


HUB Canada



KONICA MINOLTA

# DiMAGEine the possibilities

**HUB**

DIGITAL LIVING

Photo/Video Imaging  
Brought to you by  
KONICA MINOLTA

Audio

Mobile

Personal Computers

Entertainment

Home Electronics

Classifieds Shopping Guide Contests Media Kit

[e-mail this story](#) [printer friendly version](#) [post a comment](#)

## Sherlock Holmes meets data

By Dave Chappelle posted on 12/5/2002



Volunteers tracked down an individual trading child pornography online and notified the FBI, who discovered it was a juvenile living in Pennsylvania. The case was turned over to state authorities, but not before an FBI agent had unsuccessfully attempted to contact the juvenile's parents, and left his business card in the door. The mother came home, found the card, called the FBI, and invited them and state police to talk with her son the next day.

That night the son deleted his hard drive partition and reinstalled the operating system. Short of sending the drive to a full-fledged data recovery lab, the evidence was gone. However, because of the timeline of the traded images, his IP address, and his partition deletion, a case could still have been made against him--especially for willfully destroying evidence. Formatting and partitioning a drive establishes a "consciousness of guilt" says Mike McTavish, supervisor of the Pennsylvania State Police computer crime unit.

The police decided not to go to the considerable expense of pursuing this particular case, but had they chosen to, they would have an arsenal of tools at their disposal. Welcome to the world of computer forensics.

In addition to law enforcement work, McTavish is an instructor with Guidance Software ([www.guidancesoftware.com](http://www.guidancesoftware.com)) which has developed a powerful Windows-based computer forensics application called EnCase. Guidance Software is a classic "started in a garage" (by a police officer)

**INFLUENCE**

police officer,  
success story that  
now has more than  
100 employees.

**DIGITAL****LIVING**

Along with selling the software, it trains forensic examiners, and many police officers, including some from Canadian policing agencies, have gone through the training.

Guidance Software defines computer forensics as the acquisition, preservation, and analysis of digital information that meets the requirements of evidence for court presentation. Digital evidence can come from many sources, including a hard or floppy disk, USB drive, CompactFlash or SmartMedia cards, CD-ROMs, or any other data storage media.

The forensic process includes three stages: processing a case, obtaining evidence, and storing that evidence. In our legal system, rules of evidence are fairly strict, and it must meet a certain standard before it can be presented in court.

For example, it's a lot more complicated than simply snooping around a suspect's drive using Windows Explorer. Simply booting a Windows computer alters date and time stamps and the content of the Recent and Temporary folders. In short, even the boot process and opening of Windows Explorer changes the contents of the drive, potentially undermining the integrity of evidence police may be trying to gather. If the data has been changed too much, it may not be admissible in court.

Preserving evidence for examination requires special software and techniques. DOS-based utilities used to be popular, but are limited in function and require a lot of time to be used effectively. This is where EnCase has established its following, being faster and more capable than the older tools.

Computers hold evidence better than filing cabinets, because while a paper document can be easily shredded, deleting a document from a computer disk merely deletes the file header. The file can still be located with the right tools.

"The data is there until it is overwritten," says Terry Willis, a detective with the Los Angeles Police Department computer crime unit and part-time EnCase instructor. "A suspect can upgrade a computer, format his old drive, and give it to his kids. If the kids haven't overwritten the original data, it's still there."

Willis says his jurisdiction includes Los Angeles International Airport, a hotbed of laptop theft, and EnCase is routinely used to recover them. Officers visit local pawnshops and run the software on laptops for sale. Unallocated clusters often reveal residue of an old OS (and previous ownership).

### **Escalating cat and mouse**

Because courts around the world have accepted EnCase as a standard, commercially available forensic software application, defence attorneys have switched from attacking the accuracy of the software to attacking the methodology of the operator, or forensic technician. This makes training important--and is also the reason why Guidance Software has an extensive and busy training facility in California.

Instructors are full-time law enforcement officers who use their vacations to teach. They are also very experienced with EnCase, having used it to collect evidence and present testimony in court.

The opportunity to convict child pornographers and other criminals is a major motivation for forensic examiners. What else attracts people to the world of computer forensics?

"It sounds corny, but you're getting insights into someone's true being. People do things on their computers they'd never do elsewhere" says Mike Fowler, a senior enterprise instructor with Guidance Software. (Fowler also

Flower, a senior enterprise instructor with Guidance Software. (Flower also has 14 years experience in law enforcement, and several more in private-sector network security.) "It borders on voyeurism, because you're looking at a portion of someone's life they figure no one else will ever see."

Most investigations involve files that a user thinks no longer exist. Recycle bin unallocated clusters can still contain data, even after a drive has been reformatted. On confronting users with evidence of suspicious files, investigators say they are frequently told that someone else must have put the incriminating files on their system, or that the OS put them there. However, those trained in forensics know better. "Stuff in the recycle bin is only put there by the user, not the OS," says Willis.

#### **What do they look for?**

Part of the investigation of a PC is a signature analysis, which determines if file headings and extensions match the file type. EnCase allows an examiner to match all three (Windows looks at file extensions, not the header).

Changing a file name or extension is a common method of hiding files--a step that can be incriminating evidence itself.

Date stamps can also be changed in an attempt to make it appear that the perpetrator was not aware of the crime, or that someone else added the file later. These attempts are easily found using EnCase.

Illegal images are also frequently inserted into document or text files. Software-savvy offenders have also been known to insert pornographic images of children into otherwise innocuous images, or to cover them with a white layer to make them appear blank. Signature analysis helps an examiner find these discrepancies.

EnCase can perform five file sorts simultaneously, looking for deleted and overwritten files, unallocated clusters, and all other file types.

Once an investigator finds something that might be useful, a sweep is performed, saving the relevant data to the bookmark portion of the evidence file.

Keyword searches are a major function of EnCase, but searches based on individual keywords can be time consuming. "The electronic file cabinet can be overwhelming," says Willis. Also, suspects aren't necessarily good spellers, or may intentionally misspell file titles. So, EnCase allows unlimited searches, and groups of searches, flexible and fully customizable by the examiner.

Here's how it might work. Suppose the system being examined is believed to have been used to commit credit card fraud. The user may have tried to hide the credit card numbers by entering them as one long number, or as a single long string with spaces or hyphens in between. To shorten search time something called GREP expressions are used. When properly written, a GREP expression can turn up numerous relevant keyword hits in a single search.

EnScripts might also be used. These are scripts written to save time when performing searches. The Guidance Software Web site has a members-only message board, where forensic examiners share information, EnScripts, GREP expressions, and other timesaving techniques.

This sharing of information has a Canadian twist too: instructors lavish high praise on Robert Gagnon, of the Ontario Provincial Police's e-crime section, who developed a network boot disk for EnCase investigations. Using one per machine, investigators can perform triage on multiple systems of a network without actually booting the individual computers into the native OS, thereby maintaining data integrity. No matter what network cards are installed, with this boot disk every computer in a room can be searched relatively quickly.

this boot disk every computer in a room can be searched relatively quickly. Once evidence is uncovered, the suspect machine(s) can be removed without shutting down a business.

Police have been known to shut down all computers when executing a search warrant for digital evidence at a business. If only one employee is the culprit, shutting down the entire business leaves police open to heavy criticism, if not a lawsuit. The network boot disk avoids that problem.

### **Beyond criminals**

Willis estimates that the LAPD uses EnCase in 95 percent of its computer-related investigations. Its use is not limited to law enforcement, though. Tim Margeson of data recovery firm CBL Technologies says its technicians frequently use it for a quick look at what's on the disk to be recovered. This is particularly useful when a customer needs their data recovered in a hurry.

Margeson says the keyword search function in particular is very handy, because searches performed on email address or subject names allows them to retrieve individual email messages without having to go to the hexadecimal level.

Can EnCase recover any piece of data? No. While it will read data after a format, it can't recover data that's been overwritten or encrypted files. As well, files that have been run through a program like Shredder ([www.gale-force.com/shredder](http://www.gale-force.com/shredder)) will render data unreadable by EnCase. However, most criminals merely want the goods, and usually don't use these protection methods until after they've been visited by the law.

---

### **SIDEBAR:**

#### **Tales from the computer forensic front**

##### **The chatroom tip off**

An individual in Ontario was chatting online with someone in Pennsylvania during school lunch hour. Claims about a bomb in the Pennsylvania school were made during this chat. The Ontarian notified RCMP, who notified Pennsylvania State Police, who raced to the school before classes let out for the day. To determine who made the bomb threat, all students were detained while all library computers were forensically searched and the validity of the threat ascertained.

##### **Disgruntled employee**

Much computer crime involves disgruntled employees stealing trade secrets or customer contacts and erasing data from an employer's systems. Terry Willis, a detective with the Los Angeles Police Department, recounts a slightly different case in which an art gallery employee set up a Yahoo account in the name of the employer, then used the account from home to email all clients a notice that the gallery was going out of business and to ignore the invitation to the next show.

A gallery sys admin discovered evidence of the Yahoo account creation. Under a search warrant LAPD officers used EnCase in Preview Mode to see the incriminating email, in the suspect's home. She received 90 days in jail and three years probation, and her future wages were garnished to cover the loss of business to the gallery.

##### **Building an airtight case**

Evidence taken from computers often forms only a portion of that necessary for an arrest. Investigators liken the task of case-building to gathering enough threads to make cable strong enough to prosecute an offender.

Mike McTavish, supervisor of the Pennsylvania State Police computer crime unit, recounts the case of finding the body of a woman in her 20s, found wrapped in a carpet in a garbage dump. Regular investigation found that the

wrapped in a carpet in a garbage dump. Regular investigation found that the woman's boyfriend had a company van and laptop. Matching carpet fibres were found in the van, but that wasn't enough.

Further investigation showed her to be a frequent visitor to numerous astrology sites, some of which required a password. Using EnCase to search the laptop, investigators found pages from astrology sites in the temp and cache folders, accessed within four hours of the estimated time of death. When the boyfriend couldn't provide the site passwords, the fibers and evidence that she had used his laptop so close to the time of her death helped convict him of first-degree murder.

#### **Email trail**

An individual's email is where police are most likely to find an admission of guilt, or indication that a crime has been committed. Few people are aware of email encryption tools, and fewer still can be bothered using them.

LAPD established a motive for murder by searching a man's email after the bodies of his wife and daughter were found in Los Angeles Harbor. Investigators found an email from the man to another woman living outside the country, stating that a "new life" could be started once the "old life" was gone.

#### **Timing is everything**

Windows' Recent and Temporary Internet folders are good places to look for the last actions performed on a system.

A 4:30 a.m. call to a Pennsylvania 911 operator involved a juvenile who had been stabbed in the head at his home. He told police his father had done it, but both parents denied it. Responding officers noticed an active connection on the home PC, and called the computer crime unit. From an activity timeline, an examiner concluded someone had been using the computer to view child pornography until roughly 15 minutes before the 911 call. It turned out the son had refused his father's demands to mimic what he had been viewing online, so the father stabbed him.

--Dave Chappelle

### **Comments**

#### questions

Posted by: [Anonymous](#), 1/6/2003 3:26:00 PM

Jan 7, 03

Dear Computer Paper,

In your cover article starting on page 12 (Jan 2003, by Dave Chappelle) you mentioned with the right training a person is able to recover data from a computer even after using the recycle bin and reformatting the drive. I am selling my computer and Zip disks and since they were used to store my personal banking info, passwords, notes etc, I want to be darn sure that none of this is retrievable by the next owner. Can you explain to me how I can erase everything 100% (I'm using win 98), or tell me where to get the information on how to do it (specific sites or books), or who I can call (local business or computer nerd). Keep in mind I am a home user not a business.

Ps: Could I use a magnet to erase the Zips?

Pss: I noticed that Internet Explorer stores all my past visited sites in the address area. Is there a way to delete all these (I use:  
Start/Settings/Taskbar & Start Menu/Start Menu Programs/Documents

Start/Settings/Taskbar & Start Menu/Start Menu Programs/Documents Menu/Clear and also delete the Windows/History folders. It still does not really get rid of them all).

Thanks, Karl (Vancouver, BC)

krrrl@netzero.net

### Editorial note

Posted by: [Dave Chappelle](#), 1/7/2003 12:02:22 PM

*Dave Chappelle responds:*

*Thanks for your letter, Karl.*

*You can delete items in your Internet Explorer (IE) History folder from the Clear History button in IE. You must also Delete Files, also known as cache. The Address Bar and History folders will appear full until you close and restart IE.*

*Use Windows Explorer to access the Temporary Internet Files and delete those.*

*You probably have a disk full of cookies, which will indicate everywhere you've been on the Web. Use Windows Explorer to find your cookie folder, and delete everything in there except "Index".*

*Regardless of what you delete, the Temp and Recent folders will contain roughly the last 15 or so things you've done and looked. Close all applications and documents, and wipe those out too.*

*After doing all this deleting, empty your Recycle Bin.*

*As for your Zip disks, your magnet would have to be very powerful to have any effect. To be safe, delete your data, format them, and then fill them with other data that is non-sensitive in nature. Delete again. If anyone wants to restore the data, it won't affect your banking statements.*

*Most people think formatting a hard drive will wipe out data, but as you read in the article, that's not the case. You've got to re-install the operating system. Even then, parts of data may still reside in "file slack". Thankfully, the data particles will only be readable to those with the proper training and software tools. Most of those people are busy solving crimes, not perpetrating them. Still, it pays to be safe, and you're wise to be interested in protecting yourself.*

*The best way is to delete your hard drive partition, and then create a new one. Format the new partition, and install the operating system on your drive. To delete and create partitions, use FDISK, a DOS program available in Win9x setup files. It's simple to use. You should find tutorials on the Web.*

*There are commercial programs that claim to delete data from file space, such as Shredder (<http://www.gale-force.com>), File Wipe (<http://www.alberts.com>), Evidence Eliminator (<http://www.evidence-eliminator.com>), File Assurity (<http://www.articsoft.com>), and others you can find by searching on the Web. Some vendor sites scream dire warnings of your computer vulnerability. Don't be too quick to believe them. They*

*of your computer vulnerability. Don't be too quick to believe them. They claimed our system was dangerously open, even when behind a corporate firewall using Network Address Translation.*

*Dave Chappelle's new computer security book for home users will soon be available: Protect Yourself Online: How to Cover Your Assets Every Time You Log On. <http://www.wordsmithville.com/PYOPitchWSM.html>*

**trader**  
classified media

[about us](#)

·

[permissions](#)

·

[editorial policy](#)

·

[view our TV ad](#)

**HUB Pickup Locations!**