Computer forensics’ presumed usefulness against anyone with computer savvy is minimal because such persons can readily defeat forensics techniques. Because computer forensics can’t show who put the data where forensics found it, it can be evidence of nothing.

The Need for Privacy

First, the data in “our” computers and other devices that overzealous adversaries and prosecutors present as evidence to courts as being “obviously” ours often isn’t. Just because we paid the bill for a home computer doesn’t mean that we placed an invisible force-field around it to shield it from hackers and others who, as I’ll demonstrate later, could add, remove, or alter any and all data in that computer without our knowledge.

Technology-challenged judges and juries usually assume that anything that investigators find in computers we bought could have been placed there only by ourselves. Our lawyers, who typically didn’t study computers in law school, don’t know enough to challenge such assertions, and we can end up in jail.

The key truth is that third parties often place data in devices that are ours (in the sense that we bought them) or, worse yet, in records about us that others control (such as service provider databases).

Second, modern nations’ entire economic viability is predicated on the assumption that responsible individuals and organizations can protect proprietary...
content from unauthorized access. Such content includes trade secrets, business marketing plans, and strategic planning. Without information confidentiality, commercial entities’ economic infrastructure would collapse, as would the nations where those entities reside. Laws can’t prevent thieves from stealing information any more than they can prevent murder, theft, or a planeload of innocents from being used as a missile against a building. What responsible individuals need is know-how for protecting against information theft.

Finally, civilized nations protect confidentiality for some communication types, such as attorney–client or doctor–patient discussions. Having such protections is pointless, however, if it’s technologically easy for unauthorized parties to access this information anyway. Merely stating, “You have no privacy; get over it” isn’t good enough.

We must thus address two separate issues.

First, jealously guarding your secrets is not only very proper but is also legally required in many cases. The Health Insurance Portability and Accountability Act (HIPAA) in the US issues penalties for not safeguarding patients’ medical information. Other laws provide criminal penalties for stealing trade secrets and other proprietary information. Furthermore, we, as free individuals, are under no obligation to bare our lives for anyone’s benefit. In fact, misleading others as to what we do is perfectly legal as long as we don’t intend to defraud anyone, or doing so isn’t expressly prohibited (such as when applying for a loan). Indeed, when we put on our best clothes, makeup, and behavior prior to interacting with others, we’re consciously misleading them, albeit in a time-honored, socially acceptable way.

Second, we, as responsible individuals, can preemptively defeat computer forensics to ensure confidentiality, which is one of the three tenants of security. We don’t live our lives as free people for the convenience of assorted investigators. Unlike under Pol Pot’s regime in Cambodia, where having a door or window that obscured what was occurring in your house was a crime, free people should expect to live their lives in privacy, investigators’ and busybodies’ wishes to the contrary notwithstanding.

Many have promulgated the fiction, originally attributed to J. Edgar Hoover, that “if you have done nothing wrong, you have nothing to fear.” Yet countless examples exist of people who were found guilty by juries and executed by court order, only to be exonerated posthumously on the basis of subsequent DNA evidence. The obvious conclusion is that you have a lot to fear even though you have done nothing wrong. Similarly, holocaust victims had done nothing wrong, yet history shows us that they had a lot to fear.

The Limitations of Computer Forensics
In a nutshell,

• computer forensics can’t determine who put the data on our digital devices; and
• computer forensics can never find what doesn’t exist in the first place—and numerous ways exist for using a computer in a way that generates absolutely no discoverable data by, for example, disconnecting the hard drive and booting off a bootable CD, and either uploading or saving the encrypted output in removable media.

In the context of this discussion, a “computer” isn’t just a box with a mouse, keyboard, and monitor, but any digital device we use, such as a cell phone, a GPS navigator, a digital camera, a digital voice recorder, a set-top TV converter, and so on.

Classical computer forensics creates the illusion of an airtight investigatory process by diverting attention away from the crucial fact that forensics can’t determine who put the data on a device, and focusing instead on the mechanics of the forensic ritual: investigators create an exact copy of data found on a digital device and present it to a decision authority (court, employer, and so on) without any ability to address the key question of who put the data in that device. The mechanics of the forensic ritual are indeed sound:

• Making the exact copy of the targeted computer’s data and ensuring that the copy is a clone of the original.
• Making sure this copy isn’t contaminated after it’s made so that what is presented to a court is what was copied from the forensically copied drive. This is the “chain of custody” issue.

This might appear satisfactorily complete, but it isn’t. A huge gap exists in this process that no amount of forensics can resolve: the issue of who placed the files on a computer in the first place and whether the data was altered prior to the time it was copied by forensic investigators. Files can and do end up on our computers in myriad ways without our knowledge, let alone our consent. Besides, what does “my computer” really mean? Does it denote the computer I paid for? The computer I’m the most frequent user of? Does it denote the computer of which, to the best of my knowledge, I’m the sole user? Or a computer from a third party, such as my employer or a computer leasing company?

In all these cases, including an extreme case in which an individual lives alone with a computer that was purchased brand new, a vast number of common, everyday ways exist whereby files can enter this computer without that individual’s awareness.
**Remote Hacking**

Almost every computer these days is connected to the Internet or at least to some internal network. As anyone in the field knows, a remote hacker can execute arbitrary code on such a computer in a variety of ways. The hacker can add, remove, or modify files, change the date on files, and do everything with that computer that the local user can, and without the local user’s knowledge.

**Wi-Fi Hacking**

Most computers built during the past five years come with Wi-Fi built in and usually enabled in the promiscuous mode; this means that a savvy hacker can set up a Wi-Fi access point nearby and cause this Wi-Fi-enabled computer to dutifully connect to that rogue access point. The access point’s operator can then easily add, remove, or modify files in the targeted computer, even if that computer’s owner never consciously connected to the Internet.

**“War-Driving”**

It’s well-documented that most computer users who buy Wi-Fi capability for their personal use at home don’t bother to enable any security on their Wi-Fi installation—no MAC address authentication, no encryption, no muting of the broadcasting of the SSID (Service Set Identifier; that is, the name a user gives his or her access point)—not that any of these measures are particularly effective. The Internet is full of tutorials, software, and hardware offers for enabling third parties to bypass most of these security features in minutes, with the possible exception of Wi-Fi Protected Access (WPA, the latest version of encryption of the wireless signal in Wi-Fi). Any Wi-Fi-enabled computer within range (which can be as far as 20 miles under some conditions) can access the unprotected Wi-Fi’s Internet connection and conduct illegal activities for which the hapless home Wi-Fi owner will be held accountable.

**Unsolicited Email**

During daily Internet usage, most of us receive tens to hundreds of unsolicited emails each day. We usually delete them, often unaware that this doesn’t remove anything but merely marks the space where that file was on the hard drive as available for future use. The typical recipient of such unsolicited email won’t overwrite that space during the next few months or years, except inadvertently through defragmenting. Some unsolicited emails include attachments whose mere presence on our hard drives could be cause for arrest under current laws; few of us bother to find those attachments and “delete” them either, which, again, wouldn’t remove them from the hard drive anyway. Because Windows doesn’t include any utility for overwriting anything, almost no one overwrites such incoming unsolicited attachments. Over a few years, enough junk accumulates in all our computers to “prove” to a gullible court—if carefully selected out of context by an overachieving prosecutor—that the accused has a proclivity for just about anything the prosecutor elects to claim.

**Malicious Email Attachments**

Any computer security person knows that malicious mobile code is routinely placed in images and other executable files attached to incoming emails. Even if the recipient overwrites such unsolicited attachments at some later time after opening them—and practically nobody does, as I’ve mentioned—the damage is done, and your computer has been compromised, letting an attacker access it in numerous ways, such as turning it into a zombie for a distributed denial-of-service attack or executing arbitrary code in that computer.

**Typos that Hurt**

During just a few weeks of legitimate and routine online activities, we all occasionally mistype URLs and end up inadvertently on adult sites or worse. We then retype the correct URL and forget about the incident; our computers, however, don’t forget. Over a few months or years, such pseudo-“evidence” selected out of context might convince most judges and juries that the accused has displayed “an obvious pattern” of whatever the accuser wants a court to believe.

**Freeware that Is Very Costly**

Computer-literate users know that a lot of freeware we download for normal use has a dark side. At a minimum, such software often enables a security vulnerability whereby the provider can access the affected computer. You might recall the infamous incident from a couple of years ago in which some commercial audio CDs manufactured by a major distributor contained code that installed a rootkit. That rootkit inadvertently enabled third parties to take over the affected computer.

**Defeating Computer Forensics**

Computer forensics isn’t a single technique but rather a collection of constantly evolving techniques. Some target data storage media, others the data while in transit. Still others target data entry or display devices (for example, keyloggers or printer interception devices). Some exploit somewhat esoteric, physics-based electronics properties, such as Van Eck unintended emanations from terminals,\(^1\) optical interception,\(^2\) and so on. Finally, some techniques exploit human weaknesses and inattentiveness.

Some data is more perishable than other data. We used to believe RAM was volatile as soon as you turn...
off the power switch; thanks to Ed Felten’s work at Princeton, we now know that this isn’t the case.

It follows that defeating computer forensics won’t—and never can—take a single countermeasure but a large collection of also constantly evolving techniques. The statement “I want to be safe from data theft” is an ill-posed one unless you specify exactly which threats you’re trying to protect yourself from. Just as when you want to be healthy you must follow numerous guidelines, each intended to minimize risk from a specific medical problem, defeating forensics requires an equally comprehensive collection of techniques designed to defeat different forensic attacks.

**Defeating Hostile Forensics on Data Storage Media**

The most common type of computer forensics involves a forensic attack on data storage media. You can easily defeat it by avoiding data storage media in the first place—forensics can’t find what doesn’t exist. You can disconnect the internal hard drive altogether and boot off read-only media, such as bootable CDs with built-in operating systems (for example, Knoppix or BartPE), or—depending on your BIOS—a USB thumbdrive configured for read-only usage. Bootup media can also have any complete software complement that you desire, such as word processing, encryption, or telecommunications software to let you do desired work. The output will be encrypted and only then placed in encrypted form onto some removable media.

All the forensics in the world won’t help attackers in this case because they will have no media on which to do forensics. About all they could do would be to

- preplace a hardware keylogger on the computer (a countermeasure to which I’ll address later),
- conceal an overhead camera aimed at the computer keyboard or screen, or
- intercept and reconstruct the Van Eck emanations from the terminal being used.

All three are operationally quite involved, but you can even defeat these—assuming a plausible likelihood that they’ve been deployed and that the information you’re protecting is worth the effort.

**Defeating a Keylogger**

Software keyloggers are by far the most common, and the best defense is to prevent an attacker from installing one in the first place. Regardless, if your computer’s hard disk is disconnected, and your computer is booted from a trusted bootable CD, DVD, or USB thumbdrive with its own trusted operating system and software, the keylogger problem goes away.

A hardware keylogger can be impossible to detect on a desktop computer, where it can masquerade as a ferrite core filter on the keyboard’s cable or, worse yet, be integrated into the keyboard. If you suspect a hardware keylogger, then the best countermeasure is to use a laptop because intercepting the integrated keyboard’s wiring to hide a hardware keylogger is difficult in such limited space. Alternately, you can use a virtual keyboard painted on the computer’s screen and use the mouse to select each letter; this is most suitable for entering short text, such as encryption keys and passwords.

**Defeating an Overhead Camera**

To defeat an overhead camera, you should tilt your monitor screen downward. If it’s not too bothersome, you could also place a shroud over your monitor that obscures your hands and keyboard from any overhead camera, yet allows you to see the keyboard well enough to type.

**Defeating Van Eck Radiation Interception**

As Ross Anderson and Mark Kuhn have amply demonstrated, both laptops and desktops radiate radio frequency signals that attackers can intercept and reconstruct. Laptops radiate a little less energy because power consumption is at a premium and current levels are lower, but still enough to be intercepted reasonable distances away.

Countermeasures to such attacks follow directly from basic electrical engineering:

- Work in the basement and not on a high-elevation floor where the signal has minimum attenuation on its way to an interceptor’s site. If possible, wallpaper the room with conductive material that’s grounded to a water pipe; in a jam, wallpapering with aluminum foil from the local supermarket will do.
- While using the laptop, disconnect all external connections, such as external keyboards, pointing devices, USB drives, and even chargers, to prevent them from acting as antennas. Operate the laptop off its battery, with no cable that could function as an antenna connected to it. Charge it only when it’s turned off.

**Defeating forensics requires an equally comprehensive collection of techniques designed to defeat different forensic attacks.**

- If possible, turn on as many other computers as possible in the area, so that their radiated signals will interfere at the interceptor’s site with those emanating from a laptop with sensitive information.
Digital Forensics

• Move the laptop every few minutes so that an inter-ceptor will have to readjust his settings before he can resync to and reconstruct your signal. The inter-ceptor will need such readjustments to minimize multipath interference.

In summary, even Van Eck radiation interception, an advanced attack, yet one that has been detailed all over the Internet for years, is easily negated.

Defeating Online Traffic Interception
The recommended approaches for defeating this type of attack depend on what we assume about online traffic interception: realistically, the interception will come from the ISP and not from a shady figure with alligator clips on our communications line. In general, you should establish a Secure Sockets Layer (SSL) or Secure Sockets Shell (SSH) connection with some trusted innocuous site that has agreed to serve as your staging area for connecting to whatever you want to connect to. To the extent that establishing such a connection is legally acceptable—and assuming that you trust the entity with which you make this connection—this solves the problem.

Establishing a connection to the Tor (The Onion Router) network (or one like it) is a last resort, as long as you're willing to put up with the extreme slowdown in throughput; it's also very alerting. When using this option, you should disable Java and all scripts (JavaScript, VBASIC, or ActiveX, for example).

On the other hand, interceptors often view encryption as an affront unless it appears inadvertent, such as when an employee connects to an employer's server or while a typical user places a credit-card order. In these cases, effective steganography can be preferable. The adjective “effective” specifically excludes amateurish steganography, such as most schemes that attempt to hide data in images or sound files.

Given the huge numbers of open Wi-Fi access points worldwide, you can almost always access the Internet through someone else's open and unrestrict-ed access point, such as those provided by various coffee shops, malls, and other establishments. If the subsequent connection is handled as an SSL or SSH encrypted connection to an out-of-country server, the user’s identity will be realistically impossible to reconstruct in the future.

Defeating Data Theft
When the Computer Is Off
It’s amazing that numerous effective but inexpensive products are available for implementing full disk encryption, yet most computer users don’t use them. Full disk encryption, unlike file encryption or partition encryption, provides effective protection from hostile third-party access while a computer is off. It’s effective because it protects from any and all forensic techniques: it encrypts the swap file, all temporary files, history files, spool files, and so on. Of course, the encryption key that the user chooses should be impossible to guess, even by a computer doing an exhaustive dictionary search.

Products include Pretty Good Privacy’s version 9, which offers this as one of its features, Drive Crypt Plus Pack, SecureDoc by WinMagic, and others. Each of them is available for around US$50 to $200.

Note that full disk encryption offers no protection when an authorized user leaves the computer on (or in standby or sleep mode) and the computer is connected to a network or when the user steps away and some-one else walks up to the fully enabled computer. For those situations, you must add individual file encryption over and above full disk encryption.

Defeating Remote Databases’ Data aggregation
Logically, remote databases can identify us from our IP address, any personalized cookies in our computer, or any information we volunteer to the remote site. The following recommended fixes address these concerns:

• Connect to the remote service (for example, Google) through a proxy, preferably an SSL-based one. You should ensure that the proxy anonymizes your IP address by first going to one of the many URLs that feed back to you the IP address you appear to them to be coming from.

• Remove all cookies from the computer you’re using and prevent it from writing new ones anywhere except possibly in RAM.

• Use a Web browser that doesn’t accept or store any cookies, such as NoTrax from www.heidli.de/node/7. Alternately, use Firefox in its most privacy-enhanced configuration but only after adding various add-ons, such as SquiggleSR, that send random requests to remote sites to confuse the sites about which requests you’re really interested in.

A recent paper by University of California, San Diego, researchers argues that someone with the right equipment could fingerprint your computer’s clock skew,5 which is unique even among identical models from the same assembly line. By extension, the paper argues that an attacker could track this “finger-printed” computer’s clock skew from across the world if that computer connects to a URL at which clock-skew-measuring equipment is available. If this is a concern for you, then your obvious countermea-sure is to borrow someone else’s computer—howev-er, then you’ll have to worry about what interception might occur within, or in conjunction with, that borrowed computer.
A more sinister threat is that from “Web bugs” in documents—that is, hidden HTML code that causes your computer to access a Web site every time you open the document or any copies. The fix is to open any document of suspect origin only after severing the computer's Internet connectivity.

Defeating Intrusive Border Security Confiscation

It's common these days for border-protection officials in most countries to search arriving travelers' computers, cameras, PDAs, and all other data storage media. Although you can understand nations' desire to apprehend terrorists and narcotraffickers, you’d imagine that such undesirables have developed enough sense by now to work around such simplistic interception means. The individuals who end up being inconvenienced the most are business travelers and tourists. Although even they might be willing to cooperate in counternarcotics and counterterrorism efforts, nothing limits border officials from looking at all of our data, including privileged attorney–client communications or medical information. The obvious countermeasure is to avoid carrying such data through entry ports at all; instead, you can upload it to a remote server in an encrypted form prior to travel and download and decrypt it on arrival. This is the online equivalent of vaulting over a perimeter fence.

Further Reading in Computer Forensics

The following resources are useful for further reading.

Van Eck Radiation Interception


Deleting Does Not Delete

- www.damhhave.com/LinuxOSXTricks/LinuxOSXTricks.html
- www.betologue.com/category/macintosh/pages/

HIPAA Compliance

- www.hhs.gov/ocr/hipaa
- www.hipaadvisory.com/REGS/HIPAAPrimer.htm
- www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

Counterforensics


The Sony Rootkit Scandal


Wi-Fi Attacks

- www.wi-foo.com/index-3.html
- www.pisa.org.hk/event/live-wifi-attack-defense.htm
- www.berghel.net/coll-edit/digital_village/aug-05/dv_8-05.php

Disk Wiping


Steganography

- www.jtc.com/Steganography/
- www.garykessler.net/library/steganography.html
- www.jtc.com/stegdoc/

A more sinister threat is that from “Web bugs” in documents—that is, hidden HTML code that causes your computer to access a Web site every time you open the document or any copies. The fix is to open any document of suspect origin only after severing the computer's Internet connectivity.
Defeating Remote Interception over a Network

Given the many ways whereby remote hackers and others can access a networked computer and retrieve any and all data from it, you should make a habit of having two computers: one with sensitive data that’s never connected to any network and a second that’s connected to networks but has never in its history had anything even remotely sensitive on it. The never-connected computer should have full disk encryption and Wi-Fi and Bluetooth (and soon, WiMAX) permanently disabled; ideally, it should be stored in a protected location.

Additional Counterforensic Techniques

In addition to the security measures I’ve discussed, you should consider a second tier of protective measures in the time-honored tradition of having separate layers of security and not putting all your eggs in one basket.

Encryption. Effectively unbreakable encryption is widely available today at no cost. At the same time, encryption is viewed as an affront by most investigators and law enforcers because of their “if you’re innocent, you have nothing to hide” mentality. For the average user, encryption often ends up resulting in less rather than more security—it’s such a small part of the overall process of hiding something from someone that if you haven’t attended to all the other parts, you’ll end up with a false sense of security that’s worse than no security at all. Typically, encryption won’t protect you from

• an easily guessable encryption key or one easily discoverable through a dictionary search;
• a key communicated to the intended recipient of an encrypted file through less than secure means;
• an unencrypted copy of the encrypted file that’s left behind as an ostensibly “deleted” file, one hiding in the “swap” (paging) file, one hiding in a spoof file, or one left in numerous other locations that forensics investigators routinely examine;
• a keylogger or an overhead camera; or
• Van Eck emanations interception.

Data hiding. Anyone can hide data in infinite ways, and it’s a very reputable discipline of information technology, discussed in a vast amount of open literature that in no way implies any wrongdoing.

Disk wiping. Numerous commercial and free products are available for overwriting data in computers. None are recommended because all miss some locations where data can inadvertently end up. Furthermore, overwriting a typical 1-Tbyte hard drive can take the better part of a day, which makes it impractical in an emergency.

Steganography. Hiding data in plain view is also a mature art. Although amateurish steganography, such as attempting to hide data in images, is detectable, advanced steganography isn’t and can defeat any and all computer forensics. At a bare minimum, however, you must not have any steganography software on your computer because its presence would be a tell-tale tip-off. As with any attempt at covertness, technology (such as steganography) is only a small part of the overall effort; the largest part is the operational savvy required for the overt act to be nonalerting.

Degaussing. This countermeasure is largely overestimated—it takes huge magnetic fields to degauss a hard drive. Furthermore, degaussing is useless against nonmagnetic data storage devices such as thumbdrives. You must physically destroy optical storage media (DVDs, CDs, and so on), usually via mechanical abrasion. You must overwrite solid-state memories, such as USB keys and digital camera memories, in their entirety, which is a time-consuming proposition.

Other. The imagination is the only limit in devising one-of-a-kind techniques for defeating hostile attempts to intercept data, either in transit or at rest.

Computer forensics can’t answer the fundamental question of who placed the data on the device being analyzed; this should make its findings highly suspect in a court of law. Independently, anybody who wants to can operate a computer and leave zero evidence—by operating without a hard drive and by using the many widely known countermeasures I’ve summarized in this article. In light of all the major limitations of computer forensics I’ve discussed, it’s reasonable to suspect that forensics is a dying art. Far from it! It’s a practice that investigators and attackers are using at an increasing rate because most individuals and organizations that could and should be protecting their data don’t. The problem is much worse in connection with handheld electronic devices other than computers, such as camcorders, digital voice recorders, cell phones, or GPS navigators. Each such unique device requires its own privacy-enhancing approach before you can protect its data from interception; furthermore, such ancillary electronic devices are easier to lose or steal than a bulky computer.

Forensic investigators will always have a lot of business; unfortunately, all this business will necessarily be associated with efforts to apprehend small- time crooks or to harass political dissenters. Really significant issues, such as those associated with targets of national interest, will be inaccessible to investigators because such targets use increasingly effective
counterforensics as a matter of course. Such valid targets include well-trained terrorists and narcotraf-
fickers who aren’t intimidated by laws banning this or that privacy-enhancement technique—such indi-
viduals and organizations ignore laws anyway.

References
1. R. Anderson and M. Kuhn, “Soft Tempest: Hidden Data Transmission using Electromagnetic Emanations,” In-
3. J. Alex Halderman et al., “Lest We Remember: Cold Boot Attacks on Encryption Keys.” Proc. Usenix Secu-

Michael A. Caloyannides works for Northrop Grumman and is an adjunct member of the faculty of Johns Hopkins and George Washington Universities in computing security and networks. He has worked as a senior scientist in private industry as well as in a US government agency, the latter of which awarded him its “Scientist of the Year” award. He also consults for a number of attorneys and gave an invited presentation on forensics to the Federal Judges Convention in Alexandria, VA. Caloyannides has a PhD in electrical engineering, applied mathematics, and philosophy from the California Institute of Technology. Contact him at micky@ieee.org.

The IEEE Computer Society Career Center is the best niche employment source for computer science and engineering jobs, with hundreds of jobs viewed by thousands of the finest scientists each month - in Computer magazine and/or online!

The IEEE Computer Society Career Center is part of the Physics Today Career Network, a niche job board network for the physical sciences and engineering disciplines. Jobs and resumes are shared with four partner jobboards - Physics Today Jobs and the American Association of Physics Teachers (AAPT), American Physical Society (APS), and AVS: Science and Technology of Materials, Interfaces, and Processing Career Centers.

For more information on any topic presented in IEEE Security & Privacy visit the IEEE Computer Society Digital Library at www.computer.org/csdsl

RUNNING IN CIRCLES LOOKING FOR A GREAT COMPUTER JOB OR HIRE?

The IEEE Computer Society Career Center is the best niche employment source for computer science and engineering jobs, with hundreds of jobs viewed by thousands of the finest scientists each month - in Computer magazine and/or online!

> Software Engineer
> Member of Technical Staff
> Computer Scientist
> Dean/Professor/Instructor
> Postdoctoral Researcher
> Design Engineer
> Consultant

The IEEE Computer Society Career Center is part of the Physics Today Career Network, a niche job board network for the physical sciences and engineering disciplines. Jobs and resumes are shared with four partner jobboards - Physics Today Jobs and the American Association of Physics Teachers (AAPT), American Physical Society (APS), and AVS: Science and Technology of Materials, Interfaces, and Processing Career Centers.