

VOOM Shadow 2 Details

The Shadow is not a virtual viewing tool; neither is it a write-block device, *per se*. It is a **field forensic investigation/analysis/presentation device**. Necessarily though, it does, without compromise, intercept and block writes to the suspect computer's hard disk drive (i.e. **write-block hardware is built-in**).

BREAK CONVENTION

The Shadow vs. Virtual Viewing Software

- Virtual viewing software has limited value: Extensive time is required so that the data on the suspect computer can be imaged and transferred in an effort to attempt simulated operation of the suspect computer.
- With the Shadow there is no transferring from one environment to another, thus there are no incompatibility issues. It simply intercepts and stores writes, allowing the investigator to *boot and run the suspect computer indefinitely without altering anything*.
- **With the Shadow, the time and effort required to enable operation of the suspect PC is brief (minutes) and effective (no software or hardware conflicts).**

*A computer forensic detective with a local police department stated there was a murder that occurred inside a local business. The crime was caught on security cameras located within the business, however, these images were digital and stored on a computer. Before the detective could even begin to view anything, he had to image the drive in order to preserve the integrity of the computer forensic evidence. The process took seven hours. The suspect then had more than a seven hour lead on the investigating detectives. Fortunately, the suspect was eventually caught, although it was weeks later, in another state, several hundred miles from the crime. **The detective lamented that the delay in viewing this critical information would have been avoided and the suspect may have been apprehended much sooner, perhaps before he fled the state, if the detective had access to the Shadow.***

The Shadow vs. Write-Blockers

- Simple hardware write-blockers have limited value: One can read the raw data safely, but one *cannot operate* the suspect PC using a write-blocker.
- **With the Shadow, the investigator or expert witness is at liberty to run the suspect PC indefinitely. With the Shadow in use, the suspect computer remains intact, unaltered and pristine at all times.**

BREAK THE SPEED BARRIER

The Shadow vs. Software Virtual Viewing Tools

- Again, the investigator can hook up the Shadow and begin viewing and operating the suspect computer right away (no imaging and transfer time).
- **With the Shadow, the suspect's computer runs at speed without change. This is superior to software virtual viewing tools that drastically reduce the speed at which the suspect PC image can be operated, if it can be operated at all.** Think about the murder related by the detective mentioned above. Suppose it was a child abduction. *Speed is essential.*
- **The Shadow facilitates a quick closure to many investigations with its *comprehensible and irrefutable evidence.***

BREAK DOWN THE SUSPECT

The Shadow vs. Forensic Lab Backlogs

- Forensic lab backlogs allow the suspect to develop complex defense strategies, while the emotional/psychological threat of conviction eases with time.
- With the Shadow, the evidence can be immediately and easily displayed to the suspect and legal advisor, using the suspect's own computer and software and is, thus, virtually impossible to deny. **If the evidence is there, with the Shadow it can be quickly seen by all, and the suspect is thereby positioned in a legal quagmire with NO WAY OUT.**

Will Docken, a computer forensics examiner and former U.S. Customs Special Agent has consistently reported that, from 2002 to the present, the vast majority of cases in which he has used the Shadow, the suspect has pled out.

BREAK APART LEGAL TACTICS

The Shadow vs. Forensic Lab Reports

- Forensic lab reports are typically presented as evidence in court to individuals without knowledge or experience in computer forensics. Targeting this lack of knowledge, the defense tactic can attempt to obfuscate the evidence due to the unfamiliar and difficult to understand nature of forensic lab analyses.
- **The Shadow permits *the dynamic and live demonstration of a suspect's PC operation directly in its native and intuitively understood form to laypersons.***
- **The impact of seeing the actual evidence on the suspect's own computer is *unparalleled in the courtroom.***

*The Shadow was used to present essential evidence in the recent high-profile Mark Jensen murder trial in Walworth County, Wisconsin, as seen on Court TV (TruTV) and 20/20 during January and February 2008. Mr. Jensen was convicted of first degree murder of his wife and was sentenced to life in prison without parole. **The jury specifically stated that the computer evidence presented in court (using the Shadow) was one of three critical pieces of evidence that led to their decision.***