

Knowledge of Computer Forensics Is Becoming Essential For Attorneys in the Information Age

BY STEVEN M. ABRAMS WITH PHILIP C. WEIS

The matter began as just another child custody hearing. The wife's attorney had asked for the hearing after the husband had made a threatening phone call. Claiming to be in the parking lot of the store in which the wife worked, he had let her know that he was looking through a telescopic sight, and that each person in the store was visible and within range of his firearm.

The wife's attorney fully expected that after the judge read the police report of this incident he would grant custody of the couple's 3-year-old child to his client. So he could hardly believe his eyes and ears when, rather than disputing the allegations in the police report, the husband's attorney instead placed a stack of printed e-mail messages on the judge's bench. The e-mails appeared to have been sent from the wife to various men who frequented a chat room called, "MARRIED AND CHEATING IN HICKORY."¹ Most damning of all, the e-mails had an attached digital image file that appeared to be a pornographic picture of the wife. This had been printed out and was attached to the materials given to the judge.

Based on these materials and the husband's assertions that the wife had been advertising for sexual liaisons on the Internet, the judge issued an order awarding custody to the husband. The wife was to have only limited and supervised visitation. The wife, her family and attorney were stunned by this completely unexpected outcome. The author was thereafter engaged to investigate by the wife's attorney.

The balance of the story is at the conclusion of this article, but it cannot be fully understood without some understanding of the new world of computerized evidence. As the biographical thumbnail indicates, the author is not an attorney, but rather a licensed private investigator specializing in computer forensics and computer crime investigation, focusing on civil domestic matters. The focus of this article therefore is not detailed legal analysis, but rather a technical and practical overview of this relatively recent but increasingly vital part of the legal profession.

The New Specialties: Computer Forensics And Computer Crime Investigation

"Computer forensics" is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, pagers, PDAs, digital cameras, cell phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding.

"Computer crime" investigation includes such endeavors as detecting and stopping hackers, as well as other criminals who use the Internet as the instrumentality of their criminal enterprises. Catching them often involves tracing and verifying e-mail messages, or setting traps on the Internet in the hope of reeling them in.

Most computer forensics specialists and computer crime investigators fall into one of two narrow categories: those who work for law enforcement agencies exclusively on the prosecution side, and those who work as information security experts for large corporations. That latter group focuses on keeping hackers, disgruntled employees, and other like-minded individuals from attacking the company's information resources.

The tools of the trade vary, but certain standards have developed. Although many over-the-counter software



STEVEN M. ABRAMS, M.S., P.I. is trained in computer forensics under law-enforcement supervision, and has a degree and additional certifications in computer science and electronics. He also has more than 20 years' experience working with large computer hardware and software manufacturers, and is the principal of Steve

Abrams & Co. in Mount Pleasant, S.C. He recently has been accepted for membership in the Associated Licensed Detectives of New York State.

PHILIP C. WEIS assisted in the preparation of this article. He is law secretary to Hon. Robert Roberto Jr. (Supreme Court, Nassau County), and is associate editor of the *Journal*.

programs that are available at retail business software stores can be used, more expensive but industry-established tools are preferred by professionals. These programs have already been proven to produce scientifically reliable evidence that can be used by a computer investigations expert as part of the expert's testimony.²

Three industry associations exist, and their names should be known to attorneys who are considering hiring a computer investigator. These organizations establish minimum training standards for computer forensic examiners, and promulgate industry-accepted and recommended procedures for the forensic examination of various types of computer media and electronic data storage devices. The largest and most respected of these include IACIS (International Association of Computer Investigative Specialists) and HTCIA (High Technology Crime Investigation Association). IACIS membership is restricted to sworn law enforcement personnel and full-time civilian employees of law enforcement agencies. Like IACIS, HTCIA membership consists mainly of sworn law enforcement officers and agents. However, unlike IACIS, civilian computer forensic specialists can also become members of HTCIA, provided they pass background screening. They also must agree not to work for defense counsel in a criminal matter, and need the sponsorship of two existing HTCIA members (preferably law enforcement personnel) who are familiar with their qualifications.

A third organization, HTCN (High Tech Crime Network), also certifies computer forensic examiners and computer crime investigators who can meet rigorous standards for training and computer forensic investigation experience. HTCN is the only organization that currently offers certification for those who are not sworn law enforcement or full-time civilian employees of law enforcement agencies.³

Initial Concerns of an Investigative Search

A person who performs computer forensics must have more than technical knowledge, however; an understanding of how to perform the work legally is critical. Relatedly, the work must be done in a way that preserves the value and admissibility of the evidence collected. This requires the investigator to always maintain a well-documented chain of custody, and to follow industry-established procedures for the collection, preservation, and documentation of the data. At no time should the evidence media ever be altered by the investigator. (A more detailed discussion of how the work should be performed appears below.)

Clearly, when called on to search a computer the best strategy is to obtain consent, especially written consent, from one of the adults with access to the system to be searched; in general, if the search is of a home computer,

any adult with such access can do so.⁴ Without a valid consent (or, of course, a court order granted as part of the discovery process in a pending action), the investigator, and possibly the person who hired him or her, runs the risk of criminal and possible civil liability under both state and federal statutes.⁵

Even if consent is obtained, however, not all files will be immediately available, because some may be password-protected. The person giving consent may not know the passwords. Further, the person consenting may have specifically exempted such files from the consent. Software such as the Password Recovery Tool Kit (PRTK), by Access Data Corp.⁶ can make quick work of cracking most password-protected application data files, but doing so raises the specter of a statutory violation, at least in a context other than a domestic relations matter.⁷

Although Fourth Amendment considerations that affect government searches seldom come into play for a private investigator who is not acting as an agent of the government, one must, as indicated above, be wary of committing an offense under New York State or federal law. One of the most common concerns has to do with reading someone else's e-mail. Unopened e-mail, while it is on the Internet service provider's (ISP's) mail server, may be viewed as "in transit" because it has not yet been read by its intended recipient. After it is downloaded by being opened, a copy generally will then exist on the computer's hard drive or other memory area, and thus may be seen as "in storage."

Some federal courts have made a distinction between the two with regard to liability under the Federal Wiretap Act. Under this view, accessing e-mail before it is read would be a violation, while a review after it is opened may not be.⁸ However, this is an area of the law that is not well-established; as one federal appeals court has noted, "[U]ntil Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law."⁹

Some matrimonial attorneys and private investigators advise their clients to install spy software on the family computer to catch a cheating spouse's chat room and e-mail communications. If the software works by capturing keystrokes or e-mails that are on the computer's hard drive, it is probably legal, subject to the concerns expressed above.¹⁰ However, if it operates by catching the messages from the Internet data stream, they probably violate wiretap restrictions, especially if the software itself forwards the e-mail or chat room text to another e-mail address over the Internet. Although it is unlikely that prosecutors will bring wiretap charges against a spouse in domestic litigation situations, it is certainly possible that attorneys and other legal advi-

sors could be at risk by giving this kind of advice – the use of the software has to do not only with data on the client’s spouse’s computer, but with the operation of the commercial electronic mail system itself.

For a valuable discussion of the federal rules for seizing and searching computers, members of the public can visit a Department of Justice Web site.¹¹ Although the manual found at this site pertains to criminal investigations, it can serve as a useful guide to attorneys in civil practice, especially with regard to the admissibility of evidence obtained from a search.

What a Search May Yield

Assuming that the investigator has acted legally, the next question is what his or her search might yield.

A search of the family computer often yields a bounty of financial records, personal correspondences, and other probative material that can outshine almost any other source of discovery in a civil or domestic relations case. In most instances, and as noted above, either spouse can consent to a search of the family computer, even if the other spouse, or an unemancipated minor child, objects.

It is fair to say that a good part of the value of a competent computer search lies in the fact that many people who know something about computers have an unjustified faith in their ability to hide digital information. Although it is certainly better than the time-honored act of burying the second set of books in the backyard, it is far from fool-proof, and complete reliance on encryption and passwords can prove costly.

An example drawn from the author’s own experience may make the point. In a domestic relations case, a hard drive contained financial records for a husband’s professional practice. The computer was marital property, and the wife could and did consent to a search. The forensic examination led to the identification of a series of Quicken files containing the financial records of the business, as well as personal investments. A few of the Quicken files were password protected, but, as noted above, the Password Recovery Tool Kit can decrypt the passwords used in most common Windows applications. This tool, apparently unknown to the husband or his attorney, is capable of breaking passwords in seconds. (It should be pointed out that the company that produces this product restricts access to this and another similar program to prevent misuse.) The husband first gave consent to search all his files during discovery.

At trial, the husband’s attorney was shocked to find out that the password-protected files had been opened

and reviewed. The consent that allowed a search of all his files was apparently based upon the husband’s mistaken belief that the password-protected files could not be read, but they were. What they revealed was a second set of financial records for the business, combinations to two safes the husband had in his home office, pornography, and notes the husband had written to himself about his strategy for limiting the amount of money he would have to divide with his wife as a result of the divorce. As one might imagine, he was not happy with the disclosure.

The Mechanics of a Search

Without attempting to give a short course on the more technical side of an investigation, it is important for an attorney to know at least the basics of how a search is conducted.

The first step in most computer forensic examinations is to make an exact copy of the data residing on the evidence hard disk (or other electronic digital storage device). This copy is made on a forensically sterile examination media (usually another hard drive or a CD-

ROM). This must be done because a search conducted on the original creates both the actual and perceived problem that the original has been corrupted or altered by the person performing the analysis, rendering it subject to a disqualifying objection. The

copy is what is actually evaluated but, as noted, it must be exact. There are three paramount considerations at this step.

First and foremost, the copy procedure must maintain the integrity of the original media. For this reason, making a copy from within a Microsoft Windows environment is usually not acceptable because Windows automatically writes and updates time and date stamps on each file during the copy operation. This changes the data on the source drive and violates the integrity of the original (source) media. There are hardware write-blocking devices that can be used to protect source media from these automatic changes made by Windows. By using a write-blocking device, the Windows version of Guidance Software’s EnCase or Access Data’s FTK Forensic Explorer can safely be used to image an evidence drive.

Although these devices are catching on with computer forensic technicians, many still use MS-DOS or Unix / Linux command line utilities for forensic imaging because these programs do not write on the source drive during the copy operation. In the MS-DOS envi-

CONTINUED ON PAGE 12

Many people who know something about computers have an unjustified faith in their ability to hide digital information.

ronment, the disk image utility Fastback, and the DOS boot disk version of EnCase are popular. In the Linux environment the DD utility and a GUI (graphic user interface) tool called SMART are becoming popular.

The second consideration in making a forensically sound copy is that the media onto which the copy will be placed must be "forensically sterile." This requires that any previous data be removed from the copy media with a software-wiping program that is proven to remove all data from the drive. Merely reformatting a hard drive does not actually remove all files from the drive, a fact that has caught many a cyber-criminal. Access Data Corp., Maresware, and other companies sell wiping programs that have been proven to remove all data from hard drives. Special care should be taken with any wiping software that runs from within a GUI environment such as Windows, because it is usually not possible for these programs to completely access all areas of the hard drive. Any data left behind during the wipe procedure will corrupt the forensic copy of the evidence drive, and could jeopardize the entire case.

The final consideration concerns time. Once the copy is made, the forensic examination is performed using any of a number of tools. The most popular tools in the Windows environment are Guidance Software's EnCase, and Access Data Corp.'s FTK. In a typical hard drive that contains the Windows operating system, programs, and data, there may be 30,000 or more individual files. Inspecting each file manually could take weeks, if not months. Using these forensic tools can dramatically cut the amount of time required.

By eliminating known "innocent" files such as an operating system and off-the-shelf program files, as many as half the files on the hard drive may be ignored. The way these forensic tools accomplish this recognition of known program files is by use of a "hash" algorithm. A hash algorithm uses a mathematical formula to compute a unique value from each byte of data in a file. A hash is very much like a digital fingerprint that uniquely identifies a particular file. The MD5 (Message Digest 5) hash is the most common hash algorithm in use. By computing a hash code from each file on the evidence drive, and comparing the hash against a database of hash values for all known commercial software and operating system components, the forensic software can flag each of these files as known, and they can therefore be safely ignored by the investigator.

The other initial processing typically done by forensic software is to create a key word index of all words and letter combinations on the evidence drive. This allows for lightning-fast searches for certain words, such as names, or keywords (example: "bomb") that may become of interest during the investigation of that evi-

dence drive. Another feature common to forensic software is the ability to identify and flag certain types of files, such as encrypted files, deleted files, graphics files, documents files, spreadsheets, databases, e-mails, etc. Viewers are provided to properly display each file type.

After the analysis is complete, these forensic tools produce printed reports that summarize all the evidence collected, including copies of e-mails, and thumbnail illustrations of key graphics files.

The Internet Factor

Just as there are specific software applications that have been created to assist with the forensic examination of data storage devices, there are tools used to analyze and verify e-mail, and to detect and catch hackers. This, of course, brings us to the Internet. Tracing and tracking e-mails and criminals through the Internet is possible because the communications protocol that serves as the backbone of the Net, known as TCP/IP, assigns a unique four-byte identifier to every computer device connected to the Net.

Referred to as an IP address, this identifier is often represented as four decimal numbers separated by dots, such as 123.23.12.13. Each Internet service provider (ISP) is assigned a range of IP addresses that it, in turn, assigns ("leases") to its subscribers. Some subscribers have static IP addresses that never change; others are assigned different IP addresses each time they connect to the Internet. In this latter case, ISPs maintain log files that show who was assigned any given IP address at a given date and time. However, these logs are only maintained for a matter of days or weeks, depending on the policy of the individual ISP.

The IP address of the sender is usually found in the header information that is sent with each e-mail message. Using relatively simple network tools, it is possible to get the name and contact information for the ISP who is assigned the IP address. By presenting the ISP with a search warrant in a timely manner, law enforcement can get the name and address of the subscriber who was assigned a particular IP address at a given time. It was by tracing the IP address from an e-mail sent to the media that the FBI was able, with the help of Pakistani authorities, to track down the murderers of Daniel Pearl. They were traced through a Pakistani ISP to a cyber-café in Pakistan. From that point conventional police work netted the culprits. In a civil matter, the ISPs generally will honor a court order and produce subscriber information in a similar manner to a warrant in a criminal matter.

It is important to note that e-mail headers are easily forged, especially the "from" and "reply to" fields in the

header. One should be particularly suspicious of e-mails coming from any of the free Web-based e-mail services such as Hotmail and Yahoo. These e-mail headers are the simplest to forge and sometimes the most difficult to detect. For example, any Hotmail user can easily forge the from and "reply to" addresses in a Hotmail e-mail, and make it appear that another Hotmail user had sent it, because the rest of the headers will appear exactly as they would had the apparent sender been the actual sender. As a rule, an investigator should assume that the user information given when signing up for these free accounts is completely false. In the case of e-mail services that are not free, such as AOL, the credit card information, at least, is usually correct, and that can be a starting place for an investigation.

"Married and Cheating in Hickory"

The author's involvement in the case that opened this article serves as a good example of how the foregoing applies to actual court matters.

I received an urgent call from the wife's distraught attorney on a Sunday morning following the developments in court described above. After he explained the particulars of the custody hearing and described the e-mail evidence, he asked if there were any way to verify whether these e-mails were real. His client and her father claimed that on the date the e-mails were allegedly sent she had no access to a computer, and that she was not the person depicted in the photo. The husband, I was told, was a computer programmer with access to his wife's Hotmail e-mail account and to various computers.

The next morning the wife's father and her attorney came to my office with a copy of the e-mails and the photo that had been given to the judge. In addition to the e-mails was a printout showing a transcript of a chat room ("Married and Cheating in Hickory"), in which the recipients of the e-mails were listed as participants.

I made note that the wife's e-mail address was not listed as a participant on the transcript, and that there was no evidence that she had ever been to that chat room. I also noted that the printed e-mails had no header information and were created using a free (and therefore unverified) Hotmail account. I was already skeptical of its authenticity because the computer-programmer husband had not seen fit to print the e-mail

headers, something he would be likely to do if he wanted to prove the validity of the e-mails. There was also a digital picture of a computer screen showing an Outlook Express inbox containing several e-mails, including a copy of the wife's alleged e-mail.

The key is to quickly identify and retrieve the pertinent facts before they are erased forever, and to subject the data to a fair and rigorous review by a trained expert.

Contacting the wife by telephone, I was given her Hotmail account password, and an immediate examination of the account revealed no evidence that the e-mails in question had been sent from that account. For example, none of the e-mail addresses that were recipients of the e-mails in question were in the address book.

Among all the many e-mails the wife had received, there was no e-mail from any men listed as members of that chat group. There were no pornographic pictures in any e-mail.

The most interesting clue in the pages given to the court was the photograph of the Outlook Express inbox. Along with suspect e-mail there were several e-mails from the online auction site eBay. As with all e-mails from eBay, these contained unique transaction numbers in the subject line of each e-mail. I was able to use the transaction numbers to trace the e-mails to a particular eBay user, and from the online payment site PayPal was able to get a name and address for that eBay user. It was none other than the husband's sister. That left me with this question: *Was it reasonable for the wife to send an e-mail and a pornographic photo to her sister-in-law in the middle of a divorce proceeding?* The husband contended that the e-mail was sent to the sister-in-law because it contained a hidden virus meant to infect the sister-in-law's computer.

However, once I learned that the husband maintained a large collection of virus programs on a set of CD-ROMs, the focus shifted back to him as a likely source of a virus and the e-mail.

For all the reasons above, I was convinced that the e-mails could not be verified to have come from the wife and they therefore should not have been given the weight ascribed to them by the judge. I wrote a report and an affidavit detailing my investigation and conclusions. The report was given to the guardian *ad litem*, who was charged by the court with evaluating the custody situation.

As odd as it may seem given the heated nature of the proceedings, the case ultimately ended because the couple reconciled. (Whether this was in the child's best interest I leave to others.) There was therefore no need for my testimony in open court. It should be noted that the

guardian had wanted forensic analysis of the husband's sister's computer, but without consent we would have needed a court order to conduct the investigation. The information was probably long gone in any event – the ISPs likely have long since purged any log files that would have settled the matter regarding who actually sent those e-mails.

For purposes of this article, the lesson to be taken from the case is that the judge and attorneys were misled by evidence that was of little probative value – and that the law has lagged behind the technology that can be used to manipulate it.

Conclusion

Electronic evidence can be powerful, but it is often perishable and transient, and can be misleading. The key is to quickly identify and retrieve the pertinent facts before they are erased forever, and to subject the data to a fair and rigorous review by a trained expert. Courts need to provide expedited hearings in these matters so that appropriate court orders can be issued to compel the forensic examination of vital electronic evidence, and to compel ISPs to hand over log files crucial to these cases before data is lost.

Where the court is uncertain of the procedures to follow, or lacks the expertise to properly evaluate electronic evidence, special masters, who themselves are experts in the field of computer forensics, should be appointed to aid the court. In the 21st century, the American legal system must adjust to new technology, as it has in the past.

1. To protect the identity of the parties the name of the city has been changed.
2. See generally *Daubert v. Merrell Dow Pharm.*, 509 U.S. 579 (1993); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999).
3. More information on these certification programs is available at the HTCEN Web site, <http://www.htcen.org>.
4. See *U.S. v. Smith*, 27 F. Supp. 2d 1111 (C.D. Ill. 1999) (live-in companion could consent to search of other party's computer, even though she used it only occasionally).
5. See Penal Law art. 156 (Offenses Involving Computers); 18 U.S.C. § 1030 (Computer Fraud and Abuse Act); 18 U.S.C. §§ 2510–2522 (Wiretap Act); 18 U.S.C. §§ 2701–2712 (Stored Communications Act). The federal statutes are penal in nature but also expressly provide for a private cause of action (18 U.S.C. §§ 1030(g), 2520, 2707); the New York Penal Law does not. One state court has held that no such private right can be implied. *Lawrence v. State of N.Y.*, 180 Misc. 2d 337, 688 N.Y.S.2d 392 (N.Y. Ct. Claims 1999).
6. <http://www.accessdata.com>.
7. See *People v. Angeles*, 180 Misc. 2d 146, 687 N.Y.S.2d 884 (Crim. Ct., N.Y. Co. 1999); see generally *People v. Versaggi*, 83 N.Y.2d 123, 608 N.Y.S.2d 155 (1994). There does not

appear to be any published New York authority to the effect that a spouse's password-protected files must be considered excluded from the other spouse's consent, or even the spouse's own general consent to search the computer. Given the general ability of either spouse to consent to the search of a family computer, it appears that the objecting spouse would have a difficult time convincing a court that information found in them should be inadmissible on the sole basis that they were password-protected.

8. *Eagle Investment Sys. Corp. v. Tamm*, 146 F. Supp. 2d 105 (D. Mass. 2001); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001); *Steve Jackson Games v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); but see *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir.) (refusing to distinguish stored communications from those in transit for purposes of the Wiretap Act), *opinion withdrawn*, 262 F.3d 972 (9th Cir. 2001) and *substituted opinion*, 302 F.3d 868 (9th Cir. 2002).
9. *Konop*, 302 F.3d at 874.
10. The Stored Communications Act makes it illegal for an unauthorized person to access stored electronic information (18 U.S.C. § 2701(a)), but if the home computer loaded with this software was one to which the "spying party" had routine and unrestricted access, liability under the statute seems doubtful.
11. <http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm>.