



The Devil's Advocate:

How Computer Forensics Can Support Both Sides of Computer Litigation

by Judd Robbins

In Alabama recently, I testified for the defense in a military court martial trial in a case that involved possible use (or misuse) of the Internet for interstate trafficking in child pornography. Computer experts were engaged on both sides of the issue, and there was no contention between their expert opinions. The prosecution expert did the original forensic exploration of the defendant's computers. He presented his facts about files, both existing and deleted, that were found there. No argument there. However, the Defense was able to note some degree of inattention to the Federal guidelines for search and seizure of computer evidence. This led to discussions of the ease with which anybody can change the various dates and times associated with computer files. Reasonable doubt?

The prosecution presented lists of photographic images that were downloaded from the Internet. No argument there. Many thousands of images await interested viewers on the Internet, and an increasingly large percentage of those are pornographic. However, if more than one person has access to the same Internet account via a common password (and a girlfriend in this case did have that kind of easy access to the defendant's computer), who is to say which person was actually responsible for downloading the photographs found on this defendant's computer? Reasonable doubt?

Medical evidence was brought in by the prosecution to confirm the fact that some of the pornography was of women under the age of 18. In this case, a defense medical witness spoke to the uncertainty of age determination. The defense computer expert then spoke to the ease with which photographic retouching can modify digital pictures. Not that any picture in the case was actually manipulated digitally, but only that it can and could have been done with alarming ease and subsequent difficulty in ever determining if it was ever done. More reasonable doubt?

The list can go on, and in some cases, it certainly does. The computer forensics expert can unearth incredibly damaging evidence on computer disks. It's the prosecution's job to use that evidence to cement the case. But the computer forensics expert can also help the defense to identify any weaknesses in procedure or results that can help cast reasonable doubt on the apparent findings. It's the defense counsel's job to ascertain where and what weaknesses may exist and bring them to the fore.

Give the Devil's Advocate His Due

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. Computer specialists can draw on an array of methods for discovering data that reside in a computer system, or recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, or actual litigation.

Just as statistics are often used on both sides of many arguments, so are computer specialists. Although the experts sometimes present diametrically opposing positions, it is more likely that the lawyers involved in the case choose to elicit differing but not truly conflicting statements. Experts can readily help on either side of a case, either to identify helpful prosecutorial facts or to suggest alternative possibilities to create reasonable doubt. Experts are counseled not to be advocates, and they needn't be when the facts alone offer sufficient material for legal presentation. Experts are told to answer Yes or No and not give any more than is asked. However, experts are also expected to know when to refuse to give a simple Yes or No when a more expanded answer is truly necessary to clarify a response.

Benefits of Professional Forensic Methodology

The impartial computer expert who helps during discovery will typically have experience on a wide range of computer hardware and software. This is always beneficial when the case involves hardware and software with which this expert is directly familiar. But fundamental computer design and software implementation are often quite similar from one system to another, and experience in one application or operating system area is often easily transferable to a new system.

Unlike paper evidence, computer evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. The discovery process can be served well by a knowledgeable expert identifying more possibilities that can be requested as possibly relevant evidence. In addition, during on-site premises inspections, for cases where computer disks are not actually seized or forensically copied (see below), the forensics expert can more quickly identify places to look, signs to look for, and additional information sources for relevant evidence.

I was a designated prosecution expert earlier this year in a case in Las Vegas, Nevada. During discovery, the attorneys for the prosecution were going to ask for most of the obvious things about the subject software that had allegedly performed inadequately. But they hadn't planned to ask for any earlier versions of the software in question; these versions may have still existed on the computer systems of the developing programmers or on the backup tapes of the developing software firm. These historical versions could have included helpful historical comments or earlier code that might have helped the determination of current software inadequacy. Similarly, any forensics exploration of a computer system should consider the existence and relevance of earlier versions of data files (e.g., memos, spreadsheets) that still exist on the computer's disk or on backup media, or differently formatted versions of data, either created or treated by other application programs (e.g., word processing, spreadsheet, e-mail, timeline, scheduling, or graphic).

Continued on page 8

Protection of evidence is critical. A knowledgeable computer forensics professional will ensure that a subject computer system is carefully handled to ensure that:

- no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer;
- no possible computer virus is introduced to a subject computer during the analysis process;
- extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage;
- a continuing chain of custody is established and maintained;
- business operations are affected for a limited amount of time, if at all; and,
- any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

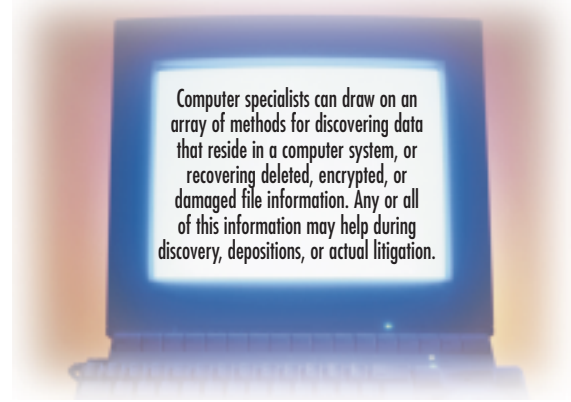
Steps Taken by Computer Forensics Specialists

The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system. These steps include:

- protecting the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction; discovering all files on the subject system—including existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files;
- recovering all (or as much as possible) of discovered deleted files;
- revealing (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system;
- accessing (if possible and if legally appropriate) the contents of protected or encrypted files;
- analyzing all possibly relevant data found in special (and typically inaccessible) areas of a disk—including but not limited to what is called 'unallocated' space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as 'slack' space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data, but once again may be a possible site for previously created and relevant evidence);
- printing out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data, and providing an opinion of the system layout, the file structures discovered, any discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination; and,
- providing expert consultation and/or testimony, as required.

Who Can Use Computer Forensic Evidence?

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists. A partial list might include the following examples:



- Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
- Civil litigations can readily make use of personal and business records found on computer systems that bear on: fraud, divorce, discrimination, and harassment cases.
- Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- Corporations often hire computer forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.
- Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
- Individuals sometimes hire computer forensics specialists in support of possible claims of: wrongful termination, sexual harassment, or age discrimination.

A Law Librarian's Guide to Computer Forensics

So what does any of this have to do with the law librarian's job? Quite a bit, of course. Fifteen years ago, very few people outside of large corporations had access to computers at all. This includes law librarians as well as the clients of the lawyers you support. Now that these lawyers' clients know how to use (and misuse) their computers, it's the lawyer's job to discover enough about that computer usage to help win their cases, whether they are the plaintiff or defendant.

When the next Defense (or Prosecution) lawyer asks you for help in locating a computer expert to help with a case, you should now understand the range of questions and issues to be faced by that expert and the lawyers involved. You should also now understand the range of skills and experience needed by the modern computer forensics expert to address those issues. Most important, however, you should now realize that it doesn't matter whether the computer forensics specialist applies his (her) skills on behalf of the prosecution or the defense. Just as lawyers are trained to argue on either side of the same case, the computer forensics expert can bring skills to bear on either side of the same case. Far beyond a devil-may-care attitude, it comes down to simply giving the Devil's Advocate his due.

Judd Robbins (pdi@knock-knock.com) is President of Presentation Dynamics, Inc., Lake Tahoe, Nevada. He is glad to offer free initial telephone consultations about any potential case. He can be reached at 702/832-8210; his home page URL is <http://knock-knock.com/jr.htm>.