EVIDENCE TECHNOLOGY MAGAZINE

The magazine dedicated exclusively to the technology of evidence collection, processing, and preservation
Volume 12, Number 4 • July-August 2014

Mobile Forensics in Court

ONLY IN THE DIGITAL EDITION

- Forensic Tips
- Accessing a Suspect's Computer in its Natural State

TOPICS IN THIS ISSUE

- Advanced Video Forensics
- Processing Car Door Handles for Prints
- Complex DNA Mixtures
- Using Correct Terminology

Accessing a Suspect's Computer in its Natural State without Compromising Evidence

Written by
David Biessener

With this approach, no changes from boot up through operation ever reach the hard drive. Because it is repeatable, evidence produced using the device has already been proven in court to be valid and admissible.

TO ACCESS A SUSPECT'S COMPUTER, traditional procedure involves removing the hard drive, creating a forensic image (a duplicate copy), and then analyzing that copy using sophisticated industry-specific software.

Although effective, this process takes many hours and allows investigators to view and present information only in a raw state—one that non-computer experts such as attorneys and juries can find difficult to understand.

As a result, computer forensic investigators are increasingly adopting a complementary tool that allows them to turn on and operate the suspect's computer without altering its contents in any way.

By doing so, investigators are able to review and navigate the computer as if the suspect turned it on and then stepped aside. This includes utilizing whatever operating system is installed, launching programs, opening files, viewing recent e-mails or images, or web history. Literally anything the computer's owner can see or do can be accessed without risk of altering the evidence.

This ability to view the computer in its natural state is speeding investigations and increasing the likelihood that the case will be resolved prior to trial.

Accessing, without Altering

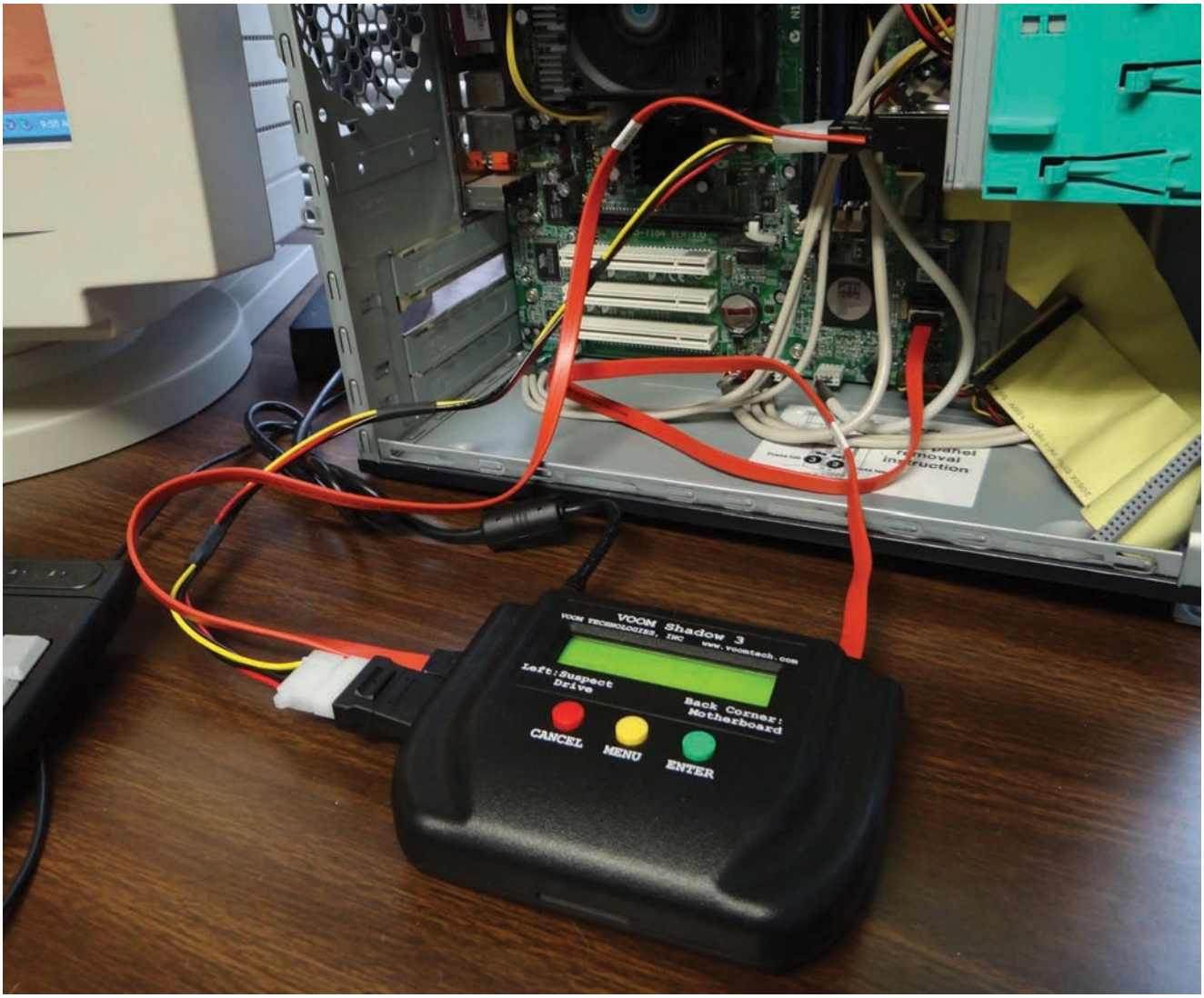
When a computer is turned on, thousands of changes are automatically made in the background. The operating system runs updates, anti-virus scans are conducted, bit logs are changed, Internet files purged—all of which can potentially overwrite or alter evidence.

To protect against this, digital forensic experts avoid turning on the computer. Instead, they remove the hard drive and make several copies before returning the original to the computer and storing it as evidence.

Next, they utilize existing forensic software tools on the market, such as EnCase, Forensic Imager, PTK Forensics, NetAnalysis Forensic Toolkit, and FTK, to index and categorize the contents of the drive copies.

Depending on the size of the hard drive, the process of copying and indexing can take 10-12 hours. Once completed, the information is available only in a raw data format with file, folder, metadata, time-stamp information, and the like. The information, though extremely detailed, can be like a second language.

One solution to this problem is to utilize a computer forensics investigation and presentation device with a built-in write-blocker. The Shadow 3 from Voom Technologies, for example, is a small, portable hardware device that is inserted between the hard drive and the motherboard. Once it is properly connected, the computer can be safely turned on. All "write" commands (changes intended for the hard drive)



are stored within the device, never making it to the hard drive. "Read-only" commands that access, but do not change information, are still allowed.

During the course of the investigation, any saved "write" commands stored in the device are still available to the processor as if they reside on the hard drive.

With this approach, no changes from boot up through operation ever reach the hard drive. Because it is repeatable, evidence produced using the device has already been proven in court to be valid and admissible.

"Prior to using the Shadow 3, I didn't have a reliable method of looking at a suspect's computer the same way the suspect would be using it," said Craig Cilley, a computer forensics expert for the Washington County (Minn.) Sheriff's Office since 2006.

Cilley is responsible for cyber crime and ICAC (Internet Crimes Against Children) cases. On occasion, the agency also assists the probation department, the county attorney's office, internal affairs, and social services with computer related issues.

He initially heard about the digital forensics tool two years ago, which

was in use at several other agencies in Minnesota.

For Cilley, this type of approach represents a "scalpel forensics" mode that saves time because he can access data without having to review every bit of information on the computer. The information in the form of screenshots, printed e-mails, etc. can be retrieved quickly enough to be shown to suspects during questioning, to secure arrest warrants, or to rule out a suspect.

Cilley still conducts "full forensics" as needed using forensic software, because it can show things behind the scenes that the user cannot see.

"I'm trying to get to a model where I don't have to do full forensics unless it's necessary," said Cilley

Pesky encryption, user log-in, and security dongle obstacles can also be resolved more quickly. If files are encrypted by Windows or third party software, often decryption occurs automatically upon successful login. If a security dongle exists, it need only be left in the USB port as normal.

If the user's login information is not available, investigators must spend valuable time trying to figure out or socially engineer it. However, there are free tools available that can be installed during the boot up process designed to eliminate the password.

Perhaps the most important value in the system is the creation of more powerful and easier-to-comprehend presentations for attorneys, investigators, judges, and juries.

Perhaps the most important value in the system is the creation of more powerful and easier-to-comprehend presentations for attorneys, investigators, judges, and juries.

The most powerful evidence, to be sure, is the easiest for the layperson to understand. Those that are not computer experts, but use computers on a regular basis, are most comfortable viewing the information in its native environment – an Excel spreadsheet open in Microsoft Excel, for example.

With the raw data produced by forensic software, computer experts are often tasked with explaining to juries how the data was collected, why it is accurate, and what it means.

Using the device, a live presentation using the suspect's computer can be conducted in court, or screen shots and video can be shown on a projector exactly as it appears on the suspect's computer.

As a standard operating procedure, Cilley installs a screen video capture utility to make a "movie" as he goes through the contents of a suspect's machine. The movie is then turned over to the prosecutor as part of his report.

"If I can show the prosecutor the movie and then they, in turn, show the defense attorney, it makes the case go through the judicial system much faster because everyone can see what the suspect was doing and they are more likely to plead the case and not go trial," says Cilley. "It's a great visual aid."

About the Author

David Biessener is the CEO of Voom Technologies, a Lakeland, Minnesota-based manufacturer of specialized digital forensics hardware. Originally introduced in 2004, the Shadow 3 is currently deployed worldwide in over 100 local, state, and federal law enforcement and justice agencies.

davidwb@voomtech.com