



NEW TECHNOLOGIES INC.

The Digital Discoverer

Trends in computer forensics & e-discovery for civil litigators

Practical Strategies for Digital Discovery: Evidentiary Considerations

BY ERIC VAN BUSKIRK, ESQ.



In part one of this two-part story (published in the February issue of *The Digital Discoverer*) the author discussed digital discovery issues to consider and resolve in the preliminary stages of litigation. In part

two, the author focuses on evidentiary issues of particular concern in digital discovery.

The Duty to Preserve Evidence

Courts have held there exists a duty to preserve evidence as soon as litigation is foreseeable or “reasonably foreseeable.” (*Shamis v. Ambassador Factors Corp.*, 34 F. Supp. 2d 879, 888-89 (S.D.N.Y. 1999)). Other courts have held the duty does not attach until a complaint is filed. (*Danis v. USN Communications, Inc.*, No. 98-C-7482, 2000 U.S. Dist. LEXIS 16900, at *99 (N.D. Ill. Oct. 20, 2000)). Although the general duty to preserve does not include the duty to preserve “every scrap of paper,” courts have ruled it does include the duty to preserve “any relevant evidence over which the [party] ha[s] control and reasonably kn[ows] or could reasonably foresee [is] material to a potential legal action.” To satisfy the duty of preservation, counsel should both quickly notify all parties, especially clients, of the duty to preserve relevant data and ensure the data are available for production. The source of the duty to preserve is usually Rule 37 or the courts’ inherent powers to preserve the integrity of the judicial

system. (FED. R. CIV. P. 37(b); *see, e.g.*, *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2nd Cir. 1999)). Some federal laws and many ethical rules also impose similar duties. (*See, e.g.*, Sarbanes-Oxley Act Of 2002, 18 U.S.C. § 1519 (2002)).

In order to fulfill the duty to preserve, attorneys should begin by sending preservation letters to all parties, especially to clients. Preservation letters should be explicit about which data should be preserved. Data should be identified by associating them with categories such as particular employees, departments, divisions, products, projects, customers, transactions, geographies, date ranges, media, or keywords. Notification to clients should be so specific, detailed and clear that they can quickly and correctly make decisions with regard to data that should be preserved or discarded. Moreover, counsel should instruct parties not to recycle storage media; not to disturb, discard or boot relevant computers; not to destroy, conceal or lose data, and to take affirmative steps to maintain and document the evidential chain of custody. If parties employ third-party electronic mail providers or offsite backup providers, counsel should send preservation letters to them as well. Further, at this stage counsel should carefully consider whether they will need data that are more difficult and costly to produce, such as disaster recovery tapes, data in legacy format, or “deleted” data. Parties might not have a “duty to restore” deleted information unless the requesting party can demonstrate a substantial need for it.

The duty to preserve evidence is not satisfied simply by the one-time event of sending preservation letters. Rather, attorneys have a duty to actively monitor throughout discovery and trial the condition of their client’s potential evidence to ensure it is available when needed. (*Danis*, No. 98-C-7482, 2000 U.S. Dist. LEXIS 16900, at *96). After preservation letters, counsel should follow up with the client multiple times in order to ensure both the client and its employees understand the importance of the duty to preserve

Inside The Digital Discoverer

Inside NTI	Pg.2
Net Threat Analyzer: Internet Lead Identification Software	
Computer Forensics In Action	Pg.3
This Issue: Company meets “impossible” discovery deadline through forensics	
Ask The Experts	Pg.4
This issue: Can computer forensics be used to analyze “known” evidence	

Computer Forensics Uncovered: WINDOWS SWAP FILE

Microsoft Windows-based computer operating systems utilize a special file as a “scratch pad” to write data when additional random access memory is needed. In Windows, Windows 95 and Windows 98, these are called Windows Swap Files. In Windows NT and Windows 2000 they are called Windows Page Files, but both have very similar characteristics. Swap files are potentially huge (20 million to 200 million bytes) and most computer users are unaware of their existence. These files can contain remnants of word processing files, e-mails, Internet browsing activity, database entries and almost any other work that may have occurred during past Windows work sessions. Data that’s transparently stored within the Windows Swap File is a significant computer security weakness that can be of benefit to the computer forensics specialist. Windows Swap Files can actually provide the computer forensics specialist with investigative leads that might not otherwise be discovered.

and are taking specific, prudent steps to satisfy it. If the court has issued a preservation order (as discussed below), copies of it should be provided to the client and its employees. Clients should also strongly consider appointing a “litigation response team,” consisting of competent, experienced, high-level employees from the legal, human resources, and information technology departments to ensure that possible evidence is properly preserved and easily retrievable.

In some circumstances a preservation letter is not enough to ensure that other parties preserve relevant evidence in their control. Where a party has a history of losing or destroying data, where the loss of documentary evidence would be absolutely outcome-determinative, or where there is an otherwise heightened need to preserve documentary evidence, attorneys have several legal tools at their disposal.

First, counsel may request a preservation

order or other order controlling the means and manner of discovery. Rule 16 allows courts to issue orders including orders “adopting special procedures for managing potentially difficult or protracted actions that may involve complex issues . . . or unusual proof problems.” (FED. R. CIV. P. 16 (c); *see* Smith, et al. v. Texaco, 951 F. Supp. 109, 111-12 (E.D. Tex. 1997). Such orders can be issued when requesting parties establish that i) there is a likelihood of success on the merits; ii) failure to issue the order will inflict irreparable injury; iii) equity is in their favor; and iv) the public interest is served. Although preservation orders can further the quest to preserve evidence, they can also impose heavy burdens on the parties they bind: it is difficult, for example, for multi-national companies to suspend document retention practices. Parties facing such orders will therefore want to consider methods to resist them through techniques described below.

Second, the parties may move for expedited discovery under Rules 26, 33, and 34. To obtain expedited discovery, courts typically require that parties show “(1) irreparable injury; (2) some probability of success on the merits; (3) some connection between the expedited discovery and the avoidance of the irreparable injury; and (4) some evidence that the injury that will result without expedited discovery looms greater than the injury that the defendant will suffer if the expedited relief is granted.” (Notaro v. Koch, 95 F.R.D. 403 (S.D.N.Y. 1982). Courts often order expedited discovery in intellectual property and constitutional cases, but there is applicable case law supporting the desire to expedite discovery to preserve digital evidence. (Mark D. Robins, *Computers and the Discovery of Evidence—A New Dimension to Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 503 (1999).

Third, parties may seek an onsite access order or an *ex parte* seizure order to preserve digital evidence. Parties request onsite access, for example, when only the producing party has software to read the information, when there is a sufficient desire to cut costs, or there is a desire to reduce the technical and business-related burdens on the producing party. (*See, e.g.*, Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999). *Ex parte* seizure orders can be issued if both “notice to the defendant would render fruitless further prosecution of the action. . . (and) there is no less drastic means for protecting [a party’s] interests.” (First Tech. Safety Sys, Inc. v. Depinet, 11 F. 3d 641, 650 (1993). Parties forced to defend against these tactics will naturally be concerned with the technical or business-related burdens and expenses they impose, as well as the risk of waiver of confidential privileges.

Inside NTI:

In each issue, we feature a key NTI employee or an important NTI technology development. This issue we feature:

Net Threat Analyzer Internet Lead Identification Software

In addition to providing computer forensics consulting services, New Technologies is a leading developer of computer forensics software tools. Many of these tools are considered industry standards for criminal justice and government investigation professionals, and several are patented – including Net Threat Analyzer (Patent No. 6,279,010).

Net Threat Analyzer software is used to quickly identify Internet leads concerning prior uses of desktop or notebook computers on the Internet. Once the user identifies a potentially interesting Internet lead, e.g., a relevant web site or e-mail address, then all occurrences can be identified and reviewed in context through the use of a computer forensic search utility like NTI’s Text Search Plus.

Net Threat Analyzer was originally developed by NTI to assist law enforcement agencies in the identification of potential Internet-related threats to children; a special law enforcement version (NTA - LE)

is provided free of charge to law enforcement computer crime specialists to help in the investigation of child pornography related cases.

After the September 11, 2001 terrorist attacks on the United States of America, Net Threat Analyzer was substantially upgraded to aid U. S. military and U. S. intelligence agencies in the evaluation of computer evidence linked to possible terrorist threats and activities. Net Threat Analyzer software also provides significant benefits in Internet related investigations conducted by corporate and government internal auditors and computer security specialists, where it’s often used to identify wrongful use of Internet accounts.



Control Spoliation

The failure to preserve evidence results in spoliation. “Spoliation” is the intentional or negligent destruction, mutilation, alteration, or concealment of possible evidence. (Burke v. Steen, *at* www.paed.uscourts.gov/documents/opinions/98D0658P.htm last visited November 11, 2002; Fada Indus. v. Falchi Bldg. Co., 730 N.Y.S.2d 827 (2001). Digital documents are more likely to spoliator than paper ones because such information is highly volatile and dynamic in nature. The simple acts of “booting up” or “booting down” a computer device can destroy digital evidence, as files are overwritten, new files are created,

and the modification, access, or creation dates of existing files are changed.

Unless the loss or alteration of digital evidence is “substantially justified,” sanctions will attach. Like the duty to preserve evidence, the power to sanction parties for spoliation derives from courts’ inherent power or from Rule 37. (*See* Fed. R. Civ. P. 37(b)(2); *Telectron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107, 126-31 (S.D. Fla. 1987) *citing* *Van Bronkhorst v. Safeco Corp.*, 529 F.2d 943, 951 (9th Cir. 1976). Sanctions for spoliation can include dismissal, default judgment, monetary sanctions, striking of pleadings, and the imposition of adverse inference. Furthermore, some jurisdictions recognize the tort of spoliation. (*See, e.g.,* *Smith v. Superior Court*, 198 Cal. Rptr. 829 (1984).

Questions of spoliation can arise, for example, when document retention policies (“DRPs”) are not properly drafted, implemented, maintained, enforced, or suspended. Parties should timely suspend their DRPs and appoint a litigation response team when litigation becomes reasonably foreseeable. Failure to do so will in some cases justify an order of default judgment. (*Wm. T. Thomson Co.*, 593 F. Supp. 1443).

Counsel must be extra-vigilant in guarding against spoliation. In some cases, opposing counsel who understand the volatility of digital information will go so far as to aggressively pursue data. The hope is that, somehow, the opponent will not have properly safeguarded its data, such that an inference of spoliation may be drawn. This practice illustrates the importance of ensuring employee compliance with DRPs, as well as promptly discontinuing DRPs at the proper time.

Parties defending spoliation claims may assert several defenses. First, they may claim that the spoliated evidence was not relevant, such that no prejudice was bestowed. (*Karl Bayer, et al., Getting and Protecting Electronic Information*, page J-10, Advanced Civil Trial Law Conference, February 22-23, 2001, at <http://www.karlbayer.com/elecdisc.pdf>, last visited November 11, 2002). Second, they may discover alternate copies of data initially thought to be destroyed, thus defeating a charge of spoliation. Finally, some cases or jurisdictions may present the opportunity to argue that the duty to preserve information had not yet attached.

In order to avoid charges of spoliation, counsel or their clients should remember to:

- Timely suspend DRPs;
- Send to opposing parties a detailed pres-

ervation letter or seek other protections as discussed above;

- Turn off digital devices only by pulling the power cord in most cases;
- Request that information be produced in native format if possible, so as to preserve meta-data;
- Quarantine digital media;
- Create “bit-stream” backups of digital media;
- Not boot-up suspect machines;
- Not redeploy machines unless the data they contain are irrelevant to imminent or ongoing litigation;
- Not allow forensically naïve network administrators or other members of the information technology department to “poke around” or otherwise investigate relevant devices.

This last point is well-illustrated by the case of *Gates Rubber Co. v. Bando Chem. Indus.* (167 F.R.D. 90 (D. Colo. 1996)). In *Gates*, each party retained a computer forensics expert in order to settle a discovery dispute regarding some deleted files. *Gates’* expert, however, made a series of mistakes that the Magistrate was careful to describe. For instance, this “expert” performed an investigation on the suspect disk drive itself rather than on a bit-stream backup image. Further, the “expert” initiated his plan to recover data by installing a copy of Norton’s UnErase™ on the target computer. This error resulted in the destruction of “7 to 8 percent of the information which would have otherwise been available.” Finally, the Magistrate noted that the expert failed to obtain the creation dates of certain important files. The expert’s failure to properly preserve evidence constituted a factor that the Magistrate “weighed against *Gates*” as he considered *Gates’* claims for relief.

Ensure Authentication

The Federal Rules of Evidence require that electronic evidence be accompanied by evidence sufficient to support a finding that the item is what its proponent claims. Counsel should consider a number of measures to avoid issues of authentication:

- Appoint a neutral computer forensics expert because such person would presumably have no motive to alter the evidence he or she inspects;
- Consider prohibiting the experts from physically touching computer systems; rather, simply instruct company employees what to do with the data and verify the results (Jay E.

Making Your Case: Computer Forensics In Action

The scenario below is based on an actual NTI case.

Company Mandated To Meet “Impossible” Discovery Deadline

A private company had contracted with a government agency to provide certain services for the agency’s employees. The government agency alleged that the company had violated its agreement, and filed a lawsuit. Discovery requests were onerous, to say the least; production of over one terabyte (1,000 gigabytes, the equivalent of 375,000,000 document pages) of data was mandated by the court within a week. Almost all the data resided on backup tapes. It would be impossible for the company to meet this request using manual methods, and they lacked the internal technical expertise to produce the massive amounts of data involved in a cohesive electronic format.

Finding both the timing and the expense of a conventional e-discovery solution untenable, the company opted to use computer forensics to compile the data necessary to meet the discovery request. To narrow the scope of meaningful data earlier in the process, forensics utilities were used to search the universe of data in its native format for relevance and responsiveness – a necessity in a discovery request of this magnitude under the given time constraints. This enabled the company to better focus its tape conversion efforts. Using further forensics processes, the company’s MS Exchange database (which housed the company’s email archives, the focus of the discovery efforts) were converted to PST files, sorted by user and searched for responsiveness. The company was able to meet its deadline; ongoing analyses have been conducted to keep the company in compliance with the discovery mandate.

Grenig, *Electronic Discovery: Making Your Opponent's Computer a Vital Part of Your Legal Team*, 21 AM.J. TRIAL ADVOC. 293, 299 (1997);

- Perform the investigation on a bit-stream backup only—never on the original;
- Ensure the bit-stream backup is identical to the source drive by using an “md5sum” hashing program, not a CRC (See Brian Deering, *Data Validation Using The Md5 Hash*, at <http://www.forensics-intl.com/art12.html>, last visited October 24, 2002);
- Consider creating images only on read-only disks, or using hardware-based “write-blockers” (Kenneth J. Withers, *Computer-Based Discovery In Federal Civil Litigation*, 2000 FED. CTS. L. REV. 2, app. at VI (Oct. 2000));
- Maintain chain of custody;
- Scan, but do not clean or alter, digital media for viruses and errors;
- Cross-validate results and conclusions by using multiple computer forensic tools.

Resist Production Wisely

Litigators will often find themselves resisting the discovery requests of opposing parties. The following tools are available to resist digital discovery, just as they are in the “traditional” form of discovery.

- As always, irrelevant data are not discoverable.
- If counsel feels that certain discovery requests are overbroad, unduly burdensome, unreasonably cumulative or duplicative, available from other sources that are more convenient, less burdensome, or less expensive, Rule 26(b)(2)(i)-(iii) will support a party's attempt to shift production costs to the requesting party or block a motion to compel.
- Counsel may resist production if the information being sought is covered by the work product doctrine, or by the attorney-client or other privileges.
- Rule 11 can be applied if opposing counsel oversteps certain boundaries.

· Because parties do not have a duty to produce documents that are not within their control, counsel may resist a production request for example “if a document sought is filed, in the regular course of business, in the offices of an affiliate several organizational tiers removed from the corporate party” (Stewart D. Aaron, *Civil Discovery* § 4.02(1)(e) (Business Law Monographs, Matthew Bender 2002).

· Finally, as discussed in the first installment of this story (published in the February issue of *The Digital Discoverer*), attorneys may pursue a protective order under Rule

26(c) to protect trade secrets or other sensitive information.

Conclusion

Digital evidence can be volatile. Litigators who do not properly manage it may find it excluded from trial. Careful monitoring and control of digital evidence helps to ensure authentication and to maintain privilege. As mentioned in the first installment, computers and digital media are here to stay, and attorneys who learn to manage this rapidly evolving sub-practice will better serve their clients.

Ask The Experts

Addressing frequently asked question from clients.

In each issue of *The Digital Discoverer*, we attempt to field a common question our clients have about computer forensics and digital discovery strategies.

Q: Can computer forensics be used to analyze “known” evidence?

A: Computer forensics is valuable for unearthing evidence that you didn't know existed. It also can be an efficient and cost-effective means for culling through known electronic evidence.

More often than not, digital discovery is treated in a manner based closely on the traditional paper discovery model. With paper discovery, documents are scanned (perhaps OCR'd), converted to TIFF files, linked to corresponding records in a database, and then searched and categorized using a litigation support program like Summation or Concordance.

Digital documents fall into three broad categories: active files, archival/legacy data, and residual data (which include file fragments, deleted files and metadata). Using the “paper” model, each category is treated differently. A litigation team might proceed in the following manner:

- ACTIVE FILES – print out and review, scan and OCR, and convert to TIFF file and commit to database
- ARCHIVAL FILES – convert to printable format, print and review, scan and OCR, and convert to TIFF file and commit to database
- RESIDUAL DATA – perform forensic processing to identify deleted files and telling computer user activity, report findings, selectively convert to TIFF file and commit to database

The computer forensics approach departs from the “paper” model in that all data is reviewed in electronic format, using forensic software tools. Many conversion steps are removed from the process, all data is reviewed in its native electronic format, and the litigation team receives preliminary results with much faster turnaround for a fraction of the cost.

While computer forensics can be applied to any situation where there's a need to make sense of e-discovery, there are certain situations where it offers a definitive advantage. These include searches across a variety of file formats; narrow searches across a broad amount of data; and searches where confidentiality is an issue.

Go Online!
See What's On
Our New Website

New Technologies, Inc., a wholly-owned subsidiary of Armor Holdings, Inc. (NYSE:AH), provides digital document discovery services, primarily through computer forensics, to civil litigators. Working with litigation team members as partners, we:

- Use forensic processes to cost-effectively manage electronic discovery efforts.
- Consult with you to determine what electronic information is valuable to a case, and how to get it in admissible format.
- Use various forensics procedures (with software tools we've developed) to find evidence on computer hard drives and other storage media.

Contact Us At:

Tel: 503-661-6912

E-mail: info@forensics-intl.com

Web: www.dataforensics.com



NEW TECHNOLOGIES INC.