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

From Season 2005 *TechBeat*

TECH b•e•a•t

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

Technology Primer: Data . . . About Your Data

In the end it was a purple-colored computer disk mailed to a television station that cracked the case of BTK, the self-designated nickname used by Wichita, Kansas, serial killer Dennis Rader. Using technology to read "hidden" information contained on the disk, police were able to trace it back to a computer at a local church where Rader served as president of the council. The information that led police to Rader is called "metadata." And simply put, it's data . . . about data.

In the cyberworld of home or office computers, metadata is information stored below the surface of documents, spreadsheets, and presentations created online through such office productivity suites as Microsoft® Office. Because this hidden data resides out of the visible interface, few users are aware that it is there. Metadata can contain personal information about the author of a file and the computer or network from which it was stored, saved, or printed. It can catalog e-mail addresses, the last 10 people who viewed the file, and/or past versions of the document. According to Salvatore Paladino from the National Institute of Justice's CyberScience Laboratory in Rome, New York, the release of such metadata can be a starting point for hackers or divulge sensitive information to those who should not have it. The improper release of metadata has caused embarrassment, resulted in the loss of intellectual property, influenced the outcome of legal proceedings, and even endangered lives.

When controlled properly, however, corporate security professionals and computer forensic investigators can use metadata to investigate, for example, an employee who is suspected of accessing a document without proper authorization, to establish a link between two suspects, or to uncover a valuable piece of the investigative puzzle.

An awareness of metadata will not only protect an organization, but also provide investigators with the ability to reveal hidden data lurking in electronic evidence. This makes it imperative that investigators be able to locate, identify, uncover, and remove metadata as needed.

To obtain a technical report that describes metadata in greater detail, go to www.cybersciencelab.com. (Registration on the Private Site is required to complete the download.) For more information about metadata training resources, contact Salvatore Paladino, 888–338–0584 or salvatore.paladino@rl.af.mil.

This article was reprinted from the Fall 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 #2005–MU–CX–K077, 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.