

Where's Waldo? He's Hiding in an MP3 File and You'll Never Find Him

May 4, 2003

By: Larry Seltzer

So afraid was the government of encryption that they once pursued [Phil Zimmerman](#), author of [PGP](#) (and according to Zimmerman [he's still under investigation](#)), for releasing free encryption software. I think it's important to oppose such investigations for reasons of libertarianism, but you have to wonder why the obsession with encryption when there are far scarier techniques available for hiding data.

If I wanted to hide data from the government or anyone else I might encrypt it, but I wouldn't stop there. If someone found the encrypted data they could possibly guess the key or use brute force to determine it. It would be far better if they didn't even know that there was data there at all. This is where steganography comes in. It's the art of hiding data, and it goes back way before computers. Invisible inks are a way of using steganography. The Germans in WWII also developed the use of micrdots, which are (typically) photographs reduced to the size of a period in an innocent-looking letter.

Steganography got some hype recently with reports, which turned out to be unsubstantiated, that Osama Bin Ladin had hidden data in pornographic pictures. Even though steganography might have been a good technique for Bin Ladin to use, I presume the porno part of the story was an attempt to insult him. But maybe the more interesting part is that it's in the nature of steganography that he could have been using it and we might not know.

As powerful as steganography is, experts don't consider it a serious problem in terms of corporate security. Tom Patterson of [Deloitte & Touche's Security Services Group for Europe, Middle East](#) and Africa says that for the employee who wants to secret away data, it's usually easy enough to do so without resorting to secret agent stuff like hiding data. Just copy it to a floppy. If the IT department really wants to protect their data, they can take active steps to lock down the computing environment by preventing unapproved applications from running, removing access to local drives, that sort of thing.

You may be wondering about the picture at the top of this column. It's my daughter, but it's not just any adorable picture of my daughter. I have used the freeware program [F5](#) to embed a message into this picture. I'm pretty sure recent versions of F5 encrypt the message before embedding them and the passphrase I used is 25 characters long, so a brute force attack will take a while.

The first reader to crack the message and report it back to me [here](#) gets a free copy of my book [ADMIN911: Windows 2000 Terminal Services](#), my second book [Linksys Networks: The Official Guide](#) or my classic copy of Gordon Letwin's Inside OS/2, the official Microsoft Guide to 1988's operating system of the future.

Note all the help you've gotten in this contest: I've told you that there is a message in a specific image, I've told you the length of the passphrase and I've told you the software used to hide the message. It's still going to take a while, unless you're very good. I'm told that there are algorithms for making things easier if you know that there is a message being hidden. Imagine if you didn't know where the message was hidden, what the software was, or even if there was a message hidden at all.

And by the way, JPG files are often used because they make fun demos, but the hot vehicle for hiding data is MP3 files. They are much larger and so can hide much more in them. A reasonably

sized MP3 file can hide as much as 500K in it, and if it diminishes the quality of the encoding, the file will fit right in with all the other lousy MP3 files out on the net.

Good guys use steganography too, generally in the field of digital watermarking. Sometimes watermarking is just to fingerprint a document to include evidence of ownership, but it gets fancier than that. For cases where a document needs to remain secret, some watermarking systems can put an extra dot in the document, and each version of the document gets the dot in a different place. If the document is ever leaked you can find the location of the dot where the source of the leak was. The math behind this technique is the same as black-hat steganography.

For further study of steganography I recommend browsing the [books](#) and [papers of Neil F. Johnson](#), and especially his [paper on Steganography](#).

Copyright (c) 2003 Ziff Davis Media Inc. All Rights Reserved.