



**AccessData®**

*A Pioneer in Digital Investigations Since 1987*

AccessData Corporation

# The Rules of Digital Evidence and AccessData Technology

White Paper

## Table of Contents

<b>The Federal Rules of Evidence .....</b>	<b>1</b>
<b>Authenticity.....</b>	<b>1</b>
<b>Best Evidence Rule.....</b>	<b>4</b>
<b>Daubert &amp; Frye.....</b>	<b>4</b>
<b>Validation of AccessData Forensic Technology.....</b>	<b>4</b>
<b>AccessData’s Technology and Case Law.....</b>	<b>5</b>
<b>Meeting the Daubert Standards.....</b>	<b>6</b>
<b>The New Federal Rules of Civil Procedure .....</b>	<b>7</b>
<b>Proper Collection and Good Faith Effort are Critical.....</b>	<b>7</b>
<b>The Collection Process and Reducing Risk .....</b>	<b>8</b>
<b>The Federal Rules and Technology .....</b>	<b>10</b>
<b>Metadata - How Important Is It? .....</b>	<b>10</b>
<b>Timely Production and Scope of Discovery .....</b>	<b>11</b>
<b>Deleted Data.....</b>	<b>12</b>
<b>Limits of Litigation Hold Technologies.....</b>	<b>13</b>
<b>Search Issues and AccessData® Technology.....</b>	<b>14</b>
<b>Mobile Phone Search Issues .....</b>	<b>15</b>
<b>Voice over Internet Protocol (VoIP) Interception and Analysis.....</b>	<b>17</b>
<b>RAM Analysis: Be Prepared.....</b>	<b>18</b>
<b>Conclusion.....</b>	<b>18</b>
<b>AccessData in Court.....</b>	<b>19</b>
<b>References.....</b>	<b>23</b>

*This paper provides legal and factual information, as well as opinions from experts qualified by U.S. Courts. However, such information is not the same as legal advice and should not be construed as such. Please consult a lawyer if you want professional assurance that our information, and your interpretation of it, is appropriate for your situation.*

---

## Introduction

This document is for users of AccessData software who wish to understand the technology and case law that supports the introduction of electronically stored evidence ("ESI") that is seized/discovered and analyzed with our products in a court of law. This document is not intended as a legal reference. Consequently, we will spend a limited amount of time detailing the basic background information relevant to the general topic of digital evidence and computer forensics.

For the sake of simplicity, one can arrange the rules relevant to ESI into two basic groups. The first, and arguably more foundational group, is the Federal Rules of Evidence ("FRE") and more specifically the way they have been interpreted by courts to accommodate digital evidence. The second group consists of the much more recent and specific amendments to the Federal Rules of Civil Procedure ("FRCP"), which significantly impact every large US and multinational company.

## The Federal Rules of Evidence

Digital Evidence presented a number of significant challenges when it first began to appear in courts. The problem with digital evidence is that it is fundamentally different from physical evidence, around which the FRE were predicated. Specifically, the challenges presented by digital evidence are due to following differences:

- 1.) Degradation:** In the world of physical evidence there is some basic acceptance that if a gun is found at the scene of a crime and is handled correctly, that will be the same gun at the point of trial. To the extent that physical evidence does change with time it is generally accepted by the courts that those changes are immaterial to the relevance of the evidence. The same cannot be said in general about digital evidence. Digital evidence is by its very nature volatile. It is not uncommon for a single bit within a large file to get altered over time, and the resulting effect on the entire document can actually be fairly large. (Note: degradation applies to the storage media itself.)
- 2.) Ownership:** It is quite difficult to determine ownership of a digital document. While it may be possible to determine on which physical machine a document was found, given the current technical realities associated with shared computer resources, networked computers and virtual machines, knowing which machine on which a document was placed is not always sufficient to prove who authored the document.
- 3.) Original Documents:** It is literally impossible to distinguish an original document from copies of it. At the most basic level, all digital documents are simply a series of zeros and ones that are interpreted by the computer. Two documents containing the exact same string of zeros and ones are in every sense identical and there is no way to determine which was created first or who created it without additional information.

These three crucial differences, as well as the subtleties associated with them, served as the impetus for the courts to essentially re-interpret the FRE in order to more clearly accommodate digital evidence. At a fundamental level, this re-interpretation required dealing with two basic evidentiary issues: Authenticity and the Best Evidence Rule:

## Authenticity

For any computer record or other evidence to be admissible against a defendant, the proponent must show that the offered evidence is authentic. The standard for determining the authenticity of a computer record is no different than authenticating any other record. However, "the complex nature of computer storage calls for a more comprehensive foundation." See *United States v. Scholle*<sup>1</sup>. The need for a more comprehensive foundation has given rise to a number of challenges to the admissibility of digital evidence over the last two decades that fall into three basic categories:

- 1) The computer-generated or computer-stored records were altered, manipulated or damaged after they were created;
- 2) The reliability of the computer program that generated the computer record; and
- 3) The reliability of the identity of the author.

Fortunately, countless cases over the last two decades have provided significant precedent regarding each of these basic challenges. There is now a classic opinion detailing the authentication process of ESI, namely Chief Magistrate Judge Paul W. Grimm's 102 page opinion in *Lorraine v. Markel Am. Ins. Co.*<sup>2</sup> That opinion struck lighting on both sides in that case for respective counsel's lack of foundation and preparation for admitting ESI and is recommended reading for all attorneys who have to admit ESI into evidence.

**Data Alteration:** In regard to challenges based on the premise that the data was altered, the courts offer extensive guidance. First and foremost, absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record.<sup>3</sup> A challenge that the offered evidence was tampered with or altered requires evidence to show that it was tampered with or altered. Merely showing that a better method is available is insufficient.<sup>4</sup>

In addition to the question of alteration, the court has also addressed questions surrounding evidence acquisitions. Specifically, the court has generally found that if an investigator can testify to the process used to acquire digital evidence and show that it is in keeping with current best practices then the evidence is admissible. This exact question was addressed in *Bone v. State*,<sup>5</sup> and the Court found that the investigator's testimony regarding how he had acquired the evidence, the steps he took to protect the validity of the evidence, and the process he had used to analyze the evidence was sufficient to establish the authenticity of that evidence.

**Reliability of the Program:** Secondly, FRE 901(b)(9) requires that "matters created according to a process or system can be authenticated with 'evidence describing a process or system used ... and showing that the process or system produces an accurate result'." The authenticity of the computer record is balanced by the reliability and accuracy of the computer program that created the record. The burden of proof is on the party introducing the evidence. As long as that party provides "sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof and how the records were maintained and produced, a proper foundation has been established."<sup>6</sup> Reliability can be established by showing that the program is used on a regular basis, such as in the ordinary course of business.<sup>7</sup> Showing that the computer record is one that is normally retrieved, kept or made in the routine of business operations shows a higher degree of trustworthiness.

Challenges based on reliability can occur when the evidence submitted is retrieved from complex accounting or order processing systems. For example an employee who is embezzling money by altering a few numbers on an invoicing system might attempt to get the digital evidence thrown out by arguing that the evidence was created by an unreliable process, namely the accounting system. In essence, he could argue it was a system glitch that caused the error, as opposed to a prolonged and systematic scheme. In this case, the courts have generally agreed that if the prosecution can show the reliability of the system in terms of its ability to correctly process millions of other transactions, then the system is considered reliable and the evidence is therefore admissible.

**The Reliability of the Identity of the Author:** A third common challenge against the admissibility of computer records pertains to whether the purported author is indeed the author stated on the computer record or the one alleged to have made the record. Proving authorship and authenticity of such a computer record is shown either through testimony or through circumstantial evidence.

When testimony regarding authorship is available, even in complex situations, it is generally sufficient to prove authorship. One of the best examples of testimony supporting authorship is

*United States v. Tank*.<sup>8</sup> At question in *Tank* was the authorship of internet chat messages, the authorship of which is intuitively difficult because these messages are identified only through a self-defined username. In considering the authorship issue, the appellate court noted that in the context of *FRE 901(a)*, the court can admit evidence if "sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity."<sup>9</sup> In addition, there needs to be a sufficient link shown between "the proffered evidence and the defendant."<sup>10</sup> To satisfy these requirements the government offered the testimony of other chat room participants and the computer server administrator. In *Tank*, the Court found that this testimony was "sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated."<sup>11</sup> Courts considering the admissibility of electronic evidence frequently use this method.<sup>12</sup> It is necessary, however, that the authenticating witness provide factual specificity about the process by which the ESI was "created, obtained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8)."<sup>13</sup>

*FRE 901(b)(3)* and *(b)(4)* also provide other methods to authenticate ESI. For example, *FRE 901(b)(3)* permits authentication by "[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." *FRE 901(b)(4)* allows authentication through "circumstantial evidence."<sup>14</sup> Other methods include the following:

- 1) Showing that the document was obtained from a machine utilized either primarily or entirely by the author of the relevant document;
- 2) Showing that the file was surrounded by other files or emails also created by the author;
- 3) Detailing the authors other activities on the relevant machine when the relevant file was created; or
- 4) Showing that the file was in a restricted area accessible only by the author, such as an email box or password protected machine.

Certain identifying marks or data contained within or associated with the ESI may also enable identification. Two common examples are "hash values" and "metadata." A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file. Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under *FRE 901(b)(4)*.<sup>15</sup>

Metadata is another method of establishing authenticity, since such information can provide information about a particular data set by describing how, when and by whom it was collected, created, accessed, or modified. Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is another distinctive characteristic of electronic evidence that can be used to authenticate under *FRE 901(b)(4)*.

There is, of course, a multitude of additional ways to authenticate ESI, including reliance upon any "self-authenticating" characteristics of the ESI itself. As Judge Grimm in *Lorraine* notes, counsel must be "creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits."<sup>16</sup> In short, lawyers must be able to authenticate the ESI that they intend to use at trial.

Generally, it is only when dealing with purely internet-based evidence provided by an Internet service provider ("ISP") that authorship can be truly difficult to prove. Unfortunately this is often the case when attempting to prove hacking and Internet theft activity but in those instances there is usually extensive additional circumstantial evidence that is obtained by law enforcement during the course of the investigation.

## Best Evidence Rule

The second major issue digital evidence presents is that it violates the Best Evidence Rule. The best evidence rule is also "referred to as the 'Original Writing Rule' because it does not mandate introduction of the 'best' evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an 'original,' 'duplicate' or, in certain instances, by 'secondary evidence—any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available."<sup>17</sup> FRE 1002 states, "to prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." Within the context of computer-generated data, FRE 1001(3) expressly states that data stored on a computer or similar device should be considered an "original." Conclusively, an "accurate" printout would be considered an original and therefore satisfy the Best Evidence Rule.

However the key word is "accurate." The rule assumes that the printout has all the relevant data to conclude its information is complete and within its original context.<sup>18</sup> In *Armstrong v. EOP*,<sup>19</sup> the Court concluded that a hard copy paper printout of an electronic document did not include all the information in the computer memory and that it failed to be a complete understanding of what actually happened. Ensuring accurate and complete data acquisition is the role of computer forensics—a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Obviously this scientific approach to ensuring the accuracy of digital evidence is critical to the issues surrounding its admissibility.

## Daubert & Frye

The courts have provided two critical bodies of law (based upon *Frye v. United States*<sup>20</sup> and *Daubert v. Merrill Dow Pharmaceuticals*<sup>21</sup>) that are relevant to computer forensics. For decades, courts have applied a "general acceptance" test to all scientific evidence and testimony. In particular, *Frye*<sup>22</sup> set the standard that: if the scientific community in that particular field, which was well recognized in scientific principle or discovery, 'generally accepted' the practice then it could be admitted in court. These principles were then updated in 2000 by FRE 702 and its amendment, which state that if there is scientific, technical or specialized knowledge needed to understand the evidence, sufficient foundation must be laid where 1) the testimony must be based on sufficient facts or data, 2) the testimony is the product of reliable principles and methods and 3) the witness has to have applied the principles and methods reliably to the facts of the case.

Seventy years after *Frye*,<sup>23</sup> the United States Supreme Court provided four specific criteria for scientific evidence in the case of *Daubert v. Merrill Dow Pharmaceuticals*.<sup>24</sup> In this case the court threw out *Frye*'s standards and drew up a whole new set of criteria to determine the reliability, relevancy and admissibility of the evidence. It also gave the courts discretion on whether to accept the scientific evidence based on those criteria. *Daubert*<sup>25</sup> held that for any scientific evidence to be admitted, it must meet four requirements:

- 1) The theory or technique utilized must have been tested and that test must be replicable.
- 2) The theory or technique must have been subject to peer review and publication.
- 3) The error rate associated with the technique must be known.
- 4) The theory or technique must enjoy general acceptance within the scientific community.

## Validation of AccessData Forensic Technology

As we stated initially, this document is not meant to serve as a legal reference and is instead intended for customers of AccessData who wish to understand the legal foundation on which our products stand. As such, we will move now from discussing the basic laws of digital evidence and directly examine the relevant technology and case law associated with our products.

First and foremost, it is worth taking a quick look at the two primary pieces of AccessData's technology that come into play when determining the admissibility of digital evidence:

**Data Acquisition:** AccessData's solutions utilize widely accepted forensic techniques for acquiring data without affecting, or minimally affecting, the target machine. Depending on the version of the product utilized, either an agent on the target machine or a hardware write blocker enables our solutions to acquire an exact bit stream copy of the target machine. All data can be acquired or selected individual files. In either case the acquired data is complete, unaffected and captured in its entirety, including all relevant metadata (a critical factor for compliance with the Federal Rules of Civil Procedure).

**Evidence Storage:** In addition to the methodology utilized to acquire the data, the storage format associated with the acquired data is also often relevant. Here again our solutions utilize widely accepted file formats for the storage of digital evidence. In addition, to our own proprietary format (AD1) we offer users the option to store the data in other popular formats, such as DD or Export Witness E01. What is common among these formats is the utilization of hashing and checksum algorithms to ensure that any changes in the preserved data occurring after seizure or during analysis are detectable. Depending on the format used, the way the forensic imaging technologies work is they take a digital fingerprint (hash) of the entire collected dataset. Some formats, such as the Expert Witness format E01, calculate checksums at pre-determined increments. Those checksums and hashes are then saved with the forensic bit stream image of the acquired evidence. When the data is reviewed at a later point, the hashes can be re-calculated and compared to the originals to identify if any changes to the data have occurred.

#### AccessData's Technology and Case Law

The case of *Gutman v. Klein*<sup>26</sup> is particularly interesting because it establishes the validity of AccessData's technology for both data acquisition and evidence storage. The relevant information from the case is as follows:

"Douglas Vitale ('Vitale'), an examiner with The Intelligence Group, a computer forensics and investigations company working on behalf of Gutman, forensically copied, or 'imaged,' the Klein laptop's hard drive on December 8, 2005. (See *Stroz Report* P 10–11)<sup>27</sup> Stroz Friedberg took possession of the forensic image .....on November 14, 2006.<sup>28</sup>

Vitale's records indicate that he began imaging the Klein laptop, a Dell Latitude with serial number CN-09C748-4815519E-2036, at approximately 4:32 p.m. on December 8, 2005, using a program called FTK version 2.2, 'an accepted tool under industry standards, to perform the imaging and create a forensic duplicate of the hard drive.'<sup>29</sup> Due to a likely battery malfunction on Vitale's computer, the forensic image was recorded as having occurred on January 1, 2000.<sup>30</sup> However, the hash value, or unique 'digital fingerprint' of the imaged data, verified as accurate and thereby demonstrated that the image was 'accurate and complete.'<sup>31</sup>

The importance of this case for the use of AccessData's Forensic Toolkit® (FTK®) is extensive. First and foremost, the case explicitly establishes FTK as an acceptable industry standard for collecting digital evidence. Secondly, in the case, the defense argues that the inconsistency in the imaging dates indicates Stroz Friedberg had failed to authenticate the ownership of the evidence and therefore the evidence was inadmissible. The court however finds that the hashes used by FTK to authenticate the image and establish a chain of custody are sufficient to "establish the usage and ownership history."

## Meeting the Daubert Standards

In addition to the acceptance of the underlying AccessData technologies utilized, AccessData's solutions have been upheld countless times in court as meeting the standards set forth by the *Daubert*<sup>32</sup> case discussed above. As you will recall that case established four standards: Has FTK<sup>®</sup> Technology Been Reliably Tested? Has FTK<sup>®</sup> Technology Been Given Peer Review? What is the error rate? and Has FTK Been Generally Accepted by the Computer Forensics Community? Each question will be reviewed in detail below.

### **Has FTK<sup>®</sup> Technology Been Reliably Tested?**

AccessData's technology has been extensively tested, both by our development staff and by the community at large. Probably the most widely accepted testing body is the National Institute of Standards and Technology (NIST), which is a department under the US Department of Commerce. NIST conducts periodic tests of commercially available digital investigation solutions. NIST's Office of Law Enforcement Standards and Information Technology Laboratory formed a joint project with the National Institute of Justice (NIJ) called the Computer Forensic Tool Testing Project (CFTT). In 2008, the CFTT conducted a thorough examination of AccessData's Forensic Toolkit (FTK) technology for the purposes of disk imaging. The results of those tests are available in a National Institute of Justice Special Report, which can be downloaded at [http://www.cftt.nist.gov/disk\\_imaging.htm](http://www.cftt.nist.gov/disk_imaging.htm).

In addition to NIST and the CFTT Project, AccessData's digital investigation technologies are frequently evaluated by federal agencies, state agencies and law enforcement organizations. AccessData maintains collaborative relationships with these entities to optimize development efforts.

### **Has FTK<sup>®</sup> Technology Been Given Peer Review?**

AccessData's solutions are utilized by more than 30,000 investigators, and AccessData has allowed its solutions to be scrutinized by countless industry experts, federal agencies and publications, including but not limited to the following:

- Gartner
- Stroz Friedberg
- SC Magazine
- NIST
- Department of Defense Cyber Crime Center
- Department of Justice

### **What are the Error Rates?**

Error rates are not generally a relevant category within the field of computer forensics, because there are essentially no errors in data acquisitions. There is no replicable error rate. If something does happen to the acquired data, it is fully revealed by the hashing and checksum techniques, which we discussed above. That said, what is more relevant within the field of digital evidence is the concept of supported platforms. AccessData widely publishes all the platforms and file systems supported by our products.<sup>33</sup>

### **Has FTK Been Generally Accepted by the Computer Forensics Community?**

AccessData's solutions have been widely accepted throughout the forensics community in the United States and around the world. Not only are there more than 30,000 copies of our software in use, but our solutions are utilized by the largest law enforcement agencies in the world, including the SEC, FBI, USSS, UK Met Police, IRS, ICE and countless others. In addition to our extensive user base, AccessData hosts a message board with more than 2,600 active members, trains more than 4,000 people annually, and hosts the largest computer forensics conference in the United States.

Finally, our forensic technology is referenced in specific case law validating its acceptance by the forensics community. In the case of *United States v. Gaynor*,<sup>34</sup> the Court explicitly acknowledged FTK® (AccessData's flagship technology) and EnCase (Guidance Software's product) as the most commonly used forensic tools used by forensic examiners for computer investigations.

## The New Federal Rules of Civil Procedure

The second group of rules relevant to digital evidence is the much more recent and more specific amendments to the Federal Rules of Civil Procedure (FRCP). On April 12, 2006 the U.S. Supreme Court approved a significant amendment to the FRCP. The new rules directly addressed the issue surrounding the use and production of electronic evidence in civil cases. While the changes were extensive and nuanced, there were four key revisions that provide significant guidance for companies facing litigation.

- **Scope of Discovery:** First and possibly most important is that the new rules provided a very broad definition of “electronically stored information” that must be disclosed. In fact, the new FRCP requires an exhaustive search for all electronically stored information that is “in the possession, custody, or control of the party.” Even when data is “identified as not reasonably accessible because of undue burden or cost,” its location and description must be disclosed.<sup>35</sup> These changes have been interpreted to mean a thorough search of all active or stored data, as opposed to all available data, which would include the recovery of deleted documents.
- **Early Review and Production:** The new rules also require extremely quick production of electronic evidence. Specifically, the new rules require that a comprehensive search of electronic data be done prior to the first pre-trial conference.<sup>36</sup> Discovered data must be disclosed “without awaiting a discovery request” with the only exception being privileged data.<sup>37</sup>
- **Native Production:** While FRCP 26(f)(3) allows for the parties to discuss the form in which data is produced. While the rules do allow for native file production, significant case law indicates a requirement for native production in certain circumstances, including the landmark *Williams*<sup>38</sup> case, in which the Court ruled that the electronic spreadsheets kept in the ordinary course of business, were to be produced “in native format ...with their metadata intact.”
- **Sanctions:** Finally the new rules provide for significant sanctions in the event that data is not produced in a timely manner or deleted.
  - **Data is not Produced:** When data is not produced, sanctions can be significant, such as the monetary fines awarded in *Todd v. Guidance Software*.<sup>39</sup> In addition, the court can appoint external experts to retrieve the data from the company if the company is unable to produce the data themselves.
  - **Data is Produced Late:** When data is produced late the fines are typically monetary as in the case of *Serra Chevrolet, Inc. v. General Motors*<sup>40</sup> where a sanction of \$50,000 per day was awarded until the data was produced.
  - **Data is Deleted:** When data is deleted the new rules apply a “routine, good-faith operation” standard to determine whether the data was deleted as part of normal procedures or if it was knowingly deleted to hide evidence. If the data was deleted as part of a normal process, Rule 37(f) protects the company from sanctions. However, if it was deleted for other reasons, sanctions can range from fines to entry of default judgment, as awarded in *Arista v. Usenet.com*.<sup>41</sup>

## Proper Collection and Good Faith Effort are Critical

When dealing with discovery matters, the courts have confirmed that ESI collected by FTK technology and produced in the form of FTK-generated reports has been sufficient to satisfy discovery requirements.<sup>42</sup> These findings provide assurance that using the software with proper methods would satisfy discovery requirements, save time in collection and thereby reduce costs.

However, while computer forensic technology, such as FTK, can ease the burden of collection, this technology also makes it easier to prove a party is not disclosing everything requested. Using this type of technology, a forensic expert is able to track collection efforts and timeline ESI production to illustrate a party's good faith effort or a party's failure to comply. Even more than before, it is critical for an organization to legitimately and appropriately produce ESI requested through discovery motions. Failure to produce ESI in strict compliance with the Federal Rules has resulted in the United States District Court sanctioning parties, ordering the compensation of the opposing party's attorney and expert witness fees in gathering the undisclosed ESI, and even going as far as considering dismissal of a case when destruction of ESI has been proven.

In *In re Atlantic*,<sup>43</sup> the court held that Defendant's corporate counsel's failure to cooperate in discovery warranted compensation of plaintiff's attorney fees and costs incurred in pursuing discovery. Defendant made contradictory statements regarding several issues, one of the issues was regarding whether FTK was used for document recovery and Defendant's technology manager testified that no such program was used to search and recover any documents. Meanwhile, a court appointed computer expert testified that he found evidence that proved FTK had been used but that the documents had just not been turned over to Plaintiff. Not only did the court accept the data searched for and produced by FTK, but relayed repercussions of what happens when parties do not cooperate in good discovery practice. The United States District Court easily found bad faith discovery methods with the assistance of a court appointed expert, utilizing computer forensic methodology.

Not only is it beneficial to use an expert and the proper accepted software in ESI production, but it is mandatory under the FRCP 26(a)(2)(c). The rule mandates that a "party must make [expert] disclosures at the times and in sequence that the court orders."<sup>44</sup> In making the good faith effort of showing cooperation of discovery disclosures, it would be beneficial to the party to use software that has been acknowledged as an acceptable method of production of ESI, such as FTK. In 2008, the Court in *Rivera-Cruz*<sup>45</sup> held that, even though the expert failed to apply his forensic methods correctly to the facts of the case, the proper methods and software, FTK, was used as it was the same product used by the United States General Services Administration. Using the proper tools from the beginning can diminish further doubt by opposing parties and prevent opposing parties from bringing in motions against proper discovery methods and further delaying litigation, which can cause more expenses and, more importantly, bad faith presumption on a party's case.

Once a person or company is a party to a litigation matter or know they will be, they have a duty to preserve relevant discovery. In *Zubulake IV*, the court stated "the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."<sup>46</sup> An organization's choice of technology to fulfill this obligation is critical to avoid court sanctions and embarrassing court losses.

### The Collection Process and Reducing Risk

Documents and other information are central to every legal matter—even for those matters that don't involve litigation. For matters involving litigation (even potential litigation), and extra duty—preservation—is imposed upon the party.<sup>47</sup> Spoliation of evidence, when there is a duty to preserve it, can prompt a court to impose sanctions on you (the attorney) and/or your company. Sanctions are often monetary,<sup>48</sup> but other sanctions include: the striking of pleadings,<sup>49</sup> default judgment,<sup>50</sup> dismissal of the case<sup>51</sup> or an adverse inference.<sup>52</sup>

The duty to preserve implies two subsequent actions, namely the *identification* of the relevant information, and the *collection* of that information for review and possible production/presentation. Thus, for each case the attorney must find the relevant information and decide how to preserve it.

The preservation of the information, however, can be affected by *how* the information is collected. Consequently, a sanction-averse attorney would do well to acquaint him/herself with their collection options.

There are many "right" and some "wrong" ways to collect and to preserve potentially relevant evidence. No matter what, however, the attorney and/or client will need to take some action and that action will likely entail some software application in order to take advantage of any safe harbor provisions.<sup>53</sup> What constitutes a right or a wrong collection process can be subjective, with the last word belonging to a judge. From the attorney's standpoint, there are only two main varieties of collection procedures: *copy/sequester*, and *in-place hold* (also referred to as *hold in-place*). Each procedure has benefits and shortcomings. More importantly, each procedure has a different potential for sanctions by a court.

Attorneys prefer the copy/sequester method because it mirrors sound forensic guidelines promulgated by many law enforcement agencies, such as the U.S. Department of Justice.<sup>54</sup> The copy/sequester method doesn't make a single copy of the original document. Instead, two copies are typically made. Experts utilize the second copy (called a "working copy") for analysis. The first copy is left undisturbed and can be used to obtain working copies of the document if the review/examination process corrupts the original working copy.

If there is a question regarding the integrity of the document, the question can be resolved by reference to the first copy in a manner easily defensible to a court.<sup>55</sup> The copy/sequestration method, if done with a competent forensic software application, can make an exact copy the document itself and the associated metadata while leaving the original document in place for further use by the client. Remember, if not done correctly, the process of copying can result in spoliation of the evidence.

In the past, some attorneys were concerned whether the copied electronic files adhered to the best evidence rule.<sup>56</sup> This isn't a problem in today's computerized legal environment. Recall that the best evidence rule was promulgated in the 19th Century, when it was difficult to make copies of a document at all, let alone precisely. However in the 21st Century, making *precisely identical* copies of an electronic document is trivial and reliable with the right software. Because precisely identical copies of electronic documents and their associated metadata can be readily made, creating authenticatable copies of ESI—if done properly—does not subject the attorney to a sanctions motion for spoliation of evidence.

While copying electronic documents and their associated metadata can be readily accomplished, the attorney needs to ensure that the copying is done properly. Simply making copies by burning CD's, copying files to thumb drives or "ghosting" may seem adequate, but unless you are very careful, you will likely alter (irreparably) some of the metadata associated with the original file, thus tampering with the evidence.<sup>57</sup> In some cases, the altering of such metadata has resulted in sanctions.<sup>58</sup> It is always better to use a forensics tool that is designed to preserve all of the evidence when making a copy using default settings.

Sequestration of the copied evidence is the obvious second step in the method. Sequestration can take many forms, such as locking the hard drives containing the copies of the evidence in a secure locker in the legal department, or storing the information at an offsite location. There is no objective standard for the sequestration step, although attorneys should exercise reasonable judgment. The key is separating the first (archive) copy of the information from both the original copy and the working copy used by attorneys and experts, and maintaining the security of the various copies. This ensures that there is a source where, if all else fails, a precise copy of the original evidence is available to remedy problems.

As the name suggests, in-place hold allows the original electronic documents to remain in where they are. The benefits are obvious. The attorney doesn't have to disrupt access to her client's data during a copying process. However, in order to adhere to litigation hold notices or other

preservation considerations, the attorney must impose some safeguards so that the original electronic documents are not disturbed. This can be accomplished by forcing the client to save new/updated documents to another location. Unfortunately, not only does the “copy new/updated files to a new place” method disrupt the client's normal business operations, that method also requires strict cooperation by the client and their employees. Worse, to avoid frustration, some employees may not adhere to the terms of the litigation hold, and destroy the evidence.<sup>59</sup> Circumvention of the in-place hold methodologies, particularly those employing agent-less software applications, rely upon features<sup>60</sup> of the underlying operating system.<sup>61</sup> However, employees using tools readily available on the Internet can modify the privilege levels of relevant files and thus tamper with the evidence.<sup>62</sup> Worse, even after software guards have been put in place, some custodians have been known to destroy the machine containing the evidence.<sup>63</sup>

While the Federal Rules don't preclude the in-place hold methodologies, “[c]ourts may consider the actions taken by counsel to ensure compliance with a party's preservation obligation.”<sup>64</sup> Indeed, the Court in *Hawaiian Airlines* noted that the defendant had alternatives to the in-place hold scheme that they had adopted, and sanctions were appropriate because the collection/sequestration option was not taken.<sup>65</sup> The Sedona Conference has recently noted the need for quality assurance as part of the attorney's duty.<sup>66</sup> Indeed, the trend is to impose a duty on the attorney to require a certain level of quality assurance for the operations performed under his or her direction.<sup>67</sup>

Finally, one may question whether storing new/updated copies of the original documents in a different location is any less trouble than the copy/sequester method because, in both cases, there are two sets of documents in two locations. Wouldn't it have been simpler to make a copy of the original set of documents and allow the client to continue using their machines in the normal fashion?

If the “in-place hold” method fails for some reason, the requesting party can file a motion under Rule 34(a)<sup>68</sup> and ask the Court to require the responding party to provide access to their system to the requesting party's forensic expert or to a Court-appointed special master.<sup>69</sup> If there is evidence of spoliation, sanctions could be imposed on the producing party and their attorneys.<sup>70</sup>

Under the copy/sequester method, about the only thing that can go wrong is the mechanical failure of the device containing the sequestered data. Such failures *do* happen.<sup>71</sup> However, no court has ever held that against an attorney or party for such a mechanical failure outside the control of the attorney or her client.

Because employing the copy/sequester method reduces the potential for sanctions against the attorney and the client, most attorneys when faced with a choice will avoid the “in-place hold” method for preserving electronically stored information.

## The Federal Rules and Technology

Since the change in the federal rules there have been many cases that have further defined and provided insight into the interpretation of these rules. There has also been a large amount of practical experience gained as companies both attempted to comply with the rules, as well as test their boundaries. While none of this experience directly references any particular products, the last few years have made it clear that there are a few technological requirements that corporations should focus on when purchasing an eDiscovery solution:

### Metadata - How Important Is It?

The importance of metadata is growing as more and more judges require its production. That said, the issue is actually fairly nuanced. The most accurate statement regarding metadata is that it is as important as the prosecution wants it to be. If the prosecution asks for the production

of metadata in the initial 26(f) meeting, or prior to a significant amount of data being produced, then the courts have almost universally required its production.

“There is a clear pattern in the case law concerning motions to compel the production of metadata. Courts generally have ordered the production of metadata when it is sought in the initial document request and the producing party has not yet produced the documents in any form. See *Payment Card*, 2007 WL 121426, at \*4 (directing production of metadata for any documents not yet produced); Hagenbuch, 2006 WL 665005, at \*4 (granting motion to compel production in native form); *In re Priceline.com*, 233 F.R.D. at 91 (production ordered in TIFF format with corresponding searchable metadata databases).”<sup>72</sup>

Even when the data has been produced, if the evidentiary value of the metadata is clear or at least should have been clear, the court has required its production in native form, as in the case of *Williams*,<sup>73</sup> when the Court “ordered production of Excel spreadsheets with metadata even though no request had been made initially because producing party should reasonably have known that metadata was relevant.”<sup>74</sup>

If, however, the request for production comes well after documents have already been produced and the evidentiary value of the metadata is not immediately clear, then the courts have been more reluctant to require its production:

“[S]ee *Mich. First Credit Union*, 2007 WL 4098213, at \*2 (court denied production despite timely request for metadata because it was not relevant and production would be unduly burdensome). On the other hand, if metadata is not sought in the initial document request, and particularly if the producing party already has produced the documents in another form, courts tend to deny later requests, often concluding that the metadata is not relevant. See *Autotech Techs.*, 248 F.R.D. at 559-60 (court refused to compel production of metadata not sought in initial request); *D’Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.D.C.2008) (same); *Payment Card*, 2007 WL 121426, at \*4 (denying motion to compel metadata for documents already produced in TIFF format because another production would be unduly burdensome); *Ky. Speedway*, 2006 WL 5097354, at \*8 (motion to compel production of metadata denied when request first came seven months after production); *Wyeth*, 248 F.R.D. at 171 (documents produced in TIFF format were sufficient since parties never agreed on form of production).”<sup>75</sup>

Despite the nuanced nature of the law, the point here for any company looking to implement an eDiscovery solution is that you absolutely must have a solution that can collect and produce relevant metadata.

### Timely Production and Scope of Discovery

The speed and scope of production are very important issues when considering which eDiscovery solution to implement and have also been an area of interest in case law. Case law, as well as the new federal rules, are fairly clear that if the machine is on the network it is within scope. In fact over the past several years the court has become extremely unforgiving regarding “undue burden” arguments attempted by defense. One particularly compelling case regarding these issues is *Todd v. Guidance Software*.<sup>76</sup> In this wrongful termination case, Todd requested production from Guidance Software of all documents related to her and discussions regarding her performance and employment. The case is important because of the way Guidance Software responded to the request and the resulting conclusions formed by the court.

- **Filter:** The investigator at Guidance Software tasked with the discovery apparently filtered data that was reactive to the agreed upon search terms based on his perception of relevance. In the words of the judge: “The problem that I see

immediately [is that] he acted like a filter. That's not his job. That's not what discovery is all about.....It's inexcusable."<sup>77</sup>

- **Data Corruption:** Guidance Software ultimately claimed that the inability to produce data stemmed from the corruption of their Exchange server shortly after the departure of Todd. In reaction to this admission in combination with the slow data production the judge concluded: "Was there hiding the ball going on? Circumstantial evidence, but it is very, very persuasive that this was being done." The arbitrator went on to say that the behavior of Guidance Software "and the naivete that they thought they could get away with boggles the mind."<sup>78</sup>
- **Time and Scope:** In addition to the above issues the case takes a very interesting look at the issues of both time and scope. On May 9, 2008 the court entered a sanction order requiring Guidance Software to execute a board search and return the resulting data immediately. Guidance reacted by saying it was "unable to comply.... Because of the scope and breadth of the searches proposed and the number of custodians designated by Todd were overboard. Instead, GSI indicated that the search would require 12–14 days to complete." In response Todd offered expert testimony that "the search terms and number of custodians was reasonable... and that it was possible to conduct the search within 24 hours." In reaction to the two respective arguments, the judge ruled that "GSI has not fulfilled its obligations to produce all discoverable documents."<sup>79</sup>
- **Court Reaction:** The court reacted in three distinct ways to the incomplete and improper production. First and foremost, Guidance Software was sanctioned and required to pay expert fees to evaluate its collection. Secondly, the judge concluded that relevant data had been withheld or destroyed and allowed Todd to stipulate the existence of several incriminating emails without objection. Finally, the judge ultimately found in favor of Todd.<sup>80</sup>

This case is compelling for companies to consider when looking at an eDiscovery solution, because it speaks not only to scope but also to time considerations. It is clear from this case and many others that the courts are no longer receptive to delays or claims of undue burden. As a result, companies need to implement solutions that can quickly respond to relatively large-scale discovery requests. In short, the solution needs to be truly distributed and automated.

### Deleted Data

In most cases, deleted data has generally been considered beyond the scope of most discovery requests, but that is not always the case and it is important for companies to realize that they can be compelled to produce deleted documents. This is particularly true for governmental organizations, as it was in the case of *State ex rel. Toledo Blade Co. v. Seneca County Bd. of Comm'rs*.<sup>81</sup> In this case, the Ohio Supreme Court ruled in a 7-0 decision that "the Seneca County Board of Commissioners had to make reasonable efforts to recover and provide the Toledo Blade newspaper with emails that had been deleted in violation of the County's records retention policy and disposition schedule. The fact that these emails had been deleted did not relieve the County from its obligation to produce this information because deleted computer files are still discoverable."

In another example, *Smith v. Slifer Smith & Frampton/Vail Associates Real Estate LLC and W. Seibert*,<sup>82</sup> the Court granted the plaintiff's motion for sanctions for destruction of evidence and granted Plaintiffs expert costs, which could have been avoided had destruction of evidence been disclosed in a timely manner. Here, the plaintiff had asked for ESI and after the defendant had produced the documents, the plaintiff then asked for supplemental discovery stating that the discovery was not complete because only "active" ESI had been turned over.

The Defendant then used FTK to produce a second set of discovery. In their request, the plaintiff asked for production of ESI pursuant to Fed. R. Civ. P. 34(b)(1)(c), either in the form in which the data was ordinarily maintained or reasonably usable, or in a form which includes all data and

metadata and is readable and searchable in Microsoft Word. The Court stated that the production of ESI in the form of the FTK report was generally acknowledged as an “acceptable method of production of ESI.”<sup>83</sup>

It is no surprise that destruction of evidence by either party whether it is material or not can become a huge issue during litigation. While the party seeking discovery has the burden of proving that any such destruction of evidence has occurred, it has become all too easy for a party to find wrongdoing through court-ordered forensic experts. Should the expert find any evidence that the party failed to turn over, destroyed or tampered with any requested ESI, sanctions can result and fees can be compensable.

Attorney’s fees and expert fees can become uncontrollable if an organization must compensate the opposing party’s fees due to failure to use good discovery practice. The court in *Smith* found that Plaintiff’s ability to litigate their claims were substantially prejudiced by Defendant’s failure to preserve potentially relevant information and therefore found that Defendant’s failure to preserve ESI had forced the Plaintiffs to incur considerable discovery expenses. The court therefore ordered Plaintiffs an award of their attorney fees and costs for the motion of additional discovery expenses. Litigation is always expensive and having to compensate the other party for additional costs such as these shows the importance of practicing good discovery through good faith and proper court approved methods.

More important than sanctions, an adverse instruction to the jury at trial may be permitted if destruction of evidence is illustrated. The opposing party must show with sufficient evidence which a “reasonable trier of fact could infer that the destroyed evidence would have been the nature alleged by the party affected by its destruction.”<sup>84</sup> However if there is a showing of bad faith on the party that destroys evidence, through sufficient circumstantial evidence, the jury could conclude that the missing evidence was unfavorable to that party. Obviously any such inference could be destructive, which goes to show that proper electronic discovery methods must be used.

### Limits of Litigation Hold Technologies

The last area we are going to examine here is the limitation of litigation hold technologies. These technologies are absolutely critical for virtually every company subject to US law because of the prominent place litigation hold notices take in case law. Despite the importance of these solutions it is critical for companies to understand that they do not represent a complete solution, nor do they reduce the company’s obligation to produce evidence subject to the litigation hold notice. This issue is made crystal clear in the case of *In re Hawaiian Airlines, Inc.*,<sup>85</sup> in which defendant Mesa Air relied on litigation hold notices to ensure that key data was preserved. Unfortunately Mesa's CFO used the litigation hold notice as a virtual call to action and downloaded and executed wiping tools designed to eliminate all relevant data on his computer. In this case, Mesa Air argued that because the CFO had acted alone in direct conflict to the litigation hold notice that had been sent, Mesa should not be subject to sanctions or summary judgment. In his ruling the judge disagreed with the arguments put forth by Mesa Air and concluded that “Mesa should also be responsible for the intentional destruction by one of its highest ranking officers of evidence.”<sup>86</sup> To justify his decision, the judge pointed to the fact that “Mesa could have prevented Mr. Murnane from destroying evidence, or at least limited his ability to destroy evidence, by taking reasonable, inexpensive, and non-burdensome steps. Mesa failed to do so and is responsible for the consequences of that failure.”<sup>87</sup>

To remedy the prejudice resulting from the destruction of data, the judge entered a finding of fact that Mesa Air not only had destroyed critical evidence but that the evidence validated Hawaiian Airlines claims. In addition he held open the possibility that Hawaiian Airlines “may also be entitled to costs and reasonable attorneys’ fees as a further sanction.”<sup>88</sup>

The important point raised by the case of *In re Hawaiian Airlines*<sup>89</sup> is that so-called “hold in place” technologies do not protect a company from claims of spoliation, especially if that spoliation is

perpetrated by an employee who is even moderately skilled technically. As a result, companies need to ensure they not only have litigation hold capabilities, but that they also have an eDiscovery solution with the following two key capabilities:

- **Integration with Litigation Hold:** Companies should work to ensure that whatever technology they select for their eDiscovery solution offers some degree of integration with their litigation hold technology. At a minimum, companies need the ability to specify employees that might be critical to a given case and execute a proactive collection against prior or in conjunction with the sending of litigation hold notices.
- **Automated Forensic Collection:** Companies need a solution that automates both the identification of data relevant to a given case, as well as the collection and preservation of that data. In addition, the solution should be able to execute a complete disk image of particularly critical resources (the computer of the Mesa CFO comes to mind).

### Search Issues and AccessData® Technology

The issue of search scope is unusually relevant in the field of digital evidence and digital forensics. Warrants and scope of search rules were all crafted around the simple realities of the physical world. The idea being that a warrant sets down the scope of the allowable investigations and any evidence found by searching outside of the permitted scope is not admissible. In the physical world these rules are easy to understand and easy to comply with. However, in the digital world, they are not nearly as transparent.

The question investigators often face when they have a warrant to search a computer related to a specific matter is: What am I allowed to do before I step outside the rights granted by the warrant? While there is no blanket answer to this question, the case of *United States v. Mann*<sup>90</sup> sheds some light on the issue. In this case, Mann was charged with possession of child pornography. The pornography was found on Mann's computer subsequent to a search of his computer equipment under a search warrant. In the course of the investigation, the investigating officer utilized FTK—which was described as “software commonly used by many forensic computer examiners,”<sup>91</sup>—to image and analyze four items of the suspect's digital media. The investigator did not limit his search by file timestamp, file name, file location or by any other criteria. Indeed, the investigator utilized the known file filter (KFF) technology provided by FTK to remove standard system files from his search, as well as detect any known instances of child porn. When the investigator found files known to be child pornography, he looked at them “without obtaining another search warrant.”<sup>92</sup>

The defense challenged the admissibility of the evidence, because the warrant was granted pursuant to an issue of voyeurism and not pornography and therefore “the search exceeded the scope of the warrant.”<sup>93</sup> Specifically, the defense argued that the specific language of search warrant authorized officers to search for “video tapes, CDs or other digital media, computers, and the contents of said computers, tapes or other electronic media to search for images of women in locker rooms or other private areas”<sup>94</sup> as opposed to child pornography. However, Mann argued “that upon suspecting child pornography, the police officers were required to obtain a separate warrant.”<sup>95</sup>

The court ruled that “[t]he search was executed within the scope of its authorization, with limited exceptions” and that the evidence should therefore be admitted. The court provided the following reasoning for allowing the evidence:<sup>96</sup>

1. “The warrant did not, by its terms, restrict the police officers from viewing files that might have been downloaded to Mann's computer. The warrant did not restrict the officers from decrypting files or viewing files that had been erased. The warrant did not restrict the police officers from viewing files related to Mann's internet activities, newsgroup participation, computer files, e-mail, papers and business records, jacks, adaptor cords.”<sup>97</sup>

2. "A police officer may properly seize evidence of a crime without a warrant if: (1) a law-enforcement officer is lawfully present, (2) an item not named in the warrant (or, likewise, outside the scope of consent) is in the plain view of the officer, and (3) the incriminating nature of the item is immediately apparent (i.e., the government can show probable cause to believe the item is linked to criminal activity)."<sup>98</sup>

The plain view doctrine cited is of particular importance in computer forensics both to law enforcement and to corporate practitioners. Not only is it well tested within US courts<sup>99</sup> but many corporate customers have utilized the plain view doctrine when conducting network-based forensic investigations to ensure that evidence found in the course of a search is admissible.

In *United States v. Graziano*,<sup>100</sup> the Court provided even stronger language supporting the broad interpretation of warrants relative to digital evidence. In this case, FTK was again used to search and analyze a computer and again the defense challenged the admissibility of the data on the grounds that "the warrant is facially overbroad and invalid because it did not require a certain search methodology or limit the search of computers to certain keywords or terms." In this case the court explicitly addresses the issue of search terms and found the following:

"there is nothing in the language of the Fourth Amendment, or in the jurisprudence of the Supreme Court or the Second Circuit, that requires such a rule in the context of a search of computers. See *Dalia v. United States*.<sup>101</sup> ('Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that ... search warrants also must include a specification of the precise manner in which they are to be executed.')"<sup>102</sup>

In fact, the Supreme Court has noted that, as a general matter, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant."<sup>103</sup> The reason for not imposing a protocol requirement on law enforcement in conjunction with search warrant applications for computer searches is obvious-in most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities. In other words, to require courts in advance to restrict the computer search in every case to certain methodologies or terms would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents, or placing such documents in areas of the computer that would not normally contain such files/documents. In today's technological age, a computer should not be a safe-haven for criminals to hide evidence of their criminal activities by unnecessarily limiting law enforcement's ability to search only certain files/documents on a computer with a certain name or term, or located in a certain area of the computer hard drive. Therefore, although the Second Circuit has not decided this precise issue, this Court declines to adopt a rule that would invalidate search warrants which did not contain a specific methodology explaining how the computers would be searched."<sup>104</sup>

While neither case enables a blanket statement to be made regarding the admissibility of digital evidence obtained as part of a warrant-based search, the case law is fairly robust in its support of the plain view doctrine and the open-ended searching of digital media when the warrant doesn't explicitly limit the scope.

### Mobile Phone Search Issues

Mobile phone data has become commonplace in the area of forensics. Nearly everybody has a cell phone and the data these devices contain is frequently highly relevant in the context of an investigation. The interesting question regarding mobile phones is therefore not how relevant they are, but in what context are investigators or officers of the law allowed to seize and analyze the data on them? The question is not at all clean cut, because regardless of how you think of cell phones, they straddle several key concepts from the perspective of the law.

From one perspective it is easy to think of them as small computers and therefore subject them to the laws associated with computers. From another perspective, a cell phone is a container of sorts, no different from a box that a law enforcement officer is often permitted to open. Finally, it is also easy to see them as something much more personal than either a computer or a box, because they almost always contain large amounts of very personal information. Regardless of how you see them, what is truly relevant is the perspective of the law and more importantly how they should be viewed relative to the Fourth Amendment, protecting people against unreasonable search and seizure.

Unfortunately there is very little case law address the seizure of mobile phones and the two significant cases that do exist, one from the 9<sup>th</sup> Circuit and one from the 5<sup>th</sup> Circuit are completely contradictory. In *United States v. Edwards*,<sup>105</sup> the 9<sup>th</sup> Circuit Court ruled that mobile phones are effectively computers and therefore require a warrant to search. "Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, e-mail, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through e-mail and text, voice and instant messages."<sup>106</sup> Given the capacity for storage possessed by cell phones the court pointed out that ruling any other way than requiring a search warrant "could have far-ranging consequences."<sup>107</sup>

While the prosecution attempted to argue that the seizure of cell phones is allowed as part of the booking process, the Court in *Edwards* concluded that the government had failed to show any purpose other than furthering the criminal investigation:

"The court finds that the government has not met its burden to show, by a preponderance of the evidence, that it is standard police practice to search the contents of a cellular phone as part of the booking process....Indeed, the government has not articulated any reason why it is necessary to search the contents of a cell phone in order to fulfill any of the legitimate governmental interests served by a booking search: namely, to deter theft of arrestees' property and false claims of theft by arrestees, and to identify contraband and other items."<sup>108</sup>

In the 5<sup>th</sup> Circuit, however, the court reached a very different conclusion. In *United States v. Finley*,<sup>109</sup> the defendant was searched incident to his arrest. During the search, police took the defendant's cell phone they had found on his person and conducted a search pursuant to the defendant's arrest. The Court found that the search was lawful and that the "reasonable search" was not "constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial."<sup>110</sup> *Finley*, like *Edwards*, also addressed the issue of a person's reasonable expectation of privacy relative to mobile phone data. However in *Finley*, unlike in *Edwards*, the judge ruled that while Finley did possess a reasonable expectation of privacy, the officer had the right to search that phone as part of the booking process, and therefore the cell phone data was admissible.

Courts have attempted to resolve the tension between *Finley* and *Edwards*. For example, in *People v. Diaz*, 165 Cal. App. 4th 732, 81 Cal. Rptr.3d 215 (2d Dist. 2008), the defendant's cell phone was seized from his person incident to his arrest, but the cell phone itself was searched 90 minutes later. The Court, upholding the validity of the search, noted that "courts have upheld delayed warrantless searches of wallets (see, e.g., *United States v. Passaro* (9th Cir. 1980) 624 F.2d 938, 944), purses (*People v. Decker* (1986) 176 Cal.App.3d 1247, 1252 [222 Cal. Rptr. 689]), address books (*United States v. Rodriguez* (7th Cir. 1993) 995 F.2d 776, 777-778) and pagers (*United States v. Chan* (N.D.Cal. 1993) 830 F.Supp. 531, 536)."<sup>111</sup>

## Voice over Internet Protocol (VoIP) Interception and Analysis

While Forensic Toolkit<sup>®</sup> is used to analyze mobile phone data, another AccessData technology, SilentRunner, can be used to intercept, analyze and preserve voice over Internet protocol data. Voice over Internet Protocol (VoIP) refers to voice traffic over an Internet Protocol (IP) based broadband network. There are three types of VoIP services: computer to computer, telephone to computer and telephone to telephone. The main distinction to the landline telephonic communication is not *how* the communication is given or received, but rather in the data conversion that occurs during VoIP transactions. VoIP converts ordinary audio telephone signals into data packets that are sent over the Internet using Internet Protocol.<sup>112</sup> Because of the conversion into data packets, the VoIP transaction is not treated as telecommunications services but as information services.

In *Southwestern v. Mo. PSC*,<sup>113</sup> the court followed the FCC interpretation of VoIP classification—that it is a hybrid service, which has both telecommunications and information components and that because of its "capabilities for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information," VoIP falls "exclusively within the information service category if the telecommunications and information services are sufficiently intertwined." Furthermore, the Court in *Vonage v. Minn. PUC*<sup>114</sup> interpreted the Communications Act of 1996 and concluded that the VoIP service provided by Vonage "constituted an information service, because it offers the 'capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.'" The distinct categorization of VoIP transactions as information services weakens the argument that these communications are protected from wiretapping, as were the old landline telecommunications.

The Fourth Amendment and the Federal Wiretap Act of 1968<sup>115</sup> are the two bodies of law that grant wiretapping protection. In *Katz v. United States*,<sup>116</sup> the U.S. Supreme Court interpreted the Fourth Amendment and stated the two part test of when a person's telephone calls are protected: 1) a person must have a "reasonable expectation of privacy" and 2) the expectation must be one that society is prepared to recognize as reasonable. *Katz* only applies when the government is an actor or a private party is acting on behalf of the government. The Federal Wiretap Act, however, protects parties against third-party interception of telecommunications and information services, although there is a reduced protection when it is deemed information services. Incidentally, courts have permitted the interception of Internet data under the Act, since most of the time the data is stored on the third party's computers.<sup>117</sup>

The distinguishing features between the two are that third-party interception of landline phone calls requires tapping physically into the telephone line and listening in real time, whereas VoIP transactions store data and interception only requires a personal computer and some enabling software. The Federal Communications Commission (FCC) went on record to state that "it does not matter that there is a 'voice' at both ends of an IP-PSTN call [computer to phone VoIP]. The same is true of voicemail, which the FCC has long recognized is an information service."<sup>118</sup>

On the issue of VoIP interception in the workplace, privacy protection would be addressed in the same way as it would with data traversing the network. The very relationship as employee and employer would subject the data to some level of monitoring by the employer—the exceptions being the telephone and any mail through the US Post Office.<sup>119</sup> Once again the categorization of VoIP as an information transmission and also the existence of the employee-employer relationship would sum up the protection level of VoIP transmissions to a reduced level of protection. Most companies have a policy statement explaining the scope of their monitoring and monitor such communications in the ordinary course of business, which allows for a lesser degree of privacy protection for the employee. Interception of personal matters or non consensual interception by companies are highly discouraged and, in fact, is protected against by the Electronic Communications Privacy Act (ECPA).<sup>120</sup>

While the same information can be transmitted through landline or VoIP, the two different platforms of sending the message can change who is allowed and not allowed to listen in on the

call. VoIP transmission technology is growing rapidly, because of its low cost and bandwidth efficiency. Therefore, it is an issue to be tracked closely until a definite answer is given on what can and cannot be intercepted.

### RAM Analysis: Be Prepared

Everyone in the forensics industry knew it was inevitable, but just the same, I think everyone dreaded the day the courts woke up to the true relevance of information contained in random access memory ("RAM"). Nonetheless that day has come and we now have several key court decisions, such as *Columbia Pictures Industries Inc. v. Bunnell*,<sup>121</sup> in which the preservation of data contained in RAM was deemed both discoverable and relevant. While the actual instances in which RAM are still rare, that dynamic is clearly set to change as the amount of RAM available on a standard computer continues to rise exponentially, and particularly with the widespread use of so-called "virtual machines."

One should expect that, in the near future, seizure of RAM by law enforcement agencies will become standard best practice. AccessData's users are particularly well positioned when this shift occurs, because all of our products contain the ability to both acquire and analyze RAM. In fact, there is no difference, from the perspective of the user, between the acquisition and analysis of RAM and that of more traditional memory.

### Conclusion

While it is true that neither the current case law nor the Federal Rules of Civil Procedure directly specify technology, it is equally true that together they provide companies with some very clear key requirements. AccessData's eDiscovery solution is the only solution on the market that matches all of these requirements in full. Our enterprise-class architecture allows us to not only search thousands of computers in a matter of days, but we also have the most comprehensive data access capabilities available. We search and collect from every widely accepted operating system, every major email type, and search and collect from more than 30 of the most common data repositories, including Documentum, OpenText, FileNet, SharePoint and Symantec's Enterprise Vault. We support a number of data collection options, including capturing complete forensic images or forensic acquisition of individual files that support native file production with metadata preservation. All collections performed using AccessData technology can be made in a forensically sound manner, meaning that the collected data is not altered and that all relevant metadata is preserved. Finally, we offer integrated litigation hold capabilities and integrate with other market-leading litigation hold products.

## AccessData in Court

AccessData's FTK is the standard computer forensic product used by the U.S. Federal Bureau of Investigation. As such, FTK is constantly being recognized by courts as an effective tool to extract and analyze electronically stored information. In addition to the cases mentioned in the main body of this document, here are a few more representative cases:

### ***United States v. Potts, 2008 WL 2051090 (D. Kan. 2008).***

In this case, the defendant moved to suppress evidence gathered through an "overly broad" search warrant. Attachment B of the warrant "lists evidence pertaining to images of child pornography, and sexual activity with children." *Id.* at \*5. "The search warrant authorized a search of defendant's residence, including any computers and electronic storage devices found in defendant's residence." *Id.* The judge noted that the examiner of the computer, Sergeant Owen, "did not engage in an impermissibly broad search for the items listed in the warrant." *Id.* at \*22. Because, "[w]hile the warrant allowed Sergeant Owen to open every file and look at the first few pages, he did not need to do so because such a broad search is unnecessary with modern forensic software." *Id.* at \*21. The court specifically identified "forensic software, including Forensic Toolkit" (FTK). *Id.* at \*10.

### ***Tauck v. Tauck, 2007 Conn. Super. LEXIS 2618 (Conn. Super. Ct., Sept. 21, 2007).***

In a bitter divorce case, which cost more than \$13 Million in legal fees for both sides, computer forensics was used to determine whether allegations, made by Nancy Tauck against her husband, Peter Tauck, were valid. Nancy Tauck accused her husband of possessing child pornography, and Peter Tauck's old Toshiba laptop was one of the materials seized and examined. An expert from Global CompuSearch LLC, a computer forensics service provider, examined the laptop for the husband and served as his expert witness, testifying at the trial. After forensic analysis, Marcus Lawson, President of Global CompuSearch LLC, refuted the claims made by Nancy Tauck. Global CompuSearch was given six hard drives to examine in which there were found numerous "suspect" images. However it was also discovered that 148 of those images were downloaded on May 5, 2005, which was the date Peter Tauck's passport verified that he was in Tahiti. The question then became: "From what location were the images downloaded?" Global CompuSearch found an Internet protocol ("IP") address that led them to conclude the download took place from within the state of Connecticut, where the wife was at the time. The forensic expert further stated that he found no evidence that anyone had altered the system date on the computer. Furthermore, Global CompuSearch found that a substantial number of files on other computers had been deleted from the internet cache folders. With this information, they were able to illustrate that some deliberate action was taken to eliminate information on that computer so there would be no internet browsing history to show which sites were visited. The Court found that the evidence did not corroborate Nancy Tauck's allegations and that it was clear that the download of the suspected photographs took place when Peter Tauck was half way across the globe. The Court concluded from the forensic evidence that Nancy Tauck, or other unknown persons, planted the images onto the computer while Peter Tauck was away.

### ***Commonwealth v. Koehler, 914 A.2d 427 (Pa. Super. 2006).***

In this criminal case, the Court found that there was reasonable suspicion to conduct a warrantless property search of a parolee's residence and computer. The search resulted in a computer forensic analysis that uncovered sufficient evidence that Mr. Koehler possessed child pornography. The computer forensic examination of Koehler's computer hard drive was performed by Erie County Detective Jessica Lynn, who used FTK to analyze the images on Koehler's computer. Detective Lynn discovered 235 video clips depicting children and more than 300 items that were suspect as child pornography. Detective Lynn's findings against Appellant resulted in 19 charges filed against him which lead to Koehler being sentenced to 12 to 24 months of incarceration for each of his fourteen counts.

***United States v. Calimlim*, 2005 WL 2922193 (E.D. Wis., November 4, 2005).**

The government's examiner used FTK to search data and unallocated space, which included e-mails, the internet, typed documents, and deleted items. The examiner conducted the forensic examinations using the keyword and scanning methodologies available in FTK.

***United States v. Fumo*, 2007 WL 3232112 (E.D. Pa, October 30, 2007).**

In this case, the government had used FTK to examine Fumo's computer system. The Defendant moved the court to compel the government to disclose the search protocol and keyword terms under Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure in order to determine whether the search and seizure violated his Fourth Amendment Rights. The Court concluded that the "requested information [was] not material to application of the exclusionary rule" and denied the motion.

***United States v. Luken*, 515 F.Supp.2d 1020 (D.S.D, August 21, 2007).**

In this opinion, the Magistrate Judge recommended that the Defendant's motion to dismiss be denied. The Magistrate determined that the Defendant had consented to the search of his laptop, and the evidence of child pornography found using FTK by the agent was admissible.

***United States v. Richardson*, 583 F.Supp.2d 694 (W.D. Pa. October 31, 2008).**

Agents used FTK to search the Defendant's laptops, where child pornography was found.

***Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y., October 15, 2008).**

In this civil action, the defendant was suspected of accessing the website www.ntfs.com and deleting files from a laptop before handing over the device for discovery. The plaintiff's examiner used FTK to image the hard drive of the laptop. The court-appointed forensic expert, Stroz Friedberg, referenced in his report that FTK version 2.2 is an "accepted tool under industry standards, to perform the imaging and create a forensic duplicate of the hard drive."

***State v. Voorhees*, 2008 WL 2579709 (Ohio App. 3 Dist., June 30, 2008).**

In a child rape case, the State's forensic examiner used FTK to find more than 1,700 images of child pornography and videos on the Defendant's computer and under which account they existed and/or were accessed.

***United States v. Mann*, 2008 WL 1701743 (N.D. Ind., April 8, 2008).**

In this criminal case involving child pornography, a laptop was seized into evidence and examined using FTK. The court indicated that FTK is a "software commonly used by many forensic computer examiners." FTK was used for various purposes of the computer investigation, including KFF alerts (known file filter) and uncovering websites that the Defendant had visited. A motion to suppress the evidence by Defendant was only granted in part for the physical objects recovered (papers, cords, adapters). However, the motion to suppress evidence from computer investigation was denied.

***United States v. Graziano*, 558 F.Supp.2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y., March 20, 2008).**

In an arson case, the defendant moved to suppress fruits of the search of his home and computer. "In terms of the procedure employed during the search of the computer, [the examiner] used a software package called Forensic Tool Kit ("FTK"), which searches through the entire file system..." *Id.* 558 F.Supp.2d at 313. "In the instant case, when the files were sorted by FTK, [the examiner] recognized that there was a significant amount of evidence found in the internet history files." *Id.* at 314. Further utilizing FTK, the examiner was able to identify a file "search [3].htm" that contained evidence of "an AOL search using the terms 'arson rico laws' at one time in the search box." *Id.* The Court concluded that "the examiner's search of the computer and discovery of that evidence was executed in a manner that was within the scope of the warrant and was reasonable under the Fourth Amendment." *Id.* at 317.

***United States v. Sage*, 2007 WL 4592074 (W.D.Mo., December 27, 2007).**

In this statutory rape case, a motion to suppress the computer evidence was denied. The forensic examiner used FTK to examine the Defendant's computer and used FTK to organize the materials and retrieve the evidence that linked the Defendant to the under-aged victim and other younger males.

***United States v. Gaynor*, 2008 WL 113653 (D.Conn., January 4, 2008).**

This opinion focused on a motion to provide copies of ESI to Defendants who were charged with possession of child pornography. The Adam Walsh Act prohibited the Defendants from obtaining copies of child pornography (even as evidence) limited its exposure to the Defendants by requiring any viewing to be done at a government facility. The Court acknowledged FTK and EnCase as the most commonly used forensic tools used by forensic examiners for computer investigations. The government offered to provide Defendant's examiner with a computer that met the minimum system requirements for both FTK and EnCase so that an examination could be conducted.

***United States v. Flinn*, 521 F.Supp.2d 1097 (E.D. Cal., October 16, 2007).**

In Flinn, the Defendant was charged with receiving and possessing child pornography. The government seized the defendant's computer where he had allegedly received and stored the child pornography. Due to the Adam Walsh Act, the government could not release any copies or duplicative material since the material contained child pornography. Rather, under 18 U.S.C.A. § 3509(m)(2)(B), the government was required to provide the Defendant "ample opportunity for inspection, viewing, and examination at a government facility." The Court recognized this statute to mean that, where the government can supply "reasonably up to date hardware and software tools and facilities such that a defendant can construct a reasonable, available forensic defense."

The facility used was the former McClellan Air Force Base where computers were available with all of the relevant materials to perform a forensic analysis. The software implemented and made available for use was FTK-1 which the Court recognized as a "standard." The Court found that the available hardware and software provided was sufficient to uphold the Defendant's discovery rights and thereby denied the Defendant's motion to use its own facilities to examine mirror images of the evidence on their own computer.

***United States v. Eberle*, 2006 WL 1705143 (W.D. Pa, June 15, 2006).**

In Eberle, the question was whether certain ESI was on a particular computer. The question was resolved using FTK, whereby "Detective Lynn performed a more targeted search known as a 'hash value check,' whereby she searched for a specific identifier, known as an MD5 hash, that is particular to an internet image, much like a fingerprint. This hash check similarly failed to uncover any of the images that had been uploaded onto the Yahoo! Server in 2001." *Id.* at \*2.

***United States v. Aldeen*, 2006 WL 752821 (March 22, 2006).**

Defendant Ahmed Aldeen, moved the court to order the government to provide him with a mirror image of his computer hard drive allegedly containing images of child pornography. This case was prosecuted prior to the Adam Walsh Act that enables the government to prevent release of any material or copies of materials seized that involve child pornography. At the time however, the court did find the defense argument so convincing that it allowed the defendant's computer experts to utilize their own personal computers so that they could run two computer programs, one being FTK, to examine the videos.

***In re Atlantic Intern. Mortg. Co.*, 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).**

In this bankruptcy proceeding, attorneys for the debtor hired a forensic examiner to conduct an investigation of certain electronic documents, and the examiner used FTK to perform the examination.

***Sanders v. State*, 191 S.W.3d 272 (Tex.App. - Waco, March 8, 2006).**

In this case, the examiner, who was trained and well versed in FTK, discovered multiple instances of child pornography on the Defendant's computer. The appellate court refused to overturn the lower court's acceptance of the expert's testimony..

***United States v. Butts*, 2006 WL 3613364 (D. Ariz., December 6, 2006).**

In this Adams Walsh Act issue, the government moved the court to limit Defendant's access to the electronic evidence. Since the Adams Walsh Act was effective *after* the filing of the present case, the court had the option of denying the government's motion for reconsideration. However, the court granted the government's motion and limited the Defendant's ability to review the evidence. FTK was used by the Defendant's expert to examine the evidence.

## References

---

- <sup>1</sup> *United States v. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977).
- <sup>2</sup> *Lorraine v. Markel Am. Ins. Co.*, 241 FRD 534 (D. Md. 2007).
- <sup>3</sup> See, e.g., *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997) (party's allegation of tampering with the computer files of co-defendant was "almost wild-eyed speculation . . . [without] evidence to support such a scenario" so that the evidence could be authenticated. FBI agent who was present when the defendant's computer was seized can authenticate the seized files).
- <sup>4</sup> See, e.g., *United States v. Glasser*, 773 F.2d 1553,1559 (11th Cir. 1985) (the "fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness.").
- <sup>5</sup> *Bone v. State*, 771 N.E.2d 710, 716 (Ind. Ct. App. 2002) (reviewing whether data from defendant's computer was sufficiently authenticated).
- <sup>6</sup> *United States v. Briscoe*, 896 F.2d 1476, 1494 (7<sup>th</sup> Cir.1990) (citing *United States v. Croft*, 750 F.2d 1354, 1365 (7th Cir.1984) at n. 7)
- <sup>7</sup> See, e.g., *United States v. Salgado*, 250 F.3d 438, 452 (6<sup>th</sup> Cir.2001)
- <sup>8</sup> *United States v. Tank*, 200 F.3d 627 (9<sup>th</sup> Cir. 2000).
- <sup>9</sup> *Id.* at 630.
- <sup>10</sup> *Id.*
- <sup>11</sup> *Id.* citing *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts . . . would have affected only the weight of the printouts, not their admissibility.").
- <sup>12</sup> See , e.g. , *United States v. Kassimu*, 188 Fed. Appx. 264, 2006 WL 1880335 (5th Cir. 2006) (computer records authenticated by witness with personal knowledge).
- <sup>13</sup> *Lorraine*, 241 FRD at 557.
- <sup>14</sup> See, e.g., *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authentication of e-mail by circumstantial evidence such as the presence of defendant's work e-mail address and use of the defendant's nickname in the e-mail).
- <sup>15</sup> *Lorraine*, 241 FRD at 557. See also United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information , available at <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf> (encouraging parties to discuss hash values when producing electronic records in discovery to facilitate later authentication).
- <sup>16</sup> *Lorraine*, *supra*, note 2.
- <sup>17</sup> *Id.* citing Fed. R. Evid. 1001 advisory committee's note. Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the "original writing rule."
- <sup>18</sup> See, *Armstrong v. Executive Office of the President*, 810 F. Supp. 335, at 342 (D.D.C. 1993).
- <sup>19</sup> *Id.*
- <sup>20</sup> *Frye v. United States*, 54 App. D.C. 46, 293 F. 1013 (D.C. Cir. 1923) (affirming a lower court's sustaining of an objection to the introduction of expert witness testimony affirmed).
- <sup>21</sup> *Daubert v. Merrell Down Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
- <sup>22</sup> *Frye*, *supra*, note 20.
- <sup>23</sup> *Id.*
- <sup>24</sup> *Daubert*, *supra*, note 21.
- <sup>25</sup> *Id.*
- <sup>26</sup> *Gutman v. Klein*, 2008 U.S. Dist. LEXIS 92398, 2008 WL 4682208 (E.D.N.Y. Oct. 15, 2008).
- <sup>27</sup> *Stroz Friedberg, LLC, Forensic Analysis of the Klein Laptop Pursuant to Court Order in Gutman, et al. v. Klein, et al.* (Nov. 2, 2007)
- <sup>28</sup> *Gutman*, *supra* note 26.
- <sup>29</sup> *Id.* at 10.
- <sup>30</sup> *Id.* at 12.
- <sup>31</sup> *Id.*
- <sup>32</sup> *Daubert*, *supra*, note 11.
- <sup>33</sup> At the end of 2008, the file systems supported were FAT16, FAT32, NTFS, CDfs, HFS, HFS+, Ext2FS, Ext3FS, Reiser, UFS1, UFS2, EFS, JFS, LVM, SafeBoot, Utimaco, Credant, VMware, LVM2, every possible CD/DVD format [VCD, SVCD, SACD, CD-ROM, CD-ROM XA, CD-R, CD-RW, CD-MRW, DVD-ROM, DVCD, DVD-RAM, DVD-R, DVD-RW, DVD+R,DVD+RW, DVD+MRW, DVD+R Dual Layer, DVD-R Dual Layer, DVD+RW Dual Layer, DVD+VR, DVD+VRW, DVD-VR, DVD-VRW, DVD-VM, DVD-VFR, BD-ROM, BD-R, BD-R DL, BD-RE, BD-RE DL, BD-R SRM, BD-R RRM, BD-R SRM+POW, BD-R SRM-POW, BDAV,

---

BDMV HD DVD-ROM, HD DVD-R, HD DVD-R DL, HD DVD-RW, HD DVD-RW DL, HD DVD-RAM, and HD DVD.

<sup>34</sup> *United States v. Gaynor*, 2008 WL 113653 (D. Conn. 2008).

<sup>35</sup> FRCP 26(b)(2)(B).

<sup>36</sup> FRCP Rule 16(b).

<sup>37</sup> FRCP Rule 26(a)(1).

<sup>38</sup> *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005).

<sup>39</sup> *Todd v. Guidance Software, Inc.*, No. 8:08-CV-01354, (C.D. Cal. filed Dec. 16, 2008)

<sup>40</sup> *Serra Chevrolet, Inc. v. General Motors Corp.*, 446 F.3d 1137 (11th Cir. 2006).

<sup>41</sup> *Arista Records, LLC v. Usenet.com, Inc.*, 2009 WL 1873589 (S.D.N.Y. June 30, 2009).

<sup>42</sup> See "AccessData in Court," *The Rules of Digital Evidence and AccessData Technology, AccessData Corp.* 2009. Available at <http://www.accessdata.com/>

<sup>43</sup> *In re Atlantic Intern'l Mortg. Co.*, 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).

<sup>44</sup> *Id.*

<sup>45</sup> *Rivera-Cruz v. Latimer, Miaggi, Rachid & Godreau, LLP*, 2008 WL 2446331 (D. Puerto Rico 2008).

<sup>46</sup> *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y.2003) ("*Zubulake IV*").

<sup>47</sup> "The duty to preserve evidence 'arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" *Acorn v. City of Nassau*, 2009 WL 605859 at 2 (E.D.N.Y. March 9, 2009) citing *Zubulake v. UBS Warburg LLC* ("*Zubulake IV*"), 220 F.R.D. 212, 216 (S.D.N.Y.2003) (which quoted *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001)). "Once the duty to preserve arises, a litigant is expected, at the very least, to 'suspend its routine document and retention/destruction policy and to put in place a litigation hold.'" *Id.*, citing *Zubulake IV*, 220 F.R.D. at 218; and also *Doe v. Norwalk Cmty. Coll.*, 2007 U.S. Dist LEXIS 51084, at \*14 (D. Conn. July 16, 2007) (a party needs to take affirmative acts to prevent its system from routinely destroying information).

<sup>48</sup> See, e.g., *Kipperman v. Onex Corp.*, 2009 WL 1473708 (N.D. Ga. May 27, 2009) (\$1,022,700 in monetary sanctions levied against the defendant for "a textbook case of discovery abuse.")

<sup>49</sup> FRCP Rule 37(b)(2)(iii): "striking pleadings in whole or in part". See, e.g., *Channel Components, Inc. v. Am. II Electronics, Inc.*, 915 So. 2d 1278 (Fla. Dist. Ct. App. 2005) (striking of pleading considered, but not imposed by the Court).

<sup>50</sup> FRCP Rule 37(b)(2)(vi): "rendering a default judgment against the disobedient party". See, e.g., *Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y. Oct 15, 2008) (Magistrate Judge recommended default judgment in favor of plaintiff, plus attorneys fees); *Atlantic Recording Corp. v. Howell*, 2008 WL 4080008 (D. Ariz. Aug. 29, 2008) (default judgment warranted after "brazen destruction of evidence").

<sup>51</sup> FRCP Rule 37(b)(2)(v): "dismissing the action or proceeding in whole or in part". See, e.g., *Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. Feb. 13, 2009) (all of plaintiff's claims were dismissed, and an adverse inference instruction awarded to defendant's cross-claims after plaintiff intentionally discarded her laptop in spite of a duty to preserve it).

<sup>52</sup> See, e.g., *Smith v. Slifer Smith & Frampton/Vail Assocs. Real Estate, LLC*, 2009 WL 482603 (D. Colo. Feb. 25, 2009) (Despite lack of evidence of a "smoking gun," the Court awarded an adverse inference against the defendant because documents were destroyed well after the litigation hold notice was put in place.)

<sup>53</sup> The safe harbor provisions are identified in FRCP Rule 37(e). See, e.g., *Gipetti v. UPS, Inc.*, 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) (Plaintiff's motion for sanctions were denied in view of a safe harbor provision because the documents that were destroyed were done so in accordance with the company's document retention policy and there was no apparent relevancy of those documents to the case given the Plaintiff's cause of action).

<sup>54</sup> See, e.g., "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July 2002 at p. 53, available at <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf>. Judge Scheindlin in *Zubulake V* arguably endorsed elements of the copy/sequestration method when she set forth three factors that counsel should take in conjunction with the litigation hold, one of which was: "Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place." *Zubulake v. UBS Warburg*, 229 F.R.D. at 422, 434 (S.D.N.Y. July 20, 2004) (emphasis added).

---

<sup>55</sup> The integrity of the copy can be verified by comparison to "hash values" using a cryptographic function, such as the Message-Digest algorithm "MD5". See, e.g., *Xpel Techs. Corp. v. Am. Filter Film Distributions*, 2008 WL 744837 (W.D. Tex. Mar. 17, 2008) ("all images and copies of images shall be authenticated by generating an MD5 hash value verification for comparison to the original hard drive."); *Bro-Tech Corp. v. Thermax, Inc.*, 2008 WL 724627 (E.D. Pa. Mar. 17, 2008); *Creative Sci. Sys., Inc. v. Forex Capital Mkts., LLC*, 2006 WL 870973 (N.D. Cal. Apr. 4, 2006) (Unpublished).

<sup>56</sup> The best evidence rule is also "referred to as the 'Original Writing Rule' because it does not mandate introduction of the 'best' evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an 'original,' 'duplicate' or, in certain instances, by 'secondary evidence'—any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available." *Lorraine v. supra*, note 2 citing FED. R. EVID. 1001 advisory committee's note. Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the 'original writing rule.'" *Id.*

<sup>57</sup> See, e.g., Craig Ball, "Don't Mess With System Metadata" Law Technology News, April 23, 2009, available at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202430116124>.

<sup>58</sup> See, e.g., *Krumwiede v. Brighton Assocs., L.L.C.*, 2006 WL 1308629 (N.D. Ill. May 8, 2006) (a plaintiff who destroyed metadata in the process of copying files was subject to a default judgment on the first four claims and ordered to pay costs—including expert fees and attorney fees— associated with the sanctions motion).

<sup>59</sup> *In re Hawaiian Airlines*, 2007 WL 3172642 (Bkrcty. D. Hawaii, Oct. 30, 2007) (company sanctioned when its Chief Financial Officer wiped files from his laptop computers after he was informed of a litigation hold notice).

<sup>60</sup> All operating systems utilize mass storage devices (such as hard disks or flash drives) that are formatted with a file system. File systems typically have a system of allocating privileges for reading, modifying or otherwise utilizing files contained within the file system. For example, normal users are typically not allowed to modify files associated with the core software applications required for standard operation of the machine.

<sup>61</sup> Typical operating systems include the various flavors of Microsoft Windows, Apple's OS X, and Linux.

<sup>62</sup> One such tool is Ophcrack (<http://ophcrack.sourceforge.net/>), which is a Linux LiveCD that can be used to find the passwords associated with the Windows machine, including the administrator's password. Ophcrack is free and works on any flavor of Windows, including Vista. Another popular tool is "ntpasswd" which is freely available at: <http://home.eunet.no/pnordahl/ntpasswd/>. Ntpasswd can reset the administrator's password to whatever the employee desires. Note, the tools mentioned previously are commonly used by system administrators to fix problems encountered during the normal operation of PC's. In other words, these tools are not aberrant or illegal hacker software, but instead have legitimate uses.

<sup>63</sup> *Kvitka, supra*, n. 51, is a case where the plaintiff destroyed her laptop after being apprised that she was under an obligation to preserve it, and did not reveal the loss of the laptop to the Court when a judge asked her about the state of some of the contents of the laptop.

<sup>64</sup> "The Sedona Conference on Legal Holds: The Trigger & The Process" (August 2007 Public Comment Version) by the Sedona Working Group at 12, citing *Zubulake V*. The paper is available at [http://www.thesedonaconference.org/dltForm?did=Legal\\_holds.pdf](http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf)

<sup>65</sup> "Mesa could have taken reasonable steps that would have prevented, or mitigated the consequences of, Mr. Murnane's destruction of evidence. For example, Mesa could have made a backup of Mr. Murnane's H drive and the hard drives of Laptop 1 and Laptop 2 promptly after HA filed suit. Doing so would not have been costly, burdensome, or unduly disruptive of Mesa's business. Instead, Mesa simply told Mr. Murnane to preserve all evidence and trusted him to comply. Even though Mr. Murnane was a valued, trusted, high level employee of the company, Mesa could and should have taken reasonable steps to prevent all of its employees from doing wrongful and foolish things, like destroying evidence, under the pressure of litigation. Because Mesa failed to take such steps, Mesa facilitated Mr. Murnane's misconduct." *In re Hawaiian Airlines, Inc., Debtor; Hawaiian Airlines, Inc. v. Mesa Air Group, Inc.*, 2007 WL 3172642 at \*6 (Bkrcty. D. Hawaii, Oct. 30, 2007).

<sup>66</sup> The Sedona Conference, "Commentary on Achieving Quality in the E-Discovery Process" (May 2009 Public Comment Version) available at: [http://www.thesedonaconference.org/content/miscFiles/publications\\_html?grp=wgs110](http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110)

<sup>67</sup> See, e.g., *Wingnut Films v. Katja Motino Pictures Corp.*, 2007 WL 2758571, at \*5 (C.D. Cal. Sept. 18, 2007) (a producing party must make a "reasonably diligent search for e-mails and other electronic documents").

<sup>68</sup> "(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs,

---

sound recordings, images, and other data or data compilations stored in any medium – from which information can be obtained, translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b)." FRCP 34(a).

<sup>69</sup> See, e.g., *White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc.*, 2009 WL 722056 (D. Kan. Mar. 18, 2009) (although intrusive, "request for inspection for forensic or mirror imaging of computers [are] neither routine nor extraordinary.") citing *G.D. v. Monarch Plastic Surgery, P.A.*, 239 F.R.D. 641 (D.Kan. 2007); *Balboa Threadworks, Inc. v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668 (D.Kan. Mar. 24, 2006); *Jacobson v. Starbucks Coffee Co.*, No. 05-1338-JTM, 2006 WL 3146349 (D.Kan. Oct. 31, 2006).

<sup>70</sup> See, e.g., *Kipperman*, *supra* note 48 (court imposed \$1,022,700 sanction for discovery abuse); *Oz Optics, Ltd. v. Hakimoglu*, 2009 WL 1017042 (Cal. App. Apr. 15, 2009) (appellate court upholds \$90,000 sanction); *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.*, 2009 WL 546429 (M.D. Fla. Mar. 4, 2009) (court imposed sanctions on plaintiff and counsel).

<sup>71</sup> Hard disks do fail, more often after a few years of non-use, which is well within the time period of lawsuits. Many vendors who store data know this, and offer to "spin up" the hard disk periodically to ensure operation over extended periods of time.

<sup>72</sup> *Aguilar v. Immigration and Customs Enforcement Div. of U.S. Dept. of Homeland Sec.*, 2008 WL 5062700 (S.D.N.Y. Nov. 21, 2008).

<sup>73</sup> *Williams*, *supra*, note 38, 230 F.R.D. at 654.

<sup>74</sup> *Id.*

<sup>75</sup> *Aguilar*, *supra*, note 72.

<sup>76</sup> *Todd v. Guidance Software, Inc.*, *supra*, note 39.

<sup>77</sup> *Id.*

<sup>78</sup> *Id.*

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *State ex rel. Toledo Blade Co. v. Seneca County Bd. of Comm'rs*, 899 N.E.2d 961, 2008 WL 5157133, (Ohio 2008).

<sup>82</sup> *Smith v. Slifer Smith & Frampton/Vail Associates Real Estate LLC and W. Seibert*, 2009 WL 482603 (D. Colo. Feb. 25, 2009).

<sup>83</sup> *Smith & Estate of Smith v. Slifer & Frampton/Vail Associates Real Estate, LLC and Peter W. Seibert*, 2008 WL 4523269 (D. Colo. July 7, 2008).

<sup>84</sup> *Id.*

<sup>85</sup> *Hawaiian Airlines*, *supra*, note 59.

<sup>86</sup> *Id.*

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

<sup>90</sup> *United States v. Mann*, 2008 WL 1701743 (N.D. Ind., April 8, 2008)

<sup>91</sup> *Id.* at \*2.

<sup>92</sup> *Id.* at \*3.

<sup>93</sup> *Id.* at \*1.

<sup>94</sup> *Id.* at \*5.

<sup>95</sup> *Id.*

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.* citing *United States v. Raney*, 342 F.3d 551, 558-59 (7<sup>th</sup> Cir. 2003); *United States v. Bruce*, 109 F.3d 323, 328-29 (7<sup>th</sup> Cir. 1997).

<sup>99</sup> See, e.g., *United States v. Wong*, 334 F.3d 831 (9<sup>th</sup> Cir. 2002); *United States v. Gray*, 484 F.2d 352 (6<sup>th</sup> Cir. 1973).

<sup>100</sup> *United States v. Graziano*, 558 F.Supp.2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y. Mar 20, 2008). *But see, United States v. Hamilton*, 579 F.Supp.2d 637, 77 Fed. R. Evid. Serv. 874 (D.N.J. Sep 28, 2008).

- 
- <sup>101</sup> *Dalia v. United States*, 441 U.S. 238, 257, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979).
- <sup>102</sup> *Id.*
- <sup>103</sup> *Dalia*, 441 U.S. at 257, 99 S.Ct. at 1682.
- <sup>104</sup> *Id.*
- <sup>105</sup> *United States v. Edwards*, 415 U.S. 800 (1974).
- <sup>106</sup> *Id.*
- <sup>107</sup> *Id.*
- <sup>108</sup> *Id.*
- <sup>109</sup> *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007).
- <sup>110</sup> *Id.*
- <sup>111</sup> In their opinion, the *Diaz* Court addressed both *Finley* and *Edwards* as well as *United States v. Chadwick*, 433 U.S. 1 (1977).
- <sup>112</sup> Bick, Jonathan, *Calculating Hidden VoIP Costs*, N.J. L.J. (Nov. 07, 2007), a copy of which is available at: <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=900005495393>
- <sup>113</sup> *Southwestern Bell Tel., L.P. v. Mo. PSC*, 461 F.Supp. 2d 1055, 2006 U.S. Dist. LEXIS 65536 (E.D. No., 2006), *affm'd*. *Southwestern Bell Tel., L.P. v. Mo. PSC*, 530 F.3d 676; 2008 U.S. App. LEXIS 13062; 45 Comm. Reg. (P & F) 540 (8th Cir. 2008).
- <sup>114</sup> *Vonage Holdings Corp. v. Minn. PUC*, 290 F.Supp. 2d 993 (D. Minn. 2003).
- <sup>115</sup> *Calculating*, *supra*, note 112.
- <sup>116</sup> *Katz v. United States*, 389 U.S. 347 (1967).
- <sup>117</sup> *Calculating*, *supra*, note 112.
- <sup>118</sup> *In re Schools and Libraries Service Support Mechanisms*, 18 F.C.C.R. 9202, P29 n. 49 (2003).
- <sup>119</sup> Galkin, William S., *The Computer Law Report*, Dec. 28, 1995.
- <sup>120</sup> *Electronic Communications Privacy Act of 1986*, 18 U.S.C. §2510 et. seq.
- <sup>121</sup> *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. June 19, 2007), motion for rehearing den'd, 2007 U.S. Dist. LEXIS 63620 (C.D. Cal. Aug. 24, 2007).