

## BLACK TECH FORENSICS

### Steganography and its Derivatives: Steganalysis and Chaffing

G. Stevenson Smith

The level of concern related to the use of steganography as a means of sending secret messages has increased since the terrorist attacks in New York and Washington, D.C. Although it was not proven, a number of news reports suggested that al-Qaeda terrorists had used the Internet and steganography to send secret messages to their followers around the world prior to the attacks (Kolata, 2001). On the Internet, an example of steganography is the hiding of encrypted messages or files within digital photographs or music files for retrieval by someone with a secret password. Steganography can be used for the unauthorized removal of intellectual property and financial files from the corporate workplace without anyone's knowledge. Financial information can be sent to another site over the Internet or hidden in laptops within pictures of an employee's family or in the graphic of the company's logo. These hidden files can be placed on public web sites to be downloaded by anyone. The digital files may be slightly altered, but the changes are imperceptible to the human eye and when music files are played, any change is undetectable to the human ear. For example, is the hidden file in the author's photo perceptible?



It was never shown that terrorists used steganography, but if they had used this method of communication, it would have been very difficult to detect its use. Steganography allows anyone to remove information from a work site without detection or to communicate with others without leaving a trail in traditional e-mail records. For example, if a picture were downloaded at an anonymous public Web site such as a computer at a library, college lab, or Internet café, the computer logs would not provide a useful trail as to who had actually downloaded the file.

Individuals who want to break the electronic trail between themselves and their co-conspirators could use a combination of these methods.

Steganography refers to "covered writing", and it has a long tradition in the history of communication. Unlike cryptography, steganography conceals the basic existence of the message by hiding it in plain sight. Herodotus describes the use of these methods when around 440 B.C. messages were tattooed on the shaved head of trusted slaves, and the message became hidden in plain sight after the slave's hair had regrown. To uncover the message, the recipient of the message had the slave's head shaved. This technique allowed for the sending of messages without

---

G. Stevenson Smith is Professor of Accounting at West Virginia University, Morgantown, WV USA.