Locard's Principle

Anyone entering a crime scene leaves something behind or takes something away.

By Craig Ball

Devoted viewers of the TV show "CSI" know about Locard's Exchange Principle: the theory that anyone entering a crime scene leaves something behind or takes something away.

It's called cross-transference, and though it brings to mind fingerprints, fibers and DNA, it applies to electronic evidence, too.

The personal computer is Grand Central Station for PDAs, thumb drives, MP3 players, CDs, floppies, printers, scanners and a bevy of other gadgets. Few systems exist in isolation from networks and the internet. When these connections are used for monkey business, such as stealing proprietary data, the electronic evidence left behind or carried away can tell a compelling story.

Recently, a colleague who owned a very successful business called me to complain about an employee who'd quit to start a competing firm. My colleague worried that when the employee walked out the door, years of collected forms, research and other proprietary data might have exited as well.

Of course, the departing employee swore he'd taken nothing, but the unconvinced boss needed reassurance that someone he had trusted hadn't betrayed him. He asked me to examine Mr. Not Me's laptop.

Stolen data has to be accessed, copied and then find its way out of the machine.

A SMART MOVE

Turning to a forensic specialist was a smart move. Had the boss yielded to temptation and poked around the laptop, Locard's Principle dictates that he would have irretrievably contaminated the digital crime scene. Last access dates would change. Log entries would be overwritten. Some deleted data might disappear forever.

More to the point, an unskilled examiner would have overlooked the wealth of cross-transference evidence painting a vivid picture of theft and duplicity.

Stolen data has to be accessed, copied and then find its way out of the machine. Whether it's sent to a printer, e-mailed, burned to optical disk, written to a floppy or spirited away on a thumb drive, each conduit carries data away and leaves data behind as evidence of the transaction.

Forensic analysis of the employee's laptop turned up many examples of Locard's Principle at work. Windows employs a complex database called the Registry to track preferences and activities of the operating system and installed applications. When a USB storage device like a thumb drive connects, however briefly, to a Windows computer, the operating system interrogates the attachment and dutifully records information about the device and the date in the Registry.

A moment-by-moment analysis of every file accessed shortly before the employee's departure and of the Registry revealed attachment of a thumb drive — an event reinforced by the system accessing the sound file played when a device attaches to a USB port. "Bonk-bink."

This immediately preceded access to many proprietary files on the network, concluding with the system accessing the sound file signaling removal of the USB device. "Bink-bonk."

Further examination showed access to other proprietary data in conjunction with use of the system driver that writes data to recordable CDs. This evidence, along with an error log file created by a CD burning application detailing the date and time of difficulty encountered trying to burn particular proprietary files to CD-R, left no doubt as to what had transpired.

COUP DE GRACE

The coup de grace demonstrating the premeditated nature of the theft emerged from a review of files used to synchronize the laptop with a smartphone PDA. These held records of cell phone text messaging between the employee and a confederate in the firm discussing what files needed to be spirited away.

Though the messages weren't created on or sent via the laptop, they transferred to the laptop's hard drive unbeknownst to the employee when he synched his PDA. Armed with this evidence, the boss confronted the still-employed confederate, who tearfully confessed all to the sadder-but-wiser employer. Case closed, but no happy ending.

STORIES TO TELL

Computers, like crime scenes, have stories to tell. Data and metadata in their registries, logs, link files and abandoned storage serve as Greek chorus to the tragedy or comedy of the user's electronic life. Most cases don't require the "CSI" treatment, but when the computer takes center stage, don't overlook the potential for computer forensic analysis — and Dr. Locard's Exchange Principle — to wring decisive evidence from the machine. LTN

***Craig Ball**, a member of the LTN edtiorial advisory board, is a litigator and computer forensics/EDD special master, based in Montgomery, Texas. E-mail: craigball@gmail.com.*