

TEKNOSERVICE ERASE SYSTEM – ERASER

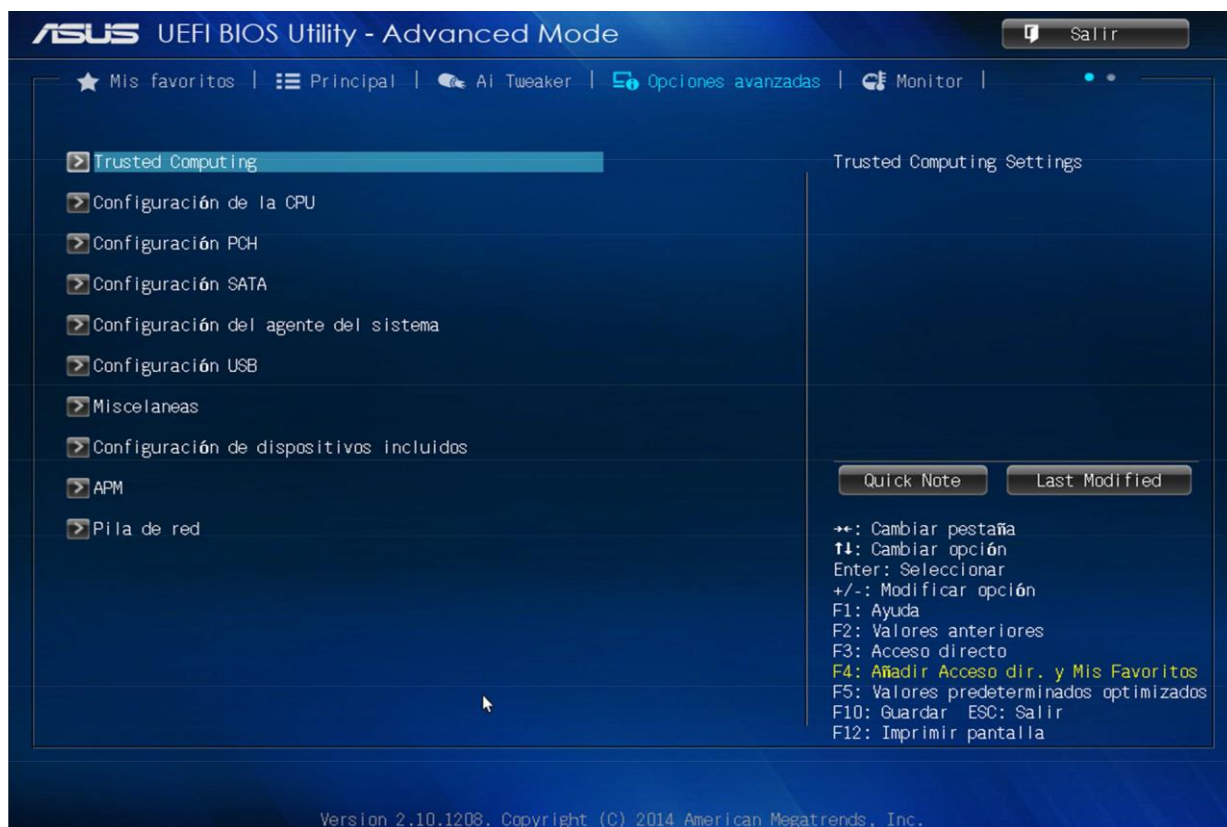
BIOS PREPARATION

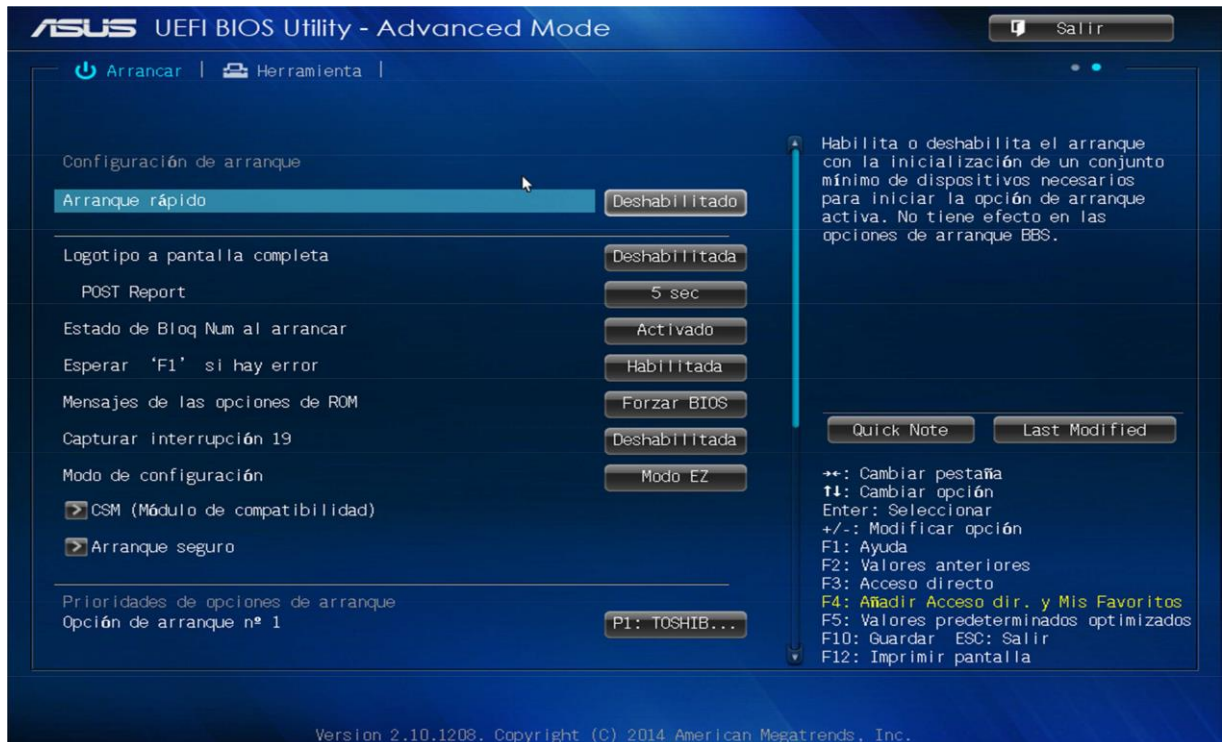
To proceed to activate the disk erase system, it is necessary to activate it from the BIOS. To do this, after starting the computer, press the F2 key to enter the BIOS.

The access to the BIOS must be protected by password, so that users cannot manipulate it, for security.

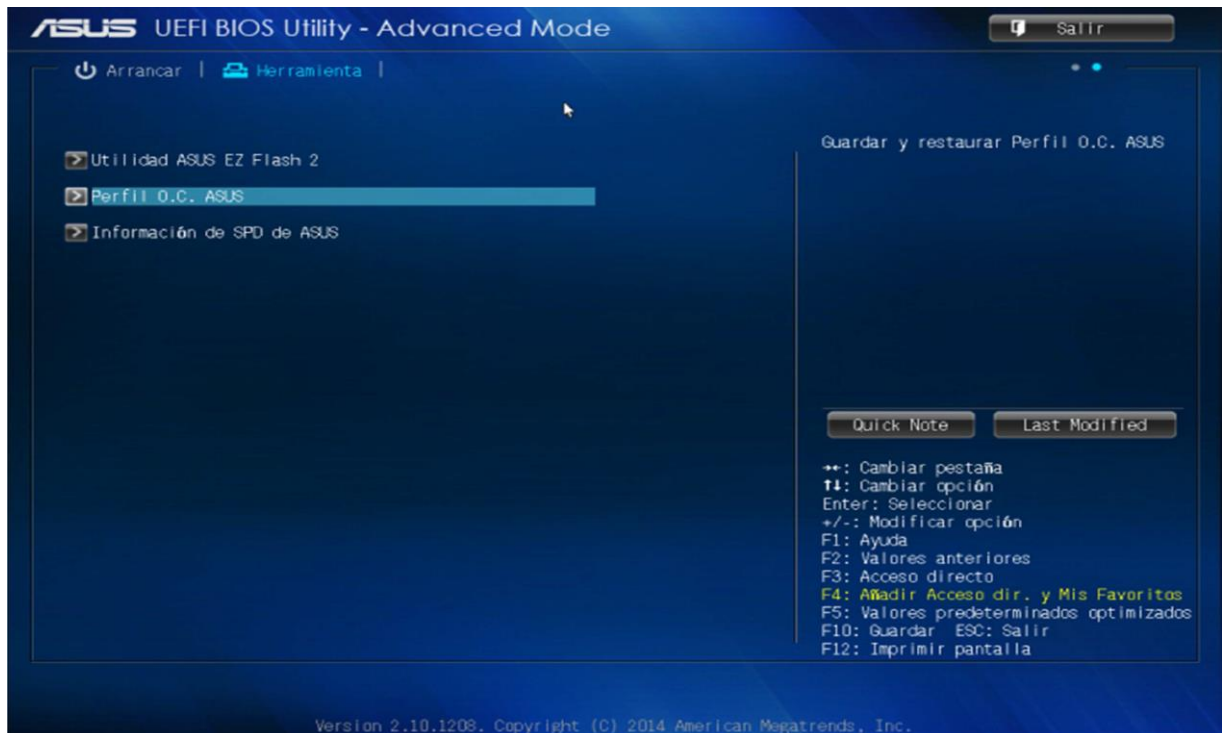
The default password is **ttl**.

Once inside the BIOS, in the **main menu**, we select the **advanced options** tab. Just below the **exit button** we will click on the second circle (the gray one) to see the next advanced options menu.

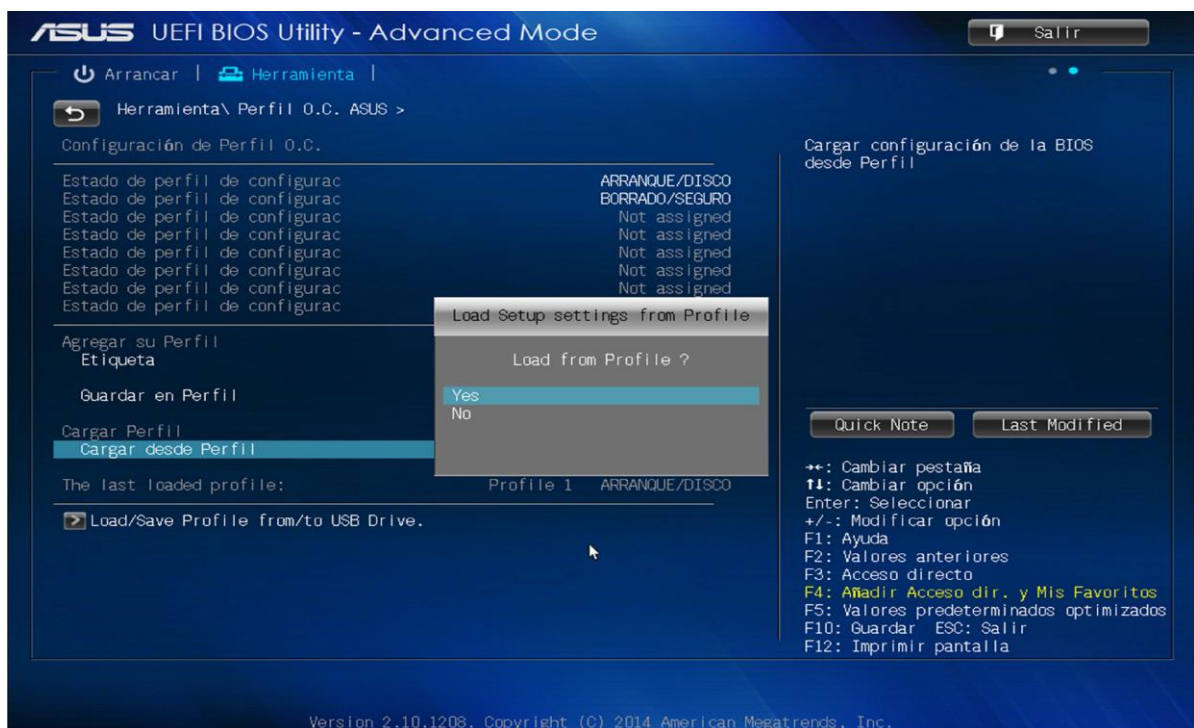
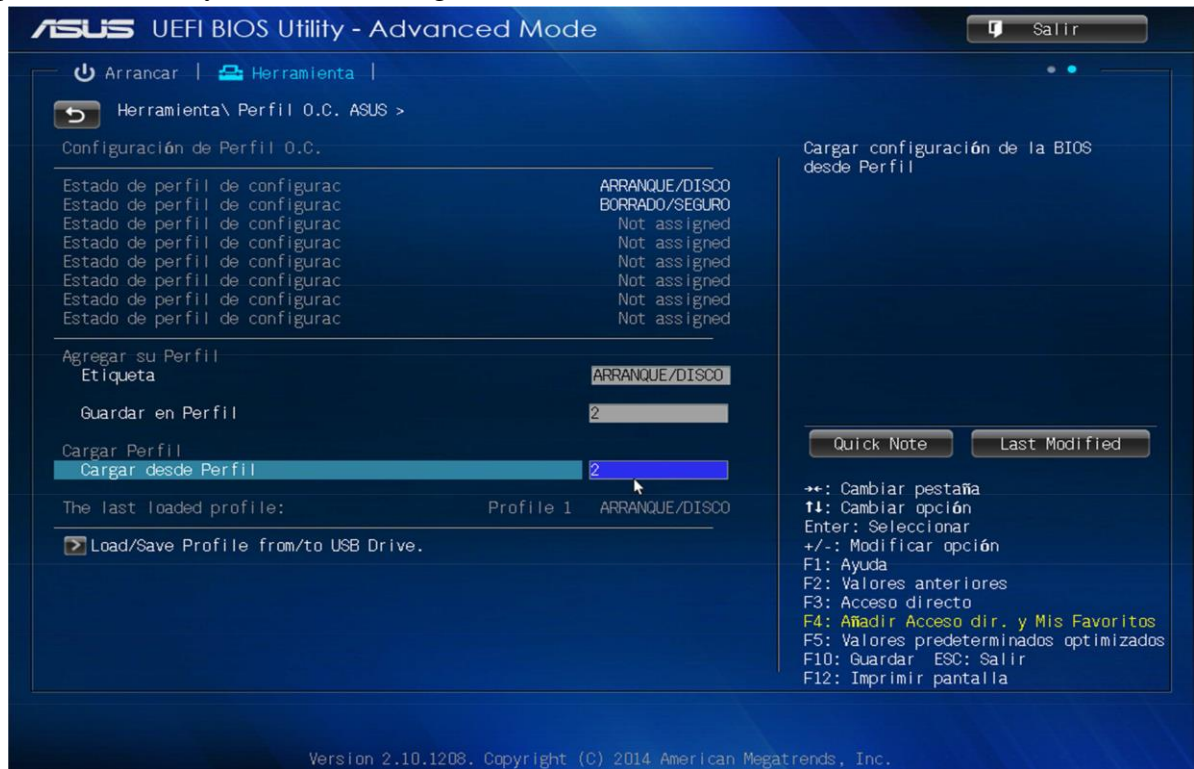




Inside the second menu of advanced options we will click on the tools tab where we will select the "OC" profile option Asus.



Next we will position ourselves on the option **load from profile** and we will type option No. 2, in this way we will load the option of secure deletion. Before leaving the BIOS, we will press the F10 key to save the changes we have made.

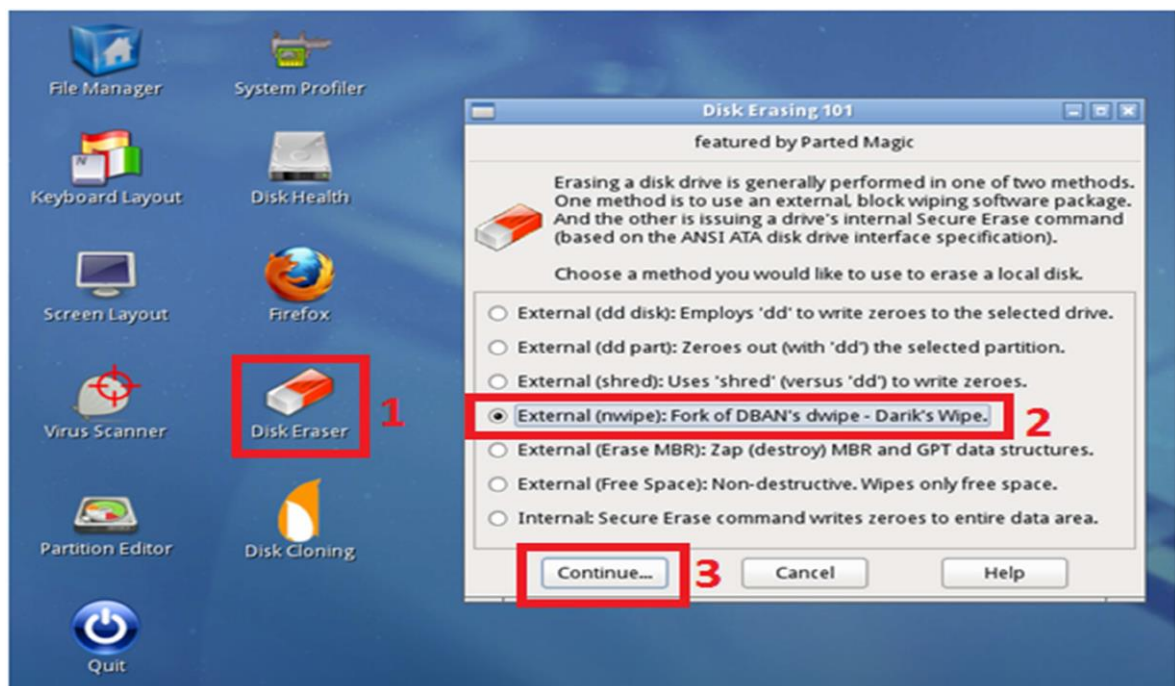


Once all the changes in the BIOS configuration have been made, **DURING THE START OF THE MACHINE**, we will press the F8 key repeatedly to show us a boot menu in which we will select the Kingston pendrive (8 gigabytes) in which we will find the application Secure erase.

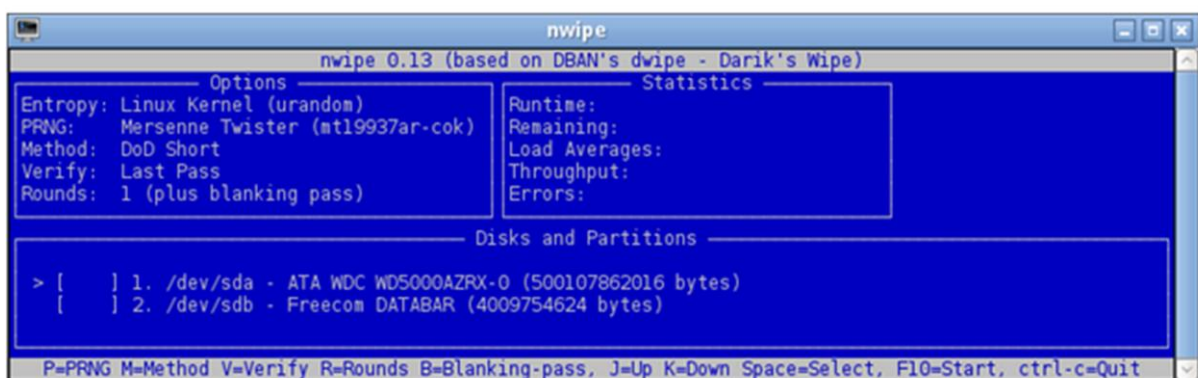
ERASER

When starting from the option of the pendrive, a small Linux system will be started that contains rescue tools among which we will choose the **DISK ERASER** application. At this point, the erase system will automatically start.

After the initial load, a screen will appear where we will launch the disk deletion process.

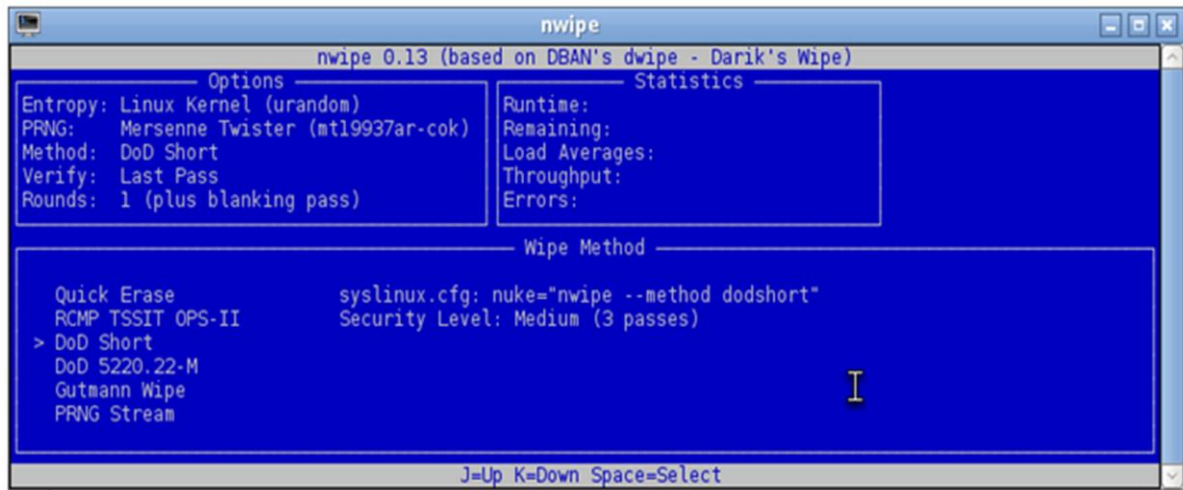


Double click on the "Disk Eraser" icon (1), a window will appear where we select the option "External (nwipe): Fork of DBAN's dwipe - Darik's Wipe" (2) and press the "Continue" button (3).



METHODS OF DELETING

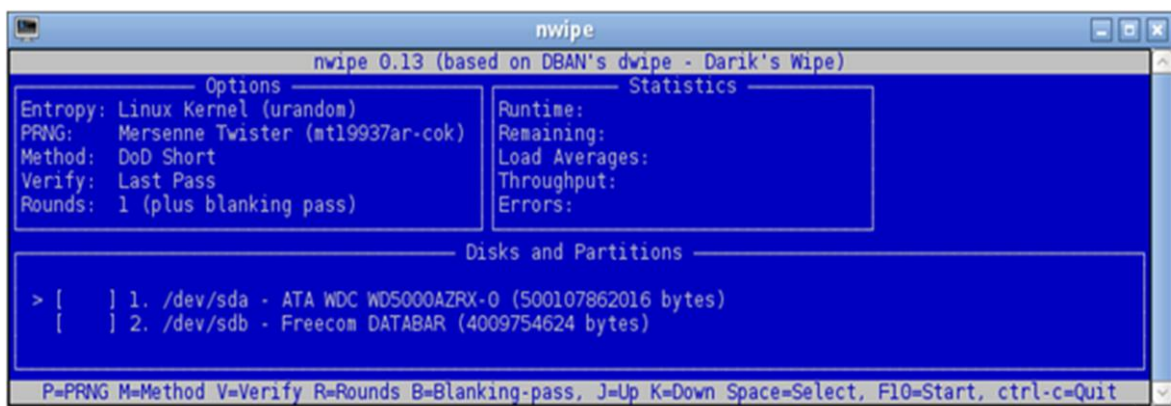
The available erase methods are as follows (**M** key (Method) in the initial screen):



The DoD Short method appears, which is also the recommended one.

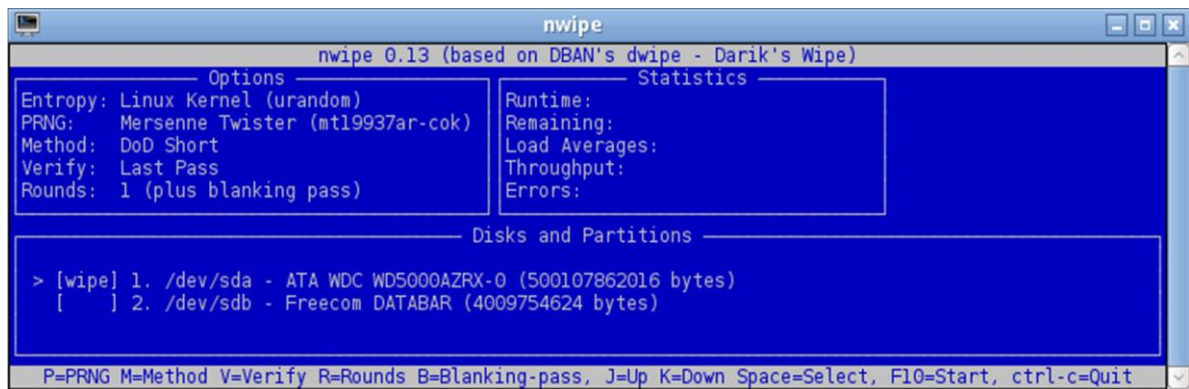
The minimum estimated characteristics and times are the following:

Methods of deleting	Characteristics	Minimum Estimated Time
Quick Erase	Writing of Zeros	2 hours
RCMP TSSIT OPS-II	Canadian Standard	10 hours
DoD Short	Department of American Defense – 3 passes	5 hours 30 minutes
DoD 5220.00-M	Department of American Defense – 7 passes	10 hours
Gutmann Wipe	Gutmann Method	40 hours
PRNG Stream	Writing random data	3 hours



At this point, we are ready to carry out the deletion.

Select the hard drive to be erased (using the "**Space**" key) **"/dev/sda - ATA WDC WD5000AZRX-0"** and it will be marked as **"[wipe]"**.



```
nwipe
-----
nwipe 0.13 (based on DBAN's dwipe - Darik's Wipe)
-----
Options                               Statistics
-----
Entropy: Linux Kernel (urandom)        Runtime:
PRNG:  Mersenne Twister (mt19937ar-cok) Remaining:
Method: DoD Short                       Load Averages:
Verify: Last Pass                       Throughput:
Rounds: 1 (plus blanking pass)          Errors:

-----
Disks and Partitions
-----
> [wipe] 1. /dev/sda - ATA WDC WD5000AZRX-0 (500107862016 bytes)
[ ] 2. /dev/sdb - Freecom DATABAR (4009754624 bytes)

-----
P=PRNG M=Method V=Verify R=Rounds B=Blanking-pass, J=Up K=Down Space=Select, F10=Start, ctrl-c=Quit
```

Next, press **F10** to start the deletion. This process destroys the contents of the disk. The status of the deletion process (Statistics) will appear on the screen.

Once the deletion has been completed, the confirmation of the deletion (sucess) will appear on the screen.

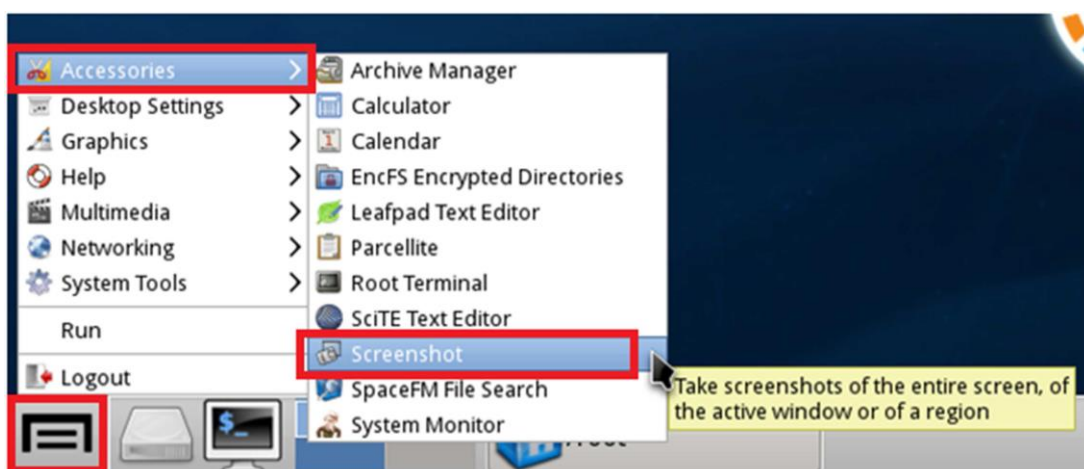


```
ATA WDC WD5000AZRX-0
(sucess)
```

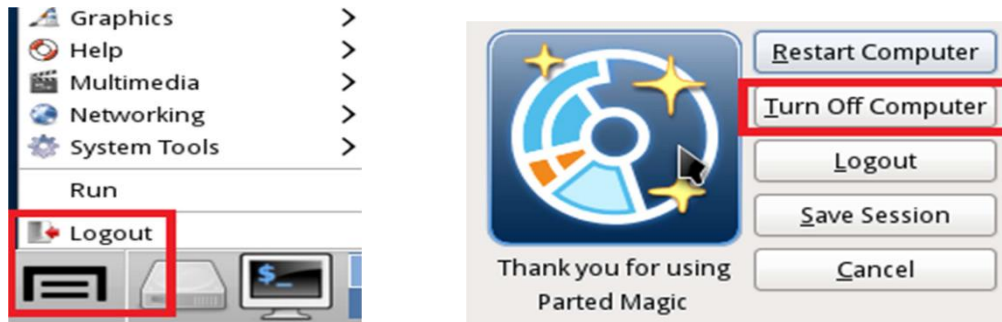
LOG

The log file of the deletion process can be retrieved from the path `"/root/nwipe.log"`. This file can be stored in an external device, such as a USB memory, through the **"Copy"** action and later **"Paste"**.

It is also possible to take a screenshot to a file using the "Screenshot" utility.



Once the disk erasing is finished, in order to exit the system, we select "**Logout**" and press the "**Turn Off Computer**" button:



The system will turn off.

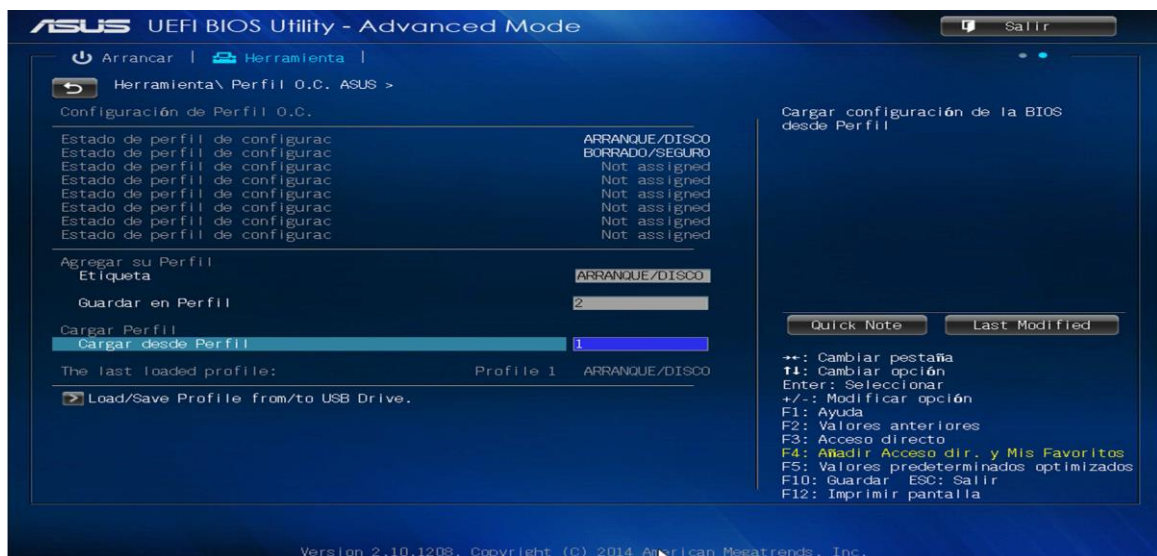
RESET THE BIOS

In order to make the system available for normal booting for the use of the user operating system, it is necessary to configure it through the BIOS.

To do this, after starting the computer, press the F2 key to enter the BIOS.

The access to the BIOS must be protected by password, so that users cannot manipulate it, for security. The default password will be **ttl**.

Once inside the BIOS, we will follow the previously detailed steps to change the boot profile (BIOS **main menu** **advanced options** under the **exit button** click on the second circle inside the second menu we will click on tools profile "OC" Asus. Option to load from profile type option N°1 and save configuration by pressing F10.



The system will reboot and start loading the Hard Disk Operating System.