UPDATE

APRI

American Prosecutors Research Institute

The **National Center for Prosecution of Child Abuse** will be producing a quarterly newsletter, **Child Sexual Exploitation Update**, focusing on issues relevant to prosecution of on-line crimes against children. On-line sexual victimization of children differs from other forms of child sexual abuse in at least three ways: 1) many of these crimes cross traditional jurisdictional boundaries; 2) the technology is highly sophisticated and rapidly advancing; and 3) the victims tend to be older and more complicit in their victimization. In our quarterly Child Sexual Exploitation Update, we will try to shed light on these issues for prosecutors and other child abuse professionals.

**Unsafe Havens:
Prosecuting Online Crimes Against Children
August 30 -
September 3, 2004
Ernest F. Hollings National Advocacy Center**

This course is designed to offer advanced trial advocacy training in cases involving the prosecution of on-line child sexual exploitation. Due to the complexity of these cases, this advanced course will focus primarily upon the prosecutor's role in the investigation and pre-trial stages of case preparation. This innovative training will utilize a mixture of lectures, hands-on computer classes, case studies, trial advocacy exercises and small group sessions. Prosecutors will learn how to create a legally defensible computer-facilitated case while honing cutting edge techniques for use in working with the child victim. For additional information, contact Abney Durham at the NAC at (803)544-5074.

Steganography:
Implications for the Prosecutor and Computer Forensics Examiner

Gary C. Kessler[1]

"Steganography," my colleague asked, "is that a dinosaur or an icicle hanging down in a cave?"

Steganography is the science of "covered writing" and is one of the newer tools in the arsenal of the cybercriminal and cyberterrorist — or any computer-astute user. Steganography is often referred to colloquially as "stego," for example, references to "stego" software are common.

As previously described in an NCPCA *UPDATE* four years ago,[2] steganography provides the means whereby two parties can communicate in such a way that a third party is not aware of the secret communication. Historically, steganographic methods date back thousands of years and include the use of invisible ink, microdots, and tattooing the scalps of slaves. Modern steganographic applications in the digital realm provide a covert communications channel by hiding some type of binary data in another file. The modified carrier file that contains the hidden information is called the *steganographic medium*. Steganalysis is the detection and recovery of that hidden information. This is the role of the computer forensics examiner for both law enforcement and anti-terrorism investigations.

The concern in law enforcement, of course, is that steganography is being used to "protect" communication among members of a criminal conspiracy. Unlike *cryptography*, which merely obscures the communication between two parties when observed by a third party, steganography hides the very existence of the communications channel. In the arena of commercial sexual exploitation of children, law enforcement concerns involve the use of steganography to exchange and to hide child pornography.

Consider the following hypothetical scenario. By pre-agreement, the leader of a child pornography distribution ring puts items for sale on eBay every Monday and posts photographs of the items. The items for sale are legitimate; bids are accepted, money is collected and products are dutifully shipped. Nevertheless, at some pre-arranged time during the week, versions of the photos are posted that contain hidden pictures. The ring members know when that time is and download the new photos. Unless the individuals are under active investigation, it is unclear that anyone will notice this activity. Furthermore, the sheer volume of people downloading the pictures will make it difficult to distinguish between the legitimate buyer and the conspirator.

For steganography to be effective, the sender and receiver have to agree upon the carrier files that will transport the hidden messages, the steganographic software to employ, and, possibly, a password. As one may imagine, there are literally an infinite number of audio and image files that can be used as carriers, and users can continue to produce such files forever. The StegoArchive[3] lists more than 100 steganographic programs for Windows, DOS, Linux, and other operating systems.

Today's steganographic programs can hide any type of binary data into nearly any type of image, audio, or video file. Data can even be hidden inside executable files[4] and spam messages.[5] This flexibility is what makes steganography so problematic for digital forensics investigators and prosecutors alike. To date, little steganography has been found in criminal cases so there is a mindset that it isn't being used. One of the reasons that it isn't being found, however, is because most investigators do not routinely search for steganographic tools and frequently use improper methods when they look for steganographic content. In an informal survey conducted in late 2003,[6] many investigators reported using the very steganography software that a suspect might use to hide information in order to detect steganography in suspect files. Steganographic software is great for hiding information but wholly inadequate for steganographic detection and steganalysis.

Investigators need to take a systematic approach to searching for steganographic content. At this time, the "official" computer forensics manuals[7,8] don't provide any steganographic guidelines. Prosecutors might also consider carefully crafting search warrants permitting more detailed forensic examinations for steganalysis. In the interim, consider the following suggestions.

First, look for clues that might suggest the use of steganography, such as:

The technical capabilities or sophistication of the computer's owner. Look at the books, articles, magazines, and software manuals in the suspect's library; the literature that the suspect possesses gives clues as to his/her interests and capabilities as well as the software that might be available.

Software clues on the computer. Steganographic investigators need to be familiar with the name of common steganographic software and related terminology, and even Web sites about steganography. Investigators should look for file names, Web site references in browser cookie or history files, registry key entries, e-mail messages, chat or instant messaging logs, comments made by the suspect, or

receipts that refer to steganography. These will provide hard clues prompting the investigator to look deeper. Finding similar clues for cryptography might also lead one down this path.

Other program files. Non-steganographic software might offer clues that the suspect hides files inside other files. Users with binary (hex) editors, disk wiping software, or specialized chat software might demonstrate an inclination to alter files and keep information secret.

Multimedia files. Look for the presence of a large volume of suitable carrier files, e.g., files large enough for steganographic use. While a standard Windows computer will contain thousands of graphics and audio files, for example, the vast majority of these files are very small and are an integral part of the graphical user interface. A computer system with a significant number of large files that could be steganographic carriers is potentially suspect; this is particularly true if there are a significant number of seemingly duplicate carrier files.

Type of crime. The type of crime being investigated may also make an investigator think more about steganography than other types of crime. Child pornographers, for example, might use steganography to hide their wares when posting pictures on a Web site or sending them through e-mail. Crimes that involve business-type records are also good steganography candidates because the perpetrator can hide the files but still get access to them; consider accounting fraud, identity theft (lists of stolen credit cards), drugs, gambling, hacking, smuggling, terrorism, and more.

Second, use steganalysis tools that are up to the task. WetStone Technologies' Gargoyle,[9] for example, will examine a suspect hard drive for remnants of files associated with any of the stego software distributions currently available. Stegdetect[10] is a program that can detect content hidden in JPEG files using several steganographic techniques. WetStone's StegoWatch[11] is similar to stegdetect, but can detect hidden content in almost any type of image file using a wide set of steganographic algorithms.

An additional problem when searching for steganography is the small size of the programs and the fact that most can run on a computer without being installed on the hard drive, coupled with the ever-present USB memory key (for example, thumb drives), now also available embedded in a watch[12] or Swiss army knife.[13] An entire suite of steganographic software can be carried on, and run from, a $30 memory key, leaving no trace on the hard drive. Search warrants must be carefully written so that police can find and seize these types of devices.

After all of this, finding a file with hidden data and even the correct steganographic software may not be the end of the search — most steganographic software also employs a password used for cryptography and/or randomization to open the file. If the steganographic software needs a password, that requires additional investigation.

Hiding information inside a carrier file has at least one legitimate purpose: An author can use digital *watermarking* to assert ownership of copyrighted digital intellectual property.[14,15] This application has several subtle differences from the more nefarious uses of steganography, however. For instance, digital watermarking generally hides only a small amount of repetitive information in the carrier file, does not necessarily hide the watermarking information, and is designed so that the watermark can be removed while maintaining the integrity of the carrier document.

Although the hypothetical eBay scenario presented earlier — or one like it — is a viable method for both terrorists and child pornographers to communicate, it is impossible to know how widely it is being used for these purposes.[16] It is likely, though, that the use of steganography will increase, and it will be a growing hurdle for law enforcement activities. There are some brief references in the literature to the link between child pornography and steganography,[17,18,19] but ignoring the significance of steganography because of the lack of statis-

tics is "security through denial" and not a good strategy. Steganography will certainly not be found if no one is looking for it.

In the aftermath of the 9/11 terrorist attacks, a number of articles suggested that al Qaeda terrorists employed steganography, using pornography as their carrier media.[20,21] Steganography and pornography may be technologically and culturally unexpected from that particular adversary but this tactic demonstrates an ability to think "out of the box." Prosecutors and computer forensics investigators must also think and investigate creatively.

Additional note: A technical version of this article, with examples and technical details, will be published in July 2004;[22] sample carrier and steganographic files, as well as sample steganographic software, can be downloaded from the author's Web site.[23] In cooperation with WetStone Technologies, the author will be co-teaching a steganography investigators course in Burlington, Vermont in August 2004.[24] For information, please contact the author.

1 Associate Professor, Computer & Digital Forensics Program, Champlain College, Burlington, VT. 802-865-6460, *gary.kessler@champlain.edu*

2 Astrowsky, B.H. STEGANOGRAPHY Hidden Images, A New Challenge in the Fight Against Child Porn." *UPDATE*, Vol. 13, No. 2, 2000. Also available: http://ndaa-apri.org/publications/newsletters/ update_volume_13_number_2_2000.html.

3 *http://www.stegoarchive.com/.*

4 *http://www.crazyboy.com/hydan/.*

5 *http://www.spammimic.com/.*

6 Security Focus. Forensics mailing list, personal communication, Dec. 1-26, 2003.

7 U.S. Department of Justice. *Electronic Crime Scene Investigation: A Guide for First Responders.* Office of Justice Programs, National Institute of Justice, Technical Working Group for Electronic Crime Scene Investigation, NCJ 187736, July 2001. Also available: http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

8 U.S. Department of Justice. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Criminal Division, Computer Crime and Intellectual Property Section, July 2002. Also available: http://www.cybercrime.gov/s&smanual2002.pdf.

9 *http://www.wetstonetech.com/gargoyle_ns.html.*

10 *http://www.outguess.org/detection.php.*

11 *http://www.wetstonetech.com/stegosuite_ns.html.*

12 See an example at *http://www.thinkgeek.com/gadgets/watches/5eec/.*

13 *http://www.swissbit.com/file/2/ct_621_ctDownload1.pdf.*

14 Arnold, M., Schmucker, M., and Wolthusen, S.D. *Techniques and Applications of Digital Watermarking and Content Protection.* Artech House, Norwood, Massachusetts, 2003.

15 Kwok, S.H. "Watermark-based Copyright Protection System Security." *Comm. ACM*, October 2003.

16 Hosmer, C. and Hyde, C. Discovering Covert Digital Evidence. *Digital Forensic Research Workshop (DFRWS) 2003*, August 2003 [Online]. (January 4, 2004). Available: http://www.dfrws.org/dfrws2003/presentations/Paper-Hosmer-digitalevidence.pdf.

17 Anon. "Child Pornography On Internet In this new age ..." Available: http://www.instant-essays.com/computers/child-pornography-on-internet.shtml.

18 Jossi, F. "Hiding in Plain Sight." *WIRED Magazine*, June 2001. Also available: http://www.wired.com/wired/archive/9.06/mustread.html?pg=9.

19 Renold, E., Creighton, S.J., Atkinson, C. and Carr, J. "IMAGES OF ABUSE: A review of the evidence on child pornography." National Society for the Prevention of Cruelty to Children (NSPCC), Oct., 2003. Also available: http://www.nspcc.org.uk/inform/Research/Summaries/ImagesOfAbuse.pdf.

20 Kelly, J. Terror groups hide behind Web encryption. *USA Today*, Feb. 5, 2001. Also available: http://www.usatoday.com/tech/news/2001-02-05-binladen.htm.

21 Manoo, F. The Case of the Missing Code. *Salon.com*, July 17, 2002 [Online]. (December 29, 2003). Available: http://www.salon.com/tech/feature/2002/07/17/steganography/.

22 "An Overview of Steganography for the Computer Forensics Examiner." *FBI Forensics Science Communication*, (in press, expected July 2004) (http://www.fbi.gov/hq/lab/fsc/current/index.htm).

23 *http://digitalforensics.champlain.edu/fsc/.*

24 *http://digitalforensics.champlain.edu/stego.html.*

APRI

American Prosecutors Research Institute
National Center for Prosecution of Child Abuse
99 Canal Center Plaza, Suite 510
Alexandria, Virginia 22314
www.ndaa-apri.org