EECS565 Intro to Computer and Information Security

Mini Project 2

Environment Setup

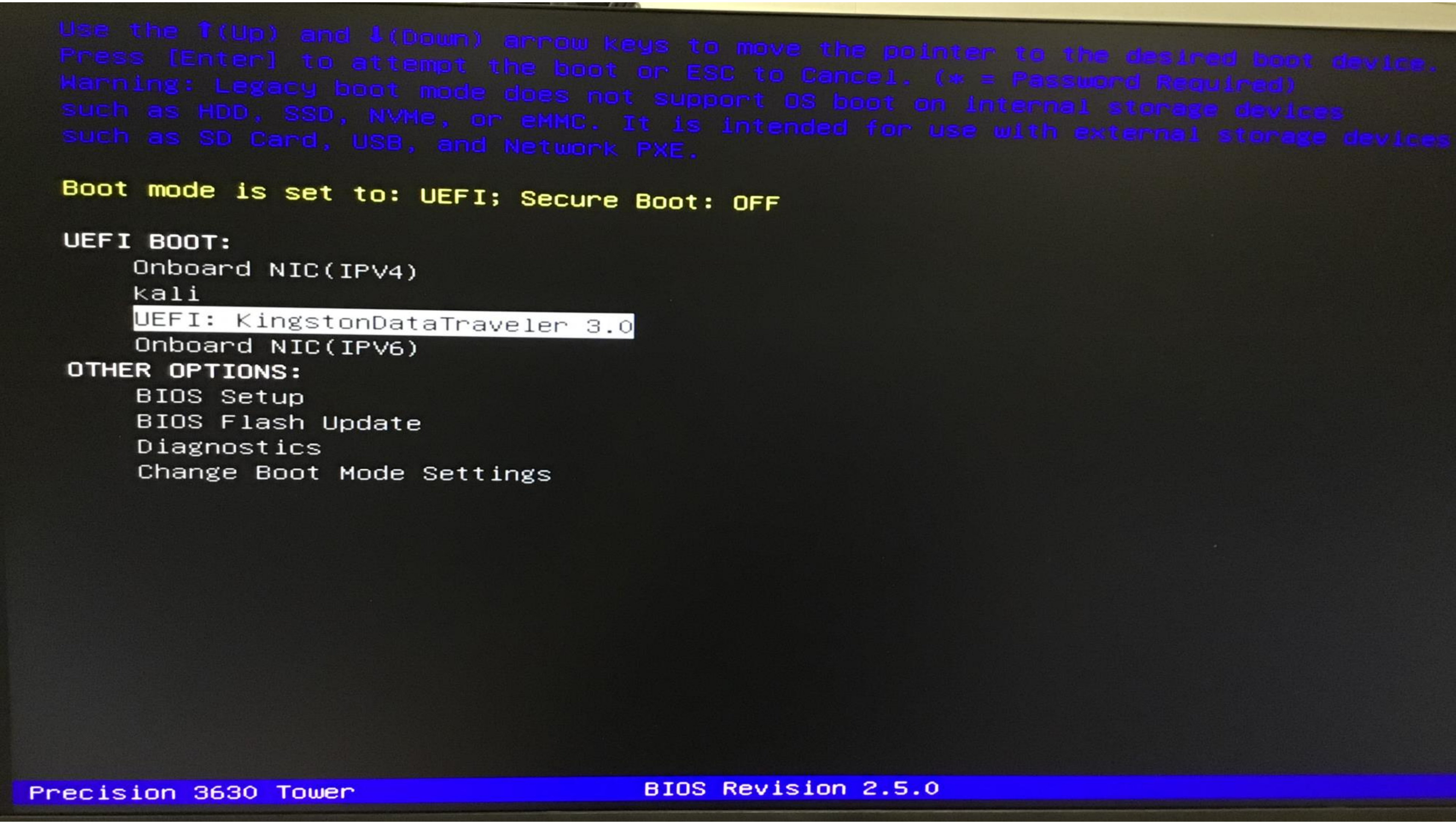
BOOT

Press Power button

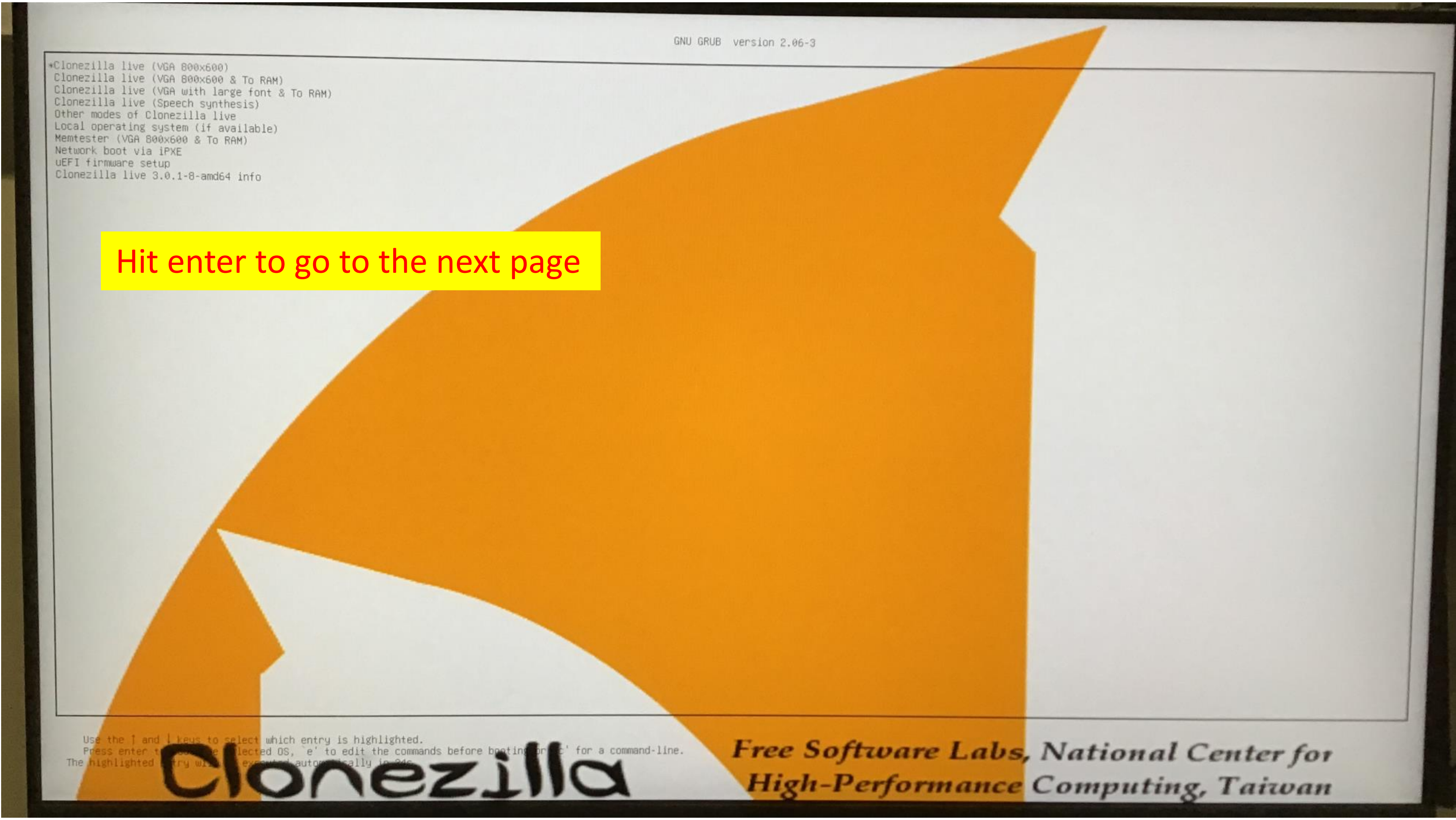
When it is just power on.

Or just restart the workstation

Keep Pressing **F12** for accessing this Boot Menu



```
Use the ↑(Up) and ↓(Down) arrow keys to move the pointer to the desired boot device.
Press [Enter] to attempt the boot or ESC to Cancel. (* = Password Required)
Warning: Legacy boot mode does not support OS boot on internal storage devices
such as HDD, SSD, NVMe, or eMMC. It is intended for use with external storage devices
such as SD Card, USB, and Network PXE.

Boot mode is set to: UEFI; Secure Boot: OFF

UEFI BOOT:
     Onboard NIC(IPV4)
     kali
     UEFI: KingstonDataTraveler 3.0
     Onboard NIC(IPV6)
OTHER OPTIONS:
     BIOS Setup
     BIOS Flash Update
     Diagnostics
     Change Boot Mode Settings

Precision 3630 Tower                    BIOS Revision 2.5.0
```

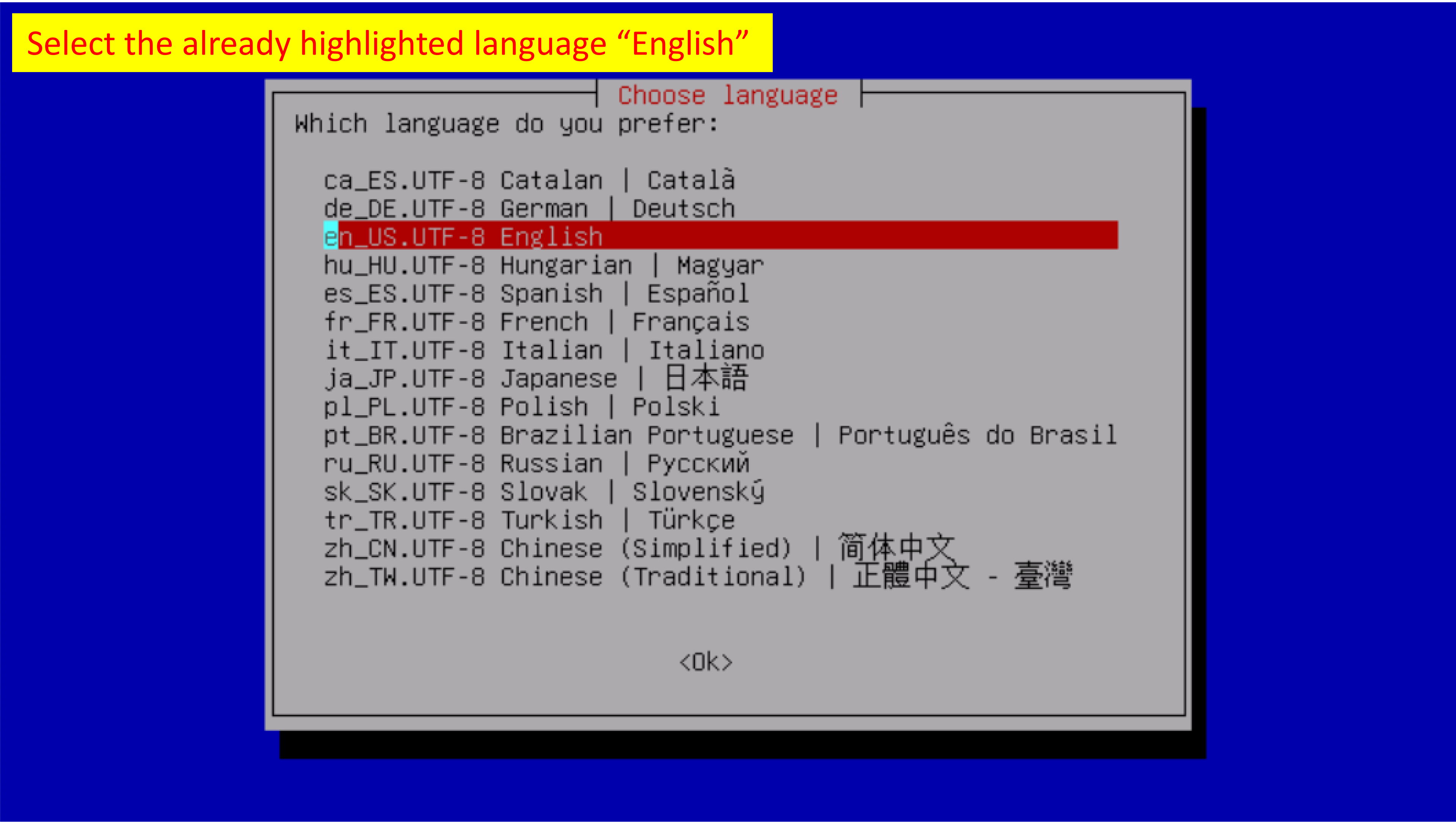


```
                                   GNU GRUB  version 2.06-3

*Clonezilla live (VGA 800x600)
 Clonezilla live (VGA 800x600 & To RAM)
 Clonezilla live (VGA with large font & To RAM)
 Clonezilla live (Speech synthesis)
 Other modes of Clonezilla live
 Local operating system (if available)
 Memtester (VGA 800x600 & To RAM)
 Network boot via iPXE
 uEFI firmware setup
 Clonezilla live 3.0.1-8-amd64 info

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 24s.
```

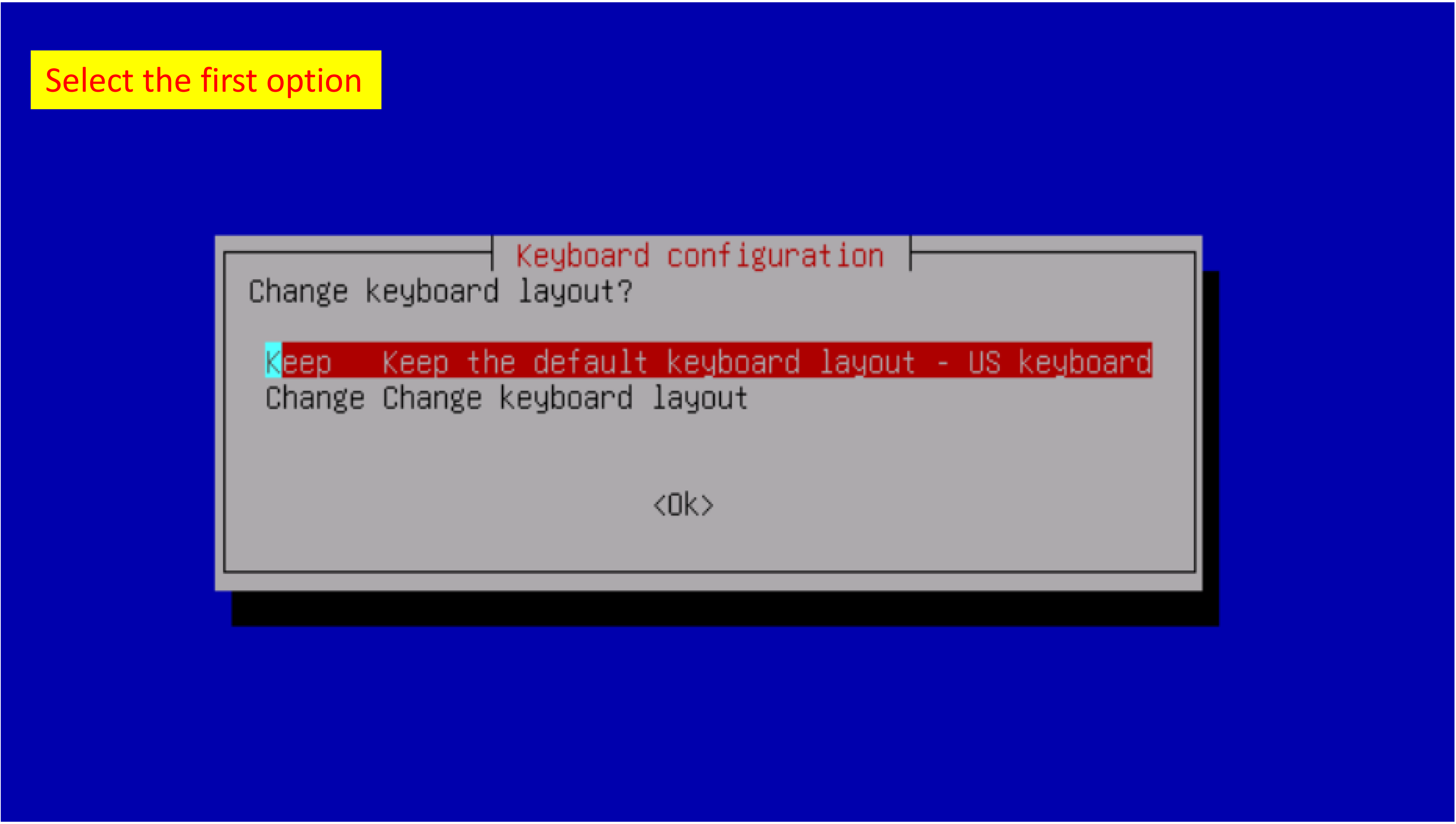
Clonezilla
Free Software Labs, National Center for
High-Performance Computing, Taiwan

Hit enter to go to the next page

Select the already highlighted language “English”

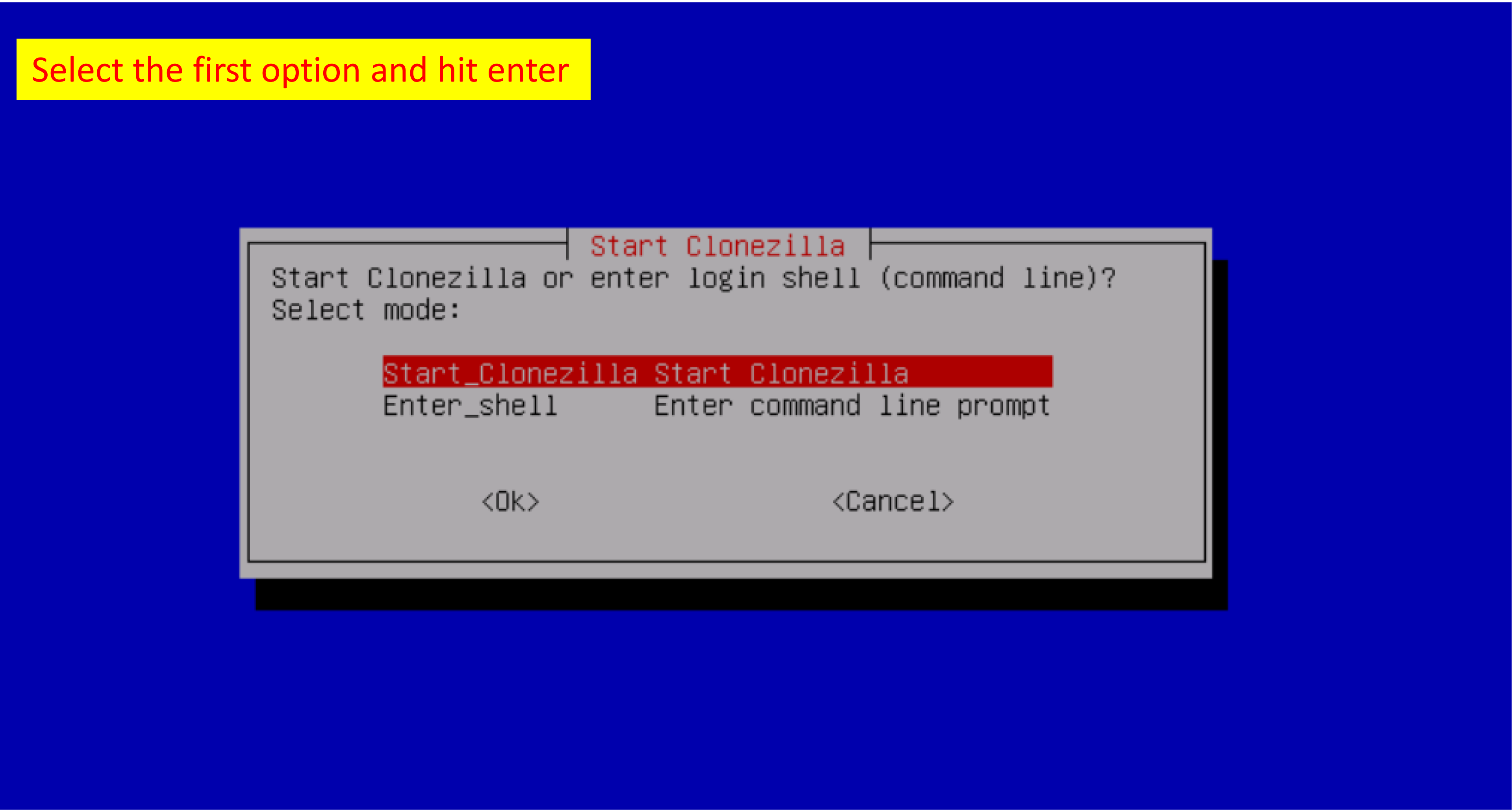


```
Choose language
Which language do you prefer:

  ca_ES.UTF-8 Catalan | Català
  de_DE.UTF-8 German | Deutsch
  en_US.UTF-8 English
  hu_HU.UTF-8 Hungarian | Magyar
  es_ES.UTF-8 Spanish | Español
  fr_FR.UTF-8 French | Français
  it_IT.UTF-8 Italian | Italiano
  ja_JP.UTF-8 Japanese | 日本語
  pl_PL.UTF-8 Polish | Polski
  pt_BR.UTF-8 Brazilian Portuguese | Português do Brasil
  ru_RU.UTF-8 Russian | Русский
  sk_SK.UTF-8 Slovak | Slovenský
  tr_TR.UTF-8 Turkish | Türkçe
  zh_CN.UTF-8 Chinese (Simplified) | 简体中文
  zh_TW.UTF-8 Chinese (Traditional) | 正體中文 - 臺灣


                        <Ok>
```



Select the first option

```
Keyboard configuration
Change keyboard layout?

  Keep   Keep the default keyboard layout - US keyboard
  Change Change keyboard layout

                    <Ok>
```

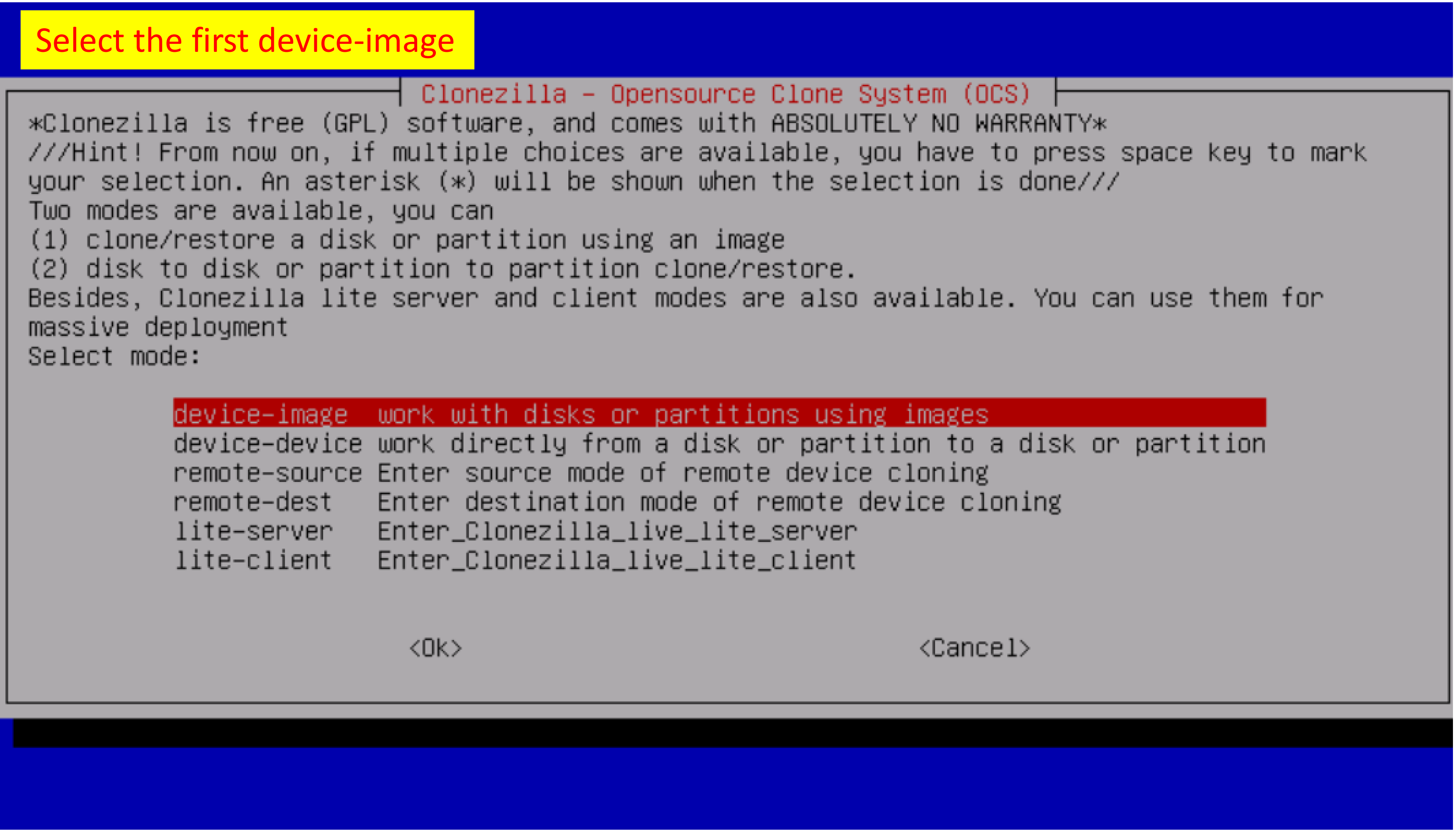


Select the first option and hit enter

Start Clonezilla

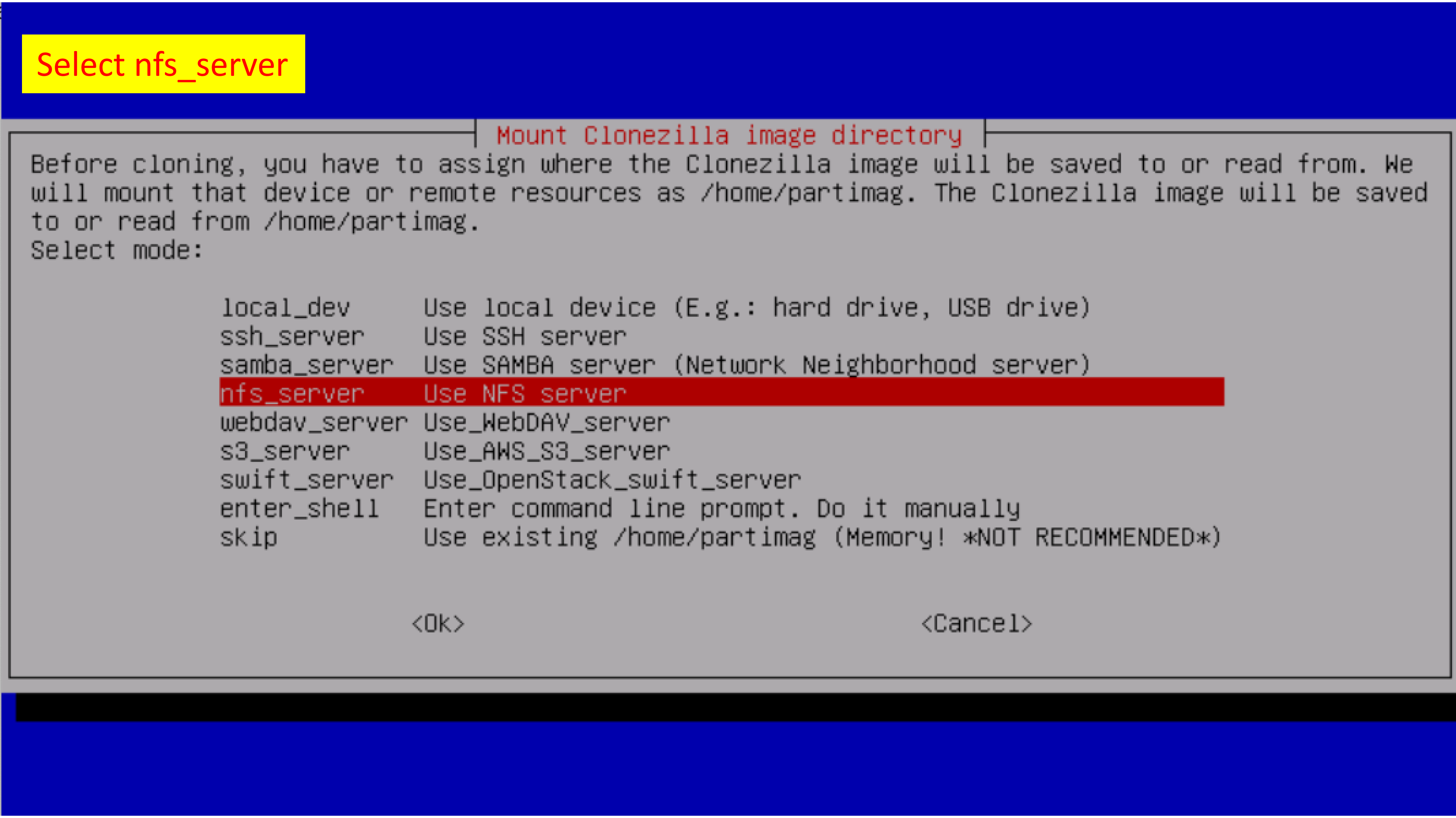
Start Clonezilla or enter login shell (command line)?
Select mode:

Start_Clonezilla Start Clonezilla
Enter_shell Enter command line prompt
<Ok>
<Cancel>



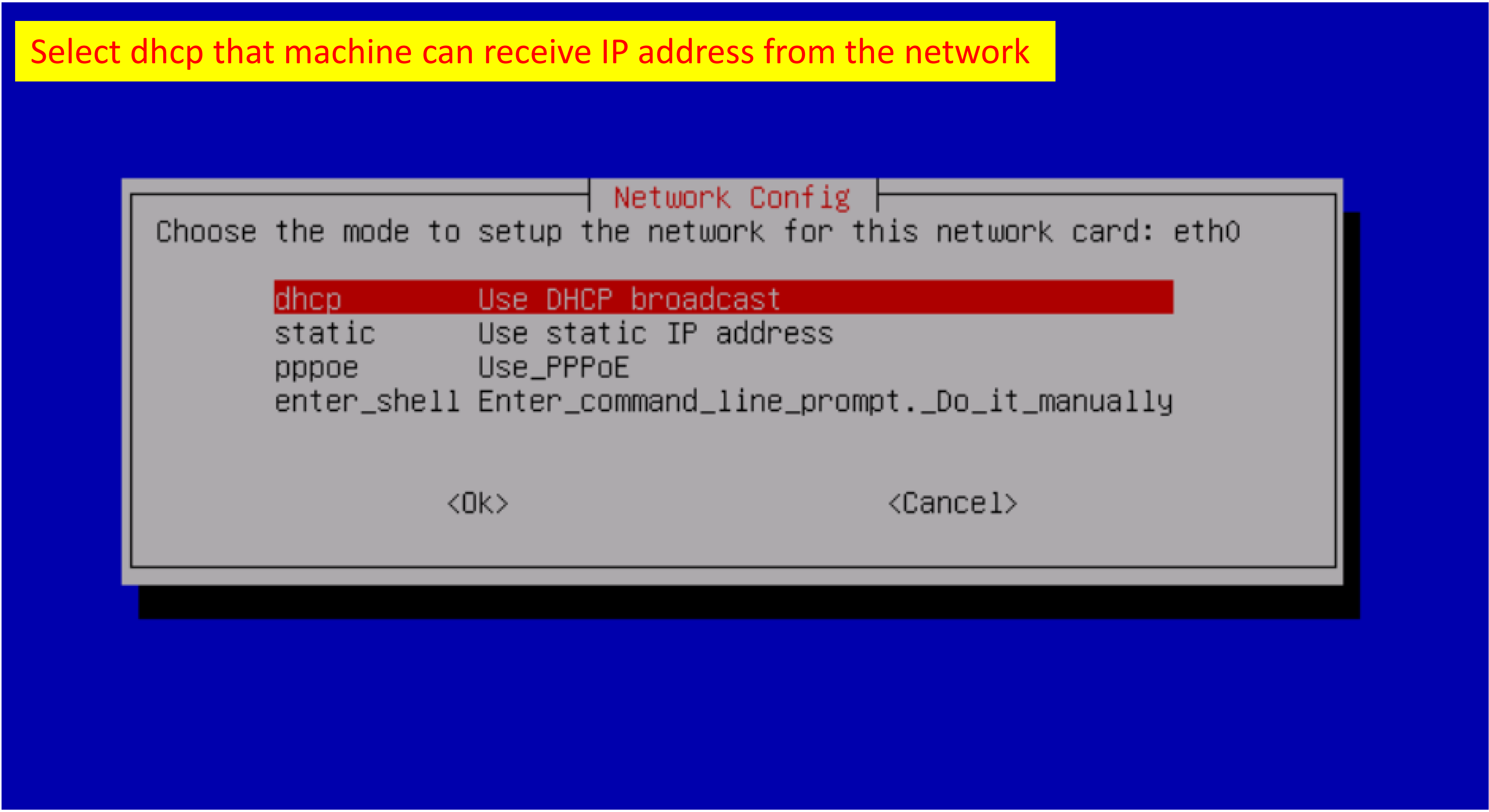
Select the first device-image

```
Clonezilla - Opensource Clone System (OCS)
*Clonezilla is free (GPL) software, and comes with ABSOLUTELY NO WARRANTY*
///Hint! From now on, if multiple choices are available, you have to press space key to mark
your selection. An asterisk (*) will be shown when the selection is done///
Two modes are available, you can
(1) clone/restore a disk or partition using an image
(2) disk to disk or partition to partition clone/restore.
Besides, Clonezilla lite server and client modes are also available. You can use them for
massive deployment
Select mode:

          device-image  work with disks or partitions using images
          device-device work directly from a disk or partition to a disk or partition
          remote-source Enter source mode of remote device cloning
          remote-dest   Enter destination mode of remote device cloning
          lite-server   Enter_Clonezilla_live_lite_server
          lite-client   Enter_Clonezilla_live_lite_client


                    <Ok>                                  <Cancel>
```



Select nfs_server

```
Mount Clonezilla image directory
Before cloning, you have to assign where the Clonezilla image will be saved to or read from. We
will mount that device or remote resources as /home/partimag. The Clonezilla image will be saved
to or read from /home/partimag.
Select mode:

             local_dev      Use local device (E.g.: hard drive, USB drive)
             ssh_server     Use SSH server
             samba_server   Use SAMBA server (Network Neighborhood server)
             nfs_server     Use NFS server
             webdav_server  Use_WebDAV_server
             s3_server      Use_AWS_S3_server
             swift_server   Use_OpenStack_swift_server
             enter_shell    Enter command line prompt. Do it manually
             skip           Use existing /home/partimag (Memory! *NOT RECOMMENDED*)


                         <Ok>                                <Cancel>
```



Select dhcp that machine can receive IP address from the network

Network Config

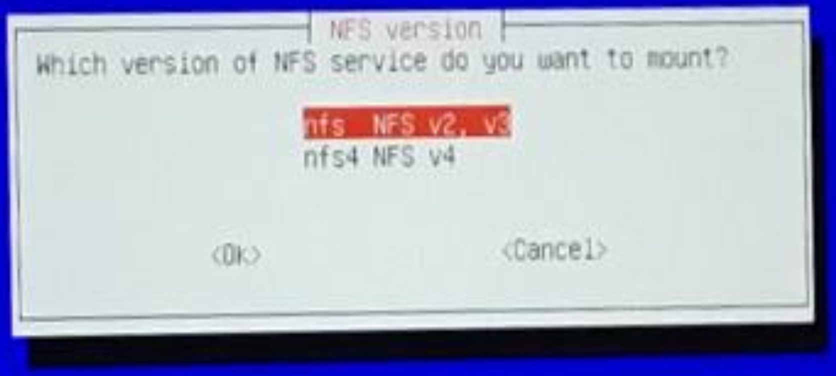
Choose the mode to setup the network for this network card: eth0

```
dhcp        Use DHCP broadcast
static      Use static IP address
pppoe       Use_PPPoE
enter_shell Enter_command_line_prompt._Do_it_manually
```

Select NFS v2, v3

Although nfs4 may also work but it is slower as it may load

Extra security packages

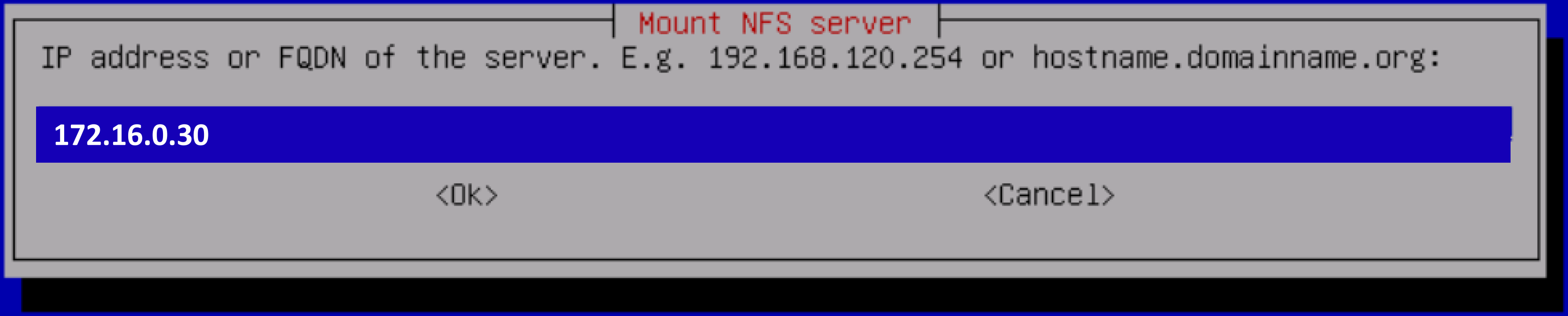


NFS version

Which version of NFS service do you want to mount?

```
nfs  NFS v2, v3
nfs4 NFS v4
```

Enter the IP address of the NFS Server



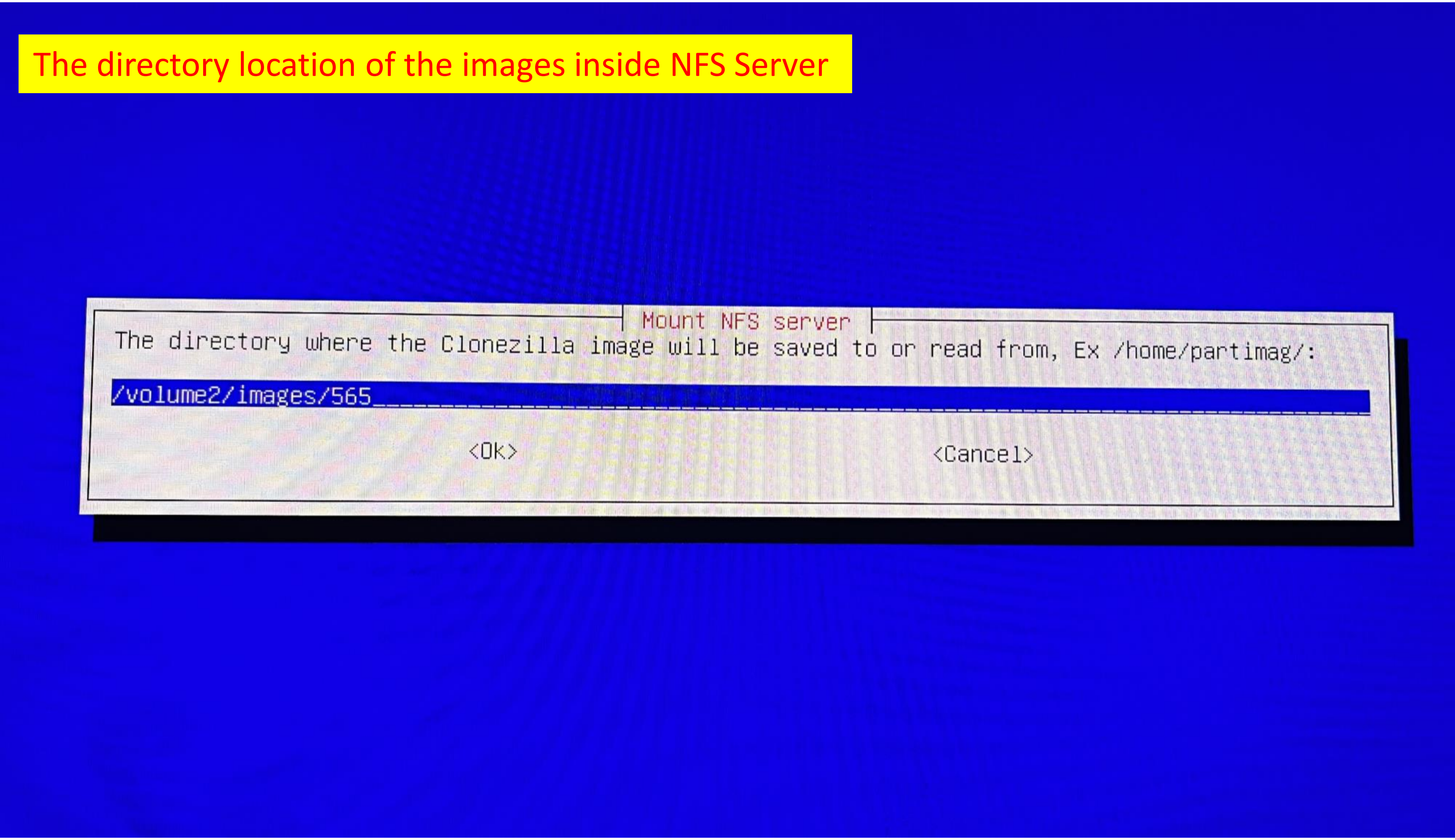
Mount NFS server

IP address or FQDN of the server. E.g. 192.168.120.254 or hostname.domainname.org:

172.16.0.30

Remember num lock if your use digital pad

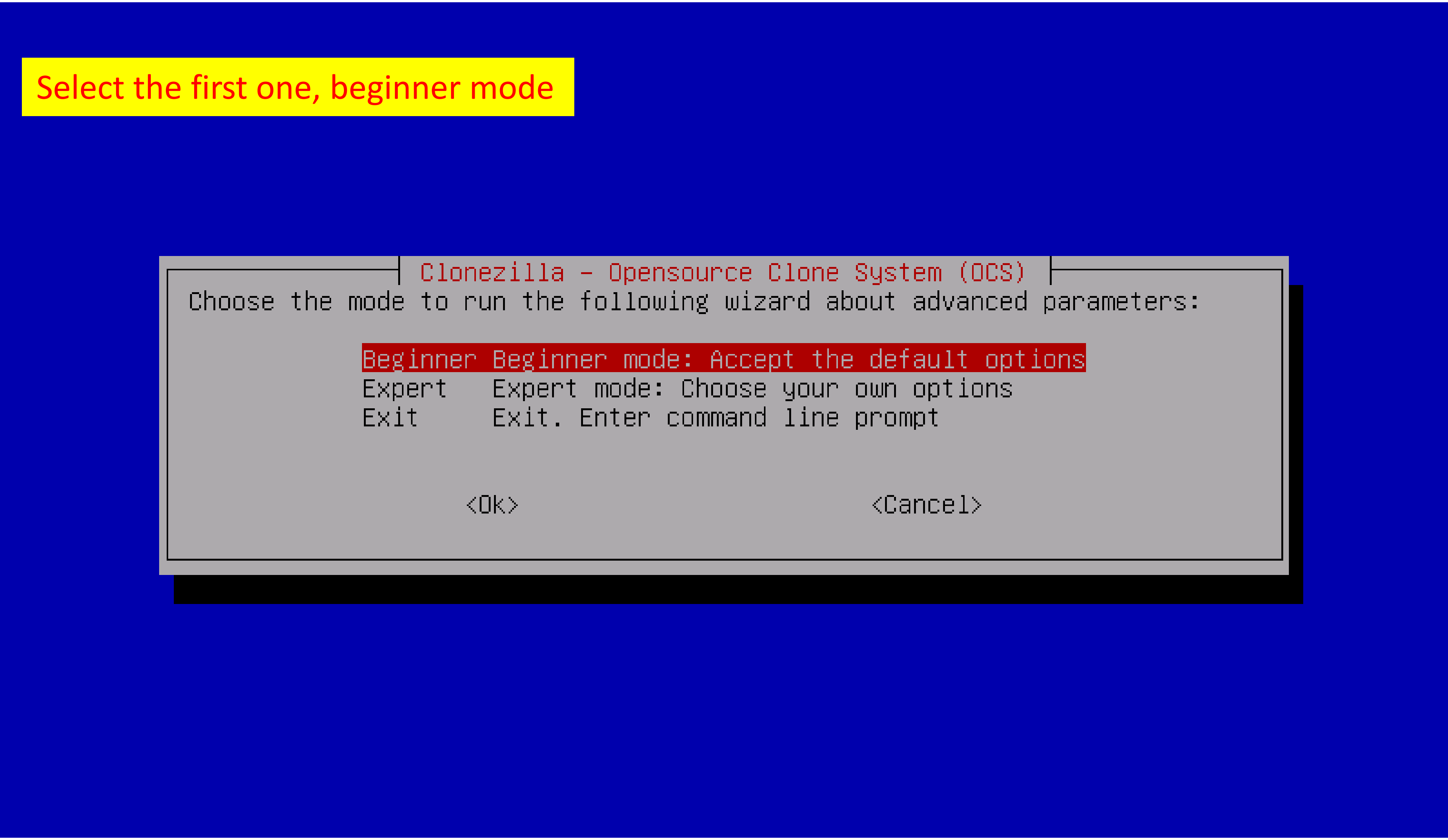
The directory location of the images inside NFS Server



Mount NFS server

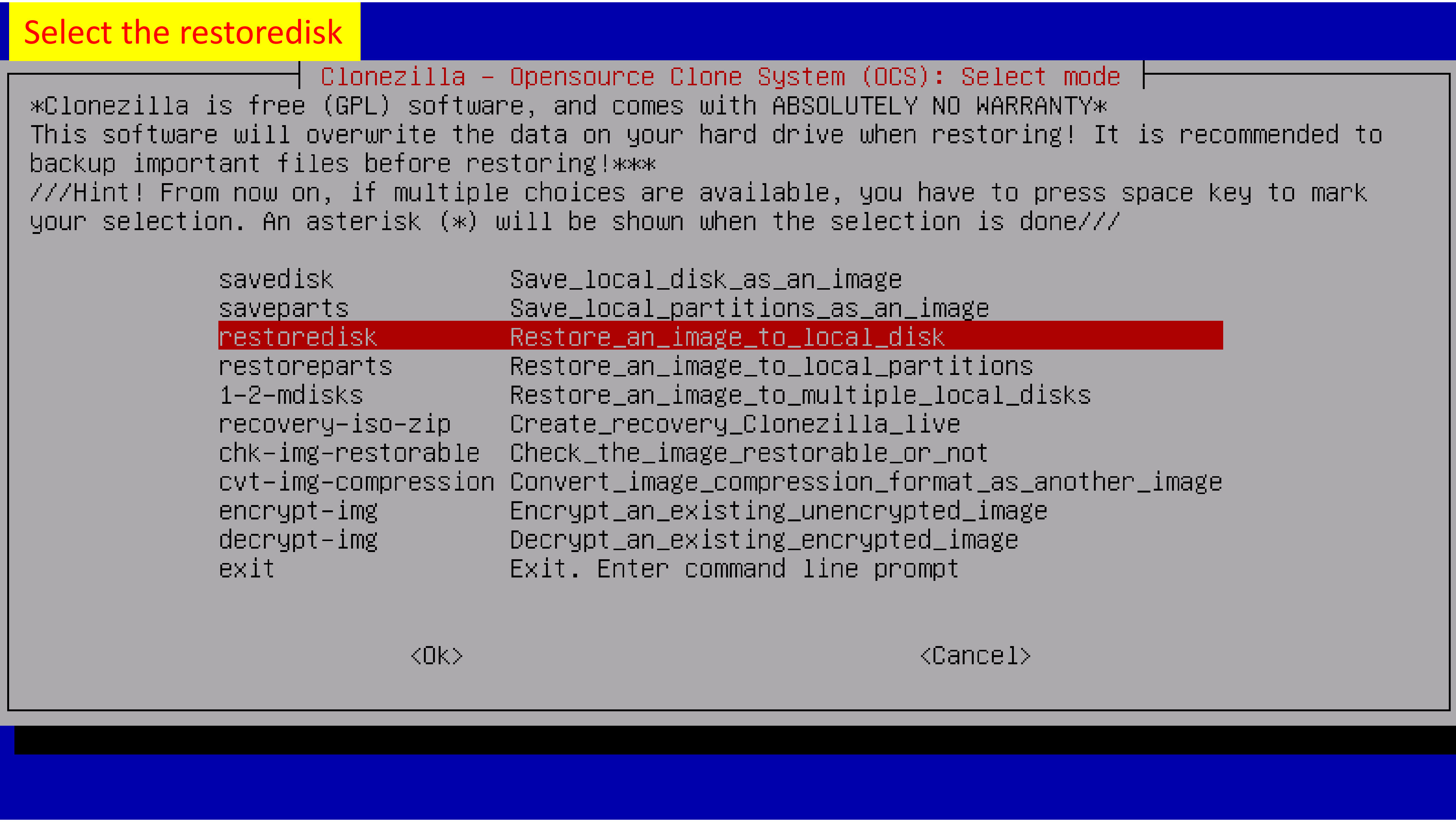
The directory where the Clonezilla image will be saved to or read from, Ex /home/partimag/:

```
/volume2/images/565
```



Select the first one, beginner mode

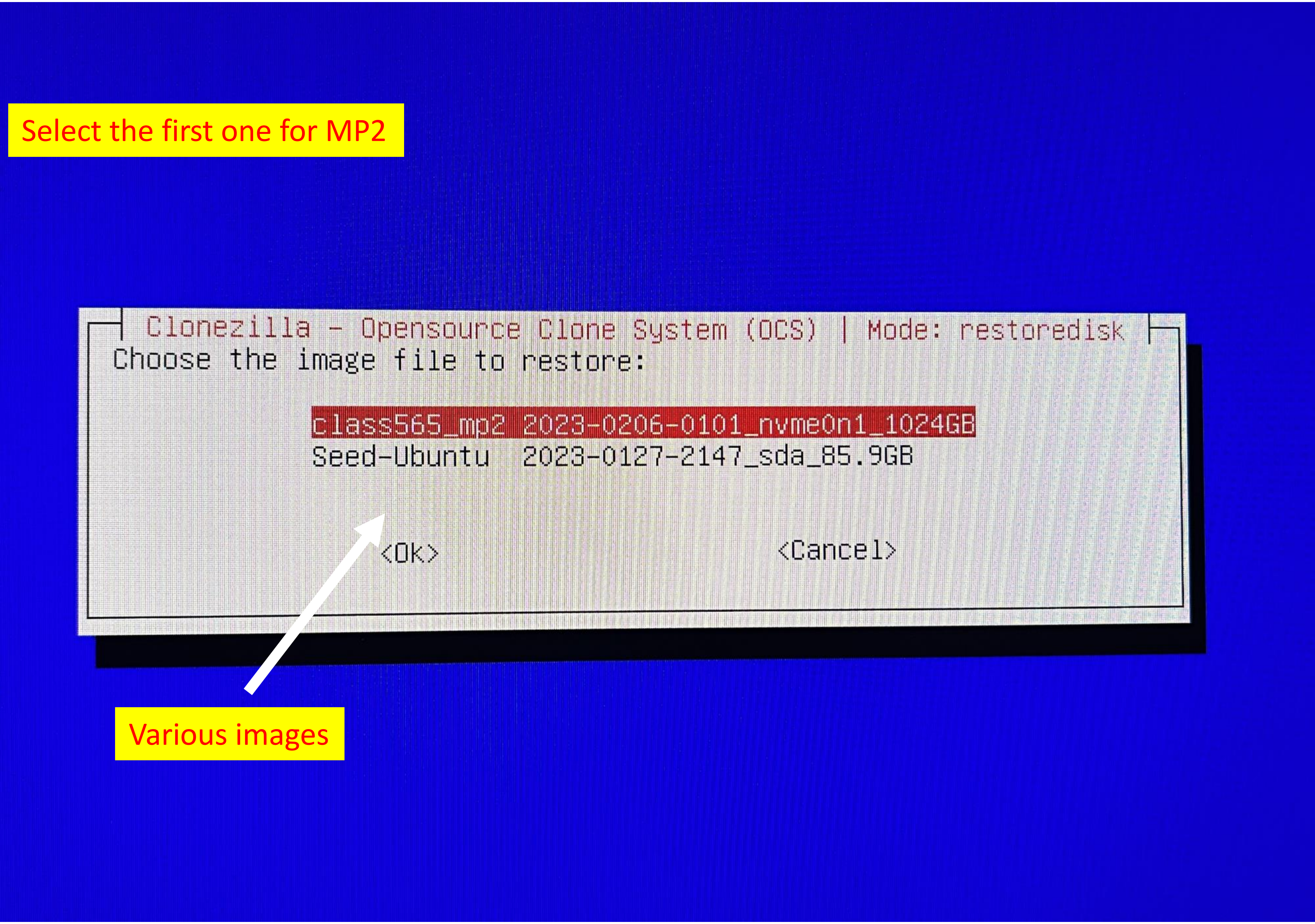
```
Clonezilla - Opensource Clone System (OCS)
Choose the mode to run the following wizard about advanced parameters:

        Beginner Beginner mode: Accept the default options
        Expert   Expert mode: Choose your own options
        Exit     Exit. Enter command line prompt

            <Ok>                          <Cancel>
```



Select the restoredisk

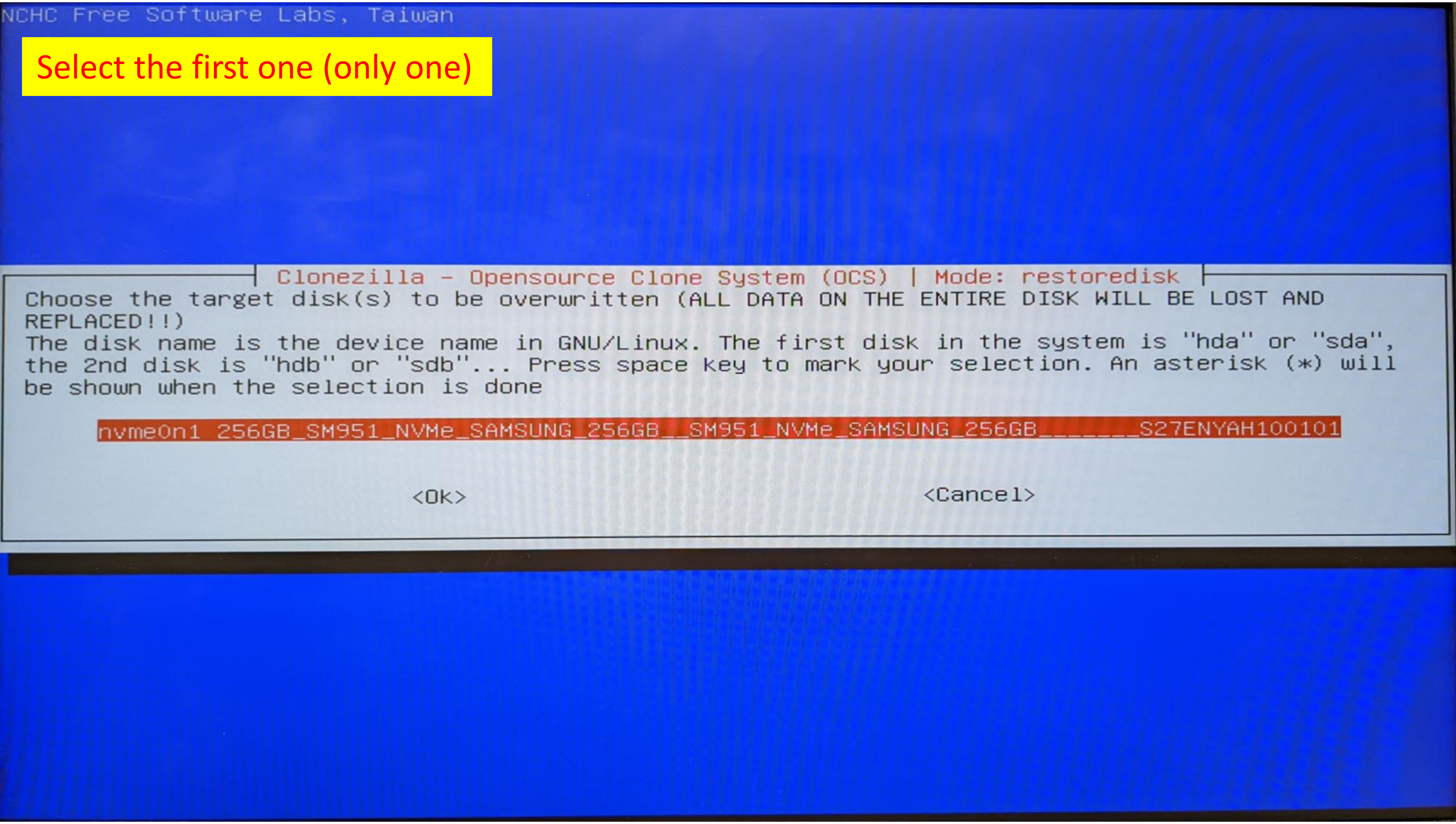
```
Clonezilla - Opensource Clone System (OCS): Select mode
*Clonezilla is free (GPL) software, and comes with ABSOLUTELY NO WARRANTY*
This software will overwrite the data on your hard drive when restoring! It is recommended to
backup important files before restoring!***
///Hint! From now on, if multiple choices are available, you have to press space key to mark
your selection. An asterisk (*) will be shown when the selection is done///

             savedisk            Save_local_disk_as_an_image
             saveparts           Save_local_partitions_as_an_image
             restoredisk         Restore_an_image_to_local_disk
             restoreparts        Restore_an_image_to_local_partitions
             1-2-mdisks          Restore_an_image_to_multiple_local_disks
             recovery-iso-zip    Create_recovery_Clonezilla_live
             chk-img-restorable  Check_the_image_restorable_or_not
             cvt-img-compression Convert_image_compression_format_as_another_image
             encrypt-img         Encrypt_an_existing_unencrypted_image
             decrypt-img         Decrypt_an_existing_encrypted_image
             exit                Exit. Enter command line prompt
```

Select the first one for MP2



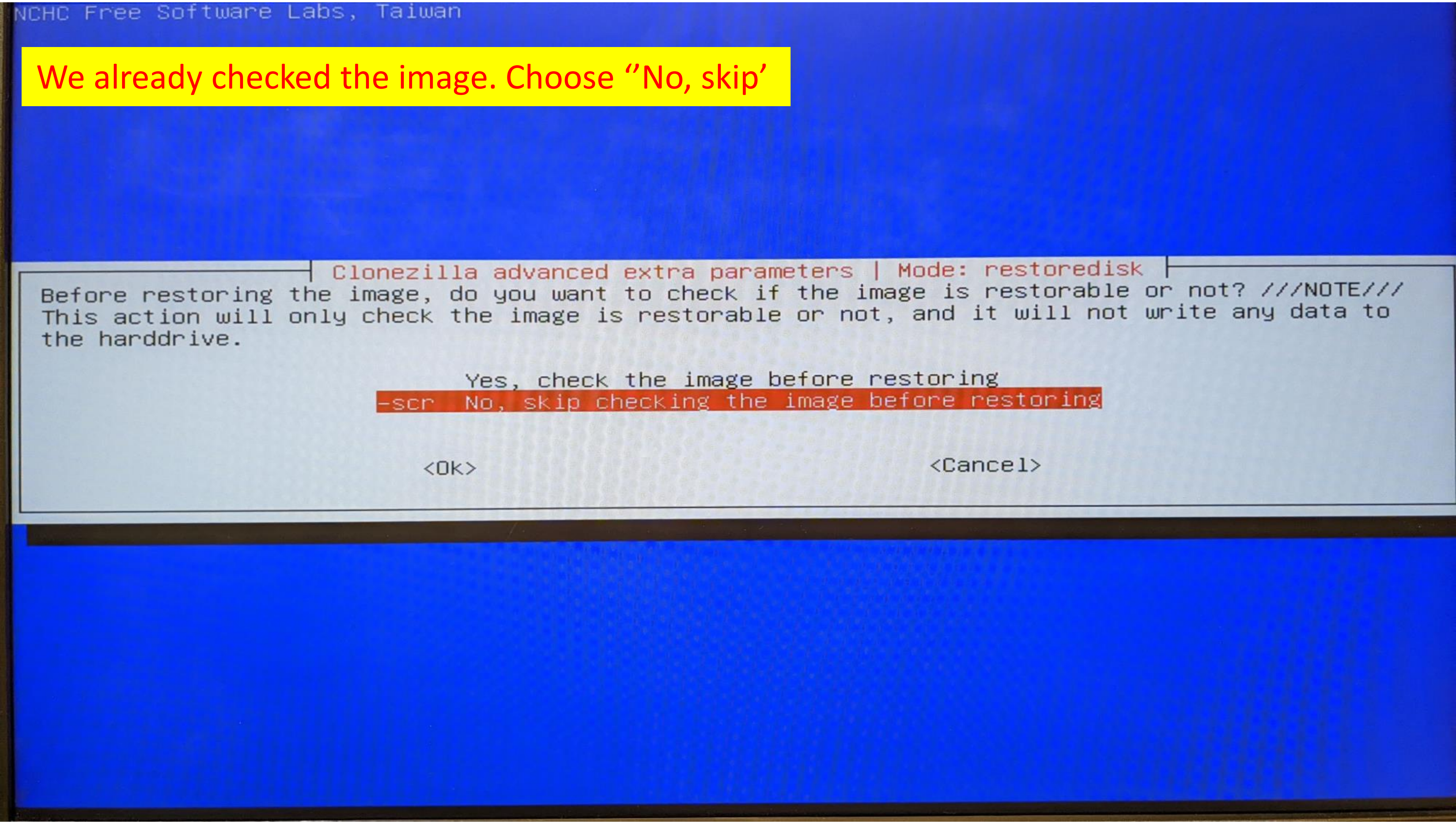
```
Clonezilla - Opensource Clone System (OCS) | Mode: restoredisk
Choose the image file to restore:

          class565_mp2 2023-0206-0101_nvme0n1_1024GB
          Seed-Ubuntu  2023-0127-2147_sda_85.9GB

            <Ok>                    <Cancel>
```

Various images



Select the first one (only one)

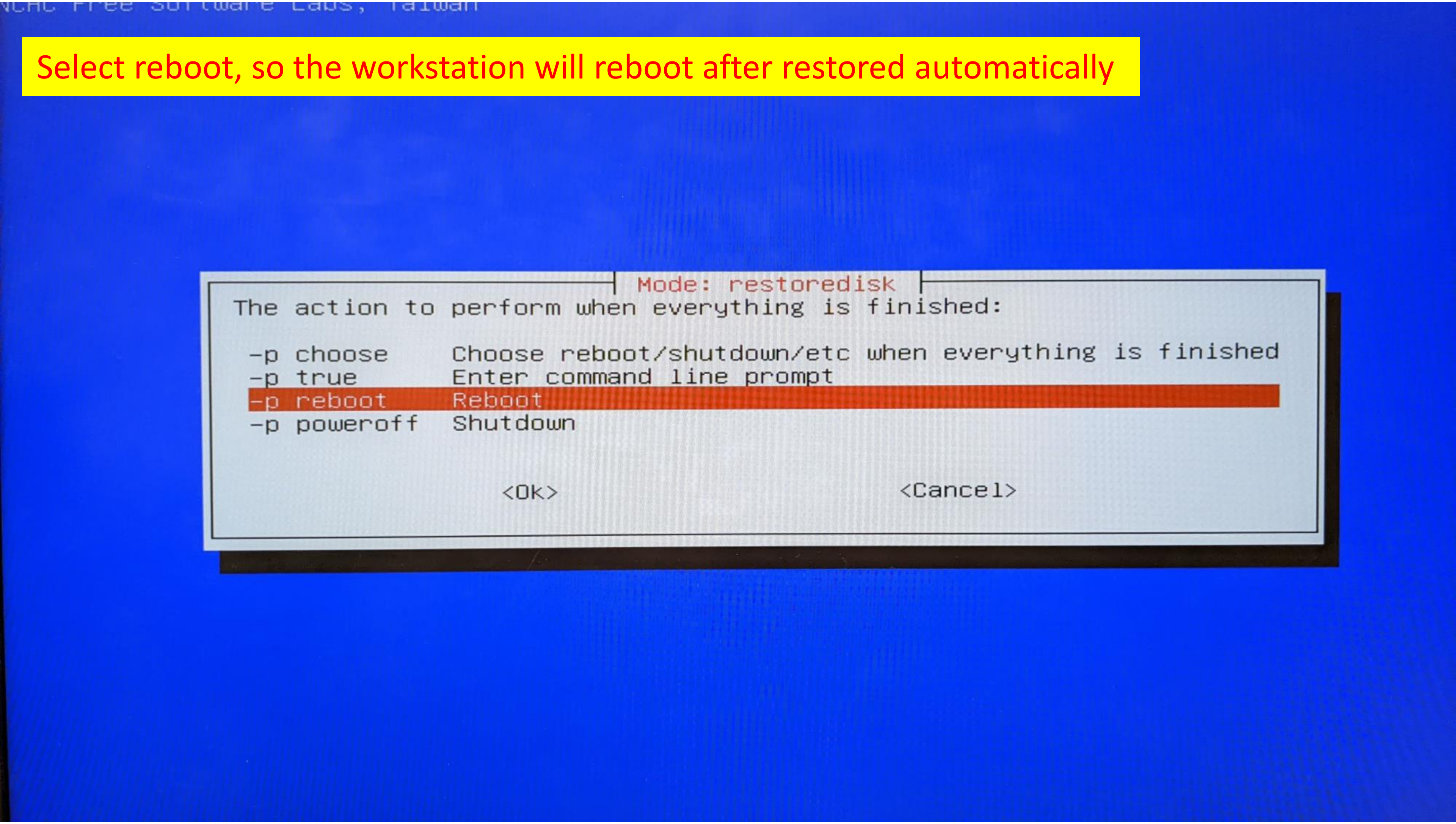
```
NCHC Free Software Labs, Taiwan

        Clonezilla - Opensource Clone System (OCS) | Mode: restoredisk
 Choose the target disk(s) to be overwritten (ALL DATA ON THE ENTIRE DISK WILL BE LOST AND
 REPLACED!!)
 The disk name is the device name in GNU/Linux. The first disk in the system is "hda" or "sda",
 the 2nd disk is "hdb" or "sdb"... Press space key to mark your selection. An asterisk (*) will
 be shown when the selection is done

     nvme0n1 256GB_SM951_NVMe_SAMSUNG_256GB__SM951_NVMe_SAMSUNG_256GB_______S27ENYAH100101

                    <Ok>                                  <Cancel>
```



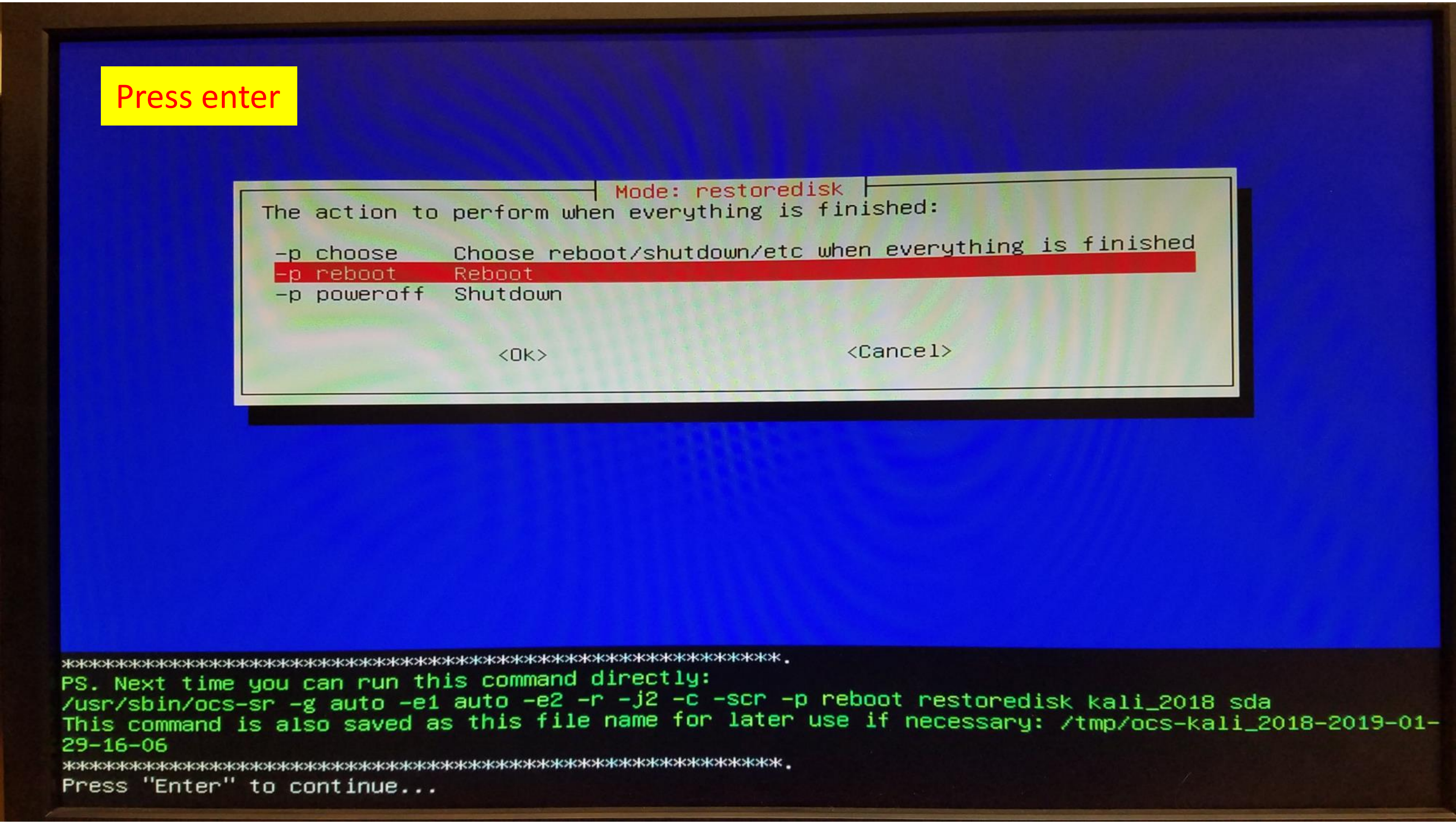
We already checked the image. Choose ''No, skip'

```
NCHC Free Software Labs, Taiwan

┤ Clonezilla advanced extra parameters | Mode: restoredisk ├
Before restoring the image, do you want to check if the image is restorable or not? ///NOTE///
This action will only check the image is restorable or not, and it will not write any data to
the harddrive.

                  Yes, check the image before restoring
          -scr    No, skip checking the image before restoring

              <Ok>                                    <Cancel>
```

Select reboot, so the workstation will reboot after restored automatically



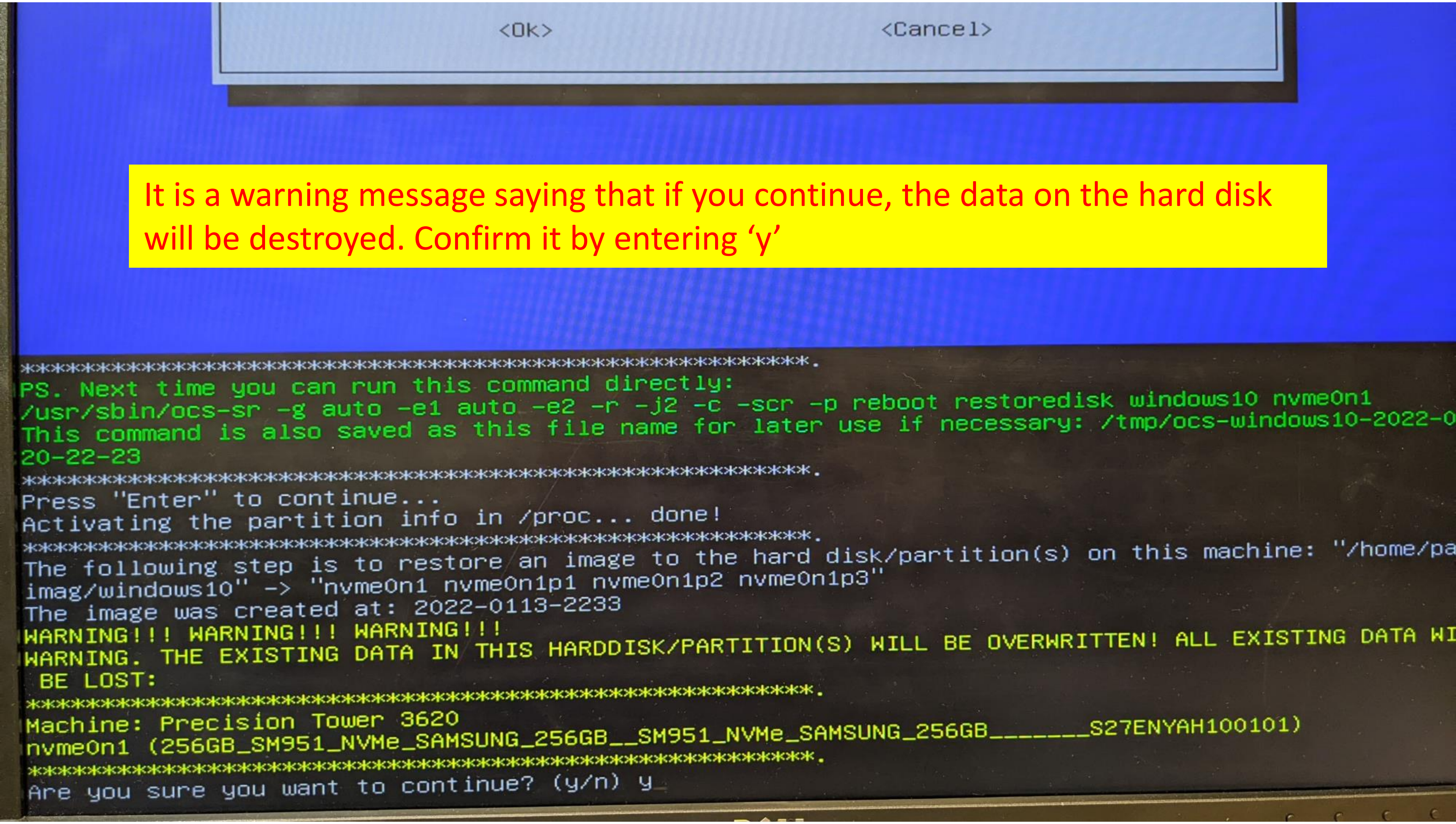
```
NCHC Free Software Labs, Taiwan

┤ Mode: restoredisk ├
The action to perform when everything is finished:

  -p choose     Choose reboot/shutdown/etc when everything is finished
  -p true       Enter command line prompt
  -p reboot     Reboot
  -p poweroff   Shutdown

           <Ok>                        <Cancel>
```



Press enter

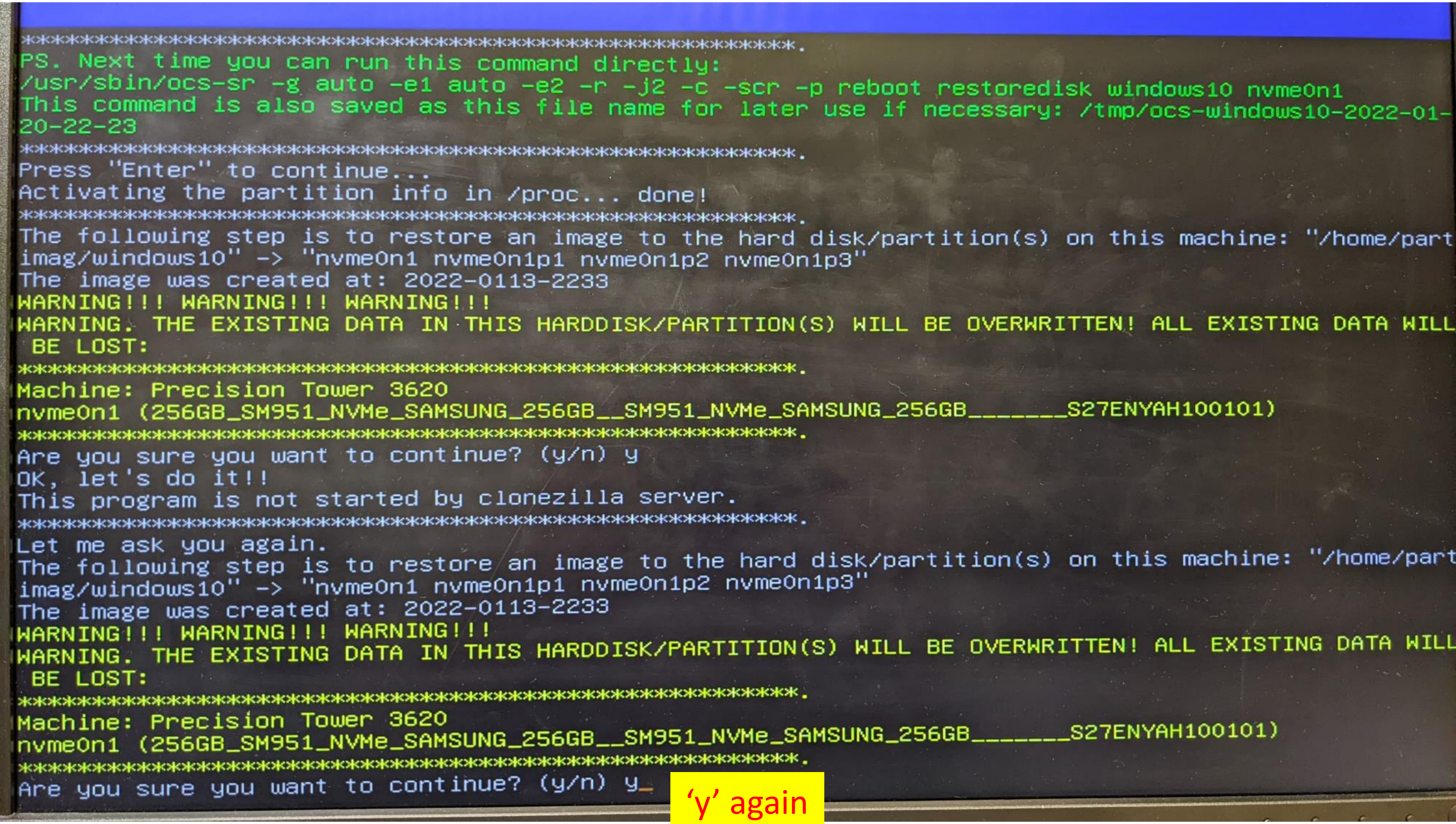
```
Mode: restoredisk
The action to perform when everything is finished:

  -p choose     Choose reboot/shutdown/etc when everything is finished
  -p reboot     Reboot
  -p poweroff   Shutdown

                  <Ok>                         <Cancel>
```

```
*****************************************************.
PS. Next time you can run this command directly:
/usr/sbin/ocs-sr -g auto -e1 auto -e2 -r -j2 -c -scr -p reboot restoredisk kali_2018 sda
This command is also saved as this file name for later use if necessary: /tmp/ocs-kali_2018-2019-01-
29-16-06
*****************************************************.
Press "Enter" to continue...
```



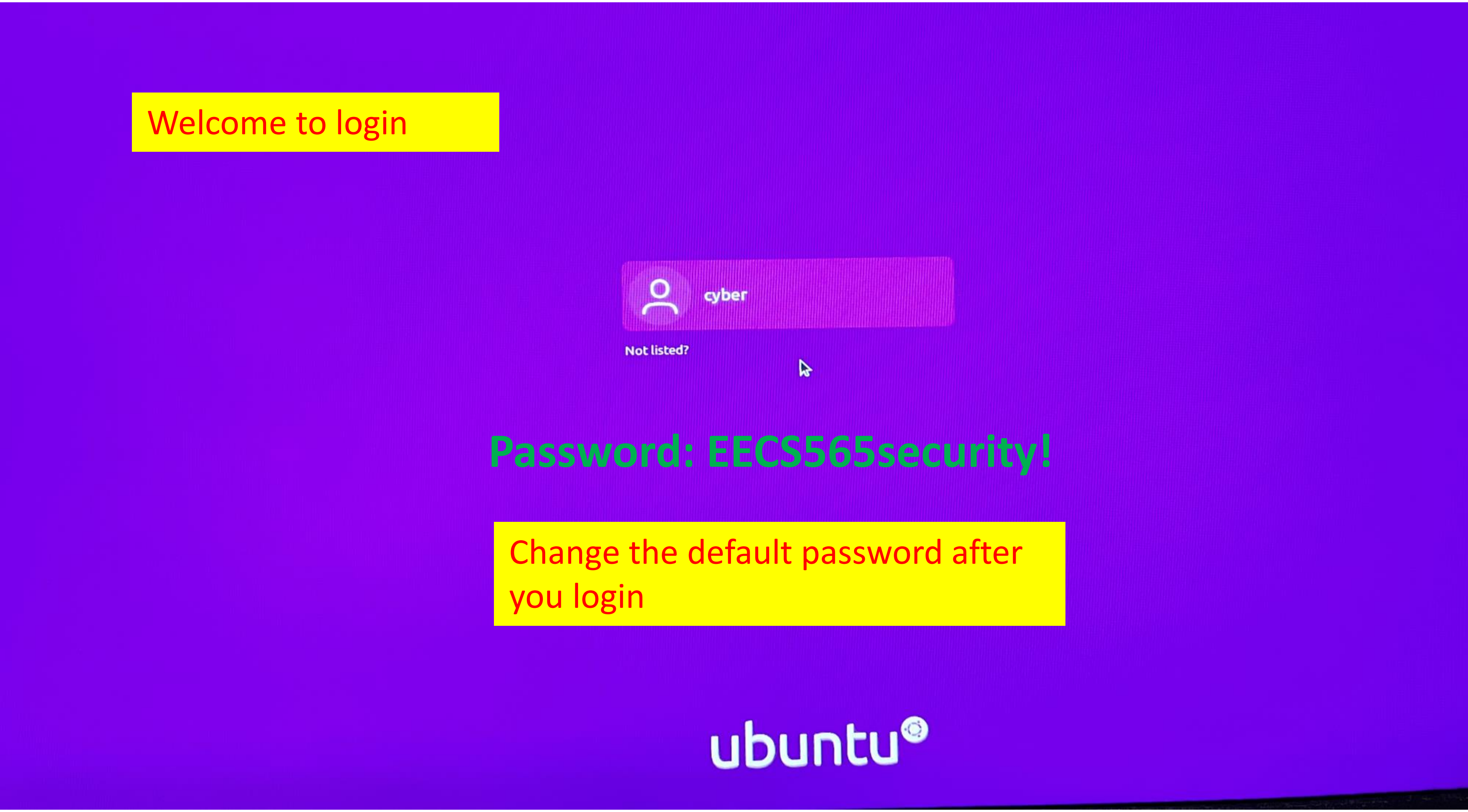
It is a warning message saying that if you continue, the data on the hard disk will be destroyed. Confirm it by entering ‘y’

```
********************************************************.
PS. Next time you can run this command directly:
/usr/sbin/ocs-sr -g auto -e1 auto -e2 -r -j2 -c -scr -p reboot restoredisk windows10 nvme0n1
This command is also saved as this file name for later use if necessary: /tmp/ocs-windows10-2022-0
20-22-23
********************************************************.
Press "Enter" to continue...
Activating the partition info in /proc... done!
********************************************************.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/pa
imag/windows10" -> "nvme0n1 nvme0n1p1 nvme0n1p2 nvme0n1p3"
The image was created at: 2022-0113-2233
WARNING!!! WARNING!!! WARNING!!!
WARNING. THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WI
 BE LOST:
********************************************************.
Machine: Precision Tower 3620
nvme0n1 (256GB_SM951_NVMe_SAMSUNG_256GB__SM951_NVMe_SAMSUNG_256GB________S27ENYAH100101)
********************************************************.
Are you sure you want to continue? (y/n) y
```



```
********************************************************.
PS. Next time you can run this command directly:
/usr/sbin/ocs-sr -g auto -e1 auto -e2 -r -j2 -c -scr -p reboot restoredisk windows10 nvme0n1
This command is also saved as this file name for later use if necessary: /tmp/ocs-windows10-2022-01-
20-22-23
********************************************************.
Press "Enter" to continue...
Activating the partition info in /proc... done!
********************************************************.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/windows10" -> "nvme0n1 nvme0n1p1 nvme0n1p2 nvme0n1p3"
The image was created at: 2022-0113-2233
WARNING!!! WARNING!!! WARNING!!!
WARNING. THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
 BE LOST:
********************************************************.
Machine: Precision Tower 3620
nvme0n1 (256GB_SM951_NVMe_SAMSUNG_256GB__SM951_NVMe_SAMSUNG_256GB_______S27ENYAH100101)
********************************************************.
Are you sure you want to continue? (y/n) y
OK, let's do it!!
This program is not started by clonezilla server.
********************************************************.
Let me ask you again.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/windows10" -> "nvme0n1 nvme0n1p1 nvme0n1p2 nvme0n1p3"
The image was created at: 2022-0113-2233
WARNING!!! WARNING!!! WARNING!!!
WARNING. THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
 BE LOST:
********************************************************.
Machine: Precision Tower 3620
nvme0n1 (256GB_SM951_NVMe_SAMSUNG_256GB__SM951_NVMe_SAMSUNG_256GB_______S27ENYAH100101)
********************************************************.
Are you sure you want to continue? (y/n) y_
```

‘y’ again



Welcome to login

Password: EECS565security!

Change the default password after you login

Acknowledgements

- We thank Dr. Bardas and his TA Kabir for sharing the materials and the infrastructure created for EECS 465.

- This computer lab will be shared with students in EECS 465 and JayHacker Security Club.