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

TECH b•e•a•t

From Fall 2009 *TechBeat*

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

Tool Helps Automate, Expedite CyberCrime Probes

Computer hard drives collected by law enforcement officers in various searches of suspects' homes offer a "virtual treasure trove" of evidence in the hands of a trained forensic investigator. Manually searching each of them for evidence of peer-to-peer (P2P) network sharing of child pornography will take many hours, perhaps days, while the investigator's backlog continues to grow. However, the investigator recently learned about P2P Marshal™, a tool funded by the Office of Justice Programs' National Institute of Justice (NIJ) available via a free download. A few mouse clicks later, the investigator is ready to install and run a program that will take only minutes to reveal the same information.

Individuals engaged in a variety of cybercrime, most notably sharing of child pornography, widely use P2P file sharing, a function best known to the general public through services similar to Napster®. Other cybercrimes that may use P2P networks include theft of copyrighted music and theft of classified government information.

Developed by ATC-NY, a subsidiary of Architecture Technology Corporation, P2P Marshal™ automatically detects use of P2P client programs, extracts configuration and log information, and lists both uploaded and downloaded shared files. It has extensive search capabilities, produces reports in several formats and runs on Microsoft® Windows®-based operating systems. P2P Marshal also provides a detailed log file of all activities it performs.

"There's a difference between just having contraband images and disseminating them, which is obviously a more serious crime," says Frank Adelstein, technical director with ATC-NY. "An investigator needs a sense of how the suspect used the P2P tools, whether he was specifically searching for child pornography or whether he downloaded a big block of pictures and didn't know they were included.

"In order to prove intent, an investigator really needs to understand how these programs work, and every P2P program out there works a little bit differently. An investigator might have to spend a lot of time researching programs before he or she can even begin to look for information. P2P Marshal automates all of this as much as possible."

Using the tool not only saves time and thus helps eliminate backlogs, it might even help an investigator prove links between individuals and help departments expand investigations. Adelstein says that Derek Bronner, an ATC-NY employee with a law enforcement forensics background, identified a need for assistance with these issues, leading to the decision to respond to a 2006 NIJ solicitation. ATC-NY also partnered with several law enforcement agencies during the development process, obtaining their feedback and offering them the opportunity to help with beta testing.

According to Julie Baker, general manager, ATC-NY has since received numerous e-mails from officers and agencies thanking the company for developing the tool and saving investigators tremendous amounts of time. Early in 2009, P2P Marshal surpassed the 1,000-mark for registered users, while Version 1.0 of the tool was still available. Version 2.0, released in summer 2009, can be run from a USB drive and taken out into the field, whereas Version 1.0 had to be installed on a computer at a facility and run from there. This increased capability makes Version 2.0 available to field investigators and to probation and parole officers checking on compliance.

"The tool is straightforward to use, but it's important to understand what [constitutes] useful evidence and what conclusions can be drawn and what questions can be answered," Adelstein says. "There are a bunch of P2P networks out there that have very different properties and it's useful to have an understanding of how they work. As an example, someone might want to find the source of a file, and it could be that 100 different people contributed to it, so in that case, the question is meaningless."

"The tool is very easy to use. It walks an investigator through the process," says Judson Powers, a lead developer and trainer. "For those who are just getting into peer-to-peer forensics and need to get up to speed on some of the details, we offer a one-day, hands-on training class."

The class, which costs $495, offers not only training on the use of P2P Marshal, but also training on computer forensics related to P2P use in general.

The class covers an overview of the architecture of P2P file-sharing systems and their legitimate and illegitimate uses, forensic details commonly seen in criminal investigations, forensic analysis of client evidence and its potential pitfalls, hands-on exercises using manual analysis, and detailed instruction and hands-on exercises using P2P Marshal. At the end of the course, participants receive certification.

Powers says that ATC-NY has received comments about how easy the tool is to use from users who did not take the class, and he sees the major benefit of the class as providing understanding about P2P networks in general rather than specific information on using P2P Marshal.

"The class is really most useful for someone who isn't doing this kind of computer forensics already," Powers says.

Accessibility is not limited to law enforcement agencies because the tool could have civil applications, but users must provide contact information in order to register. This in turn allows ATC-NY to provide users with upgrades and patches as they become available.

To obtain Version 2.0 of P2P Marshal, visit www.P2PMarshal.com. To find out about upcoming training, phone (607) 257-1975 or e-mail training @ p2pmarshal.com. For more information, contact Frank Adelstein, technical director, ATC-NY, at (607) 257-1975 or e-mail fadelstein@atc-nycorp.com.

What is a Peer-to-Peer Network?

Wikipedia provides the following definition of a peer-to-peer (P2P) computer network:

[This type of network] uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes. Sharing content files containing audio, video, data or anything in digital format is very common, and real-time data, such as telephony traffic, is also passed using P2P technology. A pure P2P network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server.

This article was reprinted from the Fall 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.