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

From Winter 2009 *TechBeat*

TECH b•e•a•t

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

Digital Evidence: Its True Value

In 2005, digital evidence from a floppy disk led investigators to the BTK serial killer, a criminal who had eluded police capture since 1974 and claimed at least 10 victims. Digital evidence from a mobile phone led international police to the terrorists responsible for the Madrid train bombings, which resulted in the deaths of at least 190 people in 2004. Digital evidence collected from computer networks at universities and military sites in the 1980s led to the discovery of international espionage supported by a foreign government hostile to the United States.

In today's world, law enforcement officers attempting to extract digital evidence face growing challenges from more types of devices with greater data storage capacity. Digital media that could be seized in relation to an offense include computers, laptops, flash drives, external storage devices, digital cameras, game units and cellular phones. Investigators, prosecutors and forensic examiners must deal with vastly more data than they did just a few years ago.

Data contained on these digital devices can assist law enforcement in a criminal investigation or prosecution of crime in a variety of ways, described below:

- Digital evidence may be found on a computer or other electronic device directly related to the offense committed. For example, law enforcement officers may be investigating a child molestation complaint. When they analyze a suspect's computer, they find multiple pictures that appear to show the suspect molesting a number of children. In another example, a small flash card from a digital camera found in the possession of a suspected car thief may contain images of stolen cars.
- Digital evidence can be used to show intent existed to commit a crime (in legal terms, mens rea) or premeditation of an act. Many digital devices efficiently track user activity; it is also possible to recover deleted files, both of which may affect a criminal investigation. Physical evidence may already point to a suspect's guilt, and digital evidence can indicate that the crime was planned in advance. For example, a man suspected of killing his wife because he had discovered she was having an affair claimed that he killed her accidentally during an argument that became violent. When a computer forensic examiner analyzed his laptop, however, she found deleted Internet history files showing searches for "perfect murder," "getting away with murder," and "quick ways to kill someone" that occurred weeks and days prior to the crime. Based on this evidence of premeditation, the defendant could be charged with murder instead of manslaughter.
- Another possible use for digital evidence is in supporting or refuting witness, victim, or suspect statements in cases of questionable credibility. For example, a suspect in a homicide case denied knowledge about the firearm used to commit the crime. An examination of his cellular phone, however, showed deleted images that implicated the suspect.
- Another useful application is to expand an investigation by revealing new crimes or suspects. For example, an identity theft investigation revealed that the suspect was part of a network that was sharing, selling and buying identity data. This resulted in an expansion of the investigation to other jurisdictions and led to additional arrests.
- An often overlooked use of digital evidence is data mining. By exporting information from multiple digital devices (such as call logs from multiple cellular phones or e-mails from computers) and importing that data into an analytical software package, investigators can diagram and visualize a criminal enterprise or a timeline of events. This graphical representation can make it easier for investigators to understand the complex relationships in a criminal enterprise or for a jury to understand criminal activity in a courtroom presentation, and could reveal possible connections between offenders.

In order to capitalize on the potential value of digital evidence, law enforcement agencies might want to develop resources for processing digital evidence, either independently or in conjunction with other agencies, under a task force model to share resources. In cases where an agency cannot support independent digital evidence recovery, federal, state and regional laboratories may be able to help.

Related reading:

- *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (http://www.ojp.usdoj.gov/nij/pubs-sum/211314.htm)
- *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm)
- *Investigations Involving the Internet and Computer Networks* (http://www.ojp.usdoj.gov/nij/pubs-sum/210798.htm)

This article was reprinted from the Winter 2009 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 #2005–MU–CX–K077, awarded by the U.S. Department of Justice.