

Cracking the Computer Forensics Mystery

by Christopher Wall and Jason Paroff

Only a few short years ago, the term “computer forensics” was a mystery to most attorneys. In the digital age, however, attorneys are discovering that a basic understanding of “computer forensics” and computer forensic protocol is crucial in both civil and criminal lawsuits. Without a doubt, most information generated today is stored electronically. In 2002, approximately 5 exabytes of new information was stored in print, film, magnetic, and optical storage media. 92% of that information was stored on magnetic media, mostly in hard disk drives.² Because of the increasing trend toward creating and using electronic documents, the computer is becoming a vital point of investigation in almost every case. Computer forensics can be essential in uncovering twenty-first century evidence.

A recent Minnesota sexual harassment and whistleblower case is a good example of how computer forensics technology can be used to solve a discovery mystery.³ In *Anderson v. Crossroads Capital Partners, L.L.C.*, the court ordered the plaintiff to furnish the defendant with copies of all relevant documents that existed on the plaintiff’s personal computer, including deleted or corrupted files. Pursuant to the judge’s order, the defendant’s computer forensic expert examined the plaintiff’s hard drive and discovered that a data wiping software application had been installed after plaintiff had agreed not to “delete any existing documents.” The court noted that the plaintiff’s “exceedingly tedious and disingenuous claim of naiveté regarding her failure to produce the requested discovery... defies the bounds of reason” and issued an adverse inference jury instruction because the plaintiff intentionally destroyed evidence and attempted to suppress the truth. *Anderson* is just one example of the ever growing host of cases in which a computer forensic examination and expert have helped decipher electronic evidence enigmas.⁴

CHRISTOPHER WALL is a Utah Bar member and a Kroll Ontrack Legal Consultant based in Washington, D.C.



Computer Forensics 101: What is Computer Forensics?

A. Defining Computer Forensics

Computer forensics is the “who, what, when, and how” of electronic evidence. Typically narrow in scope, it attempts to reconstruct events, focusing on the computer-based conduct of an individual or group of individuals. The types of cases involving computer forensics are numerous and varied – from the personal (i.e. locating hidden assets in a messy divorce case), to the political (i.e. investigating alleged misuse of government computers for political gain), to the dramatic (i.e. “What was your client’s former employee downloading from the Internet before he was fired and brought suit for wrongful termination?”).

According to the Sedona Conference, a legal and political think tank founded for the purpose of establishing reasonable standards and principles for handling electronic evidence, “computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.”⁵

At the heart of computer forensics is the idea that within the electronic realm of evidence, delete does not really mean delete. The investigations into Enron’s accounting irregularities illustrate how persistent deleted information can be. Weeks before Enron filed for bankruptcy, it became apparent that several major financial institutions had helped Enron manipulate its numbers and mislead investors with secret loans. During the subsequent investigations, one piece of evidence that received broad attention was an internal e-mail at JP Morgan Chase that described one of

JASON PAROFF is Director of Computer Forensic Operations for Kroll Ontrack, and is based in Secaucus, New Jersey.



these secret loans called a “prepay.” The email chain began, “Enron loves these deals as they are able to hide funded debt from their equity analysts because they (at the very least) book it as deferred [revenue] or (better yet) bury it in their trading liabilities.” Another internal e-mail expressed concern: “Five [billion] in prepays!!!!!!!!!!!!!!” The reply? “Shut up and delete this email.”⁶ JP Morgan’s employees apparently were not aware of what some courts have said about deleted email. According to one court, “Technically, email messages are permanently recorded since ‘most email programs keep copies of every message a user ever wrote, every message the user ever received, and every message the user deleted.’...’A deleted file is really not a deleted file, it is merely organized differently.”⁷

Indeed, where relevant information can be expected to be located, deleted data can be recovered and the results of the forensic analysis can often yield a potential treasure trove of information. Regardless of whether the information is beneficial or detrimental, counsel can best assess the merits of the case the earlier he or she knows about it.

B. The Computer Forensics Process

Given the wealth of electronic information available to individuals and corporations today, laptop and desktop hard drives or networked servers and backups are often the best place to begin collecting potential evidence. An investigation involving computer forensics typically begins by making a bit-by-bit image or copy of the hard drive or electronic media in question, thereby preserving the integrity of the original media. This image of the data includes all of the unused and partially overwritten spaces on the electronic media where important evidence may reside. When properly done, a forensically sound image does not alter the information on the original hard drive or electronic media.

Once the forensic image has been made, a computer forensic expert can search for active data (data that was immediately accessible to an individual using the computer when the image was made), recovered data (files and directories that were recovered after they had been deleted), and unused space (portions of the media that are either “free” because they have never been used or because the information contained there has been deleted, and the computer has marked that space as available for use by new information).

II. Computer Forensics Case Law: Civil and Criminal Crackdowns

In the twenty-first century, the legal community is recognizing the significant evidentiary role that computers play in civil and criminal cases. Because of rapid advances in technology, case

law and legislation dealing with computer forensics is changing daily. Some of the important computer forensic case law in both criminal and civil cases includes cases dealing with cyber sabotage, email investigations, deleted data, Internet activity, and spoliation.

A. Cyber Sabotage

Because computer crimes are increasing at alarming rates, law enforcement officers, investigators, lawyers and judges are increasingly barraged with technical issues. Accordingly, an understanding of current computer forensics law is vital in offering accurate and thorough computer expert testimony. In a 2001 case, *U.S. v. Lloyd*, testimony by computer experts led to the conviction of an individual charged with a modern “cyber-crime.”⁸ Without testimony from the computer experts, evidence of the computer “time bomb” that sabotaged operations at an engineering company would not have been recovered.

B. Email Investigations

Perhaps more than any other technological innovation, email has become an integral part of daily activity and electronic discovery. As such, computer forensic engineers are regularly called upon to investigate and analyze email communication. *United States v. Bach*, a child pornography case, illustrates precisely how computer forensics can be used where email is at issue.⁹ Pursuant to a search warrant, Yahoo! computer experts retrieved all of the information contained in the defendant’s email account. Because police were not present when the defendant’s email account was searched, the lower court ruled that the seizure of the emails by Yahoo! was unlawful. The appellate court reversed the lower court decision, finding that Yahoo!’s search of the defendant’s email account without a police officer present was reasonable under the Fourth Amendment and did not violate the defendant’s privacy rights.

C. Deleted Data

Unless steps are taken to hide or remove deleted data more permanently, computer forensic engineers can recover and examine deleted information. And lest counsel think that the deleted information is not subject to discovery, significant case law suggests the opposite.¹⁰ The case law, both at the State and Federal level, is full of civil and criminal decisions where the individual quite clearly failed to understand that the “delete” key on the keyboard is not the equivalent of a paper shredder.

For example, in *United States v. Tucker*, Utah District Court Judge Campbell found Jeffrey Tucker guilty of knowingly possessing child pornography.¹¹ Computer forensic evidence gathered from deleted Internet cache files that still resided on Tucker’s hard

drive, even after being deleted, were an integral part of the case against him. The cache files were stored on his hard drive when he visited various websites containing child pornography. Even though the files had been deleted, they were still recoverable by a computer forensics expert. Cases like *Tucker* illustrate how critical computer forensics can be in finding seemingly deleted data.¹²

D. Internet Activity

Computer forensics can also play a vital role in criminal investigations. *State v. Guthrie*, a case dealing with a criminal prosecution for murder, is a good example.¹³ In *Guthrie*, a preacher's wife was found dead in the bathtub, a victim of an apparent suicide. Suspicious of the apparent suicide, investigators began looking into the case. Shortly thereafter, a suicide note appeared. Investigators enlisted the aid of a computer forensics expert, who discovered that Guthrie's computers at home and at church had been used to conduct numerous Internet searches on subjects related to bathroom deaths. Additionally, the forensic analysis revealed that the computer-printed suicide note, offered to exculpate the defendant, was created several months after the victim's death. Needless to say, Mr. Guthrie now finds himself preaching to a congregation of a different stripe.

E. Spoliation of E-Evidence

Courts will not hesitate to admonish or sanction parties for bad faith maneuvering, rule violations, and negligent or intentional spoliation. Sanctions for such conduct have included adverse inferences or presumptions, preclusion of evidence, monetary sanctions, and dismissal or default. *Procter & Gamble Co. v. Haugen* demonstrates that Utah courts are not hesitant to impose sanctions for electronic discovery violations.¹⁴ *Procter & Gamble* was an unfair competition case in which the defendant moved for sanctions, alleging that the plaintiff violated its duty to preserve relevant email communications of five key employees. Finding that the plaintiff breached its duty to preserve, the court sanctioned the plaintiff \$2,000 – \$10,000 for each of the five employees. The court also granted the defendant's motion to dismiss the case without prejudice, since the plaintiff failed to preserve relevant electronic data that it knew was critical to the case. The court determined that the plaintiff's violation of four separate discovery orders made defending the case "basically impossible" since the crucial electronic evidence was apparently no longer available.

An Illinois federal district court also imposed sanctions for deleting electronic evidence in a recent patent infringement case, *Kucala Enters. Ltd. v. Auto Wax Co.*¹⁵ Based on digital clues left on the hard drive, computer forensic experts were able to determine that the plaintiff used "Evidence Eliminator,"

a software wiping utility, to delete and overwrite over 12,000 electronic files. An expert further determined that 3,000 additional files had been deleted and overwritten three days earlier. Although there was no clear indication that relevant evidence existed among the destroyed files, the court described the plaintiff's actions as "egregious conduct" and emphasized the plaintiff's apparent intent to destroy evidence that it had a duty to maintain. The magistrate judge recommended to the district court that the plaintiff's case be dismissed with prejudice and that the plaintiff be ordered to pay the defendant's attorney fees and costs incurred in defending the motion.

As *Procter & Gamble* and *Kucala* illustrate, courts will not hesitate to impose sanctions for intentional or negligent spoliation of electronic documents. Spoliation cases dealing with electronic evidence are legion, and the cases cited here are but a sampling of how some courts are dealing with the issue.¹⁶

III. Computer Forensics Best Practices: Decoding the Computer Forensics Mystery

When it comes to gathering and searching computer data for relevant information, many attorneys may feel inexperienced. Multiple computer systems may be involved, each of which may contain hundreds of gigabytes of data or more. Complicating matters, many different *types* of computers may also be involved, and each can contain a different operating system (i.e. Windows, Macintosh, Linux, etc.) or serve unique functions (i.e. email, database, file/print/antivirus server, etc.). Each may require different handling methods in order to effectively retrieve, copy, and search the data they possess. Listed below are three basic guidelines that counsel and their clients should follow when facing a computer forensics issue in litigation.

A. Clueing in on the Computer Forensics Process

When retrieving electronic data, the following steps should be taken: (1) consultation with clients and computer forensic experts, (2) data preservation, (3) data collection, (4) data recovery and analysis, and (5) expert testimony and reporting.

First, an attorney should consult with the client and a computer forensic expert to create a strategy for collecting, analyzing, and processing the data. The strategy may include analysis of where the critical information could exist as well as the identification of properly qualified individuals to perform the work.

Next, attorneys should take proper precautions to preserve data. In many cases, a computer forensics expert using industry best practices will first make a mirror image, which is a bit-by-bit copy of a hard drive that ensures the computer system is not altered during the imaging process. Additionally, the expert will

ensure that no possible evidence is damaged and that no computer viruses are introduced. Techniques that are generally understood within the industry and are considered to be reliable must be established for the handling of data. Though not an exhaustive list by any means, examples include chain-of-custody control, protection from magnetic fields and other dangers that can damage data, mirror imaging, and duplication techniques that do not alter the data and can verify that an exact copy was obtained, and analysis tools that accurately convey the information being reviewed.

Once the relevant data has been identified, a computer forensic expert can retrieve data from virtually all storage media and operating systems, including legacy and obsolete hardware systems. During the data recovery process, the expert will recover active data, deleted data, and/or email and access inactive and unused data storage areas. Finally, a computer forensic expert can help win a client's case by offering expert testimony and reporting. The expert can customize reports about the data collected and produced to support the case, provide data for affidavits or other pleadings, and provide expert testimony at a trial or hearing.

B. Hiring a Cybersleuth

Computer forensic investigators must have advanced computer knowledge, with specialized data recovery and computer investigation analysis skills. Ideally, such experts should have some formalized training such as law enforcement training courses offered by large departments and agencies and certification courses offered by recognized private sector companies. Not every computer forensics specialist has deep systems knowledge, and most information technology specialists know little about computer forensics procedures. The needs of a client can be broad, and often a team of individuals with different skill sets may be required to effectively handle a case heading for, or involving, litigation.

Reliable techniques and protocols may include:

- Recreating a specific chain of events or user activity, including Internet activity, email communication, file deletion, etc.;
- Searching for key words and dates and determining what resulting data is relevant;
- Searching for copies of previous document drafts;
- Searching for potentially privileged information;
- Searching for the existence of certain programs such as file wiping programs; or
- Authenticating data files and the date and time stamps of those files.

A forensic expert's job does not necessarily end with recovering a lost or deleted "smoking gun" document. Often, the expert can also determine whether an electronic file has been tampered with, altered, damaged or removed. In essence, the expert can help recreate a course of events relating to the primary user of the computer in question as if the hard drive itself were the scene of a crime or event. Once that analysis is complete, the computer forensic expert can provide expert reporting and testimony to assist the court, counsel, or the fact finder in resolving a case.

C. Solving the Computer Forensics Mystery in Court

People have been known to falsify evidence, alter it, or attribute it as something other than what it really is. As a result, courts have a right (and an obligation) to question the validity of electronic evidence. Maintaining a "chain of custody" on pieces of relevant media is the best way to proactively ensure admission of the data into evidence at trial. A proper chain of custody ensures the reliability of evidence and minimizes any risk that evidence was changed, altered, or modified from its original form on the hard drive.

When called to testify, a computer forensics expert might be asked the following questions and provide the following hypothetical responses:

1. *What is the evidence, or what does it purport to be?*

Forensics Expert: "This is a printout of data that I recovered on 1/1/04 from the hard disk drive primarily used by John Doe of the Acme Corporation."

2. *Where did it allegedly come from?*

Forensics Expert: "The hard drive was taken from the office of John Doe on 12/15/03. It was contained within a Generic PC bearing model XXXX and S/N YYYY."

3. *Who created, discovered, or recovered it?*

Forensics Expert: "The data appears to have been created by John Doe. I discovered and recovered it from his hard disk drive using computer forensic techniques."

4. *How was it created, discovered, or recovered?*

Forensics Expert: "I made an image of the hard disk drive using a forensic imaging device. This device is designed to make a perfect copy of a disk and does not alter the data on the disk being copied."

5. *Were there any material changes, alterations, or modifications during the recovery of the evidence such that it may no*

longer be what it once was?

Forensics Expert: “No. Our processes as well as the tools that we use are designed to ensure that no changes whatsoever occur to the original media and data we work on. We use write-blocking devices as an extra precaution in this regard. We test our tools, both software and hardware in order to validate that no changes are made to the original media, and to insure that a perfect image is made of that media.”

6. What has happened to it since the time it was created, discovered, or recovered? Is there any chance that the evidence was changed, altered, or modified between the time you imaged the drive and today?

Forensics Expert: “Here is our ‘chain of custody’ documentation which indicates where the media has been, whose possession it has been in, and the reason for that possession. There is no chance that during that time any of the evidence was changed/ altered/modified from the form in which it existed on the drive that we imaged on 12/15/03.

After a computer expert is able to verify the authenticity and reliability of the evidence, a court is well within its province to admit the evidence for consideration by a jury. Accordingly, an attorney will be in the best position to argue to the judge or jury the weight that should be given to the evidence. Just as the computer has become essential in modern times, computer forensic evidence is becoming a crucial aspect of many investigations and legal matters. A solid understanding of electronic evidence concepts will help attorneys solve any computer forensics mystery.

1. The authors gratefully acknowledge the assistance of Charity J. Delich, Kroll Ontrack Electronic Evidence Law Clerk and second year law student at William Mitchell College of Law.
2. Ninety-two percent of new information is stored on magnetic media, primarily hard disks. Film represents 7% of the total, paper 0.01%, and optical media 0.002%. <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#summary>
3. *Anderson v. Crossroads Capital Partners, L.L.C.*, 2004 WL 256512 (D.Minn. Feb. 10, 2004).
4. *See, e.g., In re Lorazepam and Clorazepate Antitrust Litig. v. Mylan Lab., Inc.*, 300 F.Supp.2d 43 (D.D.C. 2004) (requiring Plaintiff to take CD-ROMs to a computer forensic expert); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 WL 23018270 (E.D.Va. Dec. 5, 2003) (directing that discovery must be done with the assistance of a computer forensic expert); *Playboy Enters., Inc. v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999) (appointing a computer expert who specialized in the field of electronic discovery to create a “mirror image” of Defendant’s hard drive).
5. *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* (Sedona ConferenceSM Working Group Series 2004). <http://www.thesedonaconference.org>
6. Brown, Gary M. “Senate Investigator to Enron’s Lawyers: It’s Not Over.” *Corporate Board Magazine*, Special Legal Issue, 2003. http://www.boardmember.com/issues/archive.pl?article_id=11523

7. *State v. Townsend*, 57 P.3d 255 (Wash. 2002) (Bridge, J. concurring).
8. *United States v. Lloyd*, 269 F.3d 228 (3rd Cir. 2001).
9. *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002).
10. *See, e.g., Dodge, Warren, & Peters Ins. Servs. v. Riley*, 130 Cal.Rptr.2d 385 (Cal. Ct. App. 2003) (ordering Defendants to allow a court-appointed expert to copy the data, recover lost or deleted files, and perform automated searches of the evidence under guidelines agreed to by the parties or established by the court); *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000) (requesting party should have access to active and deleted data alike); *Caldera, Inc. v. Microsoft Corp.*, 72 F. Supp. 2d 1295 (D. Utah 1999) (finding that a series of intra-company emails offered “direct evidence” that the corporation was actively trying to destroy a competitor).
11. *United States v. Tucker*, 150 F. Supp. 2d 1263 (D. Utah 2001). *See also, United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002).
12. *See, e.g., State v. Townsend*, 57 P.3d 255 (Wash. 2002) (Bridge, J. concurring) (court affirmed that deleted information is fully discoverable if relevant).
13. *State v. Gutbrie*, 654 N.W.2d 201 (S.D. 2002).
14. *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D.Utah 1998), *rev’d on other grounds*, 222 F.3d 1262 (10th Cir. 2000). *See also, Procter & Gamble Co. v. Haugen*, 2003 WL 22080734 (D.Utah Aug. 19, 2003).
15. *Kucala Enters. Ltd. v. Auto Wax Co.*, 2003 WL 22433095 (N.D.Ill. Oct. 27, 2003). *See also, Kucala Enters., Ltd. v. Auto Wax Co.*, 2003 WL 21230605 (N.D.Ill. May 27, 2003).
16. *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D.Utah 1998), *rev’d on other grounds*, 222 F.3d 1262 (10th Cir. 2000) (where Plaintiff’s breached its discovery duties, court imposed \$10,000 in sanctions – \$2,000 for each of the five custodians); *see also Procter & Gamble Co. v. Haugen*, 2003 WL 22080734 (D.Utah Aug. 19, 2003) (granting Defendant’s motion to dismiss with prejudice where the Plaintiff failed to preserve relevant electronic data that Plaintiff knew was critical to the case, violating four separate discovery orders requiring production of the data); *Anderson v. Crossroads Capital Partners, L.L.C.*, 2004 WL 256512 (D.Minn. Feb. 10, 2004) (granting adverse inference jury instruction because the Plaintiff intentionally destroyed potentially damaging evidence); *Zubulake v. UBS Warburg*, 2003 WL 22410619 (S.D.N.Y. Oct. 22, 2003) (ordering Defendant to bear the Plaintiff’s costs for re-deposing certain witnesses for the limited purpose of inquiring into the destruction of electronic evidence and any newly discovered emails); *Landmark Legal Foundation v. Environmental Protection Agency*, 272 F.Supp.2d 70 (D.D.C. 2003) (finding the EPA in contempt and concluding that the appropriate sanction was Plaintiff’s attorney’s fees and costs incurred as a result of the EPA’s conduct); *RKI, Inc. v. Grimes*, 177 F.Supp.2d 859 (N.D. Ill. 2001) (ordering Defendant to pay \$100,000 in compensatory damages, \$150,000 in punitive damages, attorneys’ fees, and court costs).