How To Make A Forensic Copy Through The Network

Geert Van Acker

Preface

The most common ways to make forensic copy's are IDE to IDE, (and/or SATA), IDE to USB or FireWire. When it's difficult or impossible to take the hard drive out of the system, making a forensic copy through the network can be a possible solution.

Throughout this document we use the FCCU GNU/Linux Forensic Boot CD, which you can download from this site. Although this could also be accomplished using the Windows OS, it falls outside the scope of this guide.

Some conventions which are used in this document:

- Commands are always displayed in bold italic, preceded by the railway sign (#). This railway sign stands for the prompt and doesn't need to be typed.

- When we use the denomination "/dev/hdx" (for USB/FireWire you should change it to "/dev/sdx" or "/dev/ubx"), we point to the target hard drive. On this target we will place the exact copy.

- When "/dev/hdy" (for USB/FireWire "/dev/sdy" or "/dev/uby") is used, we speak about the hard drive that we want to copy.

Needs

- Two (2) FCCU GNU/Linux Forensic Boot Cd's.

- Target hard drive

- System on which we can connect our target hard drive (Intervention kit, portable with USB/FireWire, tower with IDE/SATA ...).

- Networkcable (preferably crossed linked, hub or switch).

Preparation Of The Target Hard Drive

If necessary we first wipe the hard drive (when you will store the image as a file, so not disk to disk, this step is not required).

```
# shred -z -n 0 -v /dev/hdx
```

Next, we make a partition with the fdisk command (1 primairy partition with the maximum capacity of the hard drive)

```
# fdisk /dev/hdx
```

After the partition has been created, it's adviced to restart the system in order to correctly load the partition table in the kernel.

```
# shutdown -r now
```

Now that we've created the partition, we should provide it with a filesystem:

```
# mkfs.ext3 /dev/hdx1
```

The last step is to mount the filesystem in our file structure:

```
# mount /dev/hdx1 /mnt/test
```

Network Connectivity

We'll use the TCP/IP suite in order to make the connection between the two systems. The physical link can be created with either a "crossed link" cable or with two "straight" ethernet cables connected to a hub or switch.

The two systems have to be configured in the same network address range. Use the ranges as pointed out by RFC 1918 (e.g. 192.168.0.0).

On the system where our target hard drive is mounted:

```
# ifconfig eth0 192.168.0.1
```

On the system of which we would like to make the hard drive copy:

```
# ifconfig eth0 192.168.0.2
```

Now you could test the connectivity with the "ping" command. On the system where our target hard drive is mounted:

```
# ping 192.168.0.2
```

On the system of which we would like to make the hard drive copy:

```
# ping 192.168.0.1
```

Exact Forensic Copy

To obtain a forensic image, we'll use "dd" and "netcat", both standard tools on most Unix and Linux flavors. If you don't trust the network, use cryptcat instead of netcat, the communication between the hosts will be encrypted.

First of all, we'll have to instruct netcat to listen to a port on the system that has the target hard drive.

Our command will open a port (port 2000) and listen to it (-l). It will also visualize all data it acquires (pipebench) and then write it to a file on the target hard drive.

```
# netcat -l -p 2000 -w 5 | pipebench > /mnt/test/image.dd
```

Next, we have to make the forensic copy of the hard drive and send it to the system on which netcat is listening.

```
# dd if=/dev/hdy conv=noerror,sync | pipebench | netcat 192.168.0.1 2000
```

Check whether the size of the copy is identical to the size of the original hard drive.

```
# ls -lh /mnt/test/image.dd
```

You could also compare the image file and the original hard drive with a hashing technique (sha1) to ensure that they are exactly the same.Now unmout the partition:

```
# umount /mnt/test
```

To shut the systems down:

```
# shutdown -h now
```