Getting to the Drive:

Gaining Access to your Opponent's Digital Media

Craig Ball

Getting to the Drive:
Gaining Access to your Opponent's Digital Media
© Craig Ball

Nearly all business documents are born digitally, and from sprawling servers to Lilliputian laptops, digital evidence "lives" on hard disk drives. Securing access to those drives for forensic examination paves the way to smoking gun evidence and strategic advantage.

Because of fundamental flaws in the design of all personal computer operating systems—and especially in the ubiquitous Windows operating system—deleted data isn't really deleted at all. In fact, deleted data is just hidden from view, in what's called "unallocated space," until the disk areas it occupies are overwritten by other data. Windows also traps chunks of deleted information in surplus space that trails behind almost every file it creates. This "slack space" data, invisible to the computer user and often outliving its host file, may comprise dozens or even hundreds of megabytes of potential evidence. Then, there are the many places where Windows and software applications record programs used, files opened, searches run, web sites visited, documents printed and a host of other user activity. Little Brother is also watching!

Like skin, hair, fingerprints, fibers and DNA left at a crime scene, digital detritus holds the key to the whole truth, accessible through forensic examination of the hard drive. This vast body of potential evidence is almost entirely inaccessible to the Windows user and so won't be produced, even by those faithfully fulfilling discovery duties. Likewise, opponents who, through ignorance, guile or error, fail to produce what the law requires also make it harder to get to the truth. Smoking gun digital evidence may be missed due to file encryption or compression, faulty search techniques, slipshod preservation practices or because it resides in the fields and records of a complex database, accessible only through a properly-constructed query. Too, digital evidence may not be produced because your opponent adopts a narrow interpretation of what's discoverable or simply decides their interests would be served if you just didn't see it.

Even when digital evidence is found and diligently produced, its integrity can be unwittingly compromised. There are two components to any computer-generated record: the content of the record and the layer of information that holds data *about* the data in the record. This is *metadata*. Metadata may simply reflect a file's name, size and creation date, but it can also offer insight into the source of the data, its author, time it took to create, whether others have viewed it and so on. When a file is opened, even just to check its contents, its metadata is altered in ways that could significantly impact the case. Most lawyers don't appreciate that, absent safeguards, simply reviewing electronic evidence can be an act of spoliation.

In our system of civil justice, we request information and rely upon our opponents to grasp our requests, gather the responsive information and produce what the law obliges them to surrender. Back when evidence consisted principally of paper documents, relying on our opponents' diligence and good-faith made sense. Any lawyer can read

paper records, and when paper is "deleted," it's really gone. But, as discoverable "documents" metamorphose to electronic data, litigators and in-house counsel lacking computer expertise must either blunder through or rely upon technically-adept intermediaries to access or interpret the evidence. Put bluntly, whether due to ignorance, disconnection or a lack of diligence, lawyers don't do an adequate job responding to e-discovery. How, then, can a requesting party submissively accept a representation that, "discovery responses are complete" when, to a virtual certainty, discoverable evidence resides in places the opposition rarely, if ever, explores? The answer is: You can't. *You've got to get to the drive.*

Getting to the drive means securing a forensically-sound bit stream image or clone of the hard disk drives of computers used by key players in the matter made the basis of the action, and examination of those duplicates by a computer forensics expert. Though often lumped together, it's important to consider these tasks independently because each implicates different considerations for the parties and the court.

Drive Imaging

Drive imaging is a means of evidence preservation, and the duty to preserve potential evidence is broader—and attaches earlier—than the obligation to produce. Because computers constantly write to the drive, electronic evidence—particularly recoverable deleted material--is in constant jeopardy of being altered or obliterated. Drive imaging is the only way to preserve the status quo by capturing a "snapshot" of everything on the drive, ideally as soon as a potential claim or suit arises. A drive can be imaged without the necessity of anyone viewing its contents; so, assuming the integrity of the computer forensic expert, no privacy, confidentiality or privilege issues are at stake. Accordingly, imaging should be sought at once, and courts should have no hesitation to order same. Time is of the essence, so defer issues of access and privilege for another day in favor of saving the data now.

Specialized tools and techniques that don't alter the data are used to create forensically-sound duplicates. The cost to image a drive varies with the time, travel, complexity and data volume, but typically ranges from $750.00-$2,500.00, on par with the transcript of a half-day deposition. The more drives being duplicated, the easier it is to negotiate a lower per-drive cost. It can take hours to duplicate each drive, so it tends to cost more when done onsite versus in the lab.

A drive image is fingerprinted using a cryptographic technique called *hashing*, insuring the detection of any subsequent modification of the data. Hashing generates a unique digital signature for the data. The slightest subsequent change to the data will result in a different signature when hashed; however, the signature can't be reverse-engineered to reveal anything about the data except that it has changed. If the data signature of the duplicate drive is furnished to the Court or requesting party, the producing party can serve as custodian of the duplicate, and no one need fear undetected alteration.

Strategically, just having an untouchable duplicate drive "out there" has value. Not only does it tend to keep the opposition on the straight-and-narrow, it forces any improper

actions—in the form of data shredding and hiding—to be pursued between the request and forensic duplication, making shenanigans easier to detect. Plus, the knowledge that a duplicate exists exerts a powerful influence on those who know their contraband data (e.g., pornography, evidence of marital infidelity or tax cheating) may come to light--injecting additional incentive for prompt resolution.

CAVEAT: Your opponent may try to bamboozle the court by claiming forensic imaging is superfluous, as systems are routinely backed up. A back up of a drive is not forensically-sound because it doesn't preserve all of the hidden data, particularly the deleted files in unallocated space. Further, back ups are typically selective in what they retain, rarely mirroring everything on the drive.

Access to the Data

While imaging drives to preserve the status quo should be commonplace and require little judicial scrutiny beyond cost allocation and directives to minimize inconvenience, granting a party access to an opponent's drive should hinge on a demonstrated need and a showing of relevance. Orders should include safeguards to appropriately narrow the scope of examination and protect confidential and privileged data.

The easiest, oft-overlooked way to gain access to the drive is to simply ask for it. To show good faith or head off action by the court, opposing counsel may consent to the drive being duplicated and examined by your computer forensics expert. The parties typically employ a joint protective order or "claw-back" agreement establishing that the producing party is not waiving any privilege and may seek return of confidential information. Alternatively, the parties may agree to place the drive in the hands of a jointly-selected neutral with instructions to perform specified searches and recover deleted and hidden data, then share whatever is found with the producing party. The producing party then asserts any privileges, whereupon non-privileged material is shared with the requesting party and the balance held from production pending resolution of privilege claims.

Often, getting to the drive means convincing a court to grant access to one side's computer forensic expert or to a court-appointed neutral expert. The most compelling justification for court-ordered access is that the producing party can't be relied upon to fairly or effectively preserve, locate or produce electronic evidence. If it is shown that the producing party materially failed to preserve electronic evidence (such as by disposing of computers containing discoverable material), or acted to destroy or conceal such evidence (by, e.g., file deletion or use of applications tending to frustrate forensic examination), a Court is justified in granting access to the drive or turning the production responsibility over to a neutral third-party capable of recognizing and protecting privileged information. Where the producing party hasn't lost or destroyed responsive data but has failed to take suitable steps to locate and produce it, the court may still grant access or defer same pending further efforts by the responding party

Letting an opponent get to the drive may seem like a sanction, but it's more in the nature of a remedy. The decision to grant access to the media should hinge less upon

the ill intent of the producing party than upon whether the producing party has demonstrated an inability to preserve, identify and produce electronic evidence. Certainly, in cases of discovery abuse or spoliation, the court will not only seek to ameliorate harm by affording access to the offending party's drives, but will also assess the cost of such efforts against the bad actor and weigh whether an adverse inference instruction or other sanction is warranted. Even if the destruction or omission of electronic evidence was entirely innocent, the Court should look favorably on computer forensic analysis to prevent further failure and offset past hardship.

A common refrain raised in opposition to getting to the drive will be, "Your honor, letting them have access to the drive is like letting them come into my client's home or office and just start rooting around. It's a fishing expedition!" Another defensive objection is that affording access to the drive will reveal the contents of privileged or confidential communication; in particular, attorney-client communications. While the former objection is readily addressed by requiring a showing of need and relevance and by targeting specific objectives in the examination, the concern for privileged communications is best resolved by a claw-back agreement or, better still, by use of a neutral examiner operating under orders to initially reveal findings only to the producing party facilitating objection and creation of a privilege log.

The Preservation Letter

Some charge that electronic discovery has devolved into requesting parties "setting up" opponents as targets for charges of spoliation and discovery abuse. Certainly, electronic discovery hands litigants a big stick by forcing opponents to bear the true cost of computerization. In the rush to automate, businesses largely abandoned sound records management in favor of commingling just about everything on massive networks and strewing the rest across countless local hard drives and digital devices. Moreover, data is at once hard to destroy and hard to preserve, making the potential for spoliation a sword of Damocles hanging over the head of a careless or arrogant opponent. The headaches of electronic discovery, and the hardships arising from the duty to preserve digital evidence, bring these chickens home to roost.

Notwithstanding, courts are hesitant to say "tough luck," even to those who are the architects of their own demise. So, the ability to get to the drive is enhanced by showing that an opponent's failure to meet discovery obligations is more than a technical "gotcha,' but instead grew out of laziness, ignorance or contempt. This distinction is underscored by the use of a well-drafted preservation letter early in the proceedings. Such a letter should do more than just recite a litany of retention demands. It should also serve to educate your opponent about the nature of electronic evidence and the consequences of their actions, even going so far as to set out specific methodologies (e.g., disk imaging, discontinuance of defragmentation maintenance) to partly relieve your opponent of the burden of guessing what to do. Such a letter shouldn't be framed to limit preservation duties, but should make specific duties crystal clear. The path to the disk is shortened when you can say, "Judge, we explained what they needed to do and how to do it, yet they still failed to preserve the evidence."

Fighting to gain access to your opponent's hard disk drives is not a strategy suited to every case; but, where the failure to preserve or produce electronic evidence is at issue—and particularly when the specter of attempted data destruction looms—getting to the drive is getting closer to the truth…and to victory.

Craig Ball is a trial lawyer, e-discovery consultant and certified computer forensic examiner in Montgomery, Texas. He can be contacted as craig@ball.net or via www.cybersleuthing.com.