

# Cyber criminals can be hunted down and caught



by James Kerr

## **The Problem:**

To catch a tiger, you must follow its trail. Every animal unwittingly leaves clues, like footprints in the dirt and pieces of fur on neighboring branches. If you can track those tell-tale signs, you can find your animal.

The same is true when hunting cyber criminals. They leave traces of their behavior - even when they're doing their best to cover their tracks.

The sophisticated criminals adopt complex measures to conceal their crimes. This often entails camouflaging their tactics so it's more difficult to notice any wrongdoing.

Sometimes the bad guys will bury their actions and then transfer or assign their misdeeds to innocent bystanders. Child pornographers, for example, will surreptitiously store their illegal pictures on other people's computers - not their own computers - so they can quickly deny ownership.

Low level criminals are clumsier. In the privacy of their cubicles or the comfort of their homes, those evil-doers are easily lulled into a false sense of security and will steal logins, sabotage systems and abscond with sensitive company information, leaving a steady stream of evidence.

We recently helped catch a bad guy. Here's how we did it.

## **The Solution:**

Every computer on the internet has an identifier. You can think of it as the computer version of a conventional mailing address. It's called an Internet Protocol ("IP") address.

You have an IP address. The next time you're online, go to this website: <http://whatismyipaddress.com/>. The number displayed is your IP address. It resembles something like this: 208.77.188.166.

IP addresses are important because they enable computers to find each other. When you send email to 'James Kerr, Chief Geek of SuperGeeks', your computer is really sending email to the IP address associated with 'James Kerr, Chief Geek of SuperGeeks'. Your computer doesn't know me or care about me, but it knows my IP address and that's all that really matters. The internet works.

When you complete an online form, make an online payment, post a classifieds ad online and reply to an email, your IP address is automatically assigned to that transaction. Imagine a giant rubber stamp on the internet, fixing the date, location, etc. to each of those activities.

Now, there are ways to change or even mask your IP address. The sophisticated criminals will certainly take the time to cover their IP tracks, but the not-so-experienced crooks will frequently and unwittingly reveal their true IP addresses.

Once you know the real IP address associated with a crime, you actually know quite a bit. There are reverse lookup sites which, given an IP address, will determine the address's general geographic location: <http://whatismyipaddress.com/>. You can also verify an IP address with the Internet Service Provider, though that sometimes requires a court order.

That's exactly how we helped catch that one crook. He committed his cybercrimes and left a trail of evidence. By cross-referencing his digital signature with his digital identity, we were able to produce enough electronic evidence to lead to his apprehension.

**Bottom line:** Cyber criminals can be hunted down and caught. If you suspect a person has committed a crime, take a look at the electronic evidence. (Be careful not corrupt the digital crime scene!) Those tiger tracks may be surprisingly obvious.