DEFT Zero – Quick Guide

Table of Contents

Foreword

DEFT Zero is designed to be a DEFT light version focused on the forensically copy of digital evidences (i.e. hard disks, USB devices and network shares).

DEFT Zero requires a considerably lower space in RAM and on a CDROM/pendrive. It needs about 400 Mbytes, which can even boot in the RAM preloaded mode on a obsolete and low resources hardware.

DEFT Zero is based on Lubuntu 14.04.02 LTS and its future releases will be developed in parallel with DEFT full version.

DEFT Zero can be run on newest hardware as well, since it can support 32 and 64 bits platforms, with UEFI and Secure Boot such as Macbooks and Windows 8 ready machines.

This document will cover the differences and enhancement with DEFT standard (full) version.

Boot modes

When first booting a PC with DEFT Zero, you will be prompted with three choices:

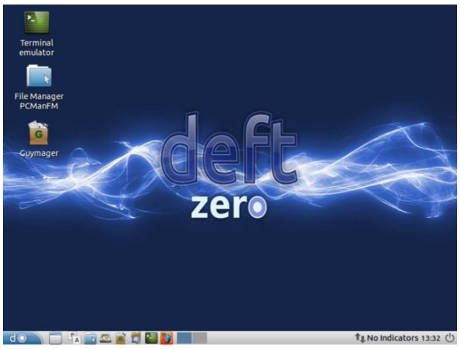
1) DEFT-Zero Linux Live (GUI mode, RAM preload)

2) DEFT-Zero Linux Live (GUI mode)
3) DEFT-Zero Linux Live (Text mode)

Please, note that modes above simply add or remove kernel parameters to the boot options you can customize on your own by pressing the “F6” key during the options screen and editing the text before the “--" trailing line.

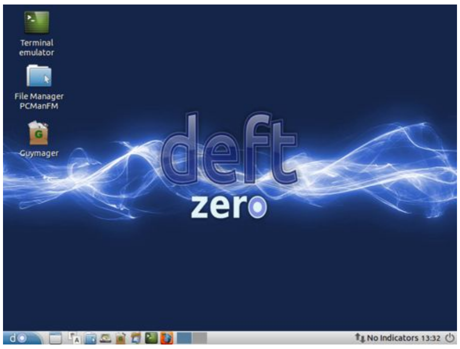
1) GUI mode, RAM preload

The first boot mode loads DEFT Zero in RAM and with the Graphical User Interface already started. The RAM loading means that, once the system is loaded, you can remove the CDROM or the pendrive from the drive/port (which can be lifesaving in oldest Macbook Air with only one USB port) and everything will continue to work smoothly. The OS and application will be loaded from the copy of the CD/USB which is performed to RAM during boot. Of course, this mode can be used only if the hardware supports at least 512 MB of RAM, which most systems nowadays do.



2) GUI mode

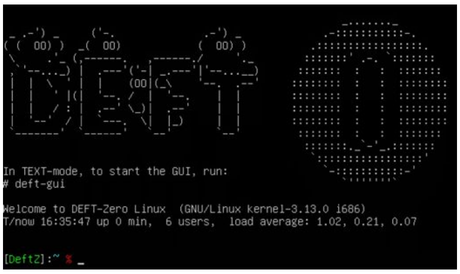
The 2nd boot mode loads DEFT Zero with the Graphical User Interface, thus consuming more RAM than the command line mode (option 3) but not as much as the RAM preload mode (option 1).



This boot mode is suggested for devices with low RAM availability but a standard video card capable of supporting a graphical environment.

3) Text mode

The 3rd boot mode loads DEFT Zero in command line mode, preventing the GUI from being started. This method uses less memory and can be employed in very obsolete hardware with graphical issues, weak CPU or less RAM than 512 MB of RAM.



```
In TEXT-mode, to start the GUI, run:
# deft-gui

Welcome to DEFT-Zero Linux  (GNU/Linux kernel-3.13.0 i686)
T/now 16:35:47 up 0 min,  6 users,  load average: 1.02, 0.21, 0.07

[DeftZ]:~ % _
```

The default keyboard loaded at boot is the English one, if you wish to switch to other keybord layouts, simply type “loadkeys it” to switch to Italian mode, “loadkeys fr” to switcth to French mode and so on.

From this mode you can switch to GUI loading the Graphical User Inerface by typing “deft-gui” at the command prompt. It’ now possible to go back to terminal window or to switch between virtual terminals by pressing CTRL+ALT+F1 for virtual terminal 1, CTRL+ALT+F2 for the second and so on. The virtual terminal hosting the graphical environment is the seventh. In order to go back to the graphical user interface simply type the shortcut CTRL+ALT+F7.

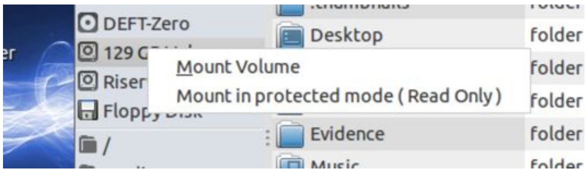
Device mount modes

As well as DEFT full version, DEFT Zero can be used to mount devices in read/write and read-only mode. The write protection policy has been enforced, so as to avoid accidental tampering of devices which, during investigations, are considered as evidence and as such must be managed. The mounting process via GUI mode is the same as in DEFT 8, while in command mode some improvements have been fulfilled in order to meet the security requirements of digital investigators.

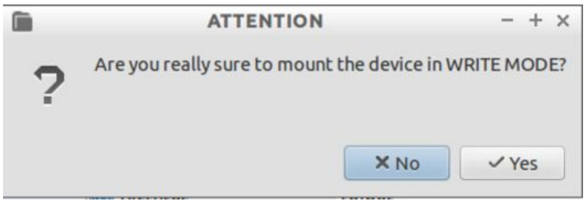
Mount devices via GUI

If you wish to mount a device in read-write mode of in read-only mode, you can either do it through the File Manager PCManFM GUI Application or via command line.

In order to **mount a device in r/w (read and write) mode** by using the GUI, you simply have to launch the File Manager PCManFM, via its icon on the Desktop or via "Menu → Accessories → File Manager PCManFM" shortcut. Right click on the device you wish to mount and choose between "Mount Volume" and "Mount in protected mode (Read Only)".



The first option mounts the device in read-write, after letting you confirm your intentions by clicking on the following warning dialogue.

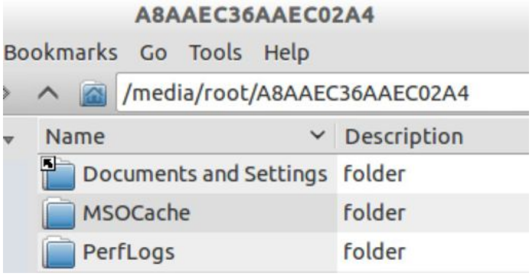

ATTENTION

Are you really sure to mount the device in WRITE MODE?

In order to **mount a device in r/o (read only) mode**, simply choose the second option, so as to be able to browse the content of the device while not letting accidental writing take place. That's the preferred mode while performing incident response or triage activities.

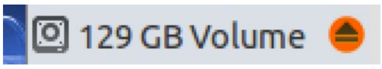
Please, note that when mounting a device/partition via the GUI application File Manager PCManFM, the automatically generated mountpoint will be located under the "/media/root" folder, in a subfolder created after the volume label/UUID of the device. In the example above, sda1 volume label is

"A8AAEC36AAEC01A4" and that's the folder where the filesystem of the device will be mounted, under the patent folder tree "/media/root".

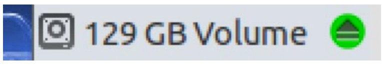


Name	Description
Documents and Settings	folder
MSOCache	folder
PerfLogs	folder

According to the mount mode you choose, the device in the list in the left column will be provided with an orange unmounts button when the triggered mount mode is read-write



or a green unmount button when the triggered mount mode is read-only.



In order to **unmount** the filesystem, in both mount modes, you simply have to click on the orange or green round button next to the device in the left column of the File Manager display window.

Mount devices via Command Line

The main difference with DEFT 8 and following versions mounting mode lays in the command line mounting process. Please, follow carefully the indications otherwise you may not be able to mount devices in write-mode via the command line.

First, launch the Terminal Emulator via the icon on the top left of the "Desktop or via the "Menu → Accessories → LXTerminal" shortcut.

In order to **mount a device in r/o (read only) mode** (in the example "sda1" is the device and partition to mount and "/mnt/c" the chosen mountpoint) simply type the following command at the command prompt:

```
# mount –o ro /dev/sda1 /mnt/c
```

Please, note that omitting the "-o ro" flag results in a "fuse: mount failed: Permission denied" error.

In order to **mount a device in r/w (read and write) mode** (in the example "sda1" is the device and partition to mount and "/mnt/c" the chosen mountpoint) you should first unlock the writing mode on the device by means of the "wrtblk-disable" script, which takes the partition as only command line parameter.

```
# wrtblk-disable /dev/sda1
```

Once unlocked the partition, you can issue the usual mount command, with no mount mode option or with "-o rw", which is just the same.

```
# mount /dev/sda1 /mnt/c
```

You can now browse the filesystem of the first partition of the device ("sda1" in the example above) and write files or folders.

The partition remains writable until the "wrtblk" command is issued, reverting the device state to the locked mode.

```
# wrtblk /dev/sda1
```

If you wish to manually edit the lock/unlock property of devices, simply use the "blockdev" command with the "--setrw" option followed by the complete path of the device first and then once again with the partition to set the read-write mode, just as follows:

```
#blockdev --setrw /dev/sda
#blockdev --setrw /dev/sda1
```

The two commands above set the write mode enabled on the device sda and its first partition sda1. In order to restore the locked mode on the partition, you should use the "blockdev" command with the "--setro" option on the device and on the partition, just as follows:

```
#blockdev --setro /dev/sda
#blockdev --setro /dev/sda1
```