

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