



NEW TECHNOLOGIES INC.

# The Digital Discoverer

Trends in computer forensics & e-discovery for civil litigators

## Practical Strategies for Digital Discovery: Preliminary Considerations

BY ERIC VAN BUSKIRK, ESQ.



Most business documents are now produced in digital form. Consequently, when disputes arise, litigators will often require the discovery of digital documents. Although the Federal Rules of Civil Procedure (the

“Rules”) have long provided for the discovery of information in digital form, litigators still face new and possibly uncharted territory when it comes to digital discovery. Failure to successfully manage important issues can affect the outcome of a case. To mitigate the risks, litigators should better understand the legal, technological and practical issues involved in discovering digital data.

This article is the first of two installments in a series that is intended to provide an overview of important preliminary issues in digital discovery. These include technical issues, as well as disclosure and privilege. Proper consideration of the propositions set forth in the two installments should provide litigators with a necessary foundation to initiate digital discovery and to ensure that evidence derived therefrom is available at trial.

### Digital Discovery is Different

Digital discovery is materially different from traditional discovery because of the manner in which digital information is handled and stored. To begin, the computer’s operating system makes temporary copies of files at certain times, such as when they are

opened or printed. The operating system uses these copies in part for backup/recovery purposes and for faster manipulation of data. Although these uses enhance the computing experience in some ways, they also decrease security because data is stored in places that the user probably is not aware. Second, digital files contain meta-data, or data about the data. Meta-data include information such as the document’s author, or its modification, access, or creation dates. Meta-data often plays an important role in cases where digital evidence is used because, for example, they can serve as the foundation of a timeline analysis. Third, as many attorneys now know, the act of deleting a file is not the same as making it unrecoverable. That is, deleted files can sometimes be restored or “undeleted.” Even some files that have purportedly been “scrubbed” can be recovered if the scrubbing software’s engineers did not properly account for alternate data streams. Fourth, when an operating system “boots-up” or “boots-down,” unintended consequences can occur. For example, the modification and access times of some files will be altered. This can harm the integrity of digital evidence, making it difficult to determine a chain of events. Fifth, if a particular digital file was created with a software application that no longer exists or is prohibitively expensive to obtain, it may be very difficult for requesting parties to read and interpret information in that file. As will be seen, these five differences and many others change the way attorneys must conduct digital discovery.

### Understand The Technology

Attorneys have a duty to obtain knowledge of the client’s and the opponent’s information technology (“IT”) infrastructure. Disclosure and discovery cannot proceed without this knowledge. The Rules permit parties to peer into other parties’ IT infrastructure through several means. Rule 30(b)(6) allows counsel to depose the IT personnel of opposing parties in order to discover where

### Inside The Digital Discoverer

<b>Inside NTI</b>	<b>Pg.2</b>
Featured Employee Anton Litchfield	
<b>Computer Forensics Uncovered</b>	<b>Pg.3</b>
This Issue: File Slack	
<b>Ask The Experts</b>	<b>Pg.4</b>
This issue: When to retain forensics consultants	

## Making Your Case: Computer Forensics In Action

*The scenario below is based on an actual NTI case.*

### Executive Proved To Have A History of Sexually Harassing Employees

A woman employed by a large defense contractor accused her supervisor of sexually harassing her. She was fired from her job for ‘poor performance’ and subsequently sued her ex-boss and the former employer. NTI was retained by the plaintiff’s attorneys to investigate allegations of the former employer’s harassing behavior. After making a mirror image backup of the ex-boss’ hard drive, NTI was able to recover deleted electronic messages that contained evidence that the ex-boss had a history of propositioning women under his supervision for ‘special favors’. The woman got her job back, and the real culprit was terminated. See other case examples at [www.dataforensics.com](http://www.dataforensics.com).

relevant data might reside. Further insight may be gained by using interrogatories or by taking testimony by deposition upon written questions under Rule 31.

**Disclose:** Rule 26(a)(1) now generally requires that parties provide to other parties a copy of, or description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses unless solely for impeachment. The duty to disclose digital evidence has been held to include the following items:

*[V]oice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, . . . other electronically-recorded information . . . (and) any back-up copies of files or archival tapes that will provide information about any 'deleted' electronic data.*

*(Kleiner v. Burns, 48 Fed. R. Serv. 3d 644 (D. Kan. 2000)).*

If parties do not properly carry out their duty to disclose, requesting parties should file a motion to compel. Motions to compel should be preceded first by the requesting

---

***“The use of computer forensic expert witnesses imposes further disclosure obligations.”***

---

parties' good-faith effort to resolve the matter with the non-disclosing party without judicial intervention. If the motion is granted or the disclosure is otherwise provided after the motion was filed, courts have the power to impose monetary sanctions, default judg-

ment, and adverse inferences. Adverse inferences are instructions to the jury that the non-disclosed evidence is presumed against the non-disclosing party. Failures to disclose also can preclude parties from introducing the non-disclosed evidence. For example, the failure to disclose a digital warning displayed by the employee's computer in the boot-up sequence may preclude the client-employer from introducing the image at trial to prove an employee had notice that his or her computer was subject to client-employer search. This example also demonstrates the importance of understanding the client's IT infrastructure as described above.

Technically knowledgeable attorneys may feel comfortable with the technical aspects of digital evidence. Other attorneys will require the services of computer forensic expert witnesses. It is simply outside the realm of most attorneys, for example, to “crack” an encrypted file, to reassemble a fragmented one, or to search for RAM slack or drive slack on a RADIUS server.

The use of computer forensic expert witnesses imposes further disclosure obligations. In particular, parties must disclose the names

## Inside NTI:

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

**Anton Litchfield,**  
Director of Forensic  
Consulting Services



### **Background:**

Anton is a court certified expert in computer forensics and Internet investigations. He has over six years of computer forensic examinations experience with New Technologies, Inc.

and with the Ontario Provincial Police of Toronto, Canada. While with NTI, Anton has conducted forensic examinations in well over 50 different civil litigation cases, including sexual harassment, medical malpractice, and theft of trade secrets suits. He also regularly serves as an expert witness on computer fo-

rensic matters. Before joining NTI, Anton served as the lead computer forensics analyst for the Child Pornography Unit of the Ontario Provincial Police.

**How he became interested in computer forensics:** Up until 1996, Anton had spent the bulk of his time doing general uniformed patrol work – the guy in the police car. In 1996, an exciting position opened up in the department's Child Pornography Unit, known as Project P. Considering that the most heavily used medium for the possession and dissemination of child pornography was the computer and the Internet he decided this would be a great opportunity to continue doing traditional police investigations, yet also learn the electronic evidence component of law enforcement.

**Most memorable case:** The CEO and founder of a company was demoted by the board of directors. Shortly after, he was terminated by the board. When he was fired he took his work PC and his laptop home with him. Approximately 4 days later he returned the two computers he took from the company as well as a PC he used at home, which had been purchased by the company. Anton performed a forensic analysis on the machines

that showed that during the 4-day period a CD-Rom burner had been installed on the computers as well as a zip drive. Analysis further showed that key company documents were copied to this removable media. The most damaging item found was a deleted Microsoft Office document titled “to do list.doc”. Contained within this document were the ex-CEO's plans to copy the company research database to his computer (valued at 100 million dollars), and a note to “find out how to destroy computer evidence”. During the court hearing, this deleted document was provided to the defendant's counsel. Five minutes later, both parties were in settlement talks.

**When he's not investigating:** Anton is married to a beautiful police detective, and has two young daughters. An avid outdoorsman, he splits his time between fly fishing (in the spring and summer) and duck hunting (in the fall). He claims to regularly out fish NTI CFO John Dethman on their home river, the Deschutes in central Oregon.

of the experts to be called at trial. Along with disclosure of the expert's identity, parties are usually required to submit and supplement a written report. This report must be prepared and signed by the expert who is to testify. It must also include information such as the opinions to be expressed by the expert, the reasons and bases therefore, as well as identification of exhibits to be relied upon and a list of the expert's publications and qualifications. The report usually must be submitted at least ninety days before trial.

Attorneys who reveal their mental impressions to expert witnesses in the course of preparation for litigation risk waiving privileges of the confidential information revealed. Although Rule 26(b)(3) purports to protect the work product of attorneys, Rule 26(b)(4) apparently degrades this protection in the eyes of some by giving parties the right to depose computer forensic experts after submission of the written report.

That is, this right to depose the expert has given rise to the argument that work product information is discoverable at the deposition if it was "considered" by the expert. (*Karn v. Ingersoll RAND*, 168 F.R.D. 633 (N.D. Ind. 1996). Some courts have found this reasoning

persuasive whether or not the expert actually "relied upon" the work product material. (*B.C.F. Oil Ref., Inc. v. Consol. Edison Co, Inc.*, 171 F.R.D. 57 (S.D.N.Y. 1997); *Musselman v. Phillips*, 176 F.R.D. 194 (D.Md. 1997); *Karn*, 168 F.R.D. 633).

### Maintain Privilege & Confidentiality

The most common privileges involved in digital discovery are likely those of the attorney-client and work product. Parties generally have no duty to disclose information covered by these privileges or any others. Parties withholding documents under a claim of privilege bear the burden of establishing the privilege claimed. In the event that protected information is intentionally divulged, it is clear that the privilege is waived for those materials. (*See, e.g., United States v. Keystone Sanitation Co.*, 885 F.Supp. 672 (M.D. Pa. 1994). However, even inadvertent disclosure of privileged information may constitute

waiver, unless the privilege holder took all reasonable steps to protect the privilege.

Inadvertent waiver is of particular concern in digital discovery because the massive volume of information makes it difficult to winnow discoverable information from that which is privileged. In exchanging digital information, parties often trade "bit-stream" images of digital media rather than the original media. A bit-stream image is a single file or group of files that, when restored, exactly reproduces the "contents" of the original digital medium, including the slack and unallocated spaces where deleted file information resides. (*See, e.g., United States v. Keystone Sanitation Co.*, 885 F.Supp. 672 (M.D. Pa. 1994). A restored bit-stream image may also be properly called a "mirror image" or a "snap-shot" of the original digital medium. Before producing bit-stream images and other information, confidential or privi-

leged information should be separated from producible information. However, the large hard disk drives of today make such screening difficult. An eighty-gigabyte hard disk drive has the capacity to hold the equivalent of a stack of paper ten thousand feet high. Screening

these devices requires significant resources, and if it is done improperly, parties might inadvertently waive their privileges. Authors have commented on ways to better screen for privileged information in heavy production cases. (TORT AND INSURANCE PRACTICE SECTION, AMERICAN BAR ASS'N, *Attorney-Client Privilege in Civil Litigation* 135 (Vincent S. Walkowiak, ed. 1997). Further, vendors have developed technologies that enable counsel to search for confidential information digitally. Reports on the quality of these technologies are so far a mix of praise and frustration.

Another way to help protect privileged and other confidential information is for parties to meet as soon as possible to agree that the inadvertent production of confidential information will not constitute waiver. The agreement should include an inspection protocol to help protect confidential information. The protocol should include measures most likely to maintain privilege and confidentiality. The

**"An eighty gigabyte hard disk drive has the capacity to hold the equivalent of a stack of paper 10,000 feet high."**

## Computer Forensics Uncovered: FILE SLACK

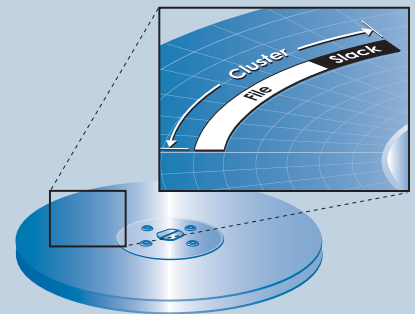


Computer forensics is a new field of endeavor, pioneered by NTI's president, Michael R. Anderson. It's also a complex field, with its

own lexicon. In each issue of *The Digital Discoverer*, we'll take a key term from the computer forensics vocabulary and provide what we hope will prove to be a useful definition.

### File Slack

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the cluster end of the last cluster assigned to the file is called "file slack". Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes



mean more file slack and also the waste of storage space when Windows 95 systems are involved. However, this computer security weakness creates benefits for the computer forensics investigator because file slack is a significant source of evidence and leads.

inspection protocol might provide for the appointment of a neutral computer forensics expert. (See, e.g., *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999). Because of the inspector's neutral status, at least one court has ruled that any disclosures to it do not constitute waiver. The neutral expert, just like any other person searching important data, should be required to sign a confidentiality agreement in order to protect trade secrets and privileged information. (Todd N. Thompson, *The Paper Trail Has Gone Digital: Discovery In The Age Of Electronic Information*, J. KAN. BAR ASS'N (March 2002). The parties should then request the court to order that discovery take place under the terms of the agreement and protocol. Some courts may not comply.

Counsel must exercise extreme caution with regard to waiver because courts are largely inconsistent when ruling on waiver issues. Prior to seeking the order of protocol, counsel should investigate the degree to which non-parties will be bound by it. Even if parties stipulate that waiver is restricted to a particular suit, courts in subsequent or parallel litigations are not bound by and might not respect the stipulation. (*Chubb Integrated Sys. v. National Bank*, 103 F.R.D. 52, 67-68 (D.D.C. 1984); WALKOWIAK, *supra* note 26.)

If the parties are not able to agree on an inspection protocol, or if onsite inspection access is requested, the responding party should motion the court for a protective order to help protect privileged or confidential information. Protective orders ensure that certain information is not revealed or is only revealed under certain limited circumstances. Before issuing a protective order, the American Bar Association has suggested that courts:

*[C]onsider such factors as (a) the burden and expense of the discovery; (b) the need for the discovery; (c) the complexity of the case; (d) the need to protect the attorney-client or attorney work product privilege; (e) whether the information or the software needed to access it is proprietary or con-*

*stitutes confidential business information; (f) the breadth of the discovery request; and (g) the resources of each party.*

*(Draft, ABA Section of Litigation Civil Discovery Standards, Para. 29 (2)(2) (1998); [www.abanet.org/ftp/pub/litigation/civildiscoverystandards.doc](http://www.abanet.org/ftp/pub/litigation/civildiscoverystandards.doc))*

Again, prior to seeking the order, counsel should consider the degree to which non-parties will be bound by it.

## Conclusion

Digital discovery is an important and relatively new sub-practice. Attorneys who duck their duties with regard to technology as it applies to litigation are doing a disservice to their clients and themselves. Understanding technical issues should assist attorneys to manage disclosure and to maintain privilege. The next installment will focus on evidentiary issues such as the duty to preserve evidence, spoliation, and authentication.

## 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:** “We’re just beginning an intellectual property case, and we suspect that some valuable evidence resides on the defendant’s computers. When is the appropriate time to retain forensics experts?”

**A:** The best time to retain a forensics expert is the minute your client retains your services as legal counsel and you suspect some, if not all of your key evidence will reside in electronic format. It’s important to act quickly because of the ease and speed in which computer-based information can be altered or destroyed. Every time a user turns on a computer and goes into Windows, thousands of pieces of information are changed. Most of this data relates to times/dates, system resources and, to a lesser extent, deleted files. All of these affected areas contain critical information related to the activities of the user in question. A competent computer forensics expert can develop a

“rapid response” plan for the litigator to present to the court to ensure key information is preserved. (We should note that “altered or destroyed” data can be often be located by forensics experts, but usually at a significant additional cost, as this sort of work is more time-intensive.)

Many don’t realize that preservation is the most important part of any electronic discovery plan, more so than the discovery itself. It’s far more preferable to preserve everything and process a small portion of the available universe of data than to allow portions of potentially critical information to disappear forever. Besides, it usually takes more time to figure out where your key information resides than it does to find hardware and media of potential significance. For example, your targeted computer may reside in a company that has 20 computer systems. It’s not unreasonable to spend a day or two on-site creating mirror image backups of all the office computers until depositions are conducted to find out which systems/workstations your defendant accessed. The time spent up front is great insurance for potential discoveries down the road. If your litigation team is not able to access those 20 computers until a year has passed, it might be too late.

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:

- 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.
- Provide expert witness testimony.

### Contact Us At:

Tel: 503-661-6912

E-mail: [info@forensics-intl.com](mailto:info@forensics-intl.com)

Web: [www.forensics-intl.com](http://www.forensics-intl.com)



NEW TECHNOLOGIES INC.