

November 14, 2005

VoomTech HardCopy II First Impressions

Summary

The VoomTech HardCopy II ("HC2") is positioned to be a self-contained imaging laboratory for the forensic computer examiner. In a package weighing less than 2 lbs., the HC2 provides a one-stop-shopping tool that will quickly become your acquisition system of choice.

No more computers to lug around! The HC2 does it all with three multifunction buttons and an LCD screen. It formats and prepares new drives. It clones and images drives. It allows you to hash drives or compute MD5 hash values during imaging and then verify your image file against the acquisition hash to confirm its integrity. It even allows you to wipe your drives when you're ready to sterilize them. And it is capable of handling any IDE/ATA, SATA, or memory device when cabled with the proper converters.

This device is an excellent example of intuitive and intelligent product design. It has become an essential part of my imaging tool kit. This little box replaces a hundred of pounds of equipment I no longer need unless there are SCSI disks or large RAID's to acquire. It provides nearly all of the imaging features that EnCase offers and the images it acquires are almost as easy to use with EnCase as native EnCase images. At best it images six times faster than what I was able to achieve with Firewire write-blockers and with slow or problematic drives it is about the same.

In short, the HC2 has become the device I turn to first for forensic imaging. Now I only use the rest of my equipment if the devices presented for imaging won't work with the HC2.

Background

One of the most difficult and expensive challenges facing the computer forensic examiner is assembling an effective field toolkit for imaging media. For most of us, this has consisted of one or more computers, several different write-blocking devices, expensive software, and a whole host of cables, adapters and power supplies. The resulting haystack of equipment is both difficult to cart around and laborious to assemble and disassemble.

VoomTech resolves most of these problems with their new HardCopy II imaging device. The HC2 is a small black box about the size of a large sandwich. It has IDE ribbon and power connectors for a source or suspect drive and a destination drive. There are also connectors for the system power supply and a serial port for terminal access and for upgrading the firmware.

Description

On top of the unit is a brilliant black-on-yellow two-line LCD display that is remarkably readable in any light. Three multifunction buttons give you access to the menus and functions of the unit. The whole kit with cables and adapters will fit in a large Fedex box and weights less than a couple of pounds.

The current version supports only IDE devices which means you can attach virtually any IDE/ATA drive and there are adapters available for notebook hard drives, serial ATA drives, and even memory devices.

About the only devices the HC2 won't handle are SCSI drives and there are rumors that this may be addressed soon.

Under the hood, the HC2 allows you to perform all of the crucial activities involved with forensic imaging. The device will allow you to prepare an unformatted destination drive and you can choose between FAT or NTFS file systems. Once the destination drive is prepared, you can perform a variety of functions with the suspect drive. You can clone the drive which creates a bitstream-duplicate of the suspect drive. You can image the suspect drive which creates a dd-style raw image file on the destination drive along with a header file describing the evidence collected (including acquisition & verification hash values). You can also create MD5 hashes of the suspect and destination drives which is useful for verifying clones. You can also format or wipe a destination drive directly from the menu buttons.

Use with EnCase

I use EnCase as my primary analytical tool and the HC2 interfaces beautifully with it. The process goes something like this: I attach the drives with the power and IDE ribbon cables and power the unit on. If necessary, I prepare the destination with the appropriate file system (NTFS should be used for images).

I usually run a system test next which scans both drives and confirms that they are available. This process takes about 30 seconds. Next I initiate the imaging procedure with MD5 hashing and instruct the HC2 to verify the acquisition once complete. This means that an MD5 hash is computed during acquisition and then written to the header file associated with the image. Immediately afterwards, the HC2 computes another MD5 hash from the image file on the destination drive and records that in the header record as well. If the two hash values don't match, you are notified on the LCD screen. This allows me to create an image and verify it while I'm on site without ever accessing a computer or another piece of equipment. The whole process is handled beautifully by the HC2.

Once the images have been collected, you can add them to an EnCase case for examination. EnCase will allow you to hash a raw image and the results from EnCase matched the hash values from the HC2 every time.

You can also instruct the HC2 to "chunk" the image files to make things easier to copy to CD-R or DVD-R discs.

Imaging Speed

The HC2 is optimized for speed. Under the best circumstances they boast speeds up to 5.5GB per minute! However, I have found that the ultimate speed depends a lot on the condition and type of hard drives and whether or not you enable MD5 hashing.

The first thing the HC2 does is allocate space on the destination drive. This is done by determining the size of the suspect drive and then pre-allocating the clusters in the file system of the destination drive. Using this approach, the imaging process is accelerated because the drive heads aren't thrashing around between data writes and resource allocation.

In my work, the MD5 hashing and verification procedure is essential. Because of this extra computational overhead, the HC2's performance is automatically halved. The fastest speeds I noted were around 2.8GB per minute with hashing enabled. VoomTech states that the HC2 will image at 2.9GB per minute with hashing enabled, but I was unable to get results that fast with the drives available to me at the time of testing. The imaging speed can be further impacted by the type of drive, the amount of cache, the UDMA mode, and the condition of the media. I ran several "torture tests" using drives that were 5-10 years old and while the performance was much less than optimal, all images were completed. My actual imaging rates were between 2.5 GB per minute and 400 KB per minute.

If you are only interested in cloning or imaging without verification, you can expect exceptionally fast speeds. The best I was able to achieve with the drives I had to test with was about 3.4GB per minute.

Error Recovery

Since it's impossible to anticipate the condition of the media one encounters in the field, it's important that the imaging tools used are robust enough to be able to handle fragile or error-prone media. The HC2 recovers nicely from errors reading sectors from the suspect drive. If MD5 hashing is enabled and the error is recoverable, the hashing continues. However if the read error is unrecoverable, HC2 moves on and aborts the MD5 hash. VoomTech is currently considering padding the missing sector(s) with a specified value and continuing to hash with these replacement values inserted into the stream. Regardless of the effect on the production of a hash value, the HC2 did quite well with an 80GB hard drive with dozens of bad sectors. Optimally this drive would have imaged at 2.5 GB per minute and would have completed in about 30 minutes. Even with all of the errors and recoveries the drive imaged in under six hours which is quite acceptable given its condition.

Wiping

The wiping command operates at top speed given the drive attached (you can only wipe a destination drive). My Western Digital 250 GB test drive was wiped in just a little over an hour at the rate of about 3.5 GB per minute. The algorithm overwrites each sector with a zero and the results were verified independently and shown to be as intended.

Conclusion

The VoomTech HardCopy II provides everything I need for imaging ATA/IDE media. It allows me to format my destination drives, image or clone my suspect drives, verify my images before I leave the scene, and document everything for my records. It's faster than anything else I've used and robust enough to recover from seriously compromised hardware. This two-pound product eliminates about a hundred pounds of gear that I used to lug around with me. As a result, the HC2 has become my primary imaging tool for IDE/ATA media. Highly recommended!