Using Emmabuntüs refurbishing USB keys

Written by Emmabuntüs collective

Updated : May 7, 2023

Using Emmabuntüs refurbishing USB keys

Publication date : 2022-01-07

Main author : Emmabuntüs collective

This document has been published as part of our reuse/refurbishing campaign together with **Debian-Facile**, **Blabla Linux** **and** **Tugaleres.com** which started in September 2020, following the diffusion of our method to realize of a refurbishing USB key, and the realization by our friends of Debian-Facile of a tutorial on this subject concerning the key based on MultiSystem (obsolete version since the announcement of the discontinuation of MultiSystem development). And our friend Amaury from Blabla Linux has made a set of videos about this, and moreover proposes to provide at cost price, plus shipping, refurbishing USB keys according to several configurations listed on this page.

To simplify the making of our refurbishing USB key (flash drive), we published a new tutorial on this subject in November 2021 using a Ventoy-based key, and allowing the realization of this key under both Linux and Windows. Then in September 2022 we added a tutorial on using the Ventoy based refurbishing key in Secureboot mode.

We thought that this would be enough to easily use our refurbishing keys, but after seeing small problems encountered by some users who bought these keys, we saw the necessity to write a small tutorial explaining how to use these keys and exposing the details of the various menus present on them.

1 - Launching the refurbishing key

To use the key, please please plug it into a USB port while the computer is turned off.

Note : if your computer has USB ports with a blue color instead of black color coding, we recommend you use that one which is a USB-3 standard much faster than USB-2 or 1.

Turn on the computer and regularly tap on a function key (F12, F9, F2, Esc, see on **this page the key that corresponds to your computer**) to bring up the "**Boot Menu**".

You should land on a screen similar to this one:

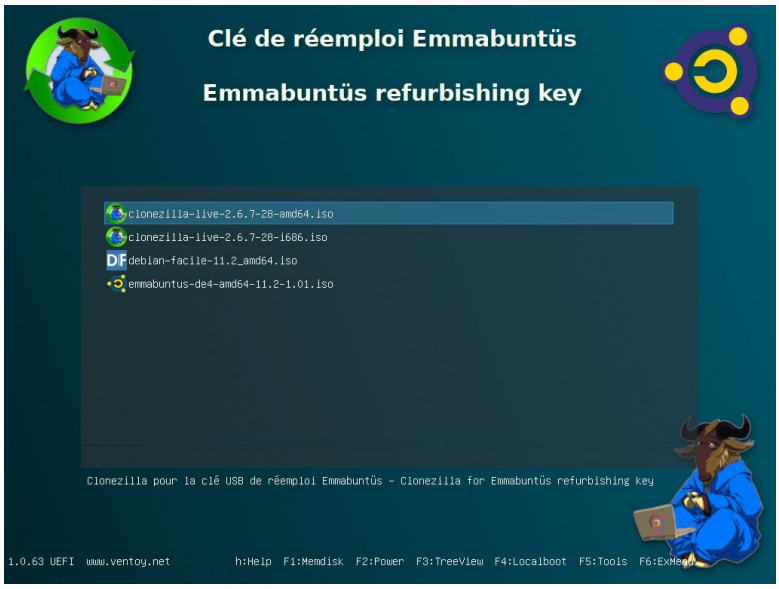
Within this menu, you should see a line with the name of your USB key. Select this line and validate your choice by pressing the "Enter" key.

Note : If this line is not present in the menu, select the line <Enter Setup>, and go check that the USB ports are enabled, and that in the "Boot Menu", the USB flash drive device is not excluded from the list of bootable devices. If this still doesn't work, it is likely that your computer doesn't support booting on this type of USB stick, so the last solution is to use a CD containing Plop Manager or our own ISO version of Plop, then boot on this CD which , in turn, will then boot the USB stick. Be careful, when using the Plop manager CD, it is important not to use a USB keyboard, which might not work properly.

•

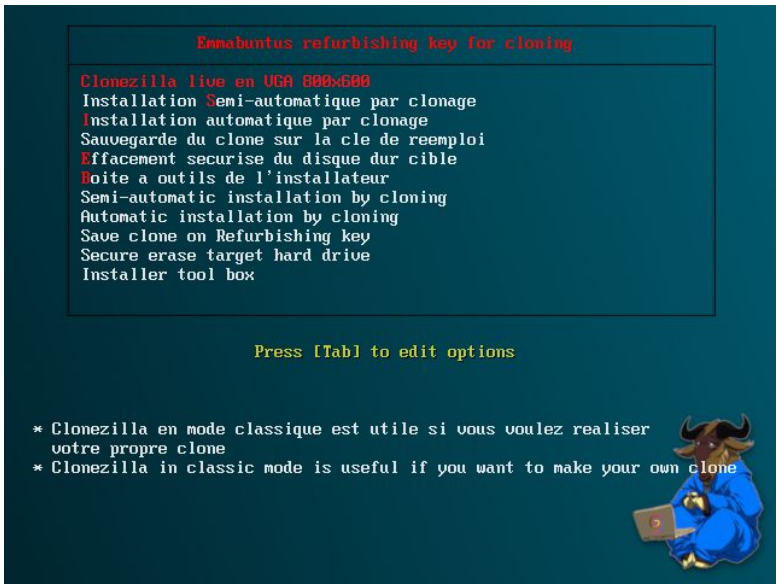
2 - Refurbishing key based on Ventoy

You should now land on this Ventoy welcome window :



In the above window, you can run the refurbishing script with either 64-bit or 32-bit Clonezilla, and you will get one of the windows below to run the cloning script :

- BIOS Legacy mode :



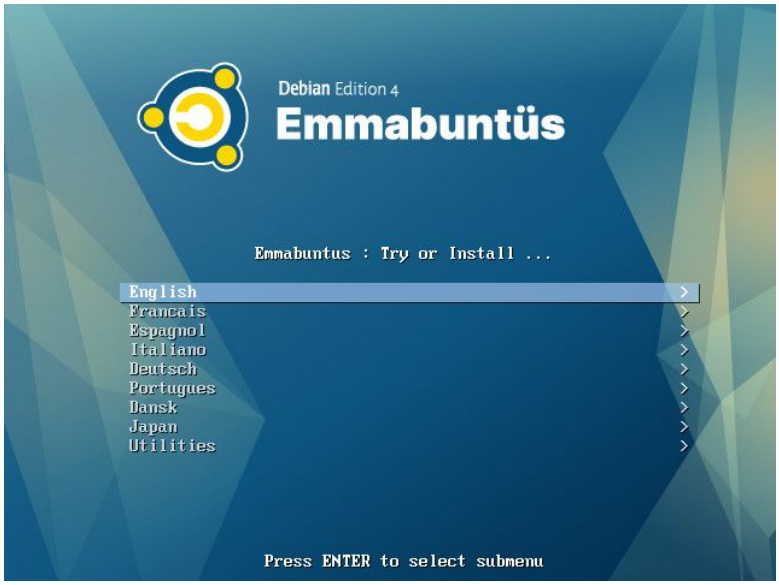
- UEFI mode :

Note : The two previous screens allow you to launch one of these commands :

- Clonezilla live : let you use **Clonezilla** in classic mode, in order for you to build your own clone ;
- Clé de réemploi installation semi-automatique : allows you to select a clone when running the script in French ;
- Clé de réemploi installation automatique : allows you to start the automatic cloning process in French ;
- Effacement sécurisé[1] : allows you to securely erase the target hard drive using the Nwipe utility for magnetic disks, with the choice of erase mode: Zero Fill, Short DoD, DoD DoD 5220.22M, and another user-defined choice in the Nwipe TUI. Hdparm is used for Solid-State Drives and nvme-cli for NVMe devices;
- Boîte à outils : let you test different computer components: memory, disk, etc;
- Sauvegarde du clone sur la clé de réemploi : allows you to automatically copy the contents of the referenced hard drive to the refurbishing key, in order to create a clone, with French messages;
- Refurbishing key semi-automatic install : allows you to select a clone when running the script in English;
- Refurbishing key automatic install : allows you to start the automatic cloning process in English;
- Clone backup : allows you to automatically copy the contents of the referenced hard drive to the refurbishing key, in order to create a clone, with English messages;

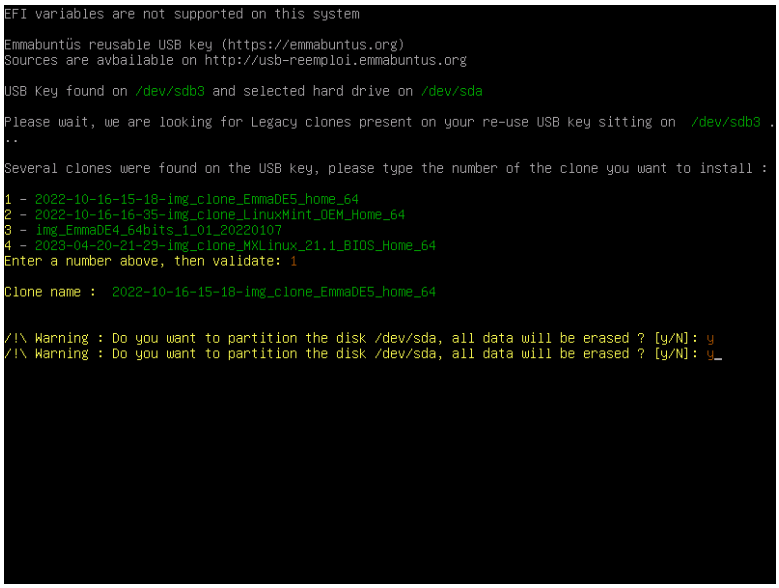
- Secure erase[1] : allows you to securely erase the target hard drive using the **Nwipe** utility for magnetic disks, Hdparm is used for Solid-State Drives and **nvme-cli** for NVMe devices with english messages;
- Tool box : let you test different computer components: memory, disk, etc;
- Information about the re-use key : describes the different ways to use these menus, and indicates the shortcut keys in English and French.

- In this particular example, the last two lines allow you to launch **DF-Linux** or Emmabuntüs DE 4 in live mode, and you will get the window below if you launch Emmabuntüs DE 4



Semi-automatic and automatic modes differences

The semi-automatic mode allows you to choose a file among the different clones available on the "IMAGES" partition, as shown in the image below, when launching the refurbishing key script:



The automatic mode, on the other end, does not allow you not to choose a clone when launching the script, but let you define it beforehand inside the "clone.ini" file. This saves time when launching the script.

Note : The semi-automatic mode is suitable for the use of a single refurbishing key per user, but if you want to use several keys per user we recommend the automatic mode which is very handy for mass re-use.

The "clone.ini" file must be present at the root of the "IMAGES" partition and allows you to define the four default clones via these four variables :

- CLONE_LEGACY_32=
- CLONE_LEGACY_64=
- CLONE_UEFI_64=
- CLONE_UEFI_SB_64=

To achieve this, enter the directory names containing the clones you want to install, for respectively the “BIOS Legacy” in 32-bit or 64-bit, the “UEFI” 64-bit, or the “UEFI+Secureboot” 64-bit modes.

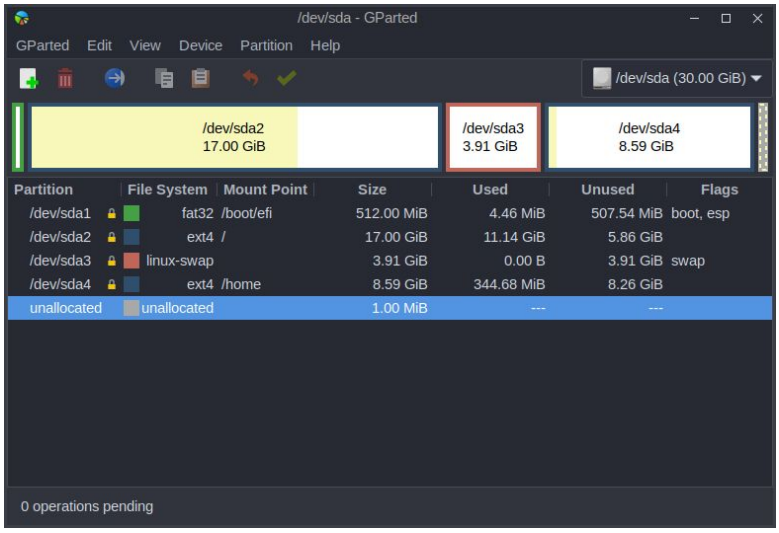
Note : The "Legacy_32" clone is installed if you are running a 32-bit version of Clonezilla, and the "Legacy_64” one if you are running a 64-bit version of Clonezilla.
The "UEFI_64" and "UEFI_SB_64" clones can only be installed if you run a 64-bit Clonezilla version.

In order to use this clone in automatic mode when your clone contains two system partitions instead of one, for example the root and the home partition, you will have to fill in one of these four additional variables present in the "clone.ini" file:

- CLONE_LEGACY_32_NUMBER_PART_EXTEND=
- CLONE_LEGACY_64_NUMBER_PART_EXTEND=
- CLONE_UEFI_64_NUMBER_PART_EXTEND=
- CLONE_UEFI_SB_64_NUMBER_PART_EXTEND=

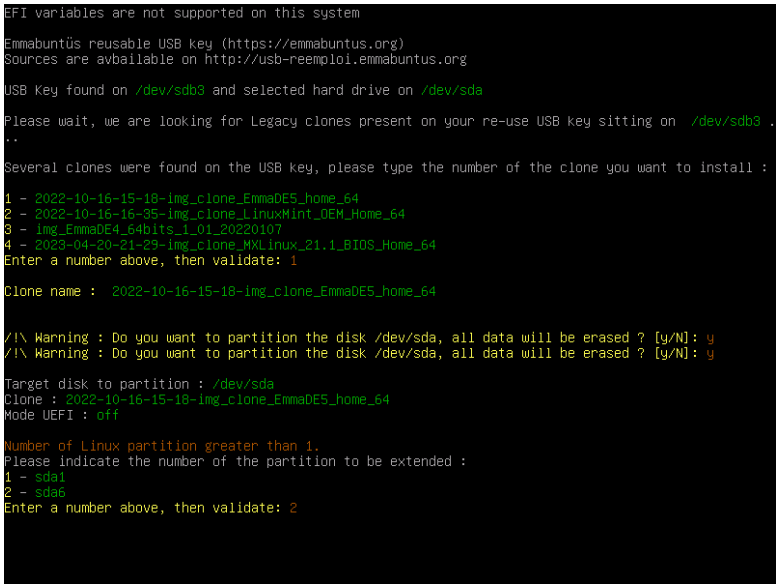
To do this, enter the number of the partition between 1 and 2 that you want to extend in the order of the partitioning scheme of your clone.

For example with the following UEFI 64 bits clone partitioning scheme:



If you want to extend the root partition on sda2, enter 1 in the variable CLONE_UEFI_64_NUMBER_PART_EXTEND, or 2 if you want to extend the /home partition on sda4.

Note: If this variable is not filled in when using cloning in automatic mode, the script will stop and then ask you to enter the number representing the partition you want to extend:



3 - What type of cloning to use ?

On your key, you can have a cloning via Clonezilla 64 and/or 32 bits. You should know that you can use 64-bit cloning in any case even to clone a 32-bit clone, except if your physical machine is a real 32-bit. In this case, you are obliged to use a 32-bit Clonezilla with a 32-bit clone.

4 - Which clone to use ?

Since the update of our refurbishing key in October 2022, it supports now the default installations of many GNU/Linux distributions. So we have decided to stop providing pre-configured clones as standard, and to stop updating the ones on this page, except for very specific requests coming from associations we work with.

If you still want to make your own clone, please look at our tutorial on "**Making a clone for the Emmabuntüs USB refurbishing key**".

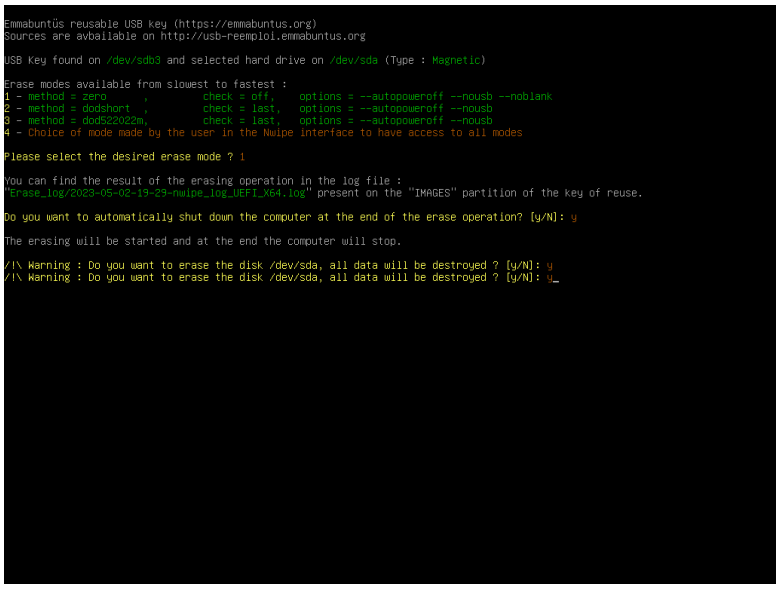
5 - Securely erase a target disk

The refurbishing key also let you securely erase a target disk whether it is a magnetic one, or a SSD or a MVMe. To accomplish this operation, when the secure erasing procedure is launched, it will determine which utility to use depending on the target disk present in the system.

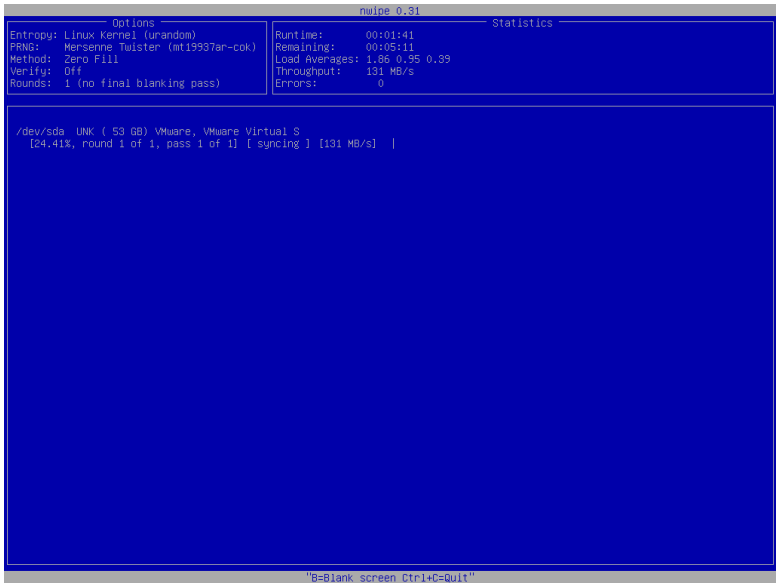
Note: This erasing procedure should only to be done if you have constraints concerning the security of the old data residing on the target disk, because this operation can last several hours in the case of a magnetic hard disk and depending on the erasing mode selected by the user.

5.1 - Magnetic disks

For magnetic hard disks, the script will implement the **Nwipe** utility in two different modes, either fully automatic by selecting the first 3 options we have predefined, or fully manual by using the last option where the user will be able to configure the Nwipe utility according to its needs :



After validation of the choice, the Nwipe utility is launched and keeps the user informed with the progress of the erasing operations :

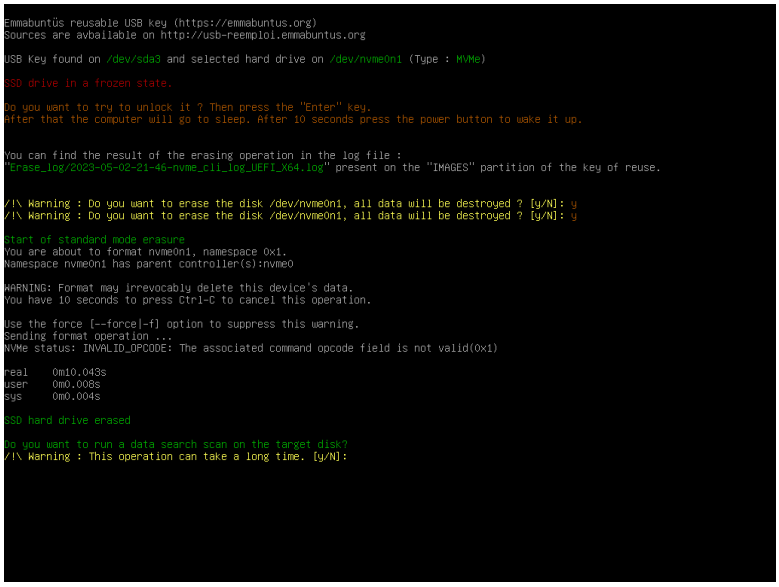


The computer will automatically shut down when the operation is done, and you will be able to find the erasing operation log file within the folder "Erase_log" of the "IMAGES" partition of the refurbishing key.

5.2 - Electronic disks

For electronic devices, the script will implement either the **Hdparm** utility for SSDs or the **nvme-cli** for **NVMe** devices.

When dealing with electronic disks, they may be in a "frozen" state, which means that the script will ask you if you agree to turn the computer off, in order to deactivate the "frozen" mode of the electronic disk:

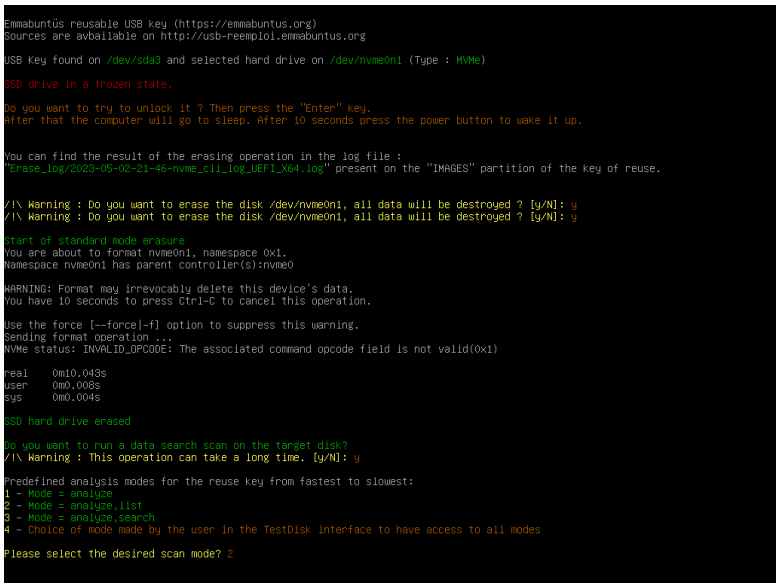


Wait for about 10 seconds after the computer has been turned off, and press the power button on the computer.

The script will then resume the electronic disk erasing procedure.

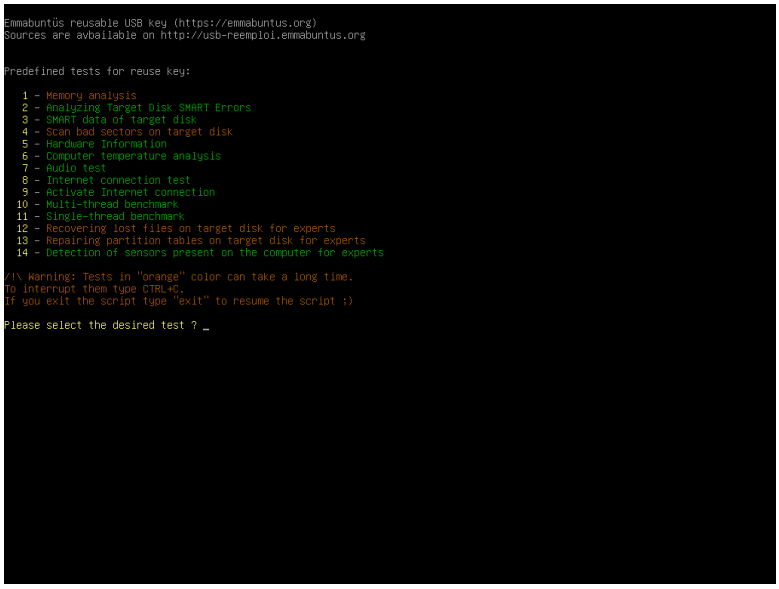
At the end of the erasing procedure of the electronic disk, the script will control if there are still data on this device and report accordingly if the operation was successful, or not.

Note: After the secure erasure operation, the script will still find data present on some SSD or MVMe disks. In this case we advise you to double-check the presence of data with the **Testdisk** utility, which is present on the refurbishing key. Therefore the launch of this utility is proposed at the end of the erasure procedure whatever the result was:



6 - Tool box

This toolbox consists of the different utilities present in Clonezilla and allowing you to test different components of the computer: memory, disk, etc :



All these utilities speak only in English, and it is unfortunately not possible for us to add their translation in other languages within Clonezilla.

In our toolbox, we have configured the utilities with predefined options to make them as simple as possible to use, except for the **PhotoRec** utility to recover lost files, and the **TestDisk** utility to repair partition tables, because their use cases are very dependent on the choices of the user, according to what he wants to accomplish.

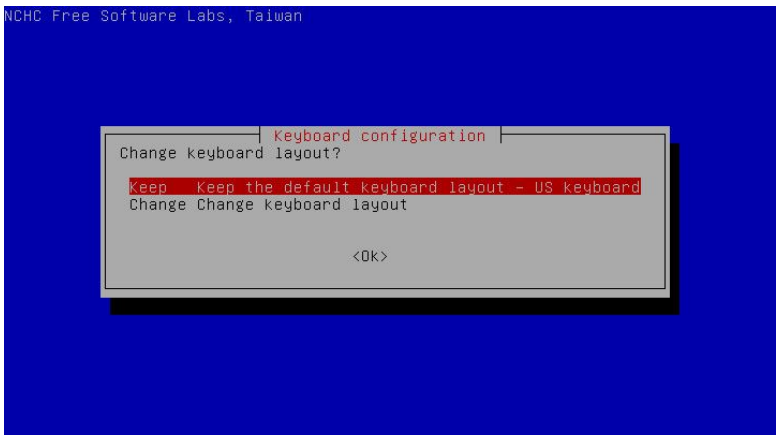
Regarding the use of these utilities we refer you to the sites of their editors or these tutorials:

- SMART : Self-Monitoring, Analysis and Reporting Technology
- Establish a Wi-Fi connection from the terminal with nmtui or nmcli
- Benchmarcking 7-Zip Compression
- How to recover deleted files or lost data
- Partition tables recovery with TestDisk

Note: If you want to use the **inxi** utility instead of **hwinfo**, please put the **inxi binary** next to this script on the USB drive and then inxi will be used instead of hwinfo.

7 - Removing the refurbishing key

It is advisable to remove the key when the computer is turned off, and for this purpose the easiest way is to press the power button for more than 4 seconds when the PC is restarting after the cloning. If you don't do this in time and your computer restarts after cloning, it will stop in the case you are using a MultiSystem refurbishing key, on the Clonezilla launcher configuration screen below:



In the case you are using the Ventoy refurbishing key, the computer will stop on the home screen of the Ventoy refurbishing key.

In these cases, simply press the power button for more than 4 seconds to turn off the computer, then remove the USB key.

8 - Tips and Advice

The management of the UEFI or BIOS Legacy boot order is different for each computer: the procedures are standardized, but it sometimes happens that one manipulation works better than another... so here is a small list of tips and advice to take into account if you encounter problems during your tests.

- UEFI management is automatically handled by the refurbishing script, however, it is best to disable UEFI on the machines to be refurbished in order to improve hardware and software compatibility. UEFI clones are only visible if the USB stick has been launched in UEFI mode;
- If you use computers featuring the SECUREBOOT, we advise you to deactivate this option if possible (you have to go through the Setup menu when starting the computer);

- Our cloning script let you clone one hard disk only, and if you have several hard disks present on the computer the script will ask you to select the target disk to be cloned.

9 - Notes

1) To better understand the interest of using Nwipe, and the issues related to data erasure, see this Wikipedia **article** explaining in particular in preamble :

Data erasure (sometimes referred to as data clearing, data wiping, or data destruction) is a software-based method of overwriting the data that aims to completely destroy all **electronic data residing** on a **hard disk drive** or other **digital media** by using zeros and ones to overwrite data onto all sectors of the device in an **irreversible process**. By overwriting the data on the storage device, the data is rendered irrecoverable and achieves data sanitization.

10 - Table of contents