing 9 pages (+ 1 headerpage)
Used for data: 287/60200 blocks/bytes, unused: 23/13240 blocks/bytes.
```

```
<>=====<> chntpw Main Interactive Menu <>=====<>
```

```
Loaded hives: <SAM>
```

- 1 - Edit user data and passwords
- 2 - List groups
- - -
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

```
What to do? [1] -> _
```

```
Loaded hives: <SAM>
```

- 1 - Edit user data and passwords
- 2 - List groups
- - -
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

```
What to do? [1] -> 1
```

```
===== chntpw Edit User Info & Passwords =====
```

RID	Username	Admin?	Lock?
01f4	Administrador	ADMIN	dis/lock
01f7	DefaultAccount		dis/lock
01f5	Invitado		dis/lock
03e9	josema	ADMIN	
01f8	WDAGUtilityAccount		dis/lock

```
Please enter user number (RID) or 0 to exit: [3e9] josema
```

```
<>=====<> chntpw Main Interactive Menu <>=====<>
```

```
Loaded hives: <SAM>
```

- 1 - Edit user data and passwords
- 2 - List groups
- - -
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

```
What to do? [1] -> 1_
```

Escribo el usuario y la opción 1 de limpiar la password

```
Please enter user number (RID) or 0 to exit: [3e9] 3e9
===== USER EDIT =====

RID      : 1001 [03e9]
Username: josema
fullname:
comment :
homedir :

00000221 = Usuarios (which has 3 members)
00000220 = Administradores (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled      | [ ] Homedir req.   | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout   | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20) | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total login count: 3

- - - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > _
```

Al final en el apartado de Lock? (Bloqueado) quedan los administradores sin contraseña

```
==== chntpw Edit User Info & Passwords ====

| RID |-----| Username |-----| Admin? | Lock? |---| |
| 01f4 | | Administrador | | ADMIN | | *BLANK* | |
| 01f7 | | DefaultAccount | | | | dis/lock | |
| 01f5 | | Invitado | | | | dis/lock | |
| 03e9 | | josema | | ADMIN | | *BLANK* | |
| 01f8 | | WDAGUtilityAccount | | | | dis/lock | |

Please enter user number (RID) or 0 to exit: [3e9] _
```

Y guardo los cambios en el archivo SAM

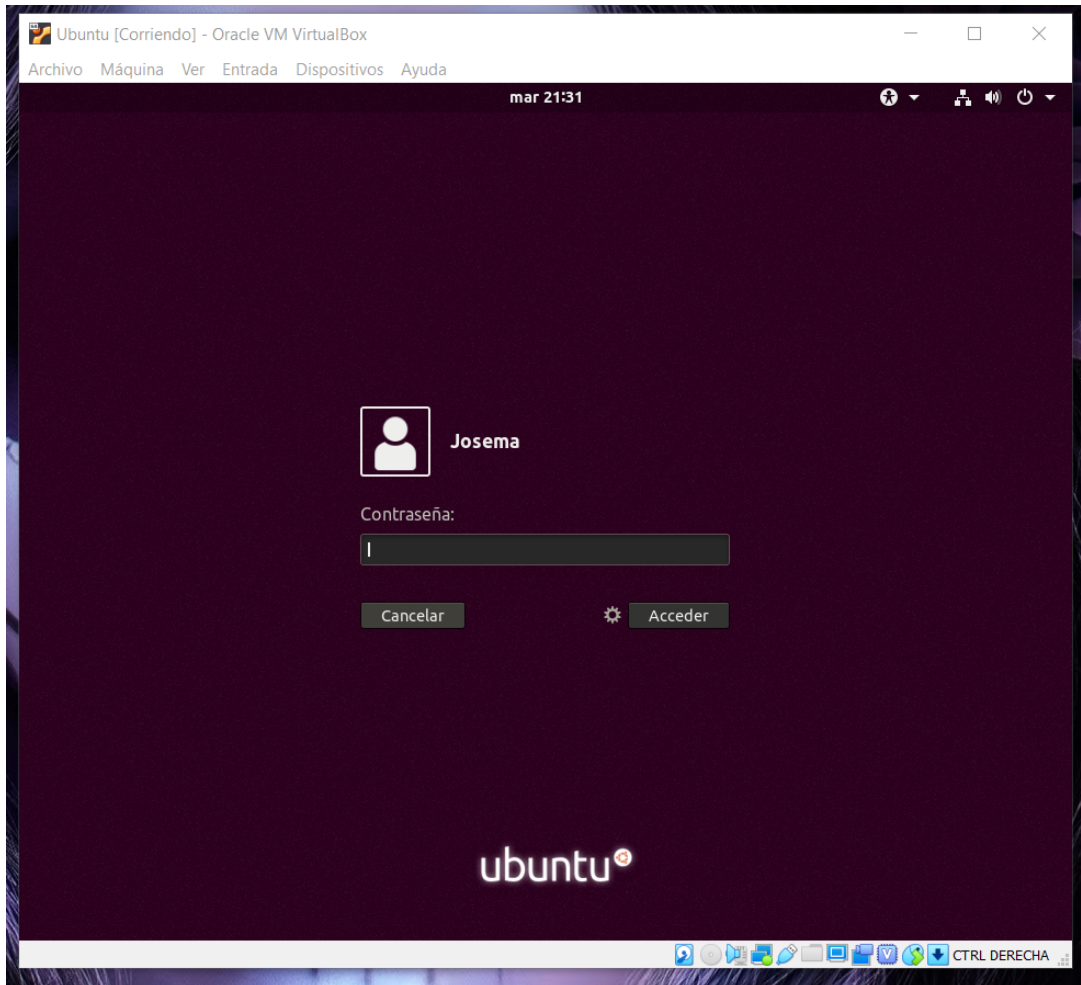
```
Loaded hives: <SAM>

1 - Edit user data and passwords
2 - List groups
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

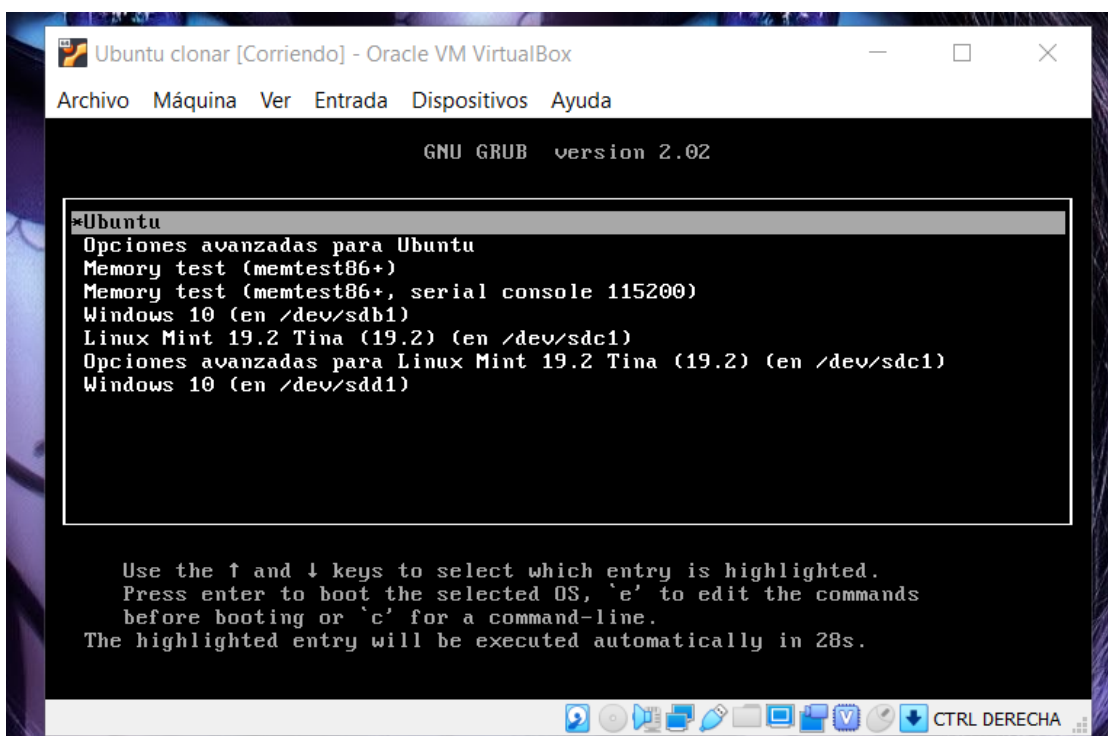
What to do? [1] -> q

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
[root@sysresccd /mnt/windows/Windows/System32/config]#
```

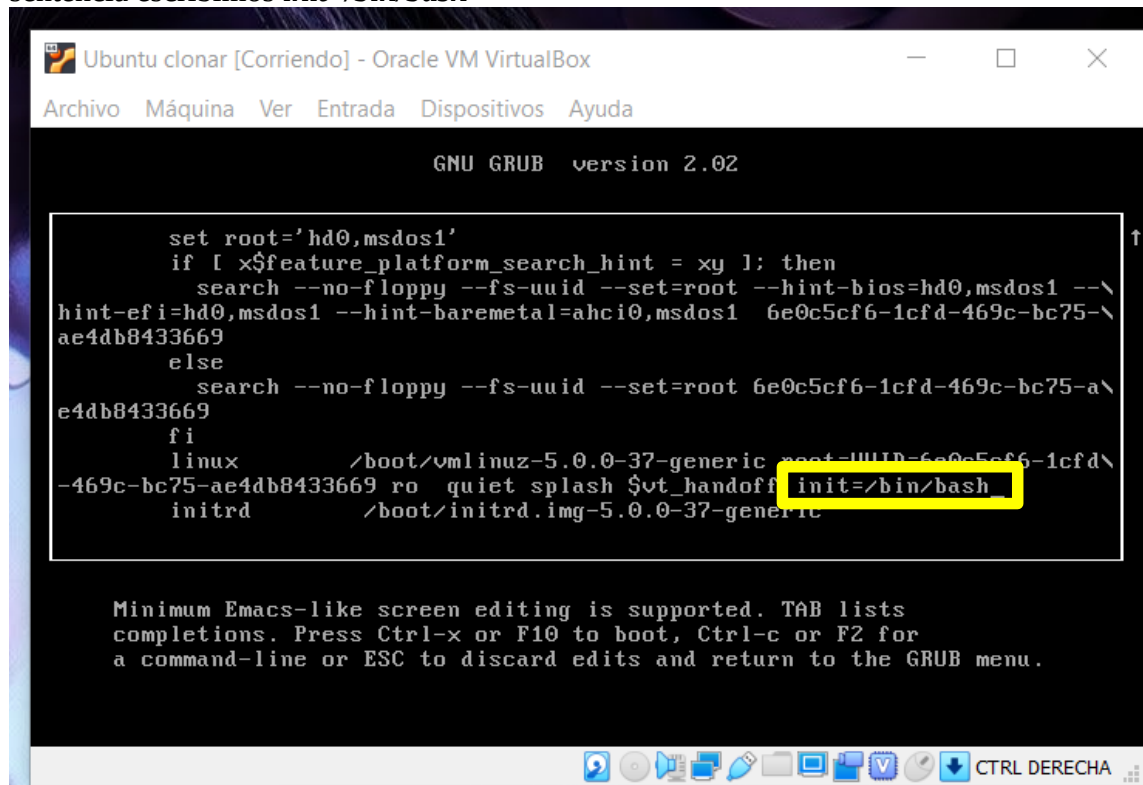
Linux: Ubuntu 18.04



Al encender la máquina nos da a elegir, pero aquí pulsamos la tecla “e”



Nos lleva a esta pantalla con código, más abajo buscamos la palabra “**linux**” y al final de esa sentencia escribimos **init=/bin/bash**



```
GNU GRUB version 2.02

set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --\
hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 6e0c5cf6-1cfd-469c-bc75-\
ae4db8433669
else
  search --no-floppy --fs-uuid --set=root 6e0c5cf6-1cfd-469c-bc75-a\
e4db8433669
fi
linux /boot/vmlinuz-5.0.0-37-generic root=UUID=6e0c5cf6-1cfd-\
469c-bc75-ae4db8433669 ro quiet splash $vt_handoff init=/bin/bash
initrd /boot/initrd.img-5.0.0-37-generic

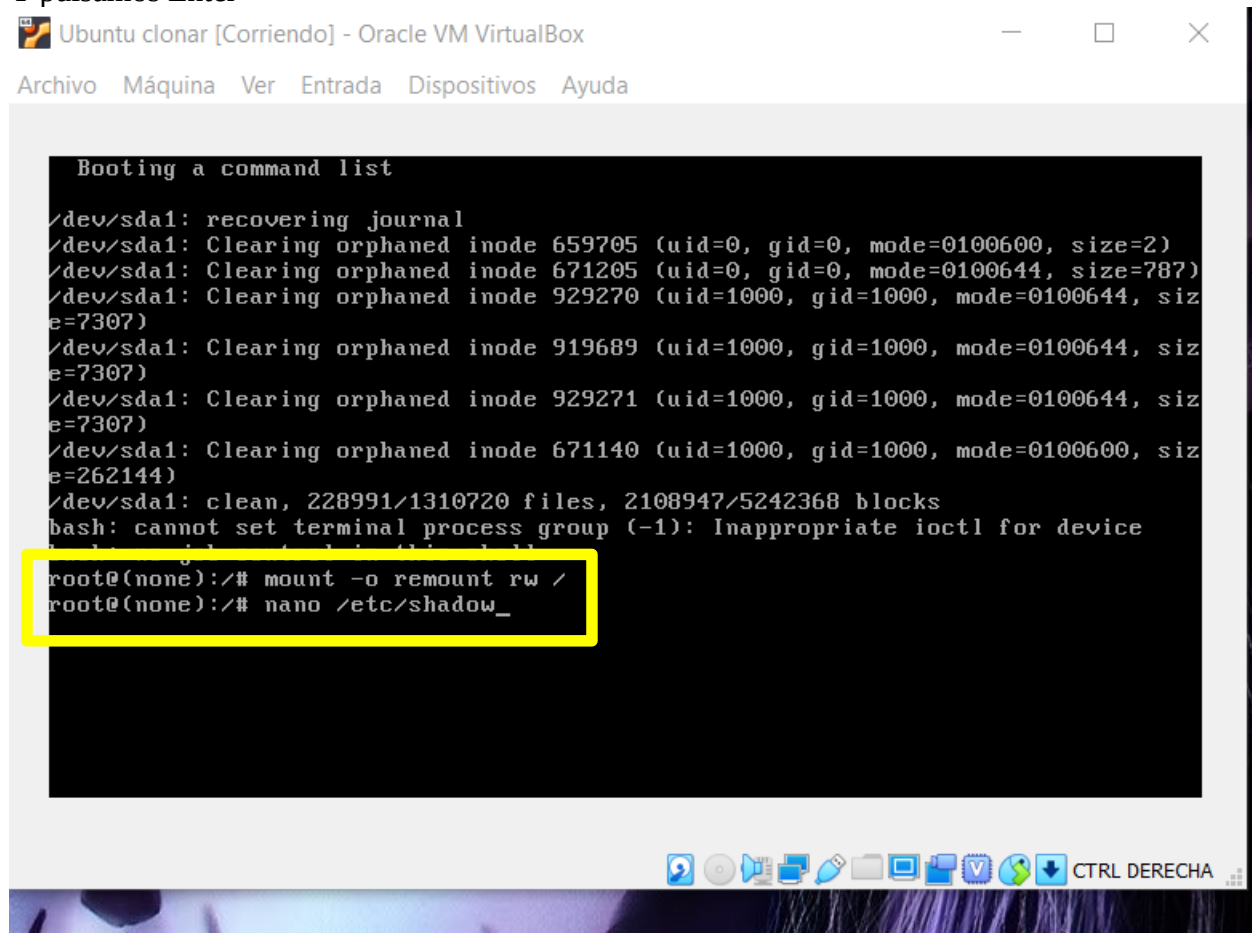
Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.
```

Pulsamos F10 y reinicia, pero se ejecuta un terminal, en el que escribiremos

mount -o remount rw /

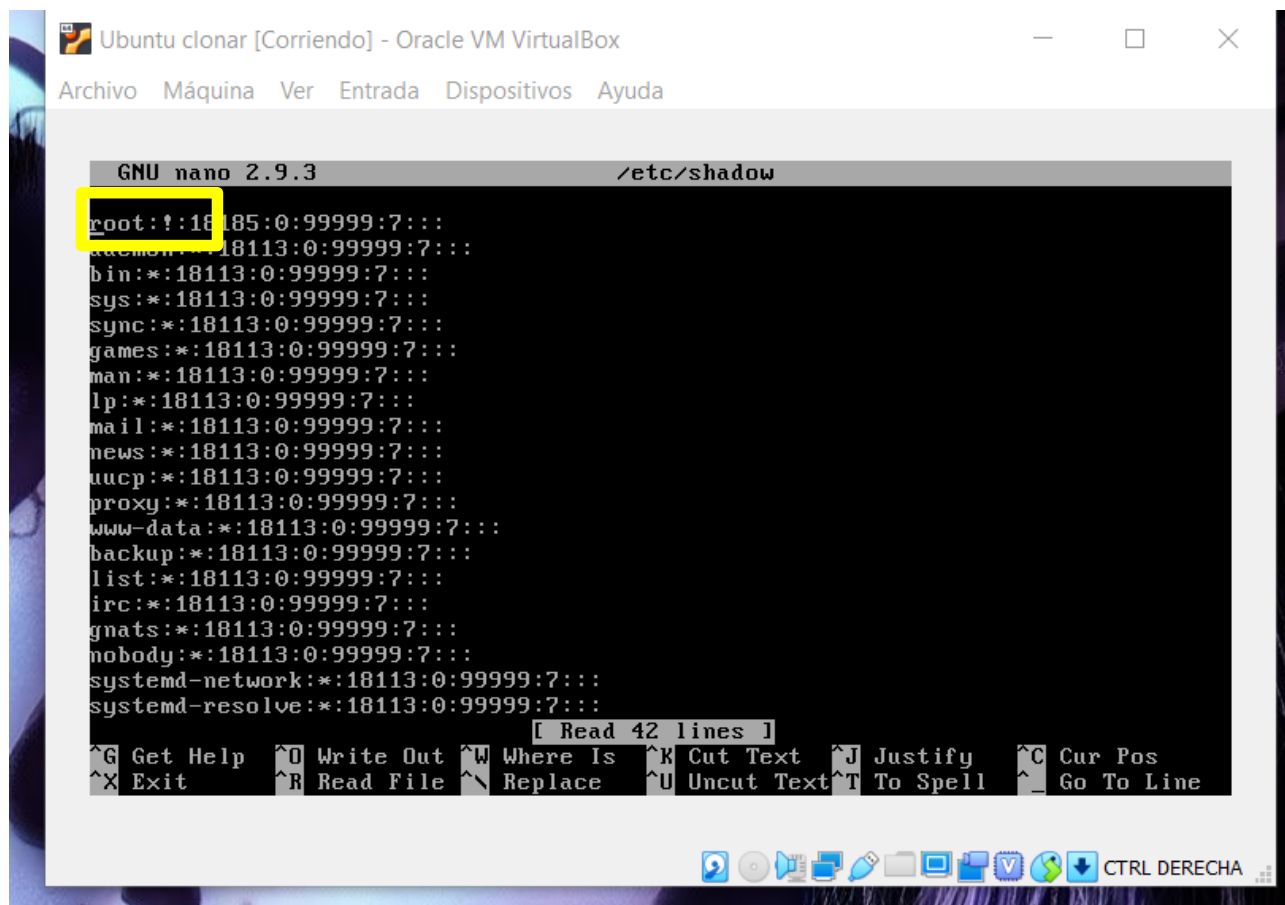
nano /etc/shadow

Y pulsamos Enter



```
Booting a command list
/dev/sda1: recovering journal
/dev/sda1: Clearing orphaned inode 659705 (uid=0, gid=0, mode=0100600, size=2)
/dev/sda1: Clearing orphaned inode 671205 (uid=0, gid=0, mode=0100644, size=787)
/dev/sda1: Clearing orphaned inode 929270 (uid=1000, gid=1000, mode=0100644, size=7307)
/dev/sda1: Clearing orphaned inode 919689 (uid=1000, gid=1000, mode=0100644, size=7307)
/dev/sda1: Clearing orphaned inode 929271 (uid=1000, gid=1000, mode=0100644, size=7307)
/dev/sda1: Clearing orphaned inode 671140 (uid=1000, gid=1000, mode=0100600, size=262144)
/dev/sda1: clean, 228991/1310720 files, 2108947/5242368 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
root@(none):/ # mount -o remount rw /
root@(none):/ # nano /etc/shadow_
```

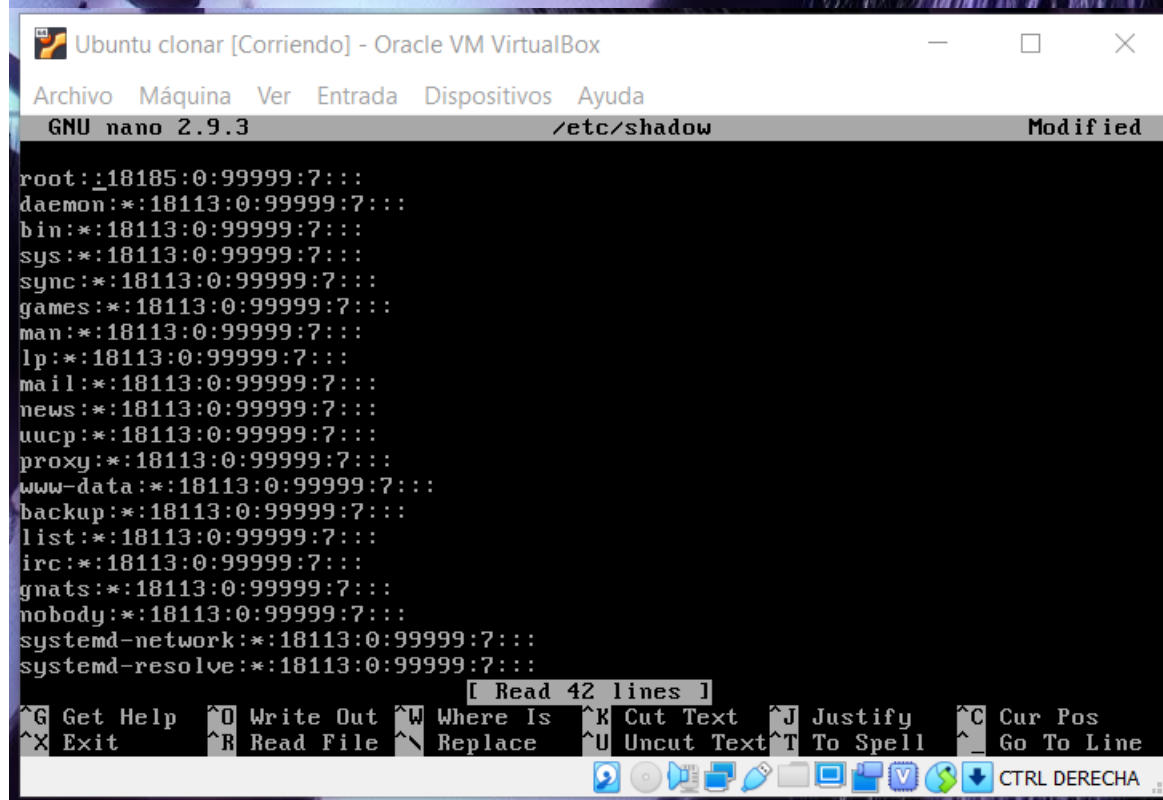
Entramos en ese fichero, y vemos que a continuación de root: hay una exclamación, borramos esta o el contenido que haya entre los otros dos puntos.



Ubuntu clonar [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 2.9.3 /etc/shadow
root:!18185:0:99999:7:::
daemon*:18113:0:99999:7:::
bin*:18113:0:99999:7:::
sys*:18113:0:99999:7:::
sync*:18113:0:99999:7:::
games*:18113:0:99999:7:::
man*:18113:0:99999:7:::
lp*:18113:0:99999:7:::
mail*:18113:0:99999:7:::
news*:18113:0:99999:7:::
uucp*:18113:0:99999:7:::
proxy*:18113:0:99999:7:::
www-data*:18113:0:99999:7:::
backup*:18113:0:99999:7:::
list*:18113:0:99999:7:::
irc*:18113:0:99999:7:::
gnats*:18113:0:99999:7:::
nobody*:18113:0:99999:7:::
systemd-network*:18113:0:99999:7:::
systemd-resolve*:18113:0:99999:7:::
[ Read 42 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```



Ubuntu clonar [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 2.9.3 /etc/shadow Modified
root:18185:0:99999:7:::
daemon*:18113:0:99999:7:::
bin*:18113:0:99999:7:::
sys*:18113:0:99999:7:::
sync*:18113:0:99999:7:::
games*:18113:0:99999:7:::
man*:18113:0:99999:7:::
lp*:18113:0:99999:7:::
mail*:18113:0:99999:7:::
news*:18113:0:99999:7:::
uucp*:18113:0:99999:7:::
proxy*:18113:0:99999:7:::
www-data*:18113:0:99999:7:::
backup*:18113:0:99999:7:::
list*:18113:0:99999:7:::
irc*:18113:0:99999:7:::
gnats*:18113:0:99999:7:::
nobody*:18113:0:99999:7:::
systemd-network*:18113:0:99999:7:::
systemd-resolve*:18113:0:99999:7:::
[ Read 42 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```


**Guardamos los cambios y reiniciamos la máquina.
Nos entra directamente sin pedir contraseña.**

