

Shadow Independent Evaluation

VOOM vs The Virus (CIH)

By Seth Fogie, Feb 24, 2004

It is not often that I come across a hardware device that makes me stop in awe of its potential. Sure, there are lot of neat toys and stuff out there such as the PDA, HUD glasses, nanobots, and more, but these are things we have been seeing in scifi shows and movies for decades. But for all the cleverness of mankind, we sometimes miss things...and one of these items is the VOOM ShadowDrive.

I should start by saying that one of the editors here at InformIT.com was keeping an eye out for cool ideas at Comdex 2003 for us (and I am sure others as well). When she returned, it was with news of the VOOM ShadowDrive, which struck her as curiously unique. Since this is sold as a forensics tool, I contacted the company and asked for one to play with as part of the work I am doing for the forensics section of the Security Reference Guide. Once I unpacked the device and set it up, I realized that this device was much more than just a simple forensics tool.

If you aren't familiar with VMWare, you need to download a demo and try it out. For security research types, VMWare is a great PC and Linux based tool that allows you to run entire computers operating systems inside an emulator shell. In addition to allowing you access to programs that run only on a certain OS, it also provides a nice sandbox environment for installing Trojans and viruses. Once the emulated system is infected or dies, you can delete the VMWare file or use a snapshot feature to quickly restore it...but there is one problem, VMWare is software based, and doesn't work for every program and can be rather slow. In addition, VMWare has no real value as a forensics tool because it uses proprietary data formats, which do not allow room for evidence images.

That said, let me introduce you to the ShadowDrive.

The ShadowDrive is "...a patented computer hardware device that is designed to aid the investigation of a computer's hard drive. It provides investigators with read write access from the host computer's perspective, while maintaining the original hard drive unchanged." From this description, you can see issues that affect software based solutions do not apply to the ShadowDrive. This is a true hardware solution that only protects the main hard drive, without impacting the rest of the computer's resources (e.g. graphics card).

Since I am the curious type, you can probably guess what I did. After setting it up, I installed programs, deleted files, etc. As advertised, the ShadowDrive worked like a charm. With three quick presses of a button (three presses are required to prevent accidental reset), the device reset and my main drive was returned to its original state. In other words, my evidence would have been protected. This means I can use the actual evidence collected from a criminal's computer during the trial without worrying about corrupting the drive and destroying the evidence.

Before going any further, the ShadowDrive is a proprietary device with a hard drive of its own inside (I opened the box and took a peek). The drive acts as an invisible buffer to which all 'writes' are recorded. At no time is the main drive to be altered, which is necessary if the evidence is to be maintained. This is not a write blocker, per se, because all writes are redirected to the ShadowDrive thus ensuring the operating programs remain running as normal. The only negative that I can come up with about this device is that it is IDE (ATAPI 4,5,6) only. [[SATA adapters accommodate this issue.](#)]

While all my testing was great for VOOM, I was slightly bored by the prospect of having something that worked as planned inside this forensics-defined environment. So, I started to think about more

extreme testing procedures that might not have been considered. I figured (without reading this pdf [voom_pdf/ShadowDriveNoOptions.pdf](#)) that the device only blocked drive writes at an upper level, which leaves out fdisk or other partitioning type tools. So, I fdisked and formatted my main disk and discovered that after the reset everything was returned to its original. At this point, I did about all you can possibly do to a drive and still expect it to work. I doubt the ShadowDrive could redirect a direct blow from a hammer!

After thinking about the damage I could cause to my 'protected' system, I recalled a nasty virus that went around a few years ago called 'The Chernobyl Virus', or CIH. I started searching the Internet, with a very locked down browser (not IE) and after a few minutes, and more than one false lead, I found a package with three main version of the virus. I emailed VOOM and told them about my plans because the CIH virus could overwrite the flash ROM on the motherboard. My test PC is old and can be tossed if it dies, but I didn't want to trash their device. They gave me the green light, so I downloaded CIH to the target PC and infected myself. Since CIH is a date control virus, I changed the date on my PC and executed the CIH infected program. My PC froze and when I rebooted it, it was thoroughly hosed. However, and as promised, once I reset the ShadowDrive, everything returned back to normal.

So, to sum this up, VOOM offers what I believe is the first hardware based write redirecting device that is not only mobile [and small], but is also very successful at protecting the main drive. This is the type of tool that could easily reduce the downtime and reset time of any security and/or virus researcher. Of course, VOOM also sells products that can help reduce the problems associated with patch and update testing. If something fails when you install a patch to your main system, simply reset the device and all the damage is instantly repaired. Finally, at \$1295 the ShadowDrive is a pretty good deal [[the Shadow II, is \\$1869](#)]. Even VMWare costs \$299, and it has no real value as a forensics tool. In addition, software based emulators are often limited in their functionality (e.g. games). Check out www.voomtech.com for more details.

SHADOW TESTIMONIAL

As a Computer Forensic Examiner and Investigator, I use the Shadow at every opportunity; there is really nothing else with which to compare it. I can boot and run any operating system. I can conduct a thorough investigation of the suspect computer very quickly. I can demonstrate live to my clients exactly what was viewed on the suspect computer in a fashion comprehensible by laypersons.

The ability to boot and run any computer with any operating system is *not* possible with any other forensic procedure or device of which I am aware to date, in this highly specialized field of computer forensic investigations. With the Shadow, it doesn't matter if it's MacIntosh, Linux, Unix, or MicroSoft from DOS to Vista, the Shadow let's you see and operate the native system. I can think back to when I was a Customs Agent and recall many instances in which, while executing a warrant, I would have benefited from utilizing the Shadow. I would have been able to boot the suspect's computer and review its contents immediately. I would have known, without delay, what was password protected and could have even quickly uploaded a password cracking tool that would have allowed me full access to all data without ever impinging on the forensic integrity of the that computer. I would *never* have had to wait to confront a suspect regarding the contents of the computer. I only wish the Shadow had been available at that time.

Without going into too much technical detail, every computer I have seen that's been used is unique. For instance, the user invokes different settings, and every upgrade to the software and operating system patch can, and most likely does, alter the system. Those alterations may result in any computer's data being stored in a different way from that of any other computer. The Shadow offers the best way to validate my findings. After booting/running the suspect computer with the Shadow and making what ever changes I require, I can then use the Shadow's 'zero function' to remove those changes. I can go back in time with restore points and see how past events unfolded, then zero the changes again and restore to a different time. This capability is vital to my investigative technique. (None of these 'changes,' however, actually write to the suspect computer – the computer has always remained in a forensically sound condition (i.e., unaltered). *What a competent examiner can do in a day with the Shadow, would surely take weeks or months using alternative forensic procedures.*

I have also found that the Shadow is *the* most effective way to review evidence with clients. As a computer forensics expert, I can show my clients exactly what the user viewed without forensic compromise. My clients don't have to be experts; they understand how to operate a computer and it is, thus, very simple when using the Shadow, to explain to them what occurred behind the scenes. This is because the Shadow enables me to present the information using familiar operating system screens directly on the suspect computer.

While you may not be able to conduct the minutia of a lab executed computer forensic examination, that which you *can* accomplish using the Shadow can't be done any other way. Using the Shadow has and continues to save me huge amounts of time and effort; in my line of work, I wouldn't be without it.

Will Docken, Computer Forensics Examiner
Will Docken Investigations

www.willdocken.com