NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Summer 2005 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Information Hide and Seek

MP3 players now replace stacks of music CDs, which not so long ago replaced even bigger stacks of vinyl records. Digital cameras now produce photos instantly, eliminating the need for film and a photo shop dropoff and pickup. Personal gaming systems are putting a dent in video arcade profits. Digital video recorders make television programs available any time of the day or night. Faster, smaller, and cheaper—everybody can benefit from these advances in technology. Everybody, including criminals.

"The long and the short of it is, 5 to 10 years ago, we did not have to worry about this type of electronic crime. Technology was big and expensive, laptops weighed 20 pounds, cost upward of $4,000, and were highly visible," says Joshua Bartolomie, an electronic crime specialist at the CyberScience Laboratory, which is affiliated with the National Law Enforcement and Corrections Technology Center–Northeast, a program of the National Institute of Justice in Rome, New York.

"Now, you can buy an enormous amount of technology at your local shopping mall," Bartolomie says. "Because of this, we are taking for granted a lot of these devices that could contain electronic evidence. For example, take a Microsoft® Xbox® or other gaming system: For as little as $30, you can modify it to use Linux®. At this point you could make it into a fully functioning file server, e-mail server, and/or peer-to-peer server and utilize it to store any type of illicit material. Most law enforcement officers won't even think to look at a gaming system when they're performing a search. They take the computer and the visible peripherals. Oftentimes they might not know to look for the gaming system or MP3 player, or any of the other dozens of devices that are available on the market today that could be utilized to store computer data."

Bartolomie says that other places criminals might hide data include—

- Digital cameras.
- DVD players that have internal hard drives.
- TiVo® systems.
- Any number of other new home entertainment systems that are on the market today.
- New computer peripherals that have multiple functionality.

"Plus, there's the added complication of emerging wireless technology," Bartolomie says. "You can purchase and hide a wireless hard drive virtually anywhere—in your garage, above ceiling tiles, even in the unfinished part of your basement. There's no direct connection to your computer to lead law enforcement to it. There are a multitude of books and websites with full instructions and tips on how to modify these items. Most people do it just for the fun of it, but they can always be exploited by those with criminal intent."

The key for law enforcement officers, he emphasizes, is awareness. "There's no solution to this problem other than old-fashioned police work." Things to be aware of when doing that old-fashioned police work, he says, include—

- If a suspect has many technology devices, such as gaming systems and MP3 players, check them thoroughly. Be on the lookout for duplicate items or other technology "toys." The overabundance of technological gadgets is an indicator that things might not be all they seem.
- If a suspect is running a Linux-based operating system, it may be an indication that he or she has computer knowledge above and beyond the average person.
- Be sure to take peripherals as well as the computer "box" as evidence. A plethora of devices are available today that look like standard peripherals, but they do much more. For example, a mouse currently on the market has the capability to act as a compact flash and secure digital card reader/writer. With this device, if an investigator does not seize the mouse, up to 6 gigabytes of potential electronic evidence could be lost.

- Common items such as pens, watches, cassette tapes, and even a Swiss army knife may hold memory cards or large amounts of built-in storage potential.

Through the CyberScience Laboratory, Bartolomie offers a presentation called "Technology Exploitation: Hide & Seek," which has been given at numerous conferences and workshops. This presentation highlights some of the potential electronic evidence that first responders might, and have, encountered. These are the electronic devices that they should be aware of in addition to the usual items, such as computers, laptops, and personal digital assistants. For more information, contact Joshua Bartolomie at 888–338–0584 or Josh@cybersciencelab.com.

This article was reprinted from the Summer 2005 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.