

# Quickstart Guide for the Knoppix v3.8.1 FCCU Forensic LinuxCD-ROM + EnCase "linen" Acquisition Utility

Robert Sheehy - [rsheehy@oig.hhs.gov](mailto:rsheehy@oig.hhs.gov)

May 5, 2005

The base CD-ROM image is from the Knoppix v3.8.1 release (April 2005), modified by Christophe Monniez of the Belgian Federal Computer Crime Unit (<http://www.d-fence.be/>) to perform computer forensic related tasks and avoid any drive writes during the boot up process (FCCU v8.0). I then further modified the FCCU CD-ROM to include the linen EnCase binary and modified the default startup bootparams to turn on DMA for IDE hard drives and to use the English/US keyboard and language settings as default.

While the system is running, you can switch between virtual consoles using the **ALT-F1**, **ALT-F2**, **through ALT-F12** command keys. This allows you to perform multiple tasks on the system while an image acquire is running.

If text scrolls down the screen, you can press **SHIFT-PAGEUP** and **SHIFT-PAGEDOWN** to go back and view the text that scrolled off the screen.

When you first insert and boot a system from the CD-ROM, you will be given a prompt where you can enter additional command line boot parameters for the Linux Kernel, but documentation of this functionality is beyond the scope of this document. You can just press enter and accept the default settings, or after 5 minutes the system will automatically boot itself if no keys are pressed.

The system then boots with a Linux v2.6 kernel, and attempts to automatically detect all IDE, SCSI, Firewire, RAID, and USB disk devices. Mount points for all drives and partitions are created in the /mnt directory. The CD-ROM filesystem is automatically mounted under the /cdrom director.

Once the system is up, you will be presented with a root command prompt.

If you ever need help with the syntax of a command, you can get a wealth of information by using the **"man"** and **"info"** commands.

*Example:*

```
man hdparm and/or info hdparm  
man bash and/or info bash
```

When all else fails, the manual can be referenced. If there is no man page, then read the source code.

To run the X-Windows subsystem and get a graphical GUI environment, run the command **"startx"**.

When X-Windows is running, you can go back to the console screen by holding down **CTRL-ALT-F1**.

You can return to X-Windows from a virtual console by holding down **CTRL-ALT-F6**.

## Basic Linux Commands You Need To Know

You can view the Linux Kernel bootup messages using the "dmesg" command.

```
dmesg | grep -i hd
```

# View the bootup kernel messages, but filter it so that only the lines containing "hd"

# are shown.

```
dmesg | less
```

# View the bootup kernel messages, and pipe it to "less", so it can be viewed page by

# page.

To change directories, use the "cd" command.

To list the contents of a directory, use the "ls" or "dir" commands.

A drive partition can be mounted using the command "mount /mnt/hdx#" or "mount /dev/hdx#".

*Example:*

```
mount /mnt/hde1
```

The command above will cause the system to attempt to mount the first partition on the MASTER IDE drive on the 3<sup>rd</sup> IDE controller in the system. The system will attempt to guess the correct file system, but sometimes you will need to specify the file system yourself using the -t command, such as "-t ntfs", "-t ext2", and "-t vfat", for NTFS, EXT2, and FAT/FAT32 partitions.

Partitions can be viewed and changed using the "fdisk" command.

*Example:*

```
fdisk /dev/hde
```

Filesystems can be created using the "mkfs" command.

*Example:*

```
mkfs.vfat /dev/hde1
```

```
mkfs.ext2 /dev/hdf1
```

Filesystems can be checked for errors using the fsck command.

*Example:*

```
fsck -y /dev/hdg1
```

Run EnCase for Linux by running the command: **linen**

To change various IDE settings and view drive specific information, you'll need to use the "hdparm" command, which accepts many different command line options. You will need to refer to the man page for this command very often. **Some command options are very dangerous, so be careful, and observe all warnings.** While some uses of hdparm command can greatly improve IDE drive performance, the wrong option on the wrong system can cause filesystem correction, and could render your EnCase evidence files useless.

The default is to turn DMA on, which should be fine on most systems. If you have problems, you can turn DMA off (which decreases performance, but is failsafe for data transfers) by running the command

```
hdparm -d0 /dev/hdx
```

```
# Replace /dev/hdx with the device you want to turn DMA off for, such  
as /dev/hda
```

## **Acquiring Digital Evidence From Macintosh Systems**

With this CD-ROM you can use EnCase to acquire Macintosh drives.

You will first need to make sure the Macintosh is powered off. How you do this depends upon the individual situation, and is beyond the scope of this document.

You will then power on the Macintosh containing the drives you want to acquire, holding down the "T" key after the startup sound plays (if speakers are not attached, then hold down the "T" key almost immediately after hitting the power button. The startup sound plays almost immediately, even if you don't hear it).

This will put the Macintosh into "Disk Mode". If you have a monitor attached, you will see a firewire logo bouncing around the screen, running as a screensaver.

At this point you can attach the Macintosh to a PC (Desktop or Laptop) using a standard firewire cable.

Once the Macintosh is plugged into the PC's firewire port, boot the PC from the CD-ROM drive. Linux will detect all the disk drives in the Macintosh as Firewire/SCSI devices, including any CD-ROM/DVD drives that are in the Macintosh.

The steps from this point on are the same as a standard EnCase acquire under Linux.

## Example EnCase Acquire using Linux

Here is an example of the commands I would type to perform a simple single drive acquisition using EnCase for Linux.

In this example case, the suspect drive has been removed from the primary onboard IDE controller, and attached to the first IDE controller of a Promise IDE controller (Ultra133 TX2, in this case). The evidence drive has been attached to the second IDE controller of the promise card.

The system is powered on with the Knoppix CD-ROM in the drive. The system needs to be configured in the BIOS to boot from the CD-ROM Drive. If you do not boot from the CD-ROM and by accident boot the suspect drive, you will change system files and alter access times on the drive.

(This will be referenced in your notes if booting does occur from the suspect hard drive. You are not contaminating evidence nor will you want to say this to defense. It will be explained as system files may be initialized but documents of a probative nature remain unchanged. If the system is running when you enter, then you down the system and reboot into the suspect system, for the most part... big deal. I would not enter that into my notes. Only if the system)

Once Knoppix is booted and you are given a command prompt, the following commands are executed.

```
dmesg | grep -i hd
```

```
# Check the kernel bootup messages, make sure the IDE drives were detected correctly.
```

```
hdparm -r1 /dev/hde
```

```
# Set suspect drive to read-only mode via ATA settings
```

```
hdparm /dev/hde
```

```
# check DMA settings & read-only status for suspect drive. (DMA should be on by# default)
```

```
hdparm /dev/hdg
```

```
# check DMA settings & read-only status for evidence drive. (DMA should be on by  
# default, and in read-write mode)
```

```
hdparm -i /dev/hde
```

```
# Get drive model, serial number, and other information from the suspect drive.
```

```
mount /mnt/hdg1
```

```
# mount the evidence drive, so we can write the images.
```

```
cd /mnt/hdg1
```

```
# change into the root directory of the evidence drive, mounted at /mnt/hdg1
```

**ls -alp**

# List contents of the current working directory (should be /mnt/hdg1)

**df -k /mnt/hdg1**

# check the amount of free space of the hdg1 filesystem

**linen**

# Run EnCase Linux Binary to create disk image

Go through the EnCase menus to Acquire the suspect drive (hde). After selecting the drive to acquire, one of the following prompts will ask you where you want the evidence images placed. If you need to create a directory on the evidence drive, at this point you can press **ALT-F2**, to get a 2<sup>nd</sup> virtual console, and execute the command:

**mkdir /mnt/hdg1/suspect1**

Of course, replace "suspect1" with whatever you want the directory name to be for your image destination.

To go back to EnCase, press **ALT-F1**. Type in the path "/mnt/hdg1/suspect1/suspect1" as the destination. Fill in all requested information, and start the EnCase acquire.

When your done imaging drives on the system, first exit linen, verify that all the image files are on the evidence drive where you expect them to be, and finally use the "**halt**" command to shutdown the system and open the CD-ROM drive.

## Known Bugs & TODO List:

I added hdx=stroke settings to the default CD-ROM bootparams. I'm not sure if this is necessary, or if this is even has any effect with the kernel used in Knoppix. . On the systems I've tried, I get error messages on bootup, and it does not appear to do actually do anything. It is my understanding that the hdx=stroke bootparam will allow the Linux kernel to see any IDE host protected area (HPA). Since I have not yet tested the CD on a drive with a host protected area, I do not know if the bootparam settings work.

Support for Auto-Geometry Resizing (CONFIG\_IDEDISK\_STROKE) was removed in Linux Kernel v2.6.7

See the following links for more documentation on the issue:

<http://marc.theaimsgroup.com/?l=linux-kernel&m=108741756915769&w=2>

<http://www.ussg.iu.edu/hypermil/linux/kernel/0406.2/0195.html>

### TODO:

-Change the init bootup scripts so that all detected IDE hard drives are set to read-only mode using a 'hdparm -r1 /dev/hdx' command.

-Create a prepdisk script to get a blank/new/unformatted drive ready to be used as an evidence drive to hold images taken of a seized machines.

-Change the init bootup script, so that if it detects a properly prepared "evidence" drive, it will automatically set that drive as "read-write", using 'hdparm -r0 /dev/hdx'.

Feel free to e-mail me any further suggestions or comments for improvement.