

Ensuring the Admissibility of Electronic Forensic Evidence

Friday, 25 August 2006

Last Updated Friday, 25 August 2006

Originally Published in Criminal Justice Magazine, Spring 2004, Volume 1

By Fred Galves and Christine Galves

Fred Galves is a law professor at the University of the Pacific's McGeorge School of Law in Sacramento, California. He teaches evidence, civil procedure, pretrial litigation, and computer-assisted litigation and has written and lectured extensively regarding the use of technology in the practice of law. Christine Galves is a lawyer and the assistant director of the California Education Master Plan Alliance, which promotes the integration of computer technology in teaching and learning.

Arguably the first reality television show, *Cops*, revealed the faces of society's most common criminals: drug offenders, thieves, and other assorted thugs. Although dismayed at some level to learn of the sheer volume of "bad guys" in our midst, we viewers also were relieved in some ways. *Cops* was a show about people we did not really know, located in parts of the city we seldom visited, engaging in activities from which we refrained. We were safe from them if we stayed out of "their world" and just ogled from afar.

Arguably the first reality television show, *Cops*, revealed the faces of society's most common criminals: drug offenders, thieves, and other assorted thugs. Although dismayed at some level to learn of the sheer volume of "bad guys" in our midst, we viewers also were relieved in some ways. *Cops* was a show about people we did not really know, located in parts of the city we seldom visited, engaging in activities from which we refrained. We were safe from them if we stayed out of "their world" and just ogled from afar.

But digital technology has changed all that in at least two significant ways.

First, this technology is allowing criminals direct access to our lives, as no proverbial right or wrong side of the tracks exists to divide the safe from the unsafe in cyberspace. Imagine that you go to a shopping mall and a criminal wants to rob you. In the recent past, that thief would have had to follow you to a vulnerable place and would have had to force you into surrendering your wallet. Now, armed with nothing more than a laptop computer and a wireless remote, that thief can use a "sniffer" program to access the credit card payment systems used by the store that just swiped your credit card. Unwittingly, you have just electronically surrendered your name, your card number, and other private information in the store's computers. This high-tech thief can snatch your financial information electronically from the convenience and safety of his or her car just outside of a business that has not secured its network from wireless hacking. If he or she were especially savvy, only a few dollars would be removed from your account at one time, remaining undetected by you. To bring the example home: one suspect in this country was found in possession of financial information of more than 1,000,000 people. (Interview with Agent M.H., Federal Bureau of Investigation, in New Orleans, La. (Nov. 19, 2003).)

Second, digital technology has introduced crime as a career to many who previously may have found that committing crimes the old-fashioned way, such as robbing or kidnapping, involved too much work or risk. Gaining the trust of a seventh grader via e-mail and then arranging to meet in a secret place to behave inappropriately is, frankly, achievable for many pedophiles who, when faced with having to physically kidnap a person and force the individual to comply, might not have the wherewithal to commit the crime. In short, to the extent that technology makes things easier, one of those things made easier is crime.

Albert Einstein said that "[t]echnological progress is like an axe in the hands of a pathological criminal." (THE QUOTATIONS PAGE, available at www.quotationspage.com.) And so it appears that technology, in addition to enhancing our lives in wondrous ways, has become a dangerous tool used by twenty-first century criminals. Both technology and law enforcement analysts warn that use of technology to perpetrate or support crime will only increase as the ingenuity of criminals grows along with the rapid development of technological devices and electronic communication. All kinds of criminals are getting into the act: from identity thieves to drug dealers; from terrorists to pedophiles; from money-laundering schemers to slick con artists; from those who turn to crime out of desperation to fill an unmet desire to those just-because-I-can criminals, such as computer virus launchers, who create chaos for sport. To protect society, law enforcement must keep up with the moving target of criminal technological advances and find efficient and ingenious ways to combat them, a goal not very easily accomplished.

But there is hope. Evidence of criminal activity is often left behind-by sophisticated high-tech criminals as well as regular thugs who just happen to use cell phones or e-mail-that can be used to help prosecute perpetrators and put them behind bars. The potential to mine evidence from technology is crying out for the training of law enforcement officers to recognize technological devices at a scene that might contain crucial information to help prosecute a criminal. Once the device potentially containing digital evidence-that is, electronic information that is either stored or transmitted in binary

systems consisting of zeros and ones-is found, it must be properly collected and transported to an appropriate digital forensics laboratory. There, digital forensics analysts who have the knowledge and experience to uncover the evidence without compromising its integrity or credibility at trial must analyze the technological devices and prepare any evidence obtained for court. Just as a strand of DNA is carefully extracted from a blood stain on a piece of broken glass that was properly collected and preserved from even the appearance of any spoliation or tampering, so too must the time of a phone call be competently removed from the chip in a properly seized cell phone.

Unfortunately, rarely do law enforcement officials fully recognize the potential for technological evidence to help solve crimes and prosecute criminals. Although training programs, similar to police academies, educate the people who are most likely to be the first to encounter potential evidence, too few programs provide meaningful training on the searching, seizing, and preservation of technological devices that may contain electronic forensics evidence. The culture of law enforcement, especially on the street, tends to be more focused on the physical demands of the job and on the collection and inspection of nontechnological evidence, such as bullets and fingerprints. But as criminals incorporate technology into their repertoire of crimes, so must officers, investigators, prosecutors, and even judges increase their knowledge of technology, especially with respect to courtroom evidence, in their respective roles of upholding justice.

The positive news is that the need for digital forensics training and laboratories is beginning to be recognized and met. For example, an innovative test site, the Gulf Coast Computer Forensics Laboratory, located in New Orleans, serves law enforcement agencies by providing research and development, training programs, and community awareness. It was initiated through the University of New Orleans with start-up funding from the National Institute of Justice and is managed by the University's Center for Society, Law and Justice. The laboratory, where digital forensics analysts use near-surgical skills to extract information from technological devices, is at once state-of-the-art and no-frills. No expense was spared on creating an environment of credibility and high integrity. To note just one example, cameras and electronic door monitors record exactly who is where with what piece of evidence at all times. Yet, with limited resources and its focus on discovering digital evidence, most walls remain bare and the carpet and desks lack any design flair. This laboratory is the largest of its kind in the southern United States and, if sustained, will be available for use by all area law enforcement agencies. But state-of-the-art labs like this are needed in every region, if not in every major city.

Much effort and specialized training of law enforcement and forensics experts over the years have developed the process of preserving and analyzing forensic evidence-fingerprinting, hair and blood analysis, DNA, ballistics, etc.-a process that criminal law has come to rely on today. Likewise, more training and resources are needed, especially in the form of more laboratories and research centers, for the practice of criminal law to benefit from electronic forensic evidence in the future. If the culture of criminal law can be convinced of the need to appreciate the extent of infiltration of technology into crime and evidence, and if a credible process for collecting and analyzing electronic forensic evidence can be established throughout the nation, technological evidence will become routinely instrumental in helping to prosecute both cyber-criminals along with traditional criminals who use technology to support elements of their crimes.

Electronic evidence: Ever present, not easily removed

Anyone and everyone-even a sophisticated hacker-using a computer for any kind of activity leaves behind potential electronic evidence. As we shop, research, and communicate over the Internet, and as we use computers, personal digital assistants, cell phones, and other devices to store, transmit, and retrieve information at home and at work, we are placing into electronic form private, sensitive, and even incriminating information that is getting stored in various databases such as Internet-connected servers, work-related networks, and on computer hard drives. This electronic trail can serve as powerful legal evidence against a suspected criminal, as it reveals highly probative "digital fingerprints" that can potentially be used to prove civil wrongs or criminal activity in a court of law.

"Technological devices contain all sorts of electronic evidence that can reveal a wide array of information," said Dr. Peter Scharf, cofounder of the Gulf Coast Computer Forensics Laboratory. "Criminal associations, for example, might be suggested by e-mail communications, writings about money-laundering schemes or terrorist plots, or spreadsheets of the division of criminal profits." He added that digital cameras or devices that store photography and video could contain still or moving pictures, for example, that evidence criminal pedophile activity, with date and time stamps to boot.

"Think of what is now stored and performed electronically," Scharf said. "Personal e-mail messages, online purchases, interactive Internet games, and other activities that involve thousands of people at once may be used to facilitate drug drops or even terrorist planning. Many criminals have left technological clues as to what crimes they have committed, be they economic fraud, computer intrusion, domestic violence, terrorist threats, harassment, stalking, extortion, gambling, identity theft. . . . The list is endless."

Technology has become such an integral part of life, with millions of people worldwide using a digital device of some sort daily. Many have been used for so long that their users do not realize that they contain electronic evidence. Printers and copiers, for example, once very basic in design, now record and store much detailed information, such as a version of all documents that have been printed or copied, under what pass code the machine was operated, and the date and time of printing or copying. All sorts of devices have digital signatures that are overlooked. Examples include digital watches, caller identification boxes, global positioning systems, and Web television. Pagers, cell phones, and answering machines

store information such as voice messages, call time and date, lists of all made and received calls, and even messages their users thought had been deleted. Even simple word processing documents contain not only the latest version of the text, but by hitting the "undo" button (to undo each of the edits) on some word processing programs that are not properly closed, it is possible to see all of the editing changes the author made to a document. All of these methods can provide a wealth of information about criminal activities, especially with respect to conspiracies, organized crime, and terrorist plots, where communication often is a necessary or fundamental part of the crime.

Unlike the act of simply smudging one's fingerprints at a crime scene in an attempt to hide or destroy that kind of physical forensic evidence, it is not easy to eliminate electronic forensic evidence. For example, e-mail is convenient and immediate, but its nature is misleading. Many people who send and receive e-mails in the privacy of their home or office begin to feel comfortable using this means to share information they consider private. Imagine an e-mail message between two criminals about a drug distribution conspiracy, containing the time and place of a particular drug transaction. After the critical information is exchanged, the two delete the messages on their respective computers to hide the communication and then proceed with the deal. Much to the consternation of these particular criminals-and to many sharers of e-mail one might assume-the act of clicking the delete button does not eliminate the information like a paper shredder physically destroys a document. Deleting a file or document by sending it to the "recycle bin" or "trash" merely sends it to another part of the computer hard drive. Even when the recycle bin or trash subdirectory is "emptied," the file or document is often maintained in a compressed form on the computer's hard drive, and thus is recoverable. That process may well require the expertise of a specialized laboratory or research center, using uncommon software, but it is no longer impossible. Similar to the law of physics that states energy is never really destroyed but simply converted to another form, electronic evidence, even if "deleted," often lives on indefinitely, deep in digital memory banks. Eventually, it might be overwritten, but not nearly as soon as one might suspect.

To wipe out some of the compressed information, criminals would have to reformat their hard drives. (This is not overly difficult, but it is time consuming and does not wipe out all data.) The only way to completely wipe out all information is to totally destroy the computer. And, even then, the e-mail message still could be stored in any or all of the network servers or Internet service providers (ISPs) used to send or receive that e-mail. Thus, irrespective of the computer hard drives, the e-mailed information would often be retrievable for a certain amount of time from network servers or ISPs, which act like way stations or relay posts for the e-mail communiqués, often keeping copies of the files and messages that pass through them, depending upon the provider.

Portable devices such as electronic organizers and memory cards that can fit into wallets or worn in lockets can contain the same information as a personal computer but allow for greater transportability of that information, for ease of smuggling or destroying them, if necessary. One or both of the criminals who exchanged e-mails might have saved the drug transaction information to a floppy disk, compact disk, or other remote memory device to keep it off of their hard drives. But unless those portable storage devices are also physically destroyed, they can be recovered and, if properly collected and analyzed, they too can produce credible evidence against their users. Hence, portable technological devices should be removed from the personal possession of a suspect during an arrest with the same care and preservation as an address book or a potential weapon.

Any hard drive that was used to view or edit the information, on a remote memory device such as a library computer used to access the information from a memory card or a printer used to make a hard copy from a compact disk, could have saved copies of the information, making it retrievable. One may even recover information about how an e-mail was created, or even retrieve the keystrokes used to draft a message, notwithstanding that the e-mail was never stored or saved as a document or file on a hard drive. This is especially true if law enforcement officers had been able to install a "spy" software program beforehand, which secretly records every keystroke made on the computer.

Given all of these possible repositories of electronic evidence of criminal activity, a growing number of law enforcement agencies now understand the potential to recover this evidence from technological devices and have begun to send their officers and agents to training programs, if available, to learn how to take advantage of it. Not only must this evidence be collected in such a manner as to avoid being suppressed at trial, it must also be analyzed carefully to fend off any claims of spoliation or tampering. It therefore becomes absolutely critical for all levels of law enforcement to be fully equipped, qualified, and trained to collect, search, and analyze electronic forensic evidence in a manner that maintains forensic integrity and thereby renders key evidence admissible at trial. The justice system has learned the lesson from the O.J. Simpson trial: even if evidence is deemed admissible, small forensic mistakes can doom otherwise powerfully credible evidence at trial. This applies to electronic information as much as any other.

Avoiding spoliation, tampering, and exclusion at trial

Evidence must be admissible at trial to be used to prosecute a criminal. Without a sufficient amount of credible evidence, the prosecution's case will suffer or be dismissed. Either an illegal search or seizure or a lack of authentication/foundation is an evidentiary hurdle that must be overcome to avoid suppression of evidence.

Probable cause and warrant requirements

With all criminal investigations and prosecutions, the first possible problem is whether law enforcement investigators had the legal right to search and seize the incriminating evidence initially. The Fourth Amendment to the U.S. Constitution and its case law interpretations govern the issues involved.

The Fourth Amendment limits the ability of government investigators to search for evidence. Courts apply the same test to electronic information as they do to any other form: that of a reasonable expectation of privacy. (*United States v. Chan*, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (applying reasonable expectation of privacy to electronic data storage).) This restricts law enforcement from investigating a person's private computer files without probable cause. When probable cause is proven absent, the evidence obtained is suppressed under the exclusionary rule. Therefore, investigators must first obtain a valid search warrant based on probable cause to "search"-which really translates to "analyze"-personal technological devices and electronic data for evidence of a crime or criminal activity. If not, they must make a careful and valid determination that a warrantless search is reasonable because the situation falls under a recognized exception to the warrant requirement. Examples would include the doctrines of consent or plain view.

Courts often analogize electronic storage devices (and the digital evidence residing in them) to closed containers in the physical world, the owners of which maintain a reasonable expectation of privacy therein. For example, obtaining a warrant to look on a hard drive solely for Excel spreadsheets is similar to getting a warrant to look only in a certain container for certain information. This seems simple enough, but many issues may arise. Armed with a warrant to search for specifically labeled information, what would occur if an investigator searched every labeled and nonlabeled file and document on a computer, perhaps all Word, PowerPoint, or PDF files? Courts differ in their approaches to this scenario. Some would allow the entire search of all files in that particular computer (see *United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001) (allowing a search of all additional files, analogizing all the data on the computer to the contents of a closed container)), while others would require the warrant to be more specific in its scope, mentioning the precise computer files and programs to be searched and seized (*United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that the scope of the warrant allowing a search for drug activity was exceeded when officers ceased that search and began searching files for child pornography); *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) (stating that a search of an entire computer is more invasive because a computer can hold so much information that the search warrant may not contemplate).) To avoid potential judicial overrulings, prosecutors and investigators need to work together to establish clear search and seizure policies for electronic evidence in their particular jurisdictions.

The potential for confusion regarding expectation of privacy is high. Sometimes a warrant is not even necessary, not because of an exception, but because the suspect maintains no legitimate expectation of privacy in the computer files in the first place. For example, if a suspect uses a computer that is openly available, with no password protection, or one in a workplace to which the employer's system administrator has direct access and can monitor all of the computer activity, he or she may have abandoned all Fourth Amendment rights with respect to that computer because it is used in such an open and public way.

Other issues could emerge if a person took a computer to a third party for repair and, while working on it, a technician stumbled across incriminating information and reported it to authorities. Generally, obtaining and reporting information in these circumstances would be valid as long as there was some manifestation that the suspect relinquished his or her reasonable expectation of privacy in the computer by placing it in the hands of a third party. Because the Fourth Amendment requires "state action," it does not apply to nongovernmental persons who might conduct searches on their own and report evidence of potential criminal activity, as long as they were not acting in any way as agents of the government. But perhaps it is not as easy as that. Some courts would likely opine that a computer owner leaving a computer with a technician did not totally abandon all reasonable expectations of privacy because the "exposure" to the public was limited to the repair shop, and it should have gone no further. (See *United States v. Barth*, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (finding that defendant retains a reasonable expectation of privacy in computer files given to a repair shop).)

Investigators thus need to be aware of the Fourth Amendment and the warrant requirement demonstrating probable cause as a protection of a suspect's reasonable expectation of privacy. Both investigators and prosecutors must be especially aware that search warrants cannot be used for "fishing expeditions." The warrant should specifically describe the things to be searched and the items to be seized. On the other hand, although it needs to be particular and specific, the warrant should be as broad as the probable cause will allow, so that the investigator is not "boxed in" and has flexibility during the search to locate all possible incriminating information. If care is not taken with the warrant protocols, the fruits of the search may well be rendered inadmissible at trial.

Warrantless searches

If time and circumstances permit, the most cautious avenue is to obtain a warrant so that investigators do not have to rely on their own personal legal assessment of the specific circumstances to see if an exception applies. However, if investigators decide to make a warrantless search where a reasonable expectation of privacy exists, one of several exceptions must apply or the evidence will be suppressed. The most obvious of these would be consent. Investigators may search without a warrant or even probable cause, for that matter, if the person with authority over the electronic information voluntarily consents to the search. Using written consent forms that explicitly set forth the scope of the

consent, rather than mere oral acquiescence, obviously is a good practice. Checking the authority to consent, especially when family members consent to a search of another family member's electronic information, is another practice that should be adhered to. This would also apply when an employer or its system administrator consents to the search of an employee's computer records.

Exigent circumstances would be another exception. Investigators may search and/or seize without a warrant if it appears that an immediate search is necessary to prevent physical harm, destruction of evidence, or some other consequence frustrating legitimate law enforcement efforts. However, one should never search beyond the point of urgency or exigency. That is, law enforcement officers may seize a laptop about to be destroyed, but they will likely need a warrant to begin searching through the computer's files once the laptop is secured.

Investigators may search without a warrant if they are in a lawful position to observe and access the evidence because its incriminating character is immediately apparent. Of course, it is better not to search beyond the point where the incriminating nature is apparent. Like the contents of closed containers, unopened computer files are not in plain view, regardless of how they are labeled. Currently, only some courts allow further computer file searches based on plain view once an investigator has already gained access to a document or file. (See, e.g., *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999); *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001); but see, e.g., *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996) (ruling that the government cannot rely on the plain view doctrine to access closed files because such files are not in plain view if they must be opened).)

Investigators may search without a warrant whenever they lawfully arrest a person. They can do a full search of the person and a more limited search of the surrounding area. This can be very important when a suspect is carrying portable memory devices, pagers, cell phones, personal digital assistants, or a laptop computer. (See, e.g., *United States v. Reyes*, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (determining that officers' accessing of an electronic pager carried by the arrested person was a valid search incident to a lawful arrest).) The problem is that some of these devices contain much more information than a wallet or an address book. Therefore, a more invasive search into all of the electronic information stored therein may be going beyond the original rationale for the search incident to a lawful arrest exception, that is, making sure there is no access to weapons. The best course is probably to seize the device but not search it until after a warrant is obtained for the information contained in it.

Finally, inventory and border searches may qualify as exceptions to the necessity for a warrant. Investigators may search in order to "inventory" the items they have seized, thereby protecting the custody of the items seized from a suspect. But searching a technological device without a search warrant will not necessarily protect the information on it, and there is usually no inventory justification for the warrantless invasive search other than documenting the device itself. Defendants can claim that the device should have been inventoried, on the spot, without accessing the electronic information contained therein, and that any prewarrant access involved unlawful searching and even tampering. When suspects cross national borders, investigators may also search without a warrant. However, just as with inventory searches, best practice is to obtain a warrant if devices or items are found. They can be seized and carefully searched later under a warrant's authority and direction.

Further decision making before a search

A full treatment of criminal procedure search and seizure issues as they relate to electronic evidence is far beyond the scope of this article. Nonetheless, law enforcement officials and prosecutors need to be well versed in this new and necessary area of law, for one mistake here could leave the key pieces of electronic forensic evidence outside the courtroom and the case up for grabs. It is therefore essential to make a series of careful decisions before a search for electronic evidence. Especially important is pulling the search team together as far in advance as possible and reinforcing specific member roles. The prosecutor should check for legal requirements while the main detective should oversee the search. A technical computer analyst who can direct and advise the detective and answer the questions of both the detective and the prosecutor is clearly one of the most important members of the team.

This is particularly true because understanding the technical device and the software to be searched is essential before planning the search or drafting the search warrant. If these are not understood, the search can be fruitless because the team does not know how to navigate through the software it is searching. Often, significant differences exist in hardware, software, operating systems, systems configurations, etc., because there are many commercial options, not to mention tailor-made software and operating systems constructed solely for particular organizations. This understanding is especially critical if businesses contract with remote service providers, which means the critical information may not even be stored on the devices located on-site. Rather, the relevant information could be off-site with network providers located in other parts of the country or the world. This information will be missed if the investigators only search local systems or are not familiar with the hardware or software, or group networking, intranets and extranets, or similar items.

Determining contingency strategies beforehand is also a necessary practice. One cannot assume that the original search strategy always will be effective or well conceived. The investigation team members need to be flexible problem solvers who can react to unforeseen configurations or new or different hardware or software.

We have already discussed the issues involved in drafting the warrant. Nonetheless, team members need to remember that it is important to make the search warrant broad enough to cover all paths that may yield critical information, but particular enough to overcome any challenge that the warrant was not specific enough to justify the search with respect to certain documents or files.

Other relevant statutes

The Fourth Amendment is not the only law to consider. Prosecutors must familiarize themselves with statutory privacy laws such as the so-called Wiretap Act, 18 U.S.C. §§ 2510-2522, and the pen register/trap and trace statute, 18 U.S.C. §§ 3121-3127, and they need to impart the specifics of these statutes to the investigators and technical personnel conducting the actual searches. Other statutory provisions may give rise to civil liability to state actors in their official capacity.

The Privacy Protection Act, 42 U.S.C. § 2000aa, is another statute that may affect searches. If a search yields evidence relating to First Amendment protected speech—such as publishing or submitting items to the World Wide Web—it implicates the Privacy Protection Act. Although exceptions exist when the search involves legitimate crime prevention or enforcement, the investigator should be careful when searching for evidence of a crime that may be mixed in with material protected by the First Amendment. He or she must refrain from viewing that material during a search.

Another statute to consider is the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712, which seeks to protect innocent third parties holding stored information, such as ISPs, or the files of their completely innocent and unrelated customers, when a search of one particular suspected customer is conducted. The idea is to protect innocent individuals' private communication on the Internet even though an ISP's records are being searched.

All of the information mentioned above should be standard knowledge for all law enforcement personnel. But navigating search and seizure laws and properly collecting, maintaining, and searching devices and electronic information are only half the battle. Actually finding incriminating electronic evidence in a technological device is the other. Just as bloodstains often must be processed and analyzed before they can reveal critical information, so too must electronic evidence. Electronic evidence is literally evidence in the form of electronic impulses stored in tiny circuitry. It can be moved across the country or even overseas in seconds, and it may be stored in various ways designed to throw investigators off track. The files may be encrypted, password protected, misnamed to seem innocuous, or mixed in with other unrelated noncriminal files or files that are legally protected by statute. And the hiding places are seemingly infinite once one ventures into cyberspace. At least one Internet game has been identified by an FBI computer crimes agent who believes an organized group of criminals had conspiratorial meetings and exchanges of criminal information under the guise of merely playing a teenager's video arcade-style game. (Interview with Agent M.H., Federal Bureau of Investigation, in New Orleans, La. (Nov. 19, 2003).)

Authentication/foundation

Once electronic evidence is found and properly searched, to be admissible in court the prosecution must "lay a foundation" for it. That is, the evidence must be "authenticated" since it is tangible evidence to be admitted as an exhibit for the jury to see, hear about, and consider. Rule 901(a) of the Federal Rules of Evidence provides that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Similar rules exist for state courts.

This basically means that some proof must be provided by the prosecution that the electronic evidence it is seeking to admit is actually the same incriminating electronic evidence that was contained within and properly extracted from the defendant's computer or other digital device. The jury can either accept or reject this evidence—believing it is or is not the actual evidence taken from defendant's computer, and determining what that evidence ultimately may or may not show—but before the electronic data can even be presented as admissible evidence in court, the prosecution has to provide some preliminary evidentiary basis that the defendant's computer documents are actually what the prosecution is claiming them to be.

The standard is the same for electronic documents as it is for hard copy documents. Usually a witness with knowledge of the hard copy documents will testify that the documents are what they purport to be. If the recipient of a letter testifies in court that he or she recognizes the letter, is familiar with the handwriting of the sender, or recognizes the substance of what is contained in the letter, a foundation has been laid because there would now be an evidentiary basis—the witness's testimony—upon which the jury can make a finding that the letter really is a letter from the sender. Similarly, if the evidence is a photograph and a witness simply says that the photograph is a "fair and accurate" representation of the crime scene, then a foundation has been laid for it.

Likewise, if a witness with knowledge about computer documents or files testifies about the existence or substance of those documents or files, then a foundation will have been properly laid for them. A computer programmer or computer analyst does not need to lay the foundation for electronic evidence, just as a photographer does not need to lay the foundation for a photograph, or the author of a letter the foundation for that letter. Of course, if a witness does not have

any knowledge or familiarity with the electronic evidence and a computer programmer retrieved it, that computer programmer would have to testify as to the process used to obtain the evidence. This is no different than having a photo camera technician testify about the process involved if a surveillance camera took a picture and there was no witness who ever saw the scene depicted in the surveillance photo in order to testify whether it was a fair and accurate depiction.

When technological hardware is offered, the standard is the same as for other tangible pieces of evidence taken from a crime scene, such as DNA, fingerprints, or a murder weapon. Imagine that an investigator finds a murder weapon at a crime scene, documents the finding, puts the weapon in a bag identifying it, properly maintains it up to the time of trial, and testifies to this course of action. A foundation has been laid for the admissibility of the weapon because there is now an evidentiary basis—the witness's testimony of his or her actions—upon which to make the finding that the weapon is the weapon taken from the scene. Similarly, if an investigator at a scene finds a technological device and testifies about how that device was obtained and maintained up through the time of the trial, then a foundation would have been laid for its admissibility, and it can be considered at trial.

Some practical matters

A "chain of custody" for a seized hardware device is advisable but not crucial for admissibility purposes if the device is not "fungible" (that is, interchangeable) or easily mistaken for something similar. (An example of traditional fungible evidence would be cocaine, which is not sufficiently unique for a witness to identify it easily. It would be difficult to know whether the evidence in hand was the same cocaine as that taken from the crime scene, different cocaine, or not even cocaine at all.) Usually, the software contained on the hardware makes a digital device unique enough to be identified or authenticated by someone with knowledge about the device and the information contained in it. Nonetheless, best practice would argue for maintaining a chain of custody because it shows that investigators have acted professionally by being very careful with the evidence, even though a chain of custody is often used only to go to the "weight" or credibility of the evidence. The custodial chain can also ward off speculative claims that evidence was planted on the computer while in police custody or was even substituted with a replacement computer.

Incorrectly storing a technological device can destroy or alter the hard drive or the data on it. These devices should not be kept in very hot conditions. Avoid the trunk of a police car for hours on a summer day. Many technological devices cannot withstand either too hot or too cold conditions, so temperatures in long-term storage areas need to be moderate and stable. Neither should technological devices be exposed to magnetic or electric fields because these fields can cause similar damage. Just as an investigator should not allow blood or hair samples to become contaminated, so should an investigator take the same special care and precautions to maintain the integrity of electronic evidence, thereby negating defense claims that the evidence should be inadmissible, or that it lacks credibility if admissible.

What if a technological device is already up and running—that is, switched on—when it is found? Enforcement officers must understand that evidence can be lost if the device is shut down, because information that is not saved before power termination can become unrecoverable. Typically, officers dealing with such a computer should make a "read only memory" copy of its contents, including the unsaved information, before any device is turned off or transported. This copy can be searched more thoroughly later, while the original device remains as is, safe and unadulterated. The "read only" nature of the copy will allow a detailed analysis and navigation through all of the files while neutralizing potential defense claims of tampering because, after the copy is made, the original hard drive remains untouched and does not have to be accessed for testing. Obviously, knowing when and how to make a copy of information on a hard drive requires basic equipment and training. It also requires software that demonstrates that nothing was or ever could be altered, lost, planted, or destroyed during the copying process itself.

Rebutting defense challenges

Although authentication is somewhat straightforward, defense counsel might challenge the prosecution's foundation for electronic evidence in several ways.

Charges that investigators have planted incriminating evidence—pictures, say, or other records—on the defendant's otherwise "clean" computer or other technological device, rather than its being legitimately found during a legal search, are more common than one might anticipate. Such charges obviously argue that the defendant is innocent and has been framed. In addition to wholesale creation of planted evidence, allegations arise that the police altered or manipulated the defendant's existing noncriminal information to make it appear incriminating. For example, a computer document of an innocent sales sheet from the defendant's garage sale, showing the sale of legitimate items, might be changed by police to add the names or nicknames of alleged drug accomplices making drug buys, thus transforming the document into an illegal drug sales record and evidence of a drug conspiracy.

The only way to combat these challenges is to make a "read-only" copy of the contents of the technological device and never reopen or access the defendant's computer until it can be done with a defense analyst present. Also, the copying software used by investigators must be able to reveal that it cannot simultaneously manipulate files while copying the hard drive. The software should solely copy information and do nothing else. Making a legitimate copy can also serve to justify a later arrest warrant or indictment without having to access the original source. Of course, the burden of proof is

on the defendant that records were planted or altered. Mere supposition that the records could have been altered, with nothing more, is considered overly speculative and at most goes only to weight, not admissibility. Still, having as tight a security system as possible is highly recommended so the weight/credibility of the evidence cannot be questioned, even as a mere speculative possibility.

Defense counsel may also argue that the existence of electronic evidence on a technological device, or especially on the Internet, does not necessarily mean that the defendant was its author or recipient, and thus does not tie him or her directly to the crime. The argument is that the connection from the electronic evidence to the defendant is missing. Someone else could have been using the defendant's computer posing as the defendant, counsel could postulate, or perhaps an illegal hacker stole the defendant's identity and was posing as him or her in cyberspace. Or perhaps anonymous e-mail or anonymous instant messages were found, but the defendant cannot necessarily be tied to these incriminating messages, given the anonymity. This is akin to shoe prints at a crime scene that match the defendant's shoes. The shoe prints do not necessarily prove the defendant was at the crime scene. Maybe the prints were made by another similar make and style of shoes, but not the defendant's, or perhaps someone else stole or borrowed the defendant's shoes and made the prints unbeknownst to him or her.

To tie the criminal to the electronic device, one cannot rely on the more traditional handwriting identification (see FED. R. EVID. 901(b)(2), (3)) or voice identification (see FED. R. EVID. 901(b)(5)), except perhaps if a cell phone is involved in the crime. These ID methods obviously do not work in a cyberspace/electronic environment. However, Federal Rule of Evidence 901(b)(4) provides the answer: "Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances" can all aid the identification process.

Circumstantial evidence of the contents or substance of the electronic communication itself-the distinctive characteristics of the document or file-supplies the otherwise missing foundation. For example, usage of particular names, specific places, telephone numbers, or other knowledge that circumstantially match with information that only the defendant could know make it very difficult for defense counsel to argue coincidence or mistaken identity. Again, these kinds of defense challenges certainly may go to weight, but often there is enough circumstantial evidence to satisfy the admissibility foundation requirement, and often enough to make the defense claim seem far-fetched.

A further way to enhance the strength of circumstantial digital evidence is to search and obtain hidden "metadata" contained in the defendant's hard drive and often on the Internet, which records (1) the exact dates and times of any messages sent or received, (2) which computer(s) actually created them, and (3) which computer(s) received them. If the metadata can be corroborated with other evidence, such as other e-mails received and sent from the defendant's computer at that same specific time and date, the extent of any coincidence or identity theft conspiracy postulated by defense counsel will seem very limited. This will enhance the credibility of the evidence and make claims of mistaken author identity or purposeful misidentification seem ridiculous. However, anonymous postings to Web sites that lack such strong circumstantial evidence will still often be excluded because there would be no other way to tie the anonymous postings to the defendant other than through mere speculation, which is not enough.

One last item regarding authentication and identification should be mentioned. Photographing the entire search and seizure scene, including the computer screens and all other technological devices found there, is strongly advised. This is a common practice in most investigations to preserve evidence, reconstruct context, and demonstrate professionalism and therefore should be used in the technology context as well. Photos provide valuable evidence as to how the suspect's particular hardware was situated and might provide insight into how it was being used. Photos also demonstrate that each device presented in court is the same one as originally found at the scene.

The need for formal training

Law enforcement officers, agents, investigators, prosecutors, and judges must understand technological devices with respect to their capacity to reveal what is often valuable and probative electronic evidence in criminal prosecutions. One way to achieve that goal is through formal training. The model provided at labs like the Gulf Coast Computer Forensics Laboratory offer a great example of what can be instituted at other future digital forensic labs. These labs can offer training courses to build awareness of what technological devices may contain powerful incriminating evidence, as well as how to properly search and seize those devices and transport them to labs for analysis. But just as importantly, these labs illustrate by example what law enforcement officers need to know. Devices are electronically logged in, and all who handle them and/or transport them to any different locale are recorded on computer and on camera. Computer analysts make copies of the contents of various devices and then extract all of the pertinent electronic evidence from these copies, using state-of-the-art expertise and experience.

But all of this potential will only be valuable if prosecutors educate law enforcement investigators and technical analysts to follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally, either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial. Technology can live up to its billing of making life easier and more efficient for all of us, despite how criminals may employ it, if we effectively use electronic evidence to prosecute those criminals and reduce the opportunities for technology to be used against us. Be it terrorism of the September 11th

variety, corporate financial securities scandals, computer hacking, identity theft, online fraud, or common drug distribution activity, society's best defense is the ability of law enforcement to be fully cognizant of and fully use the vast electronic trails evidencing criminal activity so that technology-using criminals can be brought to justice.