



From: [www.cio.com](http://www.cio.com)

## How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab

– Scott Berinato, CSO

May 31, 2007

Forensic investigations start at the end. Think of it: You wouldn't start using science and technology to establish facts (that's the dictionary definition of forensics) unless you had some reason to establish facts in the first place. But by that time, the crime has already happened. So while requisite, forensics is ultimately unrewarding.

A clear illustration of this fact comes from the field investigations manager for a major credit services company. Sometime last year, he noticed a clutch of fraudulent purchases on cards that all traced back to the same aquarium. He learned quite a bit through forensics. He learned, for example, that an aquarium employee had downloaded an audio file while eating a sandwich on her lunch break. He learned that when she played the song, a rootkit hidden inside the song installed itself on her computer. That rootkit allowed the hacker who'd planted it to establish a secure tunnel so he could work undetected and "get root"—administrator's access to the aquarium network.

The advertisement features a yellow box on the left with the text 'Software that helps you master complexity.' and a red 'LEARN MORE &gt;' link. To the right is a photograph of a traditional Japanese-style vase with red flowers on a wooden stand. At the bottom, the text reads 'Confidence in a connected world.' next to the Symantec logo.

Sounds like a successful investigation. But the investigator was underwhelmed by the results. Why? Because he hadn't caught the perpetrator and he knew he never would. What's worse, that lunch break with the sandwich and the song download had occurred some time before he got there. In fact, the hacker had captured every card transaction at the aquarium for two years.

The investigator (who could only speak anonymously) wonders aloud what other networks are right now being controlled by criminal enterprises whose presence is entirely concealed. Computer crime has shifted from a game of disruption to one of access. The hacker's focus has shifted too, from developing destructive payloads to circumventing detection. Now, for every tool forensic investigators have come to rely on to discover and prosecute electronic crimes, criminals have a corresponding tool to baffle the investigation.

This is antforensics. It is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you.

The concept is neither new nor foolproof, but in the past 12 months, forensic investigators have noticed a significant uptick in the use of antiforensics. This is not because hackers are making more sophisticated antiforensic tools, though some are. Rather, it's because antiforensic tools have slid down the technical food chain, from Unix to Windows, from something only elite users could master to something nontechnical users can operate. What's more, this transition is taking place right when (or perhaps because of) a growing number of criminals, technically unsophisticated, want in on all the cash moving around online and they need antiforensics to protect their illicit enterprises. "Five years ago, you could count on one hand the number of people who could do a lot of these things," says the investigator. "Now it's hobby level."

Researcher Bryan Sartin of Cybertrust says antiforensic tools have gotten so easy to use that recently he's noticed the hacks themselves are barely disguised. "I can pick up a network diagram and see where the breach occurred in a second," says Sartin. "That's the boring part of my job now. They'll use FTP and they don't care if it logs the transfer, because they know I have no idea who they are or how they got there." Veteran forensic investigator Paul Henry, who works for a vendor called Secure Computing, says, "We've got ourselves in a bit of a fix. From a purely forensic standpoint, it's real ugly out there." Vincent Liu, partner at Stach & Liu, has developed antiforensic tools. But he stopped because "the evidence exists that we can't rely on forensic tools anymore. It was no longer necessary to drive the point home. There was no point rubbing salt in the wound," he says.

The investigator in the aquarium case says, "Antiforensics are part of my everyday life now." As this article is being written, details of the [TJX breach](#)—called the biggest data heist in history, with more than 45 million credit card records compromised—strongly suggest that the criminals used antiforensics to maintain undetected access to the systems for months or years and capture data in real time. In fact, the TJX case, from the sparse details made public, sounds remarkably like the aquarium case on a massive scale. Several experts said it would be surprising if antiforensics weren't used. "Who knows how many databases containing how many millions of identities are out there being compromised?" asks the investigator. "That is the unspoken nightmare."

### **The Obfuscator's Toolkit**

If you were making a movie about a computer crime, the bad guys would use antiforensics. And since it's a movie, it should be exciting, so they'd use the clever and illicit antiforensic tools, the sexy ones with little or no legitimate business purpose. Liu has developed such tools under the Metasploit Framework, a collection of software designed for penetration testing and, in the case of the antiforensic tools, to expose the inherent weaknesses in forensics in hopes that the forensics industry would view it as a call to action to improve its toolset.

One of Liu's tools is Timestomp. It targets the core of many forensic investigations—the metadata that logs file information including the times and dates of file creation, modification and access. Forensic investigators poring over compromised systems where Timestomp was used often find files that were created 10 years from now, accessed two years ago and never modified. Transmogrify is similarly wise to the standard procedures of forensic investigators. It allows the attacker to change information in the header of a file, a space normally invisible to the user. Typically, if you changed the extension of a file from, say, .jpg to .doc, the header would still call it a .jpg file and header analysis would raise a red flag that someone had messed with the file. Transmogrify alters the header along with the file extension so that the analysis raises no red flags. The forensic tools see something that always was and remains a .doc file.

Slacker would probably be in the movie too. It breaks up a file and stashes the pieces in the slack space left at the end of files. Imagine you stole the Dead Sea Scrolls, ripped them into thousands of small pieces, and then tucked those pieces, individually, into the backs of books. That's Slacker, only Slacker is better because you can reassemble the data and, while hidden, the data is so diffuse that it looks like random noise to forensic tools, not the text file containing thousands of credit card numbers that it actually is.

Another tool, Sam Juicer, retrieves encrypted passwords but leaves behind no evidence it was ever run, allowing you to crack the passwords later offline. KY stuffs data into null directory entries, which will still look null to the outside world. Data Mule infiltrates hard disk drives' normally off-limits reserved space. Randomizers auto-generate random file names to evade signature-based inspection. There are tools that replace Roman letters with identical-looking Cyrillic ones to avoid suspicion and inspection. In other words, you need explorer.exe to run your computer, but you don't need explorer.exe, which looks the

same but actually starts with a Cyrillic “e” and is a keylogger.

If you want to go full-out cloak-and-dagger in your movie, you’d show off antiforensic tools that have gone solid-state. Diskless A-F is the state of the art; it avoids logging of activity all together. “There’s nothing on the disk that can’t be messed with,” says Liu. “So the arms race has left the disk and is moving into memory. Memory is volatile storage. It’s a lot more difficult to understand what’s going on in there. Disk layout is documented; you know where to look for stuff. In memory, stuff moves around; you can’t track it down.”

MosDef is one example of diskless antiforensics. It executes code in memory. Many rootkits now load into memory; some use the large stockpiles of memory found on graphics cards. Linux servers have become a favorite home for memory- resident rootkits because they’re so reliable. Rebooting a computer resets its memory. When you don’t have to reboot, you don’t clear the memory out, so whatever is there stays there, undetected. “You’ve got 128 megs of RAM in network printers that are never shut off!” exclaims Michael Davis, CEO of incident response company Savid Technologies and a veteran security researcher who worked on the HoneyNet Project. “It’s an old technique, but a common one.”

### **Antiforensics Tools That Appear Legitimate on First Blush**

Perhaps less sexy—but just as problematic to the forensic investigator—are antiforensic tools that fall into a gray middle on the spectrum of legitimacy. These include tools like packers, which pack executable files into other files. In the aquarium case, the criminal most likely used a packer to attach his rootkit to the audio file. Binders bind two executables into one, an especially dangerous tool when one of the executables is legitimate. I might have no concern clicking on firefox.exe, for example, but it could very well be bound to keylogger.exe. Virtualization is a popular trend in IT now, because it allows one machine to run many environments. Hackers simply apply the principle to their jobs; one of the virtual environments borrowing the hardware becomes theirs.

Steganography—hiding data in other data—has legitimate uses for the privacy conscious, but then criminals breaking into systems are privacy conscious too. A great way to transport data you’re not supposed to have is to hide it where it will generate no suspicion, like in photos of executives that the marketing department keeps on the network. (Disagreement reigns over the prevalence of steganography as an antiforensic technique in practice; no one disputes its capabilities or increasing ease of use, though). Disk wiping systems are valuable for refreshing and decommissioning hard disks on machines, and boosting performance. But they also serve the criminal who needs to erase his digital tracks. Some data wiping programs have been tuned to thwart the specific programs that criminals know are popular with forensic investigators, like EnCase, and they are marketed that way.

The most prosaic antiforensic tools are also the most common. Security software like encryption and VPN tunneling serve as foundations of the criminal hacker’s work once he’s infiltrated a system. “In one case, we found a large retail database that was compromised,” says Sartin. “And the first thing the hackers did when they got there was install a client VPN,” and at that point, they became virtually invisible. Another classic antiforensic technique is to partition a hard drive and encrypt one section of it, then partition that partition and encrypt a subsection of that. “Any data in that second partition I can deny ever existed,” says Henry. “Then the bad guy who is caught gives up the password or key for the first partition, which typically contains only moderately bad stuff. The really bad stuff is in the second partition, but the investigators have no clue it’s there. Forensic tools wouldn’t see the second partition; it would look like random trash.”

These techniques are not sexy—they might not make it into the movie—but in some ways they’re actually the most problematic antiforensic tools, because there are excellent reasons to continually improve encryption, secure remote access, disk partitioning and virtual environments. Better encryption stands to protect data and privacy. Secure tunnels make remote business over the Internet feasible. Virtualization is an efficiency boon. And yet, improving these products also happens to improve the criminal’s antiforensic toolkit in lockstep.

This list is only a sample of the tools used for antiforensics. Many others do clever things, like block reverse engineering of code or purposefully leave behind misleading evidence to send forensic investigators down the wrong path, wasting their time and money. Taken at its most broad, antiforensics even extends to physical techniques, like degaussing hard drives or taking a sledgehammer to one. The

portfolio of techniques available, for free or for a low cost, is overwhelming.

An antiforensic pioneer and hacker who calls himself the Grugq (sounds like “grug”) says he once presented this kind of primer on antiforensics to the police’s largest computer forensics unit in London. “It was packed with all these mean-looking coppers,” he recalls. “And here I am, this computer security guy saying, ‘You’re all [screwed] and there’s nothing you can do about it.’ When I finished, it was quiet. Only one person raised his hand. Scary geezer. Six-two, shaved head. Tattoos all over his arms. I thought he might thump me.

“But he stood up and looked like he was about to cry. All he said was, ‘Why are you doing this?’”

### **Why Are They Developing Antiforensic Tools?**

As long as five years ago, Grugq was creating antiforensic tools. Data Mule is one in his package that he calls the Defiler’s Toolkit. Likewise, Liu developed Timestomp, Slacker and other tools for the Metasploit Framework. In fact, a good portion of the antiforensic tools in circulation come from noncriminal sources, like Grugq and Liu and plain old commercial product vendors. It’s fair to ask them, as the overwhelmed cop in London did, why develop and distribute software that’s so effective for criminals?

Grugq’s answer: “If I didn’t, someone else would. I am at least pretty clean in that I don’t work for criminals, and I don’t break into computers. So when I create something, it only benefits me to get publicity. I release it, and that should encourage the forensics community to get better. I am thinking, Let’s fix it, because I know that other people will work this out who aren’t as nice as me. Only, it doesn’t work that way. The forensics community is unresponsive for whatever reason. As far as that forensic officer [in London] was concerned, my talk began and ended with the problem.”

### **Antiforensics Tools Reveal Vulnerabilities in Computer Forensics Tools**

Liu agrees but takes it further. He believes developing antiforensics is nothing less than whistle-blowing. “Is it responsible to make these tools available? That’s a valid question,” he says. “But forensic people don’t know how good or bad their tools are, and they’re going to court based on evidence gathered with those tools. You should test the validity of the tools you’re using before you go to court. That’s what we’ve done, and guess what? These tools can be fooled. We’ve proven that.”

For any case that relies on digital forensic evidence, Liu says, “It would be a cakewalk to come in and blow the case up. I can take any machine and make it look guilty, or not guilty. Whatever I want.”

Liu’s goal is no less than to upend a legal precedent called the presumption of reliability. In a paper that appeared in the Journal of Digital Forensic Practice, Liu and coauthor Eric Van Buskirk flout the U.S. courts’ faith in digital forensic evidence. Liu and Van Buskirk cite a litany of cases that established, as one judge put it, computer records’ “prima facie aura of reliability.” One decision even said computer records were “uniquely reliable in that they were computer-generated rather than the result of human entries.” Liu and Van Buskirk take exception. The “unfortunate truth” they conclude, is that the presumption of reliability is “unjustified” and the justice system is “not sufficiently skeptical of that which is offered up as proof.”

It’s nearly a declaration that, when it comes to digital information, there’s no such thing as truth. Legally anyway. As Henry likes to put it, “Antiforensic tools have rendered file systems as no longer being an accurate log of malicious system activity.”

Computer forensics in some ways is storytelling. After cordoning off the crime scene by imaging the hard drive, the investigator strings together circumstantial evidence left at the scene, and shapes it into a convincing story about who likely accessed and modified files and where and when they probably did it. Antiforensics, Liu argues, unravels that narrative. Evidence becomes so circumstantial, so difficult to have confidence in, that it’s useless. “The classic problem already with electronic crimes has been, How do you put the person you think committed a crime behind the guilty machine they used to commit the crime?” says Brian Carrier, another forensic researcher, who has worked for the Cerias infosecurity research program at Purdue University. Upending the presumption of reliability, he says, presents a more basic problem: How do you prove that machine is really guilty in the first place? “I’m surprised it hasn’t happened yet,” says Liu. “But it will.”

Under the current computing infrastructure, data is untrustworthy, then. The implications of this, of courts limiting or flat-out denying digital forensics as reliable evidence, can't be understated. Without the presumption of reliability, prosecution becomes a more severe challenge and thus, a less appealing option. Criminals reasonably skilled with antifoensics would operate with a kind of de facto legal immunity.

### **Making It Not Worth It**

Despite all that, casting doubt over evidence is just a secondary benefit of antifoensics for criminals. Usually cases will never get to the legal phase because antifoensics makes investigations a bad business decision. This is the primary function of antifoensics: Make investigations an exercise in throwing good money after bad. It becomes so costly and time-consuming to figure out what happened, with an increasingly limited chance that figuring it out will be legally useful, that companies abandon investigations and write off their losses. "Business leaders start to say, 'I can't be paying \$400 an hour for forensics that aren't going to get me anything in return,'" says Liu. "The attackers know this. They contaminate the scene so badly you'd have to spend unbelievable money to unravel it. They make giving up the smartest business decision."

"You get to a point of diminishing returns," says Sartin. "It takes time to figure it out and apply countermeasures. And time is money. At this point, it's not worth spending more money to understand these attacks conclusively."

One rule hackers used to go by, says Grugq, was the 17-hour rule. "Police officers [in London's forensics unit] had two days to examine a computer. So your attack didn't have to be perfect. It just had to take more than two eight-hour working days for someone to figure out. That was like an unwritten rule. They only had those 16 hours to work on it. So if you made it take 17 hours to figure out, you win." Since then, Grugq says, law enforcement has built up 18-month backlogs on systems to investigate, giving them even less time per machine.

"Time and again I've seen it," says Liu. "They start down a rat hole with an investigation and find themselves saying, 'This makes no sense. We're not running a business to do an investigation.' I've seen it at Fortune 100s. The company says, 'We think we know what they got and where. Let's close it up.' Because they know that for every forensic technique they have, there's an antifoensic answer. Unfortunately, the converse isn't true."

### **The Rise of Antifoensics Tools Will Force Computer Investigators to Change**

By now, it should be clear why Henry of Secure Computing has been giving a presentation called "Anti-Forensics: Considering a Career in Computer Forensics? Don't Quit Your Day Job." The state of forensics certainly sounds hopeless, and Henry himself says, "The forensics community, there's not a hell of a lot they can do."

But in fact there's some hope. Carrier says, "Yes, it makes things a lot harder, but I don't think it's the end of the world by any means." What can start to turn the tables on the bad guys, say these experts and others, is if investigators embrace a necessary shift in thinking. They must end the cat-and-mouse game of hack-defend-hack-defend. Defeating antifoensics with forensics is impossible. Investigations, instead, must downplay the role of technology and broaden their focus on physical investigation processes and techniques: intelligence, human interviews and interrogations, physical investigations of suspects' premises, tapping phones, getting friends of suspects to roll over on them, planting keyloggers on suspects' computers. There are any number of ways to infiltrate the criminal world and gather evidence. In fact, one of the reasons for the success of antifoensics has been the limited and unimaginative approach computer forensic professionals take to gathering evidence. They rely on the technology, on the hard disk image and the data dump. But when evidence is gathered in such predictable, automated ways, it's easy for a criminal to defeat that.

"I go back to my background as a homicide detective," says the investigator in the aquarium case. "In a murder investigation, there is no second place. You have to win. So you come at it from every angle possible. You think of every way to get to where you want to go. Maybe we can't find the source on the network with a scanning tool. So you hit the street. Find a boss. His boss. His boss. You find the guy selling data on the black market. The guy marketing it on [Internet Relay Chat]. You talk to them. They're using stego? Maybe we drop some stego on them. The techniques used in physical investigations are becoming increasingly important."

Indeed, if one looks back on some of the major computer crimes in which suspects were caught, one will notice that rarely was it the digital evidence that led to their capture. In the case of Jeffrey Goodin of California, the first ever under the Can-Spam Act, it was a recorded phone call with a friend who had flipped on the suspect that led to the conviction. In the case of the Russian botnet operators who had extorted millions from gaming sites, it was an undercover operation in which a “white hat” hacker befriended the criminals. In the United Kingdom, says Grugg, the police are using social modeling to try to penetrate antiforensics used on mobile phones for drug dealing. “The police’s goal is to get a confession,” he says. “They don’t care if they have compelling evidence off the disk.” In the TJX case, the only arrests made to date are based on purchases of exorbitant gift cards at the company’s retail stores, caught on tape.

It will be the interviews with those people, and not system analysis, that will lead to more information and, potentially, more arrests in the case.

“Every successful forensics case I’ve worked on turned into a physical security investigation,” says Bill Pennington, a researcher at White Hat Security and veteran technical forensics investigator. “In one case, it was an interview with someone who turned on someone else. You layer the evidence. Build it up. He sees the writing on the wall, and he cracks. But if we had to rely on what the computer evidence told us, we would have been stuck.”

### **Moving Targets**

Behind the portfolio of easy-to-use Windows-based antiforensic tools, criminal hackers are building up a next-generation arsenal of sophisticated technical tools that impress even veterans like Grugg. “There are now direct attacks against forensic tools,” he says. “You can rootkit the analysis tool and tell it what not to see, and then store all your evil stuff in that area you told the analysis tool to ignore. It is not trivial to do, but finding the flaw in the analysis tool to exploit is trivial.”

Another new technique involves scrambling packets to avoid finding data’s point of origin. The old-school way of avoiding detection was to build up a dozen or so “hop points” around the world—servers you bounced your traffic off of that confounded investigations because of the international nature of the traffic and because it was just difficult to determine where the traffic came from, really. The state-of-the-art antiforensic technique is to scramble the packets of data themselves instead of the path. If you have a database of credit card information, you can divvy it up and send each set of packets along a different route and then reassemble the scatterlings at the destination point—sort of like a stage direction in a play for all the actors to go wherever as long as they end up on their mark.

The aquarium attack, two years later, already bears tinges of computer crime antiquity. It was clever but today is hardly state of the art. Someday, the TJX case will be considered ordinary, a quaint precursor to an age of rampant electronic crime, run by well-organized syndicates and driven by easy-to-use, widely available antiforensic tools. Grugg’s hacking mentor once said it’s how you behave once you have root access that’s interesting. In a sense, that goes for the good guys too. They’ve got root now. How are they going to behave? What are they going to do with it? “We’ve got smarter good guys than bad guys right now,” says Savid Technologies’ Davis. “But I’m not sure how long that will be the case. If we don’t start dealing with this, we’re not even going to realize when we get hit. If we’re this quiet community, not wanting to talk about it, we’re going to get slammed.”

*Send feedback to Senior Editor Scott Berinato at [sberinato@cxo.com](mailto:sberinato@cxo.com)*

*2002-2007 CXO Media Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.*