Reprinted with permission from Intellectual Property & Technology Law Journal

Intellectual Property & Technology Law Journal

formerly Journal of Proprietary Rights

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 16 • NUMBER 11 • NOVEMBER 2004

The Increasing Significance of Computer Forensics in Litigation

By Robert J. Benson

During the 1990s, the advent of email changed the face of discovery in commercial litigation. Employees often made unguarded comments in emails that, in years past, would have never found their way into written memos. Emails soon became a gold mine of useful information in litigation, and today, computer-retrieved data often outweighs paper production. In *Linnen v. A.H. Robins Co.*, computer forensic engineers recovered this now infamous email that discussed the side effects of the Phen-Fen drug: "Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?"[1] The email led to one defendant's paying out one of the largest settlements in history.

As individuals have become more cognizant of the dangers of archived emails and other electronic documents, they have also developed a variety of habits for deleting information from their computer systems. However, this can lead to even greater complications in subsequent litigation: The deleted files are usually recoverable, and the fact of the deletion can lead to a court's imposing serious sanctions for attempting to destroy relevant evidence.

The Growth of Computer Forensics

Computer forensics is thus becoming one of the most important tools in litigation, and it has found its most common application in intellectual property litigation. An increasing number of courts are ordering forensic inspections of computer systems for the purpose of recovering deleted information, and those deleted files often hold the highest prospect of turning up the proverbial smoking gun. Such was the case in *MediaTek, Inc. v. VIA Technologies, Inc.*,[2] a trade secret case in which the defendant denied having possession of plaintiff's source code. A forensic inspection of its engineers' hard drives resulted in the recovery of deleted emails that attached the source code at issue. The case settled not long thereafter for a license agreement that included a royalty payment of $50 million.

But discovering key evidence is only one benefit of conducting forensic discovery. Inspecting an adversary's computer system often reveals that relevant information was deleted during the litigation, when there was a legal obligation to preserve that evidence. This can lead to sanctions ranging from the entry of default judgment[3] to giving the jury an adverse inference instruction at trial.[4] The more effectively that a party renders its prior data unrecoverable, the greater its risk of having a default sanction entered against it. Indeed, it is surprising how often information is deleted *after* a court has ordered the inspection of a computer system, which reflects a high degree of ignorance as to the forensic inspection that is about to occur and the sanctions that might result.

Obtaining Discovery of Deleted Electronic Files During Litigation

There are a variety of approaches to obtaining discovery of deleted electronic files during litigation. One approach is to bring a motion to compel another party to recover files from its own computers at its own expense. Not surprisingly, however, a litigant will rarely be satisfied with its adversary's efforts in this regard.[5] Accordingly, the most frequent approach is to seek a court order requiring the production of computer systems or

hard drives for inspection by a forensic expert hired by the other party or establishing procedures for the inspection of the hardware by a court-appointed expert.

A mere suspicion that another party has failed to fully comply with its discovery obligations is usually considered an insufficient basis for a court to order the inspection of its computer systems.[6] Nevertheless, the threshold for obtaining an inspection order is not always difficult to meet. For example, testimony by an individual that he routinely deletes email has been found sufficient to support a court order requiring the inspection of his hard drive.[7] Another common scenario is when an email is produced by one party or individual but another party or individual does not produce the same email despite being identified as the sender or a recipient of that email. This gives rise to an inference either (1) that the party has the email on its computer system but is not producing it or (2) that the party deleted the email from its system. This also can warrant an order for a computer inspection.[8] A party also may establish, through other evidence, that its adversary had possession of certain information at one time and then use the adversary's failure to produce that information in discovery as a basis for ordering a forensic inspection of its computer systems.[9]

The Availability of Injunctive Relief

While inspection of an adversary's computer system is typically done during the discovery process, it also may be achieved through injunctive relief. In certain circumstances, courts have been willing to enter a TRO or a preliminary injunction prohibiting a party from deleting electronic information or requiring that computer systems be turned over for inspection.[10] This is often combined with other relief. Procedurally, satisfying the legal requirements for the issuance of a TRO or a preliminary injunction will usually be more difficult than prevailing on a motion to compel discovery.[11] On the other hand, an injunction may be able to go further in directing a party to cease future activity that has the potential of further destroying or deleting electronic evidence and rendering it unrecoverable. Moreover, the violation of an injunction or TRO may result in a party being held in contempt of court and is likely to result in stronger sanctions than a violation of a discovery order.[12]

When seeking the right to inspect an adversary's computer system, it is important for the inspecting party to consider whether it is seeking to recover active files, deleted files, or both. This may affect the proof required to obtain the order for the inspection. For example, if the evidence shows that a party has deleted information from its computers but does not indicate that the party has withheld from discovery active information on its computers, then the court may restrict its order to the recovery of deleted files.[13] However, if the court finds that a party has engaged in inappropriate conduct by withholding or deleting relevant information on its computer systems, it may be willing to authorize recovery of both active and deleted files, even if the evidence is primarily directed toward one or the other.[14] Regardless, a litigant must be able to reasonably tie the scope of the requested relief to the evidence that warrants the inspection.

Procedures Governing Forensic Inspection of Computer Systems

In the normal course of discovery, a party simply collects its own documents for production, including information that resides on its computer system. However, if a party is ordered to produce an entire computer or hard drive for inspection, it is not physically possible to limit the inspection to relevant information.[15] For this reason, inspections are usually conducted by a computer forensic expert, with no one else being allowed to participate in the inspection itself.[16] Moreover, to minimize business disruption and to preserve the integrity of the data, the expert is often directed to make mirror images of the media, maintain custody of those images during the remainder of the litigation, and provide certain specified data to the parties.[17]

The next issue involves the scope of the search itself. Courts typically establish protocols for identifying and producing only non-privileged information that is relevant to the litigation. Relevance parameters may include limitations in time (the dates files were created or last modified) and the use of specified search terms to limit the substance of the information produced. The search also may be restricted to computer hardware that certain individuals had access to or files created by particular individuals. Moreover, if the producing party can fairly argue that privileged information may reside on the system, then that party will be afforded an opportunity to review information for privilege before it is produced to its adversary.

A separate question is whether, and to what extent, the party producing its computers for inspection should be allowed to screen recovered information before it is produced to the inspecting party. In some cases, attorneys for the party producing the hardware have been permitted an opportunity to review recovered data for relevance, responsiveness to discovery, *and* privilege prior to that information being produced.[18] However, when electronic files have been deleted, the inspecting party may not trust opposing counsel to make determinations of relevance, as documents withheld on that basis will not be reflected on a privilege log and therefore cannot be subject to scrutiny. It therefore may be advantageous to obtain a court order that allows the forensic expert to identify information that contains certain relevant search terms and produce it directly to both parties. Only information that is potentially privileged should be withheld from that production.[19] Alternatively, the forensic expert could provide all recovered information to the court for an *in camera* review, after which the court would provide all discoverable, non-privileged information to the party seeking the discovery.[20]

The party seeking discovery also should ensure that the forensic expert is allowed to determine when and how the recovered files were deleted. If files were deleted during the litigation or after the court ordered the computer inspection, this could give rise to serious sanctions. Accordingly, the forensic expert should be asked to determine when the recovered files were deleted, how the files were deleted (*e.g.* by a particular software application), and to provide any available information about deleted files that could not be recovered.[21]

The Technological Process for Recovering Deleted Information

A forensic inspection usually begins by making mirror images of the media in question. This mirror image is a perfect sector-by-sector, bit-by-bit copy of the media of the drive and includes the unused and partially overwritten spaces where important evidence may reside. Moreover, the imaging process does not require that the operating system be turned on, ensuring that the system is not altered in any way during the imaging process. This preserves the evidentiary value of the information

recovered, because even booting up a computer can alter critical evidence, such as creating new dates or modifying existing dates associated with the files in question.

Once the mirror image is created, forensic experts can search for active data, recover files and directories that have been deleted, and identify unused space (either because it has never been used or because the information contained there has been deleted by the user and then marked by the computer as available for writing new information). In addition to recovering files that have been deleted by the user, files can be recovered when a drive has been reformatted, because in most cases reformatting does not actually harm the data on the drive but only eliminates document indexes and file/folder pointers. Defragmentation of a hard drive sometimes makes its data unrecoverable, but not always. Only certain types of wiping utilities tend to render data completely unrecoverable. This procedure involves running an application that intentionally overwrites data with a pattern of 1s and 0s. Even then, however, forensic experts often can determine the date, time and specific program used to conduct the wiping, which can provide a basis for evidentiary sanctions.

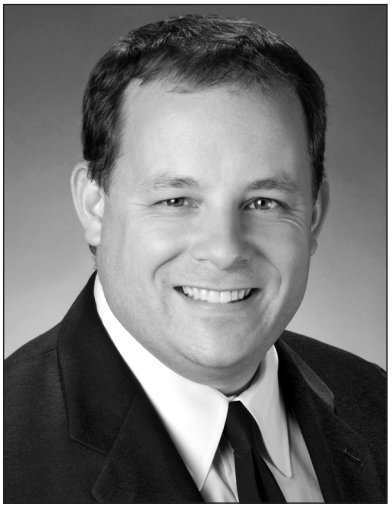
Forensic experts can do more than just recover deleted files. For example, they often can determine whether and when files have been altered, damaged, or deleted; provide a historical account of content contained in a file; determine who had access to a drive; recreate a chain of events or user activity, such as internet activity; conduct electronic searches to quickly retrieve relevant data; or recover multiple drafts of a document.

Accordingly, it is important for litigants to become familiar with the services that a computer forensic expert can provide, as well as the procedures by which computer inspections can be obtained during litigation. Forensic inspection of computer media is one of the new frontiers of discovery, and it is sometimes the most fruitful approach to obtaining the critical evidence that is needed to win a case or force it to settlement.

Notes

1. Linnen v. A.H. Robins Co., Inc., 1999 WL 426015 (Mass. Super. 1999) (granting motion to compel production of email back-up tapes).
2. MediaTek, Inc. v. VIA Technologies, Inc., Case No. C02-05016 (C.D. Cal. 2004) (order of Magistrate Robert N. Block dated Feb. 17, 2004).
3. *See, e.g.*, Computer Assoc. Int'l. Inc. v. American Fundware, Inc., 133 F.R.D. 166, 170 (D. Colo. 1990) (defendant's intentional destruction of each revision of its source code during litigation supported the entry of a default sanction). *But cf.* Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., 2003 WL 22433095 (N.D. Ill. 2003) (magistrate judge recommended that the plaintiff's case be dismissed with prejudice as a result of plaintiff's using a software program called Evidence Eliminator to delete and overwrite thousands of files prior to a forensic inspection; district court, however, postponed consideration of a default sanction to see if infringement could be adequately proved by other evidence).
4. An adverse inference instruction allows the jury to assume that the content of destroyed information would have been detrimental to the party that destroyed it. *See, e.g.*, Anderson v. Crossroads Capital Partners, L.L.C., 2004 WL 256512 (D. Minn. 2004) (forensic expert determined that plaintiff had run a data wiping software application on her hard drive during the litigation, but court found conduct was not sufficiently egregious to warrant dismissal.)
5. Such was the case in Aero Products Intern., Inc., v. Intex Recreation Corp., 2004 WL 417193 (N.D. Ill. 2004), where the defendant was ordered to recover deleted emails and other files from its own computer systems. When the plaintiff complained of the defendant's alleged failure to conduct an adequate search, the court refused to sanction the defendant because the plaintiff had not itself requested the appointment of a neutral computer forensics expert when it had the opportunity.
6. *See, e.g.*, Bethea v. Comcast, 218 F.R.D. 328, 330 (D.D.C. 2003) (motion to compel computer inspection denied); Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc., 2003 WL 1809465 (N.D. Ill. 2003) (same). However, one court ordered a forensic inspection of defendant's equipment to recover any deleted files based solely on the conclusion that defendants might have "relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant." Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652-653 (D. Minn. 2002).
7. *See, e.g.*, Renda Marine, Inc. v. United States, 58 Fed. Cl. 57 (Fed. Cl. 2003).
8. *See, e.g.*, Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., 2003 W.L. 21230605 (N.D. Ill. 2003) (motion for inspection of computer system granted when no email correspondence had been produced between the producing party and its third-party vendors or customers, and evidence existed from the third party that at least some such correspondence had taken place); Playboy Enterprises, Inc. v. Welles, 60 F.Supp. 2d 1050, 1054, (S.D. Cal.1999) (co-defendant produced copies of emails between herself and the other co-defendant, which the latter had not produced herself).
9. In *MediaTek*, the plaintiff had established a likelihood of success on its claim that defendant had misappropriated its source code (by obtaining a preliminary injunction), but defendant had not produced a single copy of plaintiff's source code during discovery. MediaTek, Inc. v. VIA Technologies, Inc., Case No. C02-05016 (C.D. Cal. 2004) (order of Magistrate Robert N. Block dated Feb. 17, 2004).
10. Dodge, Warren & Peters Ins. Services, Inc. v. Riley, 130 Cal.Rptr. 2d 385 (Cal.App. 2003) (affirming injunction).
11. *See, e.g.*, Gorgen Co., Inc. v. Brecht, 2002 WL 977467 (Minn.App. 2002) (reversing a TRO that prohibited the destruction of electronic data because plaintiff did not adequately demonstrate that it should be entitled to such "extraordinary relief").
12. QZO, Inc. v. Moyer, 594 S.E. 2d 541, 547-558 (S.C.App. 2004) (in a trade secret case, reformatting a hard drive prior to turning it over in response to a TRO was sufficient grounds for striking the pleadings of the defendant).
13. For example, in *Antioch,* 210 F.R.D. at 653, n.7, the court expressly limited its order to the recovery of *deleted* information on defendants' computer system, reasoning that defendants had the responsibility for producing information that they had access to and plaintiff had not made a sufficient showing that defendants were unwilling to produce relevant evidence that had not been deleted from their computer systems.

14. This was the case in *MediaTek*, where defendants sought to limit the court's order to the recovery of deleted files from its engineers' hard drives. However, in view of a pattern of obstructionist behavior during discovery, the magistrate judge allowed the forensic expert to recover and produce active files as well.
15. In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (reversing an inspection order because it provided direct, unlimited access to defendant's databases); Southern Diagnostic Associates v. Bencosme, 833 So.2d 801, (Fla.App. 2002) (a court order must "define parameters of time and scope and must place sufficient access restrictions" to prevent discovery of confidential information and to prevent harm to the computer system.
16. The expert may be one agreed upon by the parties or selected by the court and would be required to sign an appropriate protective order. It may be advantageous to request that the court appoint a neutral expert as an officer of the court to avoid a subsequent battle of the experts. It also may be required that communications between the expert and either party, or either party's counsel, be in the presence of or copies to opposing counsel to avoid charges that the expert has been tainted by having ex parte communications with one party or the other.
17. *See, e.g.*, *Antioch*, 210 F.R.D. at 652-653; Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 641-642 (S.D.Ind. 2000); *Playboy*, 60 F. Supp.2d at 1054.
18. For example, in *Welles*, 60 F.Supp.2d at 1054, *Simon*, 194 F.R.D. at 641-642, and *Antioch*, 210 F.R.D. at 653, defendants' counsel was allowed to review deleted emails recovered from a clients' hard drives and then only produce non-privileged communications that were responsive to particular document requests and relevant to the subject matter of the litigation.
19. In Tulip Computers Intern. B.V. v. Dell Computer Corp., 2002 WL 818061 (D.Del. 2002), after emails were sorted using agreed-upon search terms, they were reviewed by defense counsel only for privilege and confidentiality (designation under the protective order) prior to production. The court in *MediaTek* was even more restrictive. The magistrate judge rejected defendants' request to review recovered files for relevance prior to their production. Moreover, even as to privileged information, the court required that the forensic expert (rather than counsel) segregate out potentially privileged information based on certain agreed-upon criteria, after which defendants' counsel could conduct a further privilege review. *See also* First USA Bank, N.A. v. PayPal, Inc., 76 Fed. Appx. 935 (Fed. Cir. 2003) (search protocol apparently allowed experts to identify any relevant documents following an inspection of a deponent's laptop computer and then allowed the deponent an opportunity to create a privilege log prior to production).
20. *See, e.g.*, Travers v. McKinstry Co., 2001 WL 34041790 (D.Or. 2001).
21. *See, e.g.*, *Simon*, 194 F.R.D. at 641-642.



Robert Benson is a partner in the Los Angeles office of Hogan & Hartson where his practice focuses on complex intellectual property litigation for clients in the U.S., Taiwan and Japan. He has handled patent infringement, copyright infringement and trade secret misappropriation cases involving a variety of technologies and products including computer hardware, software, and consumer electronics.

HOGAN & HARTSON LLP

LOS ANGELES OFFICES:
DOWNTOWN: 500 SOUTH GRAND AVENUE; LOS ANGELES, CA 90071; 213/337-6700; 213/337-6702 (FAX)
CENTURY CITY: 2049 CENTURY PARK EAST, LOS ANGELES, CA 90067; 310/789-5100; 310/789-5400(FAX)
WWW.HHLAW.COM