

[NACDL](#)

[Home](#) > [News And The Champion](#) > [Champion Magazine](#) > [2003 Issues](#)

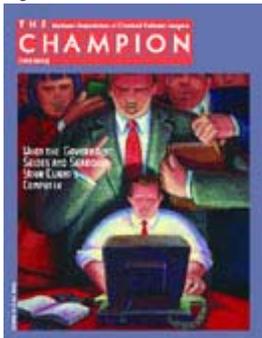
The Champion

June 2003 , Page 30

[Search the Champion](#) Looking for something specific?

Computer forensics: how to obtain and analyze electronic evidence

By Wade Davies



Computers (and the people who work with them) are strange and wonderful things. Whether we like computers or not, all of us who handle criminal cases have to learn how to deal with them as pieces of evidence. This rule applies not only to computer crime or pornography cases. In most business and home searches now, the government seizes computers. The government is looking not just at what our clients have on their computers. They are also analyzing what used to be there; when information was “deleted” and how it was deleted.

In many ways, computerized evidence must be dealt with the same way as any other type of evidence. It is subject to the same need for defense inspection, the same chain of custody requirements, and the same rules of admissibility. Defense counsel have to inspect computerized evidence as carefully as they would a stack of documents that were seized or the evidence taken after a barroom brawl.

In other ways, counsel's role in inspecting computerized evidence goes much deeper. It is not enough to accept paper printouts or the government's other representations about what is found on a computer. Not only do you have to find out what the government claims was on the computer, you have to know: How did it get there? When was it created or put on the machine? Where was it stored? What kind of file is it?

To find out these answers, you have to turn to an expert in computer forensics, and you have to know how to get the evidence and approach the expert correctly.

Finding an expert

Finding the right computer forensic expert is not always easy. Although with a quick Internet search one can find hundreds of people who claim to be qualified in computer forensics, truly capable forensic experts are rare. It is beyond the scope of this article to make any particular recommendation, but it is of utmost importance to find someone who not only knows the latest technology for examining hard drives but can communicate. Computer gurus tend to use abstruse language, even in talking about simple concepts. You need to find someone who can talk to you and, if necessary, to a jury.

It has been the disappointing experience in our firm recently that many well-qualified experts refuse to work for defense counsel. They are worried, perhaps legitimately, about being blacklisted from any government consulting work. This has been particularly true in pornography cases.

To overcome this initial reluctance, defense counsel must let the expert know up front that all we are looking for is the absolute truth. The forensic examiner can be assured that we are not looking for any particular slant but just to know what the objective facts are and the answers to the what, when, how, where questions above. If the person views himself or herself as an objective scientist, often initial reluctance to work for a defendant is overcome when the expert realizes that counsel is above board and really just looking for help understanding a complicated scientific or technical subject.

There are also credible on-line resources that can help you find the right expert. Although a search engine search for “computer forensics” or similar phrase immediately pulls up hundreds of questionable resources, many of the top examiners have a Web presence. It is also helpful to browse these sites just to get a feel for what the issues are and what it is you want to look for or accomplish. Also, there are entire periodicals devoted to computerized evidence, and the contributors to those periodicals may prove to be excellent resources.¹ Finally, and most importantly, NACDL and its members are among the best resources for finding trustworthy experts.² Talk to people who have used forensic computer examiners previously.

As with any expert, enter into a written contract. The contract should be between the expert and the law firm to ensure attorney-client and work-product privileges. The contract should require the examiner to preserve confidentiality, and should specify the type of examination to be performed and the type of report to be produced. You should talk to the examiner enough beforehand to come to an understanding of the forensic software to be used and its capabilities. The type of examination to be performed should be specified in the contract. Our experience is that the examiner will require at least a whole week to complete a full forensic evaluation of a single computer.

Thorough forensic examination, like quality legal representation, takes a long time and is expensive. If your client cannot afford adequate expert services, remember that even if you are retained and your client is rendered indigent, a federal judge has the authority to appropriate Criminal Justice Act funds for a defense expert.³

Finally, with regard to experts, identify and retain the expert early. The expert can shape the investigation and assist in what to ask for in discovery and how to ask for it.

Getting access to the real thing — unique discovery issues

If any of the evidence the prosecution intends to use comes from a computer, get access to the original computer or an exact copy: a “mirror image.” Do not accept a compact disc or a floppy containing what the government says it found on the machine. Access to the original drive is a must.

The government will often balk at giving defense counsel access to the original computers or even a mirror image. In pornography cases, the government has often taken the position that defense counsel is not entitled to a copy of the evidence at all, since the government claims it to be contraband.

Fortunately, most courts have rejected the government’s position. The text of Rule 16 of the Federal Rules of Criminal Procedure clearly requires access. The rule provides that the government must allow the defendant “to inspect and copy” a number of things, including tangible objects that the government intends to use in its case, that are material to the preparation of the defense or that were obtained from the defendant.⁴ If there is any question about the propriety of further distribution of the evidence, the court has the specific power under Rule 16(d) to enter a protective order. An appropriate example of an order allowing access with appropriate precautions has been entered by Judge Charles R. Breyer in the Northern District of California. There the government was required to allow the defense to copy the original computer files.

The court instructed defense counsel to keep the material locked and to allow only experts, investigator and paralegal, and the defendant (with counsel present) to examine the material.⁵

Similarly, in a very thoughtful opinion, Chief Judge Charles Haden of the Southern District of West Virginia ordered that defense counsel be allowed a “mirror” image of the computer hard drives in question. In that case, the government had offered to let the defense expert come to the U.S. Attorney’s office to examine the originals. The court pointed out:

The mirror-image hard drives are necessary to allow computer experts to determine when and how particular files were accessed and downloaded. Simply viewing the materials is insufficient. Similarly, allowing defense experts to manipulate the hard drives under scrutiny of the government essentially would make defense “work product” an open book.⁶

Thus, with the proper protective order, counsel should be able to obtain an exact, mirror-image of any drive from which evidence has been obtained in the case.⁷ At our firm, we have no problem with agreeing to a Rule 16(d) protective order. Because we may actually have access to contraband, restrictions on dissemination seem reasonable, and having a clearly stated order will protect defense counsel as well.

What you see is not necessarily what your client had - why access to the original is so important

In a recent case, we were given a floppy disk by the government that supposedly contained contraband pornography images taken from our client’s computer. Things did not look good for our client. Once we got our expert access to mirror images of the hard drives, however, he was able to show us that the offending images were from “banner” advertisements that our client had not sought or saved in any way. The images were from advertisements that popped up at the top of the screen when the client was looking at other sites. Our client had no recollection of seeing them and certainly no intent to possess the images. Unbeknownst to him, however, all the images that show up on one’s screen while viewing a Web page are normally stored on the computer hard drive as a temporary Internet file. The expert was also able to put together a chronology of how and when the images got on the hard drive. Had it been necessary, we could have further shown exactly what our client had been looking at intentionally (by following links on the web), and that trail was embarrassing but not incriminating.

That experience solidified for us how important it is to have access to the actual computer or a mirror image. There are certain things that can be determined by an expert examination of the hard drive that simply cannot be determined by looking at individual files. One of the important questions listed above was “How did it get there?” An expert examining the hard drive can tell when a file was created, copied or modified. If it involved a downloaded file, it is also probable that you can learn where it came from.

A mirror image is an exact copy of the hard drive. Perhaps a simpler way to copy computer files would be just to open up the menu on the original computer and copy over all the interesting files. The problem with this is that there is a lot of very interesting information that is contained in files that do not appear on the directory. The files not shown on directories can be a major source of information. For example, it may be possible to reconstruct the various versions that a file or document went through before it was saved in its final form that you could see on a computer directory or menu. Various techniques exist for getting access to all the information on a hard drive. Several different software programs might be able to provide the information needed, and getting an exact copy of the hard drive might not be the perfect solution either. The point, however, is that, working with your expert, you need to make sure you are getting access to everything on the computer in question, not just the files the government picks out for you.⁸

There are a number of forensic programs used by examiners. The copying process you want may depend upon the program to be used by your expert. Therefore, you need to consult with the expert prior to having the copying done. The expert will also want to know what program the government expert is using.

By now most of us know that deleting a file does not really make it go away. The information is not taken off of the surface of the hard disk. Rather, the file is simply no longer linked to the menus that the computer user sees. The space that the file occupies also becomes available for writing new data, but the "deleted" material will not disappear until it is completely overwritten. Of course, no deleted information would be accessible without at least a mirror image. Government technicians know how to look for deleted files. They are going to find them. Our challenge will be to learn how those deleted files got there, when and why they were deleted and where they came from. If that information is impossible to determine, the forensic examiner may be helpful in explaining that the deleted files or fragments of deleted files are not significant because there is no proof of how, when and why they got there.

Getting access to the original hard drive or a mirror image is worth fighting for if there is any question about how the evidence got there or its legitimacy.

So, what can the expert determine?

Using forensic software, a good analyst can come close to recreating the activity that occurred on the computer. Some programs even have a time line program that creates a report showing when files were created, modified and deleted.

Hash analysis is the process of taking a list of computer files and checking the target computer to determine whether any of those files are on that machine. The government uses hash analysis in pornography cases to check against a list of known child pornography files to see if files with the same characteristics are on the computer being examined.

In any case in which there is a question about files that came from the Internet, forensic analysis is a must. Very creative but misguided people create Internet technology. Pornographers have been at the forefront of writing codes that can actually take over a computer and open files that the user never intended to use. You have probably experienced some sort of "pop-up" ads when using the World Wide Web. This same technology can be applied on a large scale causing a seemingly endless series of differing pages to open on an individual's computer.

The expert can also use software to run searches for certain key words or phrases on a computer. As noted above, deleted files may still exist on the hard drive. Portions of files may still be in what experts call slack space or free space. Experts will not be able to recover all deleted files but the more recent the deletion the more likely the expert can recover the file because it likely will not have been overwritten. Deleted e-mail will most often be recoverable. Forensic examiners can check versions of a file against backups or other versions they find to determine when changes were made and what was changed. This can lead to very important historical information.

Become comfortable

With the proliferation of computerized information, we all have to learn to evaluate and use electronic evidence.

Unfortunately, most lawyers are not going to be able to evaluate the evidence just by taking a look at it. Learning how to work with an forensic expert and getting him or her on board early is essential in being able to understand and handle the challenges computerized evidence create for us. With some planning, though, even those of us who do not like to turn on computers can become comfortable with how to evaluate electronic evidence.

Notes

The Bureau of National Affairs, for example, through its subsidiary Pike & Fischer, publishes Digital Discovery & E-Evidence. See www.pf.com NACDL members have access to a forensic evidence hotline on the NACDL Web page, www.nacdl.org Upon request, I can provide you with an example of an application for expert funds we used in a retained case. Fed.R.Crim.P. 16(a)(1)(C).

visited on 9/07/2012

United States v. Pedram Ibrahimi, No. 02-0008 (N.D.Cal. 2/20/02). At the 2002 NACDL annual meeting Nanci Clarence and Geoffrey Hansen distributed copies of a number of cases allowing defense access to a mirror image of a hard drive. Just having access to those cases has allowed me to convince prosecutors that we are entitled to an exact copy of the hard drives.

United States v. Alan Tanner, No. 2: 01-00145 (S.D.W.Va. 6/26/01).

State cases seem to be in accord. See Taylor v. State, 2002 WL 31318065 (Tex. App. 10/17/02) (finding error where the defendant had not been given an exact copy of the hard drive and holding that merely allowing inspection of the questions images off of the drive was insufficient because it does not allow for proper expert analysis).

Having an "exact" image of a hard drive can pose its own problems. Just by booting up a computer, you can change the structure of the hard drive. Also, in order to use an exact mirror image of a hard drive, you might have to have the same CPU that the original drive came from.

1660 L St. NW • 12th Floor • Washington, DC 20036 • Phone: **(202) 872-8600** / Fax: **(202) 872-8690**

© 2011, National Association of Criminal Defense Lawyers (NACDL), All Rights Reserved.