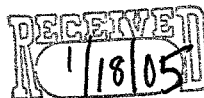


TURNING DIGITAL EVIDENCE INTO INTELLIGENCE.

46 PUBLIC SQUARE | SUITE 220 | MEDINA, OHIO 44256 | 330.721.1205

**VESTIGE****04-CV-093.***Request to Testify  
2/11 DC*

January 13, 2005

- ▶ BY TELECOPY: 202-502-1766  
Peter G. McCabe, Secretary  
Administrative Office of the U.S. Courts  
One Columbus Circle, NE  
Washington, DC 20544

Re: Testimony at Hearing Before Judicial Conference Advisory Committee on Civil Rules, February 11, 2005

Dear Mr. McCabe:

I am the Chief Legal Officer of Vestige, Ltd., a company providing attorneys across the United States with computer forensic services to assist them to identify, extract, preserve, and present relevant data, visible and invisible to computer operating systems, that is resident upon electronic media.

The president of Vestige, Ltd, Damon Hacker and I would like to attend the February 11, 2005 hearing of the Judicial Conference Advisory Committee on Civil Rules and testify regarding the proposed federal rule amendments on e-discovery.

I could not find on your website any list of requirements in order to be able to testify; and therefore if the Committee needs any more information, please just ask and it will be promptly provided.

Finally, I apologize that we were unable to provide thirty days notice of our request, but I have just recently returned to the office.

Thank you very much for your attention to this matter,

Sincerely,

Donald Wochna



. VESTIGE

RECEIVED  
2/2/05

February 1, 2005

04-CV-093

Testimony  
2/11 DC

Peter G. McCabe  
 Secretary  
 Committee on Rules of Practice and Procedure  
 Judicial Conference of the United States  
 Thurgood Marshall Federal Judicial Building  
 Washington, DC 20544

Re: Proposed Amendments to the Federal Rules of Civil Procedure: Electronic  
 Discovery and Computer Forensic Analysis.

Dear Mr. McCabe:

The Committee on Rules and Practice and Procedure (the "Committee") has an opportunity to bring rationality to the fact finding process and discovery in civil litigation by creating rules that permit technological advances to reduce the cost and increase the ease of accessing all electronically stored information. Vestige Ltd is honored to share our unique perspective on this issue and offer our critique of the Committee Notes to Rule (26)(b)(2). Our perspective is unique because Vestige Ltd is comprised of forensically trained attorneys with significant trial experience teamed with computer forensic specialists to assist attorneys to use computer forensic analysis as a primary discovery tool. As attorneys, we have litigated cases pursuant to the federal and states rules of civil procedure. As computer forensic specialists, we have helped attorneys request and produce relevant data in small and large cases. We are a unique "bridge" between the needs and issues of attorneys and the capabilities and limitations of technology.<sup>1</sup>

#### A. Fundamental Computer Data Concepts

A critical analysis of the Committee's Note to Rule (26)(b)(2) ought to begin with the recognition of a fundamental computer fact: all data that resides upon electronic media (computer hard drives, zip disks, pda, etc) is either visible to the operating system and installed programs or invisible. Visible and invisible data reside together on electronic media, physically located within centimeters of one another. Visible data physically resides in areas on the media named "allocated"; while invisible data resides in areas on the same media named "unallocated".

All data embedded on electronic media is comprised of magnetized metallic particles whose polarity can be read and interpreted by operating systems and software programs. Not all the magnetized metallic particles, however, are visible to the computers' operating system or to the software programs installed thereon. Deleted data, for example, is merely that collection of magnetized particles which are ignored by the operating system because they have been "marked" as deleted. Similarly, uninstalling software programs renders related magnetic particles (i.e. data) invisible to the operating system. It is vital to

understand that the magnetic particles that comprise the “invisible” data are physically on the same media, on the same computers and devices, as the magnetic particles that comprise the “visible” data. As a physical matter, the invisible data is just as accessible as the visible data. It resides upon the same media (client personal computer, network server, pda, etc). **Thus, when a responding party identifies the computers and electronic devices on which resides electronic, visible data, responsive to a discovery request, that party is necessarily identifying computers and devices containing “invisible” data, responsive to a discovery request.**

Data that is visible to the operating system can be rendered invisible, and data that is invisible can be rendered visible. For example, active, visible, data can become “invisible” because the software that created the data has been uninstalled. Without the software, the operating system does not recognize the data format, and the data cannot be rendered intelligible. Of course, the data could become visible by merely re-installing the software program that created the data. Similarly, visible data can be rendered “invisible” by altering the file extension of saved data. This is a favorite ploy of persons trying to use a computer to hide data. After a file’s extension is changed, the operating system cannot identify the type of file in which the data has been saved, and cannot render the data intelligible. If the file extension is set to its proper form, the data becomes visible again.

Most computer users know that deleting data renders it invisible to the operating system, but does not remove the data from the media. Many times users need to “restore” deleted data. Fortunately, technology offers computer users several software programs designed to render visible again data that has been made invisible by deletion. Some of these software programs are available at very low cost, while others are very powerful programs that do far more than merely render deleted data visible. **Computer forensic programs, for example, allow forensic analysts, in one process, to search, extract, parse, and protect visible and invisible data resident on multiple computers or devices.** Using these forensic programs, companies such as Vestige Ltd. assist responding parties to access all data (visible and invisible) on all relevant devices (computers, pda, servers), and to simultaneously extract from all these devices, all relevant data using protocols that protect privilege and confidentiality.

During the last five years, computer forensic software and protocols have created a revolution in the fact-finding function by attorneys and professionals. Using the same software heretofore used exclusively by law enforcement agencies<sup>ii</sup>, forensic analysts now quickly and easily render visible all the data on media, regardless of its location in “unallocated” or “allocated” areas. Using forensic analysis, a party is no longer limited to viewing only the data in allocated areas of the media, rendered visible by the operating system. Now all data on the media—residing in allocated and unallocated areas—can be viewed, searched, extracted, and produced.

This revolution has had enormous consequences to business. Data that used to be invisible can now be recovered as if it had always been visible. Even more significant is

the ability to simultaneously view, search, and extract visible and invisible data on multiple computers and different electronic media.

#### B. Analysis of the Committee Note 26(b)(2)

The Committee's Note focuses upon technical and business characteristics of data to determine whether data that has been requested is "reasonably accessible". Based upon the Committee's Note, data's technical characteristics include the volume of data, the variety of locations in which data might be found, and the difficulty of locating, retrieving, and producing the data. The Committee also refers to the manner in which data is used as a "business" referent to determine accessibility.

##### 1. Volume of Data.

The Committee Note appears to assume that data can become "inaccessible" at some critical volume. "Many parties have significant quantities of electronically stored information that can be located, retrieved, or reviewed only with very substantial effort or expense", "In many instances, the volume of potentially responsive information that is reasonably accessible will be very large, and the effort and extra expense needed to obtain additional information may be substantial", "The Manual for Complex Litigation (4<sup>th</sup>) Section 11.446 illustrates the problems of volume that can arise with electronically stored information:...", "with volumes of these dimensions, it is sensible to limit discovery to that which is within Rule (26)(b)(1) and reasonably accessible...".

From a computer forensic point of view, volume is not a factor limiting the identification and extraction of relevant, responsive information from large amounts of electronically stored information. Forensic analysis does not rely upon human beings to review the visible and invisible data resident on media hoping to identify relevant information. Such a review would not be consistent (even if time were spent creating protocols for use by human searchers), and would take an inordinate amount of time and be very costly. Instead of relying upon human beings to conduct searches of electronically stored data, forensic analysts use software programs to simultaneously search all data resident on all relevant media. For example, in a customary and usual case, Vestige Ltd. simultaneously searches several terabytes of data comprised of data resident on tens or hundreds of separate computers or devices. Very large amounts of data can be successfully searched in seven to ten days, continuously running search software with minimal human involvement. Volume of data is not an issue because the tremendous computing power that was harnessed to create the electronic information is harnessed by forensic analysts to locate, parse, extract, and preserve that portion of the information relevant to a particular matter. From a forensic perspective, therefore, mere volume does not render data inaccessible.

## 2. Locations of Data

The Committee Note recognizes “variety of locations” as a feature of electronically stored information, but does not explain the manner in which locations render data inaccessible.

It may be that the Committee is recognizing the distribution of data within a corporate enterprise. Such a distribution scheme is generally a “client-server” distribution, in which individuals in the organization uses individual devices (computers, pda, laptops, etc) to create and process information and to communicate with other computers, called servers. Servers generally can be considered computers on which are stored specialized information (emails, webpages) or on which are processed specialized activities. The Committee may be inferring that, at some level of distribution, data becomes inaccessible.

From a forensic perspective, distributed data is a valuable characteristic of corporate enterprises that renders data **more accessible** than the concentration of data found in servers and back-up tapes. At the individual level of a corporate enterprise (the client side), individual computers and devices are used to create a tremendous amount of data. Some of this data is visible to the individual user’s computer and device (such as saved memos, emails, financial spreadsheets), and some of the data is rendered invisible (such as deleted data, data saved with the wrong file extension, data created by the operating system). When data back-ups are made to a server, or when individuals communicate with servers and save selected data, a subset of all the data on the user’s computer or device is created on the server. This subset, however, does not include any of the “invisible” data resident on the individual’s computer, nor any visible data that the user chose not to send to the server (or that was not automatically backed-up). This data can remain resident on the individual’s computer or device until it is overwritten, which can take a very long time. The data remains resident on the device even if the media is re-formatted, or the logical volumes re-partitioned.

In order to properly conduct a forensic examination of all the devices that might contain data relevant to a matter or responsive to a discovery request, forensic companies such as Vestige Ltd create an exact clone of each of the relevant computers or devices. For example, if there are potentially 200 devices on which might be resident data relevant to a dispute, then Vestige will create 200 clones. Clones can be made of all types of devices, including computer hard drives, cell phones, pda, etc. Data on back-up tapes is typically restored to one or more computer hard drive, then a clone of these back-up hard drives is created. Creating clones of all relevant machines “freezes” all data as of the date of the clone, and gives the responding party the ability to continue to use all the relevant devices in the ordinary course of business, while searching the clones simultaneously for relevant data.

If relevant computers and devices are distributed throughout an enterprise, clones can be made locally, at night, or over a weekend, with no disruption to business. Clones can be made by local personnel using special software provided to them by forensic companies, or they can be created by forensic analysts. Several clones can be made simultaneously,

and, where time is of the essence, Computer Analysis Teams can be formed to finish the process for all clones with very little disruption. For example, Vestige has used a 6 person Computer Analysis Team to acquire 20-40 clones in less than 10 hours. If additional computers or devices are later determined to also be relevant, they can be cloned and added to the case without any disruption. On average, as the number of clones increases, the cost per clone decreases<sup>iii</sup>.

From a computer forensic perspective, the ability to inexpensively create clones of all distributed data (visible and invisible) resident on all devices (hard drives, pda, cell phones) allows the forensic examination to proceed prior to attempts to interrogate "legacy" systems or tape back-up tape systems. Location of data, therefore, does not automatically render data inaccessible.

### 3. Technical Difficulty

The Committee Note infers that the difficulty associated with the retrieval of electronically stored information may render that information inaccessible. "Time-consuming and costly restoration of the data may be required and it may not be organized in a way that permits searching for information relevant to the action. Some information may be 'legacy' data retained in obsolete systems; such data...may be costly and burdensome to restore and retrieve."

The Committee Note also derogatorily characterizes present and future technologies designed to access visible and invisible electronically stored information. "Other information may have been deleted in a way that makes it inaccessible without resort to expensive and uncertain forensic techniques, even though technology may provide the capability to retrieve and produce it through extraordinary efforts. Ordinarily such information would not be considered reasonably accessible", "Technological developments may change what is 'reasonably accessible' by removing obstacles to using some electronically stored information. But technological change can also impede access by, for example, changing the systems necessary to retrieve and produce the information", "The Manual for Complex Litigation (4<sup>th</sup>) Section 11.446 invokes Rule 26(b)(2), stating that ...'More expensive forms of production, such as production of word-processing files with all associated metadata...should be conditioned upon a showing of need or sharing expense".

The Committee Note is timely in recognizing that computer forensic analysis can access visible and invisible data on electronic media, but the Note is anachronistic when it characterizes forensic analysis as "expensive and uncertain" and as "extraordinary". This description might have been more accurate four or five years ago. Today, advances in computer forensic software and protocols have made computer forensics a primary tool for discovery because of the significant decrease in costs over traditional discovery. Vestige has found that traditional discovery constitutes about 25-33% of the total legal fees incurred in a matter. Using computer forensic analysis instead of traditional paper discovery reduces the cost of discovery by about 60% to an amount that is usually 8-12%

of the total legal fees incurred. This cost reduction is achieved because a computer forensic analysis allows the responding party to use powerful computer programs to search and extract all relevant data resident on any and all electronic media, in one process, without regard to whether that data is visible or invisible to the computer operating system. As a result of advances in computer forensic software and establishment of protocols to protect privilege and confidentiality, “invisible” data, heretofore “inaccessible”, is now no more difficult to access than “visible” data.<sup>iv</sup>

The Committee Note appears to reflect policy decisions that are hostile to the advances of technology. The result is comments in the Note that seem to insulate the producing party from a duty to produce electronically stored information, regardless of the capabilities of technology. The Committee ought to place the duty to respond to electronic discovery on the party who is best situated to adopt and integrate into their business processes, those technological solutions that render moot the technical difficulty of accessing relevant visible and invisible data. This approach would require the producing party review and produce all visible and invisible data resident on relevant electronic media unless the party could demonstrate that the data is technologically inaccessible. Technologically inaccessible data might include data that had been overwritten several times, the retrieval of which, using today’s technology, is theoretically possible but may require expensive electron microscopy analysis<sup>v</sup>. At the very least, the Committee ought to strike all characterizations of the cost and limitations of current technology, as these characterizations, even if accurate, will surely be quickly rendered obsolete.

#### 1. Business Use—deleted data and other information not used in ordinary course

The Committee Note suggests that data that is no longer used by a party is not reasonably accessible. “For example, some information may be stored solely for disaster-recovery purposes and be expensive and difficult to use for other purposes”, “Some information may be ‘legacy’ data retained in obsolete systems; such data is no longer used...”, “One referent would be whether the party itself routinely accesses or uses the information. If the party routinely uses the information—sometimes called ‘active data’—the information would ordinarily be considered reasonably accessible. The fact that the party does not routinely access the information does not necessarily mean that the access requires substantial effort or cost” “but if the responding party has actually accessed the requested information, it may not rely upon this rule as an excuse from providing discovery, even if it incurred substantial expense in accessing the information”.

The Committee ought to be concerned that, in a very significant number of cases, evidentiary data has been deleted in an attempt to prevent detection. Fraudulent financial transactions, theft of corporate intellectual property, sexual harassment, and a myriad other types of cases frequently rest solely upon invisible data, including deleted data, that has been extracted from several computers or devices. The fact that this invisible data is not used in the ordinary course of business ought not to be given any consideration when determining whether this data is reasonably accessible. Perpetrators of civil torts ought

not to be able to shield evidence of their wrongdoing from discovery on the ground that the evidence has been deleted and is not used in the ordinary course of business.

Other forms of data that are not accessed by a user in the ordinary course of business include data that is stored on a computer and accessed by other programs. For example, Internet History is stored on a computer, but is not readily producible by querying the computer. It is, nevertheless, used by the computer, albeit through the Internet browser, or some other programs. The Committee ought to be concerned that data resident on electronic media, accessed by programs, but not accessed and displayed directly, will be automatically characterized as "inaccessible".

### C. Conclusion

Recognizing that electronically stored information is an integral part of the normal discovery process is a solid base upon which the Committee's proposed rule changes must be analyzed. In the last five years, computer forensic analysis has progressed to the point that no data ought to be automatically characterizes as technologically inaccessible. Data resident on client-side devices, such as computers, pda, cell phones, and data resident on server-side devices such as servers and file storage devices can be accessed and queried using powerful forensic software and analytic protocols. As a result of the distributed nature of data in the corporate enterprise, the analysis of data on these accessible devices may render moot the need to access and interrogate legacy or back-up devices. The technological ease with which data can be accessed ought to be the primary, if not sole, determinant in establishing a duty to respond in discovery. That duty ought to rest with the responding party so as to encourage that party to adopt and integrate any and all technological solutions that render moot the cost and burden of producing relevant electronic information.

Vestige thanks you for allow us an opportunity to share our comments.

Sincerely,



Damon Hacker  
President



Donald Wochna  
Chief Legal Officer





## ENDNOTES

<sup>1</sup> We have appended to these comments two articles that Donald Wochna has written regarding the Non-adversarial nature of computer forensic analysis (Exhibit A), and the ineffectual use of Requests for Production of Documents (Exhibit B). We have also included our CV (Exhibits C and D).

<sup>1</sup> Vestige Ltd., for example, is licensed to use Encase software, a computer forensic tool currently used by over 14,000 law enforcement agencies around the world.

<sup>1</sup> See Exhibit E for hypothetical case, involving 200 computers and servers, and breakdown of estimated time and costs.

<sup>1</sup> If there is any doubt in the minds of any member of the Committee of the ease with which visible and invisible data, resident on several different electronic media, can be simultaneously searched for relevant data, Vestige Ltd would gladly demonstrate this capability.

<sup>1</sup> However, if there is a sufficient need to be able to recover overwritten data, the firms such as Vestige Ltd will develop the technology and deliver the capability to read overwritten data

<sup>1</sup> Cost estimates do not include cost of media nor costs related to archiving forensic images

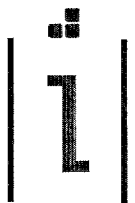


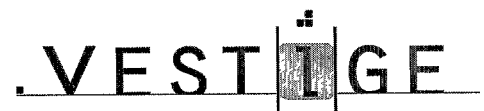
EXHIBIT A

**COMPUTER FORENSICS:  
CASE LAW AND TECHNOLOGY  
RELATED TO GATHERING FACTS  
FROM ELECTRONIC MEDIA**

**By: Donald Wochna, Esq.  
Chief Legal Officer**

**Vestige Ltd.  
46 Public Square  
Suite 220  
Medina, OH 44256  
330-721-1205**





## ABOUT VESTIGE LTD.

Vestige Ltd. is organized into Computer Analysis Teams, comprised of forensically trained attorneys and computer specialists using licensed forensic software, to locate data on electronic media that has evidentiary value, and to extract, preserve, and present that data in a manner consistent with our client's legal theories and strategies. VESTIGE's Computer Analysis Teams work with attorneys to execute search and production protocols that protect privilege and confidentiality, while extracting, parsing, and collating relevant evidentiary data. VESTIGE is a member of various law enforcement and computer forensic societies including the Northern Ohio Information & Technology Roundtable, Metropolitan Crime Clinic; National Institute of Standards and Testing, subgroup for Computer Forensic Tool Testing; and the Electronic Crime Investigation Group.



“The rules (of Civil Procedure) talk about the production of relevant information, so we seem to create the burden to seek e-data...**I can’t imagine how counsel who is responsible cannot seek relevant electronic information**”

Judge Loretta Preska  
U.S. District Court, S.D.N.Y.

“How a Judge Expects You To Handle Electronic Records in Discovery”  
July, 2003

Metropolitan Opera Association, Inc. v. Local 100, 212 F.R.D.178 (S.D.N.Y., 2003)

**Lawyers who forsake electronic discovery on behalf of a client  
due to costs, come close to professional negligence.**

Magistrate Judge John M. Facciola  
U.S. District Court, D.Col.

author of McPeck vs. Ashcroft, 212 F.R.D.33 (D.D.C., January 9, 2003)



## OVERVIEW OF FACT GATHERING BY ATTORNEYS IN A COMPUTERIZED SOCIETY

The traditional practice of law has always included the need to gather facts. Clients frequently look to their attorneys to structure, and in many cases execute, a strategy to find facts that support the client's position or allow the client to accomplish a specific goal in a variety of matters. These matters may include litigation, compliance, incident response strategies, and the creation and implementation of policies and procedures.

In order to develop fact-finding capabilities, attorneys have developed various relationships, skills and tools. Relationships may include private investigators, experts in various fields of endeavor, and in-house research capabilities. Skills may include interviewing, cross examination, and presentation. Tools include the traditional request for production of documents, deposition, trials, and internal security, computer, financial, and compliance audits.

These relationships, skills and tools served attorneys well in a pre-computer era, in which data relevant to a particular matter was found in paper copies of memos, letters, faxes, etc. In today's computer era, however, data relevant to a matter is resident on a myriad of electronic devices, comprising different forms of electronic media, processed by differing computer operating systems. Data relevant and crucial to a client's matter may now be found locked in various forms of technology such as PDA's, cell phones, laptop computers, workstation computers, servers, networks, automotive computer devices, telephones, etc. Each of these devices, in turn may have operating characteristics that uniquely affect the creation, storage, extraction, and processing of data.

In a computerized society, while attorney relationships and skills continue to be useful to attorneys, the tools traditionally used by attorneys to gather facts are hopelessly ineffective. These tools do not recognize the different devices, operating systems, or media on which is resident data crucial to a client's needs. Traditional tools do not have the capability to identify, extract, preserve, and integrate this data.

Fortunately, computerized data can be identified, extracted, preserved, and integrated into a matter using computer forensic analysis. Computer forensics is an area of specialization that uses specialized hardware and software to access data resident on electronic media used by various devices. The computer revolution has produced a concomitant revolution in fact gathering—whether for litigation, compliance, investigation, prevention, etc. Federal and state case law has recognized this revolution, and had mandated that whenever attorneys launch a strategy to gather facts relevant to a matter, they must include not only the data that is visible to a computer operating system, but also all data that has been deleted, orphaned, hidden, or otherwise rendered invisible to the computers used to create, copy, store, or process the data.



## COMPUTER FORENSICS IS CAUSING A PARADIGM SHIFT IN DISCOVERY TOWARD “NON-ADVERSARIAL DISCOVERY<sup>SM</sup>,”

- ✦ This paper analyzes relevant case law and identifies a significant shift in the focus and manner in which facts are being discovered in litigation. Basically, the traditional use by an attorney of the rules of discovery to obtain relevant “documents” is being replaced with a process and protocol using computer forensic analysis to first create “clones” of the media on which resides “relevant data” and then search those clones electronically for all relevant information. In effect, a request for production of documents is being replaced by a request for production of things: to wit, the media on which is resident data relevant to the matter.

This shift is both a reaction to the pervasive use of computers to create, store, process, and archive information in an ever-increasing number of formats, and a response to the discoverable data left behind by the unique features of computer operating systems. By first obtaining access to all media containing relevant data, and then extracting from the media all relevant data in whatever format it may exist, attorneys are able to discover both the data that is visible to the operating system (traditional documents, etc.) as well as data that is invisible and had traditionally been ignored and left behind. Because the process and protocol recognized by federal and state courts is value neutral, attorneys are offered the possibility of conducting discovery of facts in a non-adversarial forum.

“Non-Adversarial Discovery<sup>SM</sup>” is the name Vestige has given its enhancement of the process and protocol recognized by federal and state courts to acquire all relevant data and evidence in any case or matter. Non-Adversarial discovery<sup>SM</sup> is based on computer forensic analysis: the use of specialized software and procedures to identify, extract, and present all data relevant to a case, including data that has been hidden, deleted, or otherwise rendered invisible. Using Non-Adversarial discovery<sup>SM</sup> protocols, an attorney can obtain from his client and from other party litigants all relevant data in one process very early in litigation. Once all relevant data has been extracted and protected for privilege, the data can be prepared for use in court using any type of organizational technique, including electronic discovery organization software such as Summation or Case Map.

### TRADITIONAL DISCOVERY AND FEATURES OF COMPUTER SYSTEMS

Traditionally, litigators obtained relevant documents from their opponent by issuing a Request for Production of Documents. Although the Rules of Civil Procedure mandate the disclosure of relevant, non-privileged documents<sup>1</sup>, it is a rare case in which an opponent copies all relevant documents and provides them in response to the first Request. Usually, counsel must make several phone calls, write letters, monitor the partial responses provided, and constantly work to obtain as complete a production of documents as possible. Additionally, counsel had to ensure that its definition of “documents” was

<sup>1</sup> This assumes counsel has defined the term document properly.

broad enough to include all forms and formats in which relevant information may have been stored by a litigant. Constantly expanding the definition of “documents” to capture

all formats in which relevant data may be stored on computer systems used by clients and litigants is challenging in a society in which computer usage has exploded.

North American Businesses sent about 2.5 trillion email messages in 2001. The total number of electronic records produced in the world could, within the next ten years, double every sixty minutes. Sign of Times, Daily Journal Extra, October 28, 2002, Pamela Voich & Michele Lange. Email has become a treasure trove of “present-sense” impressions. In a case involving Phen-Fen drug, one email read: “Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem” Dispensing with the Truth, St. Martin’s Press, Inc. Alicia Mundy (April, 2001).

The following is a partial sample of the types of information typically found on a computer system:

- i. Correspondence
- ii. Drafts of documents
- iii. Changes to documents created and never saved
- iv. Documents created but not saved
- v. Instant messages received and sent
- vi. Emails
- vii. Attachments to emails or instant messages, including jokes, love letters, strategy discussions, observations
- viii. Folder names and file structure
- ix. Presentations
- x. Audio and video files
- xi. Pictures, including all pictures displayed from every website visited
- xii. Websites visited, including all files necessary to completely reconstruct each website in the order they were visited, and files related to the amount of time spent viewing each website
- xiii. Pictures from websites that may not have been visited but which were loaded onto computer as “pop-under” or “pop-up”
- xiv. Spreadsheets, draft spreadsheets
- xv. Accounting and tax information
- xvi. Faxes sent and received
- xvii. Images and text scanned
- xviii. Everything that has been downloaded from any computer or the internet
- xix. Contact lists, phone numbers
- xx. Credit card numbers
- xxi. Search information for all searches conducted. For example, Google searches
- xxii. Business records



- xxiii. System and program artifacts related to the manner in which a system was used, including artifacts related to copying, printing, programs installed (whether or not currently present on the system), programs frequently run, networked connections and access to other computers.

Even if attorneys could constantly refine the definitional parameters of “documents”, the operational characteristics of computers limits their usefulness in obtaining documents.

**Operational Characteristics of Computer Systems.** The fundamental feature of computers is speed. In order to achieve maximum speed, engineers have developed techniques to achieve functionality as quickly as possible. These techniques, however, have consequences that impact attorneys.

For example, computer engineers developed techniques to “delete” information as quickly as possible. None of these techniques, however, destroys the information. When a user presses the “delete” key, the computer operating system takes a number of steps only to ultimately render the file “invisible” to the operating system. Because the computer was built for speed, it takes no time whatsoever to overwrite, shred, or otherwise destroy the information. Thus, although the information cannot be “seen” by the computer, it is nevertheless present on the hard drive.

Data can become “orphaned” on a computer system. Generally data is saved on a computer in a data file that must be opened and read with particular software. If the software program that created the data file is uninstalled, deleted, or cannot be launched (such as when it has become corrupted) the data file cannot be read by the computer and is “orphaned”. Similarly, software developers sometimes update software to new versions that cannot read information created with prior versions. This feature seems especially prevalent in accounting software. For example, a financial spreadsheet created with version 1.0 of an accounting program may not be readable using an updated version of the program. Although the financial spreadsheet created with version 1.0 is resident on the computer system, it is “invisible” because the computer cannot interpret the data any longer. In effect, the data file is “orphaned” because the computer system no longer has a program available to use the file.

Data can become “hidden” on a computer system. For example, a document file (with a “.doc” extension) can be saved with a different extension (such as with a “.jpg” extension). The document will not be readable by the computer in this situation. Thus, although the data is still on the computer, the data cannot be opened.

In addition to invisible data left on computer systems, the computer’s operating system and the software programs leave a tremendous amount of information behind as they perform their functions. This information, referred to as artifacts, can be used to reconstruct the manner in which a computer was used. For example, a corporate officer may copy proprietary customer information to removable media prior to leaving a corporation to work for a competitor. Removable media may include “travel drives” shaped like wristwatches or pens that contain USB flash drives capable of storing over a



gigabyte of information. Once removed from the premises, the only evidence of this type of unlawful activity will be artifacts left behind by the operating system. These artifacts can be extracted and when properly analyzed will document the unlawful copying of data to the removable media.

These characteristics of computer operating systems and software programs have legal consequences for attorneys relating primarily to the preservation and acquisition of the “invisible” data and artifacts.

### **Scope of Visible and Invisible Information on Computers.**

All the information on a computer will be either visible or invisible to the operating system. Visible information can, of course, be intentionally rendered invisible, such as by deletion or the removal of the software program necessary to read the information. Of course, experienced attorneys find that information that intentionally has been rendered invisible (by the client or opponent) is frequently the most damaging information. Additionally, parties to litigation and their counsel have a duty to preserve evidentiary information and avoid spoliation.

In order to understand the procedures that may be needed to preserve and acquire visible and invisible information from computer systems, attorneys must understand the threats to the integrity of visible and invisible information posed by computer operating systems.

### **Ongoing Use of Computer System as Ground for Forensic Process Create Clone**

Visible and invisible data on a computer system may be destroyed by several threats including, electrical shock, viruses, physical damage to the hard drives, and systemic and intentional overwriting. Of all the threats, systemic overwriting of invisible data occurs merely from the ongoing use of the computer system on which resides relevant information.

Systemic overwriting by the operating system occurs as a result of the engineering techniques used to make computer perform rapidly. As explained above, a computer’s operating system creates thousands of artifacts and file data as it is being used. Additionally, the operating system renders invisible all data “deleted” by the computer user. All the artifacts, file data, and invisible information is written to physical locations on the computers’ hard drives. All this information remains physically written on the hard drives until such time as the operating system “overwrites” some of the data by writing new artifacts, file data, and/or invisible information at the same physical locations.

Courts are recognizing that the ongoing use of the computer operating system destroys invisible information, including data that may be relevant to the claims or defenses in a case. Antioch v. Scrapbook, 210 F.R.D. 645, 2002 U.S. Dist. LEXIS 20811 (D.Ct. Minn., April 29, 2002). Indeed, this is a significant threat that can be ameliorated only by either refraining from using the computers or by creating a forensic “snapshot” of the computers,



which includes all visible and invisible information locked into a secure, authenticated clone of the relevant hard drives.

In Antioch, the United States District Court for the District of Minnesota was faced with the issue whether, at the initial stages of litigation, to grant Plaintiff's Motion to Compel Discovery and Appoint a Neutral Expert in Computer Forensics. Plaintiff filed its motion prior to any conference required by Rule 26(f), Federal Rules of Civil Procedure, at a time

therefore when discovery was prohibited. Additionally, no Scheduling Order was in force by the Court, no Pre-Trial Conference had been scheduled, and one of the defendants had not yet filed its Answer. Antioch at page 650-651. In its motion Plaintiff argued that that "data from a computer which has been deleted remains on the hard drive, but is constantly being overwritten, irretrievably, by the Defendants' continued use of that equipment". Antioch at 651.

The Minnesota District Court granted Plaintiff's motion for expedited discovery and its motion to compel discovery on the ground "the Defendants may have relevant information on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff's claims or the Defendant's defenses. This information may be in the form of stored or deleted computer files, programs or emails, on the Defendants' computer equipment". Antioch at 652.

It is important to note that the District Court focused upon the features of the operating system as the ground upon which to compel the preservation of the data resident on the defendant's computers. The Court specifically noted that the plaintiff provided an affidavit of a computer forensic expert attesting that "data which is deleted from a computer is retained on the hard drive, but is constantly being overwritten by the new data, through the normal use of the computer equipment". Antioch at 651.

This case supports the technologically accurate legal argument that relevant data is being destroyed by the continued operation of the computer systems used to create, process, archive, or delete data. This technological argument ought to be sufficient to compel the forensic imaging of relevant computers as the only viable method of preventing the loss of relevant data.

Antioch implicitly raises the issue whether the discovering party must first prove that the producing party has engaged in deletion of information as a condition precedent to creating forensic images of relevant computers. It seems apparent that where the discovering party grounds its need to create a forensic image on the overwriting characteristics of the computer's operating system, or where the discovering party has focused upon the discovery of residual data left behind by the operating system, the producing party must create a forensic image. The producing party cannot comply with such a request using the normal operating system.



Whether a party has a duty to create forensic images of relevant computers to prevent spoliation of evidence has received some attention from an ad-hoc group of attorneys and large corporations. See discussion of Sedona Principles below.

- ✦ Finally, requiring counsel to prove deletion as a condition of obtaining an Order granting a Motion to Compel may not have much practical significance. It is hard to imagine a party successfully arguing that it has never used the delete function of its computers, or that it has never deleted any information relevant to the dispute at bar. In any event, counsel can conduct a Rule 30(B) deposition of the party to establish the existence and use of the delete function in the normal course of business. Where deletion is known to have occurred in the normal course of business, courts have uniformly held that the deleted data is discoverable.

### **DELETED DATA IS DISCOVERABLE. DELETION DOES NOT PLACE DATA OUTSIDE THE SCOPE OF DISCOVERY**

It is generally understood that deleting data does not remove it from the scope of discovery. See Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (“[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable”); Rowe Entm’t, Inc. v. The William Morris Agency, Inc., 205 F.R.D. 421, 427-431 (S.D.N.Y. 2002) (stating that “[e]lectronic documents are no less subject to disclosure than paper records,” and only questioning which party should bear the cost of such discovery, especially for backup tapes or deleted e-mails); McPeck v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) (stating that, “[d]uring discovery, the producing party has an obligation to search available electronic systems for information demanded,” and ordering a limited backup restoration of e-mails); Kleiner v. Burns, 48 Fed. R. Serv. 3d 644, 2000 WL 1909470 (D. Kan. Dec. 15, 2000) (noting that Rule 26(a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that “[t]he disclosing party shall take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any ‘deleted’ electronic data”); Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“First, computer records, including records that have been ‘deleted,’ are documents discoverable under Fed. R. Civ. P. 34.” Citing Crown Life Insurance Co. v. Craig, 995 F.2d 1376 (7<sup>th</sup> Cir. 1993; Illinois Tool Works, Inc. v. Metro Mark Products Ltd, 43 F.Supp.2d 951 (N.D. Ill. 1999)); Playboy Enter. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (“Plaintiff needs to access the hard drive of Defendant’s computer only because Defendant’s actions in deleting those e-mails made it currently impossible to produce the information as a ‘document.’”). Anti-Monopoly, Inc. v. Hasbro, Inc. WL 649934 (S.D.N.Y., Nov. 3, 1995); Seattle Audubon Society v. Lyons, 871 F. Supp. 1291 (W.D. Wash. 1994); Linnen v. A.H.Robins, Co. WL 462015 (Mass. Super., June 16, 1999). Deleting data on a hard drive does not remove the data from the scope of discovery. Dodge, Warren & Peters Ins. Servs. v. Riely WL 245586 (Cal. Ct. App. Feb. 5, 2003); Simon Property Group v. mySimon, Inc. 194 F.R.D. 639, 2000 U.S. Dist.LEXIS 8950 (S.D.Ind. 2000).

It seems well settled that discovery is not limited to only those files that are “visible” to the computer system; discovery includes files that cannot be seen by the operating system, including deleted files. In reaction to this case law, an ad-hoc group has suggested that discovery ought to be limited only to the “visible” files on a computer: i.e. those files and information purposefully stored on a computer system. Sedona Principle No. 8, “The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production”, March 2003, [www.thesedonaconference.org](http://www.thesedonaconference.org). This group has suggested that discovery ought to exclude disaster recovery backup tapes and other sources of data and documents other than the active files. *Id.* This group also suggests that, absent special need and relevance, a party responding to discovery ought not to be required to preserve, review, or produce deleted, shadowed, fragmented or residual data or documents. Even metadata (such as the dates a file was created, modified, or accessed) ought to be excluded as a rule. *Id.*


Comparing and contrasting the Sedonna principles with case law granting discovery requests for electronic data highlights the tension in the law created by the features and characteristics of computer operating systems that create significant, invisible, relevant information on the hard drives. On the one hand, this valuable information ought to be treated like any other relevant information. The fact that it is invisible to the operating system ought to be analogous to paper documents that have been torn to shreds but recovered from a waste basket. On the other hand, invisible computer data has traditionally been expensive to preserve and extract. It is understandable that defendants would object to the burden and expense of preserving this data when it is not used in the ordinary course of their business. Thus, while courts continue to grant motions to discover invisible data, the Sedonna principles argue that this data ought to be excluded.

Absent specific circumstances, preservation obligations should not extend to deleted data or residual data. While most computer systems will have a plethora of data that could be “mined”, there should not be routine authorization for such forensic recovery. If, as is typically the case, deleted data and residual data are not accessed by employees in the ordinary course of business, there is no reason to require the routine preservation of such data. The relevance of the data to the matters in question will be marginal at best in most cases, while the burdens involved will be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.

#### Sedonna Principles Comment 9.b. “Deleted Data and Residual Data”.

Although the principles seem clear, it is not difficult to imagine a case in which the Sedonna proponents, as plaintiffs, will reject these principles and find deleted data to be very relevant. In several years of practicing law and conducting forensic examinations, this author has found that deleted and residual data is usually very relevant. For example, in many sexual harassment and wrongful termination cases, corporations frequently use deleted email, instant messages, notes, jokes, love letters, etc. to establish an irrefutable factual basis authorizing the corporation’s actions. Similarly, many corporations are very pleased to extract, and anxious to aggressively use, evidence of wrongful copying of

customer lists, trade secrets and proprietary information to obtain injunctive relief against former sales personnel.

- 
 If the Sedonna proponents have a legitimate concern about extracting invisible data, it appears to be based on the cost and burden associated with computer forensic analysis. The Sedonna principles suggest that invisible data resident on computer systems ought not to be discovered where the cost and burden is extraordinary.

The proper subject of discovery is electronic data and documents that are relevant to the claims and defenses in the case, and a requesting party should not be permitted to discover electronic data and documents that do not meet this standard regardless of how technically feasible access may be. Accordingly, forensic data

collection should not be required unless exceptional circumstances warrant the extraordinary cost and burden of this approach. See *McPeck v. Ashcroft*, 212 F.R.D. 33, 365 (D.D.C. 2003) (declining to order searches of backup tapes where the burden on defendant in searching those tapes would be great and plaintiff had not demonstrated a likelihood of obtaining relevant information). Making image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues involving the interpretation of ambiguous forensic evidence.

#### Sedonna Principle Comment 8.b. "Forensic Data Collection"

This concern can be, and as a matter of fact, has been rendered moot by advances in computer forensic technology. Today, computer forensic analysis is very cost effective, especially because it captures all relevant data: visible and invisible in one streamlined process. In the final analysis, the Sedonna conference is a traditional response to the existence of evidence: the acceptance of computer forensic analysis by counsel and clients depends ultimately on whether the evidence extracted from the computer systems is helpful to the client's cause or the attorney's legal theories and strategies. In this regard, it is no different than traditional paper discovery.

#### THE COMPUTER FORENSIC PROCESS

Although the computer's operating system cannot view the "invisible" data resident on the computer's hard drives, special forensic software can read, extract, and process all data on hard drives, including "invisible" data in a non-disruptive, economical manner. The procedure used by computer forensic analysts to identify and extract all relevant data from a computer hard drive begins with the creation of a forensic mirror-image clone or copy of the relevant hard drives. *Playboy Enterprises, Inc. v. Welles* 60 F. Supp.2d 1050 (S.D. Cal. 1999). *State v. Cook* 149 Ohio App.3d 422 (2<sup>nd</sup> Dist. Mont. County, 2002)

The choice of forensic software is important. Encase software has been recognized by Ohio Courts as a reliable, precise, and accurate method of preserving electronic data.<sup>2</sup> See State v. Cook, supra. Encase is easily the most widely accepted and used forensic software, currently being used by over 14,000 law enforcement agencies worldwide.

Creating a mirror image forensic clone of a relevant hard drive requires that the computer forensic specialist have access to the relevant computers and the hard drives contained therein for an average of two to five hours.<sup>3</sup> During this period of time, the computer forensic analyst will open the relevant computer cases, remove and attach a write-blocking device to the hard drive (to prevent any change to any of the data on any of the relevant hard drives), and create an exact forensic mirror image of each relevant hard drive. Each forensic mirror image is written to a hard drive supplied by the forensic examiner. After the process is completed, the relevant computer's hard drives are placed back into the computer case from which they were removed.

## OBJECTIONS TO REQUEST TO PRODUCE RELEVANT COMPUTER HARD DRIVES

### A. DISRUPTION

Regardless of the number of relevant computers, the imaging process can be accomplished very quickly because all relevant computers can be imaged simultaneously. To further minimize any inconvenience to the producing party, forensic images of all relevant computer hard drives can be scheduled during convenient times including evenings, after business hours, Saturdays or Sundays. Imaging can occur on-site, or at any convenient location, including the offices of counsel. Indeed, the producing party can even remove the relevant hard drives and ship them to the computer forensic analyst if the producing party does not want anyone on-site.

This forensic process is not disruptive. In fact, this process is very efficient, allowing the identification and extraction of relevant data to be accomplished electronically.

### B. COST

It is generally accepted law that, absent unusual circumstances, the producing party bears the cost of the identification, extraction, and production of relevant computer data. Linnen v. A.H.Robins Co., Inc. No. 97-2307, 1999 WL 462015 (Mass. Super.Ct. June 16, 1999); Bills v. Kennecott Corp., 108 F.R.D. 459 (D.Utah, 1985). The basis of this rule is that a party choosing to enjoy the tremendous business advantages of using computers to process data, cannot shield themselves from the costs attendant to the extraction of

<sup>2</sup> Each forensic image contains embedded data that guarantees the integrity of the image at the time of its creation, and for all times thereafter. No change to the forensic image can occur undetected

<sup>3</sup> This is an average time. Many cases can be completed in less than two hours. Sometimes, the imaging process takes longer depending on the condition of the relevant hard drives, the speed at which they operate, and other factors.

relevant data in litigation. In re Brand Name Prescription Drugs Antitrust Litigation, 1995 U.S. Dist. LEXIS 8521, 1995 WL 360526 (N.D.Ill. June 15, 1995).

Parties, however, are entitled to be protected from undue expense or burden in producing data in litigation. Southern Diagnostic Assoc. V. Bencosme WL 31422863 (Fla. Dist. Ct. App., Oct. 30, 2002); Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. Dist. Ct. App. 1996); In re Brand Name Prescription Drugs Antitrust Litigation WL 360526 (N.D. Ill. June 15, 1995).

Traditionally, courts looked to several factors to determine when the costs of producing data ought to be borne by the requesting party. Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 51 Fed. R. Serv. 3d 1106 (S.D.N.Y. 2002). (Defendants argued that costs of recovering email would range from \$84,000 to \$403,000. Trial Court held "it is not enough to say that because a party retained electronic information, it should necessarily bear the cost of producing it." Court used a multi-factor test to determine when to shift the cost of production:

1. the specificity of the request,
2. the likelihood of finding relevant information,
3. the availability of such information from other sources,
4. the purposes for which the data was retained,
5. the possibility that the responding party might benefit from the production,
6. the total cost of production,
7. the relative ability of the parties to control costs and the incentives to do so, and
8. the resources of each party.

Medtronic Sofamor Danek, Inc. v. Sofamor Danek Holding, Inc., 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. May 13, 2003) (The defendant sought information contained in 2,000 GB of data stored on 515 backup tapes and in 210 GB of electronic files from plaintiff's individual employees. The plaintiff asserted that there were 993 backup tapes with over 61 TERABYTES of data and the individuals' files contained over 300 GB of data. The court analyzed the factors in Rowe to determine whether an expense is "undue." As to total cost of production factor, the Court considered:

1. Cost of restoring backup tapes;
2. Cost of designing and conducting a search;
3. Cost of privilege review;
4. Cost of physical production; and
5. Production cost summary.

The Court set forth a detailed Protocol that included the use of a computer expert).

Recent case law has suggested that a balancing approach be used to determine when, and to what degree, the costs of extracting relevant data ought to be borne by the producing and requesting parties. "Cost shifting ought to be considered only when electronic discovery imposes an 'undue burden or expense' on the responding party. Zubulake v. UBS Warburg, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y. May 13, 2003).

Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.

*Id.* at \*27-\*28.

The Zubulake court created a “Seven-Factor Test.”

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

It is important to note, however, that many of the cases addressing the allocation of cost involve forensic software more than four years old or involve back up tape technology. Changes in forensic software within the last four years have dramatically reduced the cost of imaging, identifying and extracting relevant data, and in many cases, the requesting party pays the cost to avoid any argument about cost shifting. This strategy is especially prevalent where the cost of imaging and analyzing multiple computer systems will cost less than \$7,000.00

To further reduce the cost of discovery on the parties, courts are appointing computer forensic experts as a neutral party expert to image and extract relevant data from all Relevant Computers. “Judges are getting the message. It makes more sense to look to one neutral expert, with the appropriate protocols, rather than relying on the parties to do it and duplicate their expense and effort.” Playboy Enterprises, Inc. v. Welles, 60 F.Supp.2d 1050 (S.D. Cal. 1999). Simon Property Group v. mySimon, Inc. 194 F.R.D. 639 (S.D.Ind. 2000).

#### “FISHING EXPEDITION”

After the computer forensic expert creates images of all relevant hard drives, he will simultaneously mount all images on a lab computer, and electronically search and analyze the images for relevant data. Search strategies will be created jointly by the computer forensic expert and attorneys that reflect the legal theories and strategies in the case. “Unlocking” all data on an image, conducting keyword searches, combined with analysis



of metadata and system artifacts, comprise the usual tools used to complete a forensic analysis.

Electronic searching for relevant data is the only practical means of identifying relevant data resident on a hard drive. An average size hard drive can have millions of pieces of data resident thereon, and it is impossible to search for relevant data by randomly viewing folders or files. No computer forensic expert will “browse” through the images of relevant hard drives seeking to stumble across relevant data. Nor does anyone simply open files to view their contents. All searching for relevant data is conducted electronically. As a result, non-relevant data is never identified, extracted, or viewed.

In some cases, counsel for the producing party argues that he should be given the right to approve of the search and analysis strategy used by the computer forensic expert, including the right to veto the use of search terms or analysis of system artifacts. In some cases, this argument is an attempt to prevent the discovery of relevant data.

This strategy is rendered moot by the protocol followed in state and federal cases that require counsel for the producing party receive the Initial Report of Relevant Data and redact it for privilege before the Report is produced.

### **REDACT FOR PRIVILEGE BEFORE REPORT IS PRODUCED.**

Computer forensic analysis is a tool that allows specialists to view all data on a hard drive, including all the data not seen by the operating system. Computer forensic analysis is not a tool to circumvent the law related to privileged communications. To satisfy the requirements of discovery, while allowing the producing party to review data for privilege, a standard protocol has evolved. See for example the decisions of Simon Properties, Playboy vs. Welles, Antioch vs. Scrapbook, cited herein. This protocol requires the computer forensic expert to identify and extract all relevant data, prepare an Initial Report, present its Initial Report of relevant data (which may include attorney-client data) to counsel for the producing party, while filing a copy of the Report of Relevant Data, under seal, with the Court. The computer forensic expert will also file with the Court and serve on all parties a Summary of its Report of Relevant Data, containing the following information:

- (1) Number of pages in Report, Number of tables, appendices, or exhibits
- (2) All search terms and the number of “hits” for each term
- (3) A statement of the Search and Analysis Strategy, Acquisition data related to the creation of the forensic images, and the table of contents for the report.

The computer forensic expert will copy its Report of Relevant Data onto a cdrom as a Word document or webpage. Counsel for the producing party will be able to redact the report for privileged communications as follows:

- (1) open the Report on counsel’s computer;

- (2) read the Report, and using the cursor, highlight any text for which counsel wishes to claim privilege;
- (3) “cut” the text out of the Report, and “paste” the text into a new document created on counsel’s computer;
- (4) identify the text in a privilege log;
- (5) Save the Report as Redacted;
- (6) produce to Plaintiff on cdrom a copy of the Report as Redacted and a copy of the privilege log.

This protocol is so efficient that Courts frequently order counsel for the producing party to produce a redacted report within ten days of receiving the Initial Report of Relevant Data. Moreover, this protocol completely satisfies concerns related to privileged communications, while permitting the parties to efficiently acquire all relevant data from all relevant computers.

### SANCTIONS

Parties to litigation have a duty to preserve evidence beginning at the time when a party knows or reasonably should know that the evidence may be relevant to pending or anticipated litigation. Mathias v. Jacobs, 197 F.R.D.29 (S.D.N.Y. 2000); Melendez v. Illinois Bell Telephone, 79 F.3d 661 (7<sup>th</sup> Cir. 1996). The duty to preserve data relevant to anticipated or existing litigation extends to data resident on computer hard drives and

other electronically recorded data. Kleiner v Burns, WL 1909470 (D Kan., Dec. 15, 2000); Danis v. USN Communications, WL 1694325 (N.D.Ill. Oct. 23, 2000). Minnesota Mining & Manufacturing Co (“3M”) v Pribl, 259 F.3d 587 (Wis. 2001), 2001 WL 832749 (July 25, 2001). (Seventh Circuit Court of Appeals upheld the decision of the Trial Court to give a jury a negative inference charge on the ground that the defendant’s explanation that his child unintentionally downloaded six gigabytes of music on the day before the computer was produced was properly rejected by the Trial Court).

The first rule of preservation is to do no harm to the data to be preserved. Computer data is volatile and is destroyed by the mere operation of the computer’s operating system. Antioch v. Scrapbook, 210 F.R.D. 645, 2002 U.S.Dist.LEXIS 20811 (D.Ct. Minn., April 29, 2002). Log files are changed whenever a system is started. The start process (boot-up) changes the dates and information kept in thousands of files. Housekeeping programs that format disks (Defrag), purge files after a time period, recycle back-up tapes or media must be identified and stopped as soon as possible. The obligation to preserve documents rests with senior corporate officials, who must contact information technology personnel and insure that the company’s document retention programs are modified so as not to destroy relevant data. Danis v. USN Communications, Inc. 2000 WL 1694325 (N.D.Ill. October 23, 2000). Companies cannot use a corporate retention policy to “shield” their destruction of evidence, even where the destruction occurred before litigation was initiated. Rambus v. Infineon, 220 F.R.D. 264, 2004 U.S.Dist.LEXIS 4577 (E.D.Va. March 17, 2004).

Because the normal operation of a computer system threatens to destroy the “invisible” evidence located thereon, spoliation issues can be unique. Preventing spoliation from the ongoing use of the computers has been the ground for granting expedited discovery and compelling the forensic imaging of relevant computers. Antioch v. Scrapbook, Id. Where data destruction occurs after a complaint is filed and is deliberate, sanctions can be imposed. William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984). “GNC was on notice from the inception of litigation that the [erased] records...were relevant to the litigation or at least were reasonably calculated to lead to the discovery of admissible evidence...GNC’s senior management know or should have known at the inception of this litigation that the records...were relevant to the matters in issue...and likely to be requested by Thompson during the litigation...[T]he Special Master ordered GNC to preserve all...records maintained by GNC in the ordinary course of its business at its headquarters...GNC employees were not instructed ... to preserve...records as required by the ...Order. GNC’s president ... issued a memorandum...to all GNC personnel advising them that the Order ‘should not require us to change our standard document retention or destruction policies or practices’. This instruction on its face appears to instruct GNC employees to conduct their destruction procedures as they had done in the past and it was so interpreted by the GNC employees.” The court struck GNC’s answer, entered default judgment against it, dismissed its complaint in a related case. The Court specifically rejected lesser sanctions. See also RKI, Inc. v. Grimes, 177 F.Supp.2d 859 (N.D. Ill. 2001) (Court determined that Defendant defragmented his home computer attempting to hide from plaintiff that defendant had deleted confidential information and software. The court sanctioned Defendant \$100,000 in compensatory and \$150,000 in punitive damages, attorneys’ fees, and court costs); Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D.Va. 2001). (Willful destruction of documents results in adverse inference, expenses and attorneys fees in the amount of \$179,725.70).

Data does not necessarily have to be destroyed to result in sanction. Sanctions have been issued in cases in which data was withheld (DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002). Plaintiffs given opportunity to respond to Defendant’s expert report, and Defendants denied opportunity to reply where Defendant failed to produce to Plaintiff certain database data on which Defendant’s expert relied); Sheppard v. River Valley Fitness One, 203 F.R.D. 56 (D.N.H. 2001) Court sanctioned attorney for lack of diligence in obtaining and producing computer records; GTFM, Inc., v. Wal-Mart Stores, 2000 U.S. Dist. LEXIS 16244 (S.D.N.Y. Nov. 8, 2000) Defendant must pay costs incurred by plaintiff from defendant’s failure to disclose the capabilities of the defendant’s computer system.

The powerful impact that computer forensics can have upon a case is perhaps best illustrated in Metropolitan Opera Assoc., Inc. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003). In this case, counsel for Local 100 tried very hard to avoid producing data on relevant computers. The District Court for the Southern District of New York reviewed the history of counsel’s efforts as follows:



[C]ounsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, what constitutes a 'document'...; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who (at least until July 2001) did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had 'establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests,'...and (5) in the face of the Met's persistent questioning and showings that the production was faulty and incomplete, ridiculed the inquiries, failed to take any action to remedy the situation or supplement the demonstrably false responses, failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced.

Based upon these actions, the Court ordered a computer forensic expert to assist Local 100. Rather than submit to any forensic examination, Local 100 disposed of all relevant computers. When advised that the Local had simply thrown relevant computers away, the Court sanctioned the Union, granting judgment against the Union on the merits of the case, and ordering the Union to pay Plaintiff's attorney fees related to discovery. The Court rejected less severe sanctions including adverse inference and preclusion on ground **"it is impossible to know what the Met would have found if the Union and its counsel had complied with their discovery obligations from the commencement of the action."**

Traditionally, sanctions were applied to the intentional destruction of evidence. It is significant to note that at least one court has held that **mere negligence** in preserving or promptly producing electronic information is sanctionable. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002). This is an important case, because the parties agreed that the email eventually produced during trial did not contain any relevant information. Nevertheless, the District Court vacated the trial court's order denying sanctions (adverse inference instruction) and held that pursuant to Rule 37(b)2, Federal Rules of Civil Procedure, the trial court has power to "make such orders in regard to the failure [to obey an order to provide or permit discovery] as are just." The Court also reasoned that Rule 37(c)(1), amended Dec. 2000, provides that failure to supplement discovery results in exclusion of the evidence and permits the Court to "impose other appropriate sanctions ... and may include informing the jury of the failure to make the disclosure...The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence." Id. at 108.

To obtain an adverse inference instruction, the movant must present sufficient evidence from which a reasonable trier of fact could infer that the evidence destroyed or not produced "would have been of the nature alleged by the party affected by its destruction" or non-production. The burden of proof on the movant, however, should not be "too strict

a standard of proof" so as not to "subvert the ... purposes of the adverse inference" *Id.* at 108-09. Significantly, the Second Circuit Court noted that where a party fails to hire an expert to assist with electronic production as soon as the party determines that it cannot retrieve the data, and the continued reliance upon an expert that cannot produce results, may create an inference of a "culpable state of mind" supporting a determination that the party is acting in bad faith. *Id.* at 111.

Not all courts grant sanctions based solely upon the destruction of evidence. Where the data destroyed bears no possible relationship to the matters being litigated, courts have denied sanctions. Hildreth Manufacturing, L.L.C. v. Semco, Inc., 151 Ohio App.3d 693 (3<sup>rd</sup> Dist. App. Ct. Marion Cty) (Third District Appellate Court, Marion County, affirms the decision of the Marion County Common Pleas Court, denying Semco's Motion for Contempt against Hildreth for spoliation of evidence on the ground that the Trial Court properly determined that there was no reasonable possibility that the missing hard drives contained evidence of the theft of trade secrets. Semco had argued that sanctions were proper under Rule 37(B)(2)(e), Ohio Rules of Civil Procedure and pursuant to case law in Bright v. Ford Motor Co. 63 Ohio App.3d 256, 578 N.E.2d 547 (1990). Bright Court held that sanctions against a plaintiff for the willful destruction of evidence in violation of a protective order, required that plaintiff be given an opportunity to overcome a presumption that the defendant had been prejudiced. "A sanction which in effect puts a party out of court must be based on demonstrable prejudice to the opposing party...A workable formulation of prejudice for purposes of this case is: a reasonable possibility, based on concrete evidence, that access to the unaltered (requested evidence) would have produced evidence favorable to the (defendants), which was not otherwise obtainable." Bright at 259. Rule 37(B)(2)(e) provides "If any party...fails to obey an order to provide or permit discover,...the court in which the action is pending may make such orders in regard to the failure as are just, and among others the following:...An order...rendering a judgment by default against the disobedient party." Appellate Court reasoned that Hildreth adequately rebutted the presumption of prejudice by showing that a reasonable possibility did not exist that hard drives used by a CNC machine in the normal course of the operation of that equipment, contained evidence of customer lists or other intellectual property.

## CONCLUSION REGARDING LITIGATION AND COMPUTER FORENSICS

Federal and state courts are quickly recognizing the unique challenges and advantages of discovering data relevant to a matter that resides on electronic media. The challenges are to preserve the data from destruction by forces including the computer's operating system, and to protect privileged data. The advantages are that the data can be identified and extracted using a computer forensic protocol that is non-disruptive, economical, and very powerful. Computer forensic analysis is replacing production of documents as the standard means of discovery, and offering attorneys a value-neutral mechanism to quickly determine all the facts in any case.



“Judges are getting the message. It makes more sense to look to one neutral expert, with the appropriate protocols, rather than relying on the parties to do it and duplicate their expense and effort.” Playboy Enterprises, Inc. v. Welles, 60 F.Supp.2d 1050 (S.D. Cal. 1999). Simon Property Group v. mySimon, Inc. 194 F.R.D. 639 (S.D.Ind. 2000).

## FACT GATHERING IN CORPORATE COMPLIANCE AREA: SARBANES-OXLEY AND COMPUTER FORENSICS.

In response to significant, public examples of corporate fraud such as Enron, Worldcom, the federal government authorized the Securities and Exchange Commission to combat internal financial fraud through mandated self-policing procedures by public companies. The requirements of Sarbanes-Oxley must be implemented, however, in a computer environment: where visible and invisible data resides upon a variety of devices using differing operating systems. As in the area of litigation discussed above, attorneys assisting clients meet the requirements of Sarbanes-Oxley must employ tools that allow all relevant data—visible and invisible—to be included in the compliance strategy.

### A. Sarbanes-Oxley History

Passed in July 2002, Sarbanes-Oxley passed 99-0 in the Senate and 423-3 in the House of Representatives. It was passed in response to the public hue and cry attendant various misdeeds by public companies, including the indictment of Arthur Andersen. Following that indictment were several news reports that claimed or implied that corporate wrongdoing was being covered up by massive purging of computer systems and deletion of email.

The facts about corporate fraud, including the type of fraud most often committed, are important to know in order to create internal controls that are likely to be effective. For example, internal controls to reduce physical theft may be different than those to reduce overstatement of expense account items.

A 2003 KPMG survey of 500 public companies identified expense account abuse (36%) and theft of assets (49%) as major types of fraudulent losses. Fraud was discovered in 54% of the cases by accident, 63% by employee tip, and 41% by anonymous tips. Sarbanes-Oxley is an opportunity for companies to identify the types of fraud that cause loss within their organization, and adopt internal controls that identify this loss in order to prevent it or respond to it

### B. Section 404 and 302 Sarbanes-Oxley

Section 404 requires companies to institute effective “internal controls”, which the SEC has stated “is a broad concept that extends beyond the accounting functions of a company” (68 FR 36636, 36638).



Internal controls must “provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the [company’s] assets that could have a material effect on the financial statements. (68 FR 36636, 36640)

Section 302 renders CEO’s and CFO’s personally responsible to establish and maintain internal controls. CEO’s and CFO’s must personally evaluate the internal controls of their company and assess their effectiveness. The SEC requires that the effectiveness of

internal controls be assessed by analyzing the controls used by the company related to the prevention, identification, and detection of fraud. (68 FR 36636, 36643).

Once the CFO and CEO have evaluated the effectiveness of the internal controls used by the company, they must certify that they have disclosed to the Company’s auditors and the Board of Directors’ audit committee (a) “All significant deficiencies in the design and operation of internal controls”, and (b) any fraud, whether or not material, that involves management or other employees who have a significant role in internal controls”.

These types of investigations are usually called “certification investigations”. These certification investigations are very important because individuals are being prosecuted—not the corporate entity. The challenge in a computer era is to determine whether internal controls must include the visible and invisible data resident on devices and computers throughout the corporate enterprise.

It would seem self-evident that an internal control would be ineffective in preventing or detecting fraud if the control took no action to identify relevant data that had been deleted, orphaned, hidden, or otherwise rendered invisible to a computer’s operating system. If internal controls focus only upon the visible data, a fraud can easily avoid detection by the mere expedient of deleting the evidence of a fraudulent transaction.

### C. Sarbanes and Whistleblowers

Section 301 of Sarbanes-Oxley requires that the Audit Committee “establish procedures for (A) the receipt, retention, and treatment of complaints...regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees...of concerns regarding questionable accounting of auditing matters”. While companies must follow-up regarding employee complaints, the method of follow-up must be an effective part of the companies internal control measures. In a computer era, a company probably must include the invisible and visible data in its follow-up; or risk the charge that, although warned of the fraud, and although evidence of the fraud was resident on the company’s computers (in deleted, orphaned, or hidden form), the company took no action to extract the evidence and react to the fraud.

It may be that failure to include the invisible data in scope of a company’s internal controls would constitute a failure of internal control under sections 404 and 302, supra.

If it also were interpreted as a failure of Section 301, the company could be subject to delisting (68 FR 64154).

Section 806 provides a cause of action for any employee who suffers retaliation by an employer for whistle blowing if the employee “reasonably believes” fraud is occurring. If the fraud is being investigated, it is a federal offense for an employer to retaliate against a whistleblower who is assisting law enforcement. It may be necessary to investigate both the visible and invisible data in order to make a corporate decision whether a whistleblower has a “reasonable belief” that fraud is occurring. By simultaneously investigating both visible and invisible data, it seems that a company ought to be able to document the basis for its decision to accept or reject a whistleblower complaint.

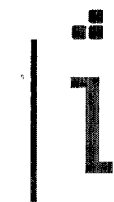
Section 409 of Sarbanes-Oxley requires timely reporting to the public. As a practical matter delaying an investigation of fraud allows perpetrators additional time in which to cover their tracks, usually by destroying evidence. If the fraud, however, is conduct that “benefits” the company, Section 802 of Sarbanes-Oxley may cause the company to be vicariously liable for the fraud. Specifically, if evidence is destroyed, penalties can be incurred of fines up to \$5 million dollars and imprisonment of up to 20 years. Destruction of evidence, however, may be more difficult to complete in a compute era, where data is distributed across several machines, can be extracted if not overwritten, and the manner in which machines have been used can be documented by operational artifacts.

In the event that a company was charged with liability for failing to fulfill its requirements under Sarbanes-Oxley, the company can mitigate or eliminate corporate liability. The SEC has indicated it will review the following areas to assess liability:

1. the degree of self-policing initiated by the company prior to the misconduct;
2. whether the misconduct was reported by the company when it was discovered, and whether the company conducted a thorough review of the nature, extent, origins, and consequences of the misconduct;
3. whether the company has remediated the situation, including modifying and improving internal controls;
4. whether the company cooperated with law enforcement, providing the SEC with all information relevant to the underlying violations.

In regards to the requirement that a company cooperate with the SEC, the SEC has indicated that cooperation is measured, in part, by the ability of the company to “identify evidence with sufficient precision to facilitate prompt enforcement actions against those who violated the law” (SEC Release No. 44969).

This requirement may, ultimately, require the use of computer forensic analysis as an integral part of a company’s internal control, because enforcement actions in the past have usually included forensic analysis of computer data. Indeed, it is standard investigative procedure for federal agencies to seize and analyze computer data as part of enforcement actions.





## **SARBANES-OXLEY AND ENVIRONMENTAL COMPLIANCE**

Although Sarbanes-Oxley is usually associated with financial fraud, its certification responsibilities may force more compliance with environmental control and reporting procedures. The Environmental Protection Agency has conducted studies critical of the degree of compliance with environmental disclosure obligations. (EPA OECA Memorandum, dated January 19, 2001, "Guidance on Distributing the 'Notice of SEC Registrants' Duty to Disclose Environmental Legal Proceedings"). In 1998, EPA reported that 74% of public ally traded companies and 96% of companies facing Resource Conservation Recovery Act corrective actions, failed to report same in their public disclosures. This failure has been characterized by EPA as putting investors at risk. Indeed, EPA has placed online the Enforcement and Compliance History database which allows the public to compare environmental actions with disclosures made in SEC filings.

In July 2004 the Government Accountability Office urged the SEC to "take steps to improve the tracking and transparency of information related to its review of companies' filings and to work with the [EPA] to explore ways to take better advantage of EPA data relevant to environmental disclosure." (GAO, "Environmental Disclosure: SEC Should Explore Ways to Improve Tracking and Transparency of Information, 1, GAO-04-808, July 2004, at <http://www.gao.gov/new.items/d04808.pdf>).

## **FACT GATHERING UNDER FEDERAL TRADE COMMISSION AND OFFICE OF THE COMPTROLLER OF THE CURRENCY**

Many regulatory agencies are adopting requirements that reflect the need to respond to information-related threats by using controls and procedures that include invisible and visible data. The FTC's Safeguards Rule, for example, requires that companies subject to FTC regulation maintain information security systems, including protocols by which to respond to system intrusions, attacks, and other failures. (16 CFR Part 314.4(b)(3)). The FTC has initiated enforcement actions for the failure to protect computer-stored customer information. Actions have been initiated against, inter alia, Guess, Inc., Eli Lilly, ACLU, and Microsoft. Specifically, the FTC alleged that these companies failed to initiate and maintain proper information safeguards, including proper incident response protocols.

OCC regulations require financial institutions to have policies and procedures that include specific steps to be taken in response to internal and external security breaches.(12 CFR Part 30. Appendix B, III(C)(g)). It is almost axiomatic that investigating such security breaches includes extracting and analyzing the invisible computer data that is available, including that data that comprise artifacts of the manner in which the system was used or compromised.



## Exhibit B

## REQUEST FOR PRODUCTION OF DOCUMENTS CAN BE A TECHNOLOGY TRAP.

Traditionally, litigators obtain relevant documents from their opponent by issuing a Request for Production of Documents. Although the Rules of Civil Procedure mandate the disclosure of relevant, non-privileged documents<sup>4</sup>, it is a rare case in which an opponent copies all relevant documents and provides them in response to the first Request. Usually, counsel must make several phone calls, write letters, monitor the partial responses provided, and constantly work to obtain as complete a production of documents as possible.

The use of computers to create, process, and store data has placed additional burdens on attorneys. Attorneys now must understand some basic computer concepts in order to determine whether they are receiving a proper production of documents. For example, most attorneys know that “deleting” a document does not remove the document from the computer’s hard drive. The document remains stored on the computer, but is merely rendered “invisible” to the operating system. Because deleted documents are “invisible” to a computer’s operating system, a party cannot produce deleted documents in response to a request for production of documents. In the past, therefore, deleted documents have usually been ignored and left behind; notwithstanding the fact that they were discoverable.

Deleted documents are not the only data that can be rendered invisible to a computer’s operating system, and thereby left out of a standard production response. It is very common to have documents created on a computer using a program that, at the time of the document request, can no longer read the documents. Accounting programs, for example, are updated each year. Some updates are not “legacy”, meaning that the updated program cannot read and interpret old files. In some cases, the program used to create relevant files has been removed from the computer, and the computer simply cannot open or read those files. All this data is invisible to the operating system, insofar as this data will not be retrieved when searching the system for documents responsive to a document request.

Data with an inaccurate file extension is also “invisible” to the operating system. Simply changing the extension associated with a file (for example changing “.doc” to “.jpeg”) will render the contents of the “.doc” file unintelligible to the operating system. This technique is a favorite amongst users trying to hide data. In some cases these users also save the file (with inaccurate extension) in a folder used by the operating system, where one would normally never look for documents and data. This data will not be produced in response to a document request.

Data that was never “saved” as a file by a user is also “invisible” to the operating system. Many attorneys are surprised to learn that a computer’s operating system automatically saves data by writing it to the hard drive without any input from the computer’s user.

<sup>4</sup> This assumes counsel has defined the term document properly.

Almost all users, however, have seen this feature work, such as when a user recovers from a transient power loss that occurred while creating a brief or memo. When power is restored and the computer is re-booted, the operating system will automatically ask whether the user wishes to open the document that was being created when the power failed. This “retrieved” document will be available, even though the user had not saved the work. The “retrieved” document was created by the operating system automatically saving the work. If the user elects to ignore this “retrieved” document, the document remains on the hard drive, but is thereafter ignored by the operating system.

A computer’s operating system also renders invisible large amounts of data used by the operating system to perform functions. For example, when printing documents, the operating system copies the data into a “spool file”—a file that the system will use to print, and afterwards ignore. After printing the documents, a copy of the document will remain in the spool file. Similarly, the operating system creates (and subsequently ignores) thousands of temporary, cache, buffer files and other types of data used by the system to perform various functions. This data is generally referred to as “artifacts” and can be analyzed to determine the manner in which a computer was used. For example, operating system artifacts can prove that a user improperly copied customer lists to a floppy drive prior to leaving a company. Artifacts could also prove that a user had removed a hard drive from a system at a time when the user knew of pending litigation. None of the data discussed above will be produced in response to a request for production of documents. While it is all discoverable, it is simply left behind on the hard drives of the relevant computers.

How important is this data? Experienced litigators know that the way in which an opponent has used its computer systems often provides a roadmap that proves essential elements of tortuous conduct. Discovering the substance of deleted documents, instant messages, emails, etc. often provides a treasure-trove of statements that support or contradict essential legal theories or strategies in a case.

Although attorneys agree that it would be very desirable to discover this data, most litigators have never tried to do so. This was because, until very recently, case law related to production of documents did not seem to easily apply to data created, processed, and stored on computers. There was no set of procedures and protocol that an attorney could follow similar to the procedures related to requesting production of documents. Additionally, it appeared to many attorneys that it was unrealistic to request access to an opponent’s computers because to do so would be disruptive, burdensome, overbroad, costly, and violative of privilege. Attorneys did not want to incur substantial research, time, and effort in motion practice to compel access where such motion did not seem likely to be granted. Most attorneys agreed that if they could economically obtain all the data related to a case (visible and invisible to the computer), without spending significant time and effort in motion practice, and without getting lost in the technical world of “computer-speak”, they would pursue the production of all such data.

Within the last two years, federal and state courts have recognized technology and protocol that permits discovery of all relevant data, including the data rendered invisible

to a computer's operating system. Attorneys can now obtain all relevant data in one simple, economical process, that is non-disruptive, properly limited to relevant data, and protecting privilege. Fortunately, the process is very similar to that used by attorneys to request production of documents.

The process begins with either (1) substituting for a traditional request for production of documents, a request to produce tangible things: to wit all hard drives on which is resident data relevant to the claims or defenses in the case, or (2) serving a traditional request for production of documents drafted to define document as any medium upon which intelligence or information is recorded or from which intelligence or information can be recorded, retrieved, or perceived, with or without the use of detection devices, including detection devices other than the operating system and programs installed on any of defendant's computers. Note that the definition of document focuses upon the substance that carries the data. Paper, for example, is a medium on which data—intelligence or information—is recorded, and from which the data can be perceived by reading. Similarly, a hard drive in a computer is a medium on which is recorded data in the form of polarized, magnetic particles, that can be perceived (i.e. understood) using a computer as a detection device. This definition includes data that cannot be recognized using the producing party's computers. Courts have recognized, however, this data can be perceived using programs and software tools available to a computer forensic expert.

Using specialized forensic software tools, a forensic expert first makes a "clone" of those computers used by a party to create, process, store, archive, or otherwise manipulate data related to a particular case. These are the "relevant computers" in a case, and identifying them at the onset of litigation is the common objective of all parties and their attorneys. At the moment when a party knows or should know that litigation is anticipated, that party has a duty to preserve electronic evidence and prevent its spoliation. Continuing to use computers on which resides visible and invisible data that is relevant to a matter overwrites the data and causes spoliation. Thus, in order to prevent the spoliation of evidence, the parties must identify the relevant computers and thereafter take action to preserve the evidence on the relevant computers. Preventing spoliation can be accomplished by refraining from using relevant computers or by creating a forensic image of each of these computers. Because it is rarely acceptable to refrain from using relevant computers, litigants most often resort to forensic imaging.

A forensic image contains all the data—visible and invisible—that is resident on the relevant computers' hard drives. Once a forensic image of each relevant hard drive is created, the computer can be returned to service, because all the data has been "frozen" on the forensic image. The forensic image is an electronic "snapshot" of each of the relevant computers.

Making a forensic image requires a computer forensic expert be granted access to the subject computer's hard drive for four to six hours. Access can be provided on-site, at a lawyer's office, at home, or at any location convenient for the producing party. To avoid disruption, access is usually granted at night, over a weekend, or during non-business hours. The forensic expert will attach to the subject computer a "write-blocking" device

which prevents any data from being written to or changed on the subject drive, while an exact, bit by bit image is copied onto a drive supplied by the forensic expert. If several relevant computers are involved in a matter, they can all be imaged simultaneously, so that making a forensic image of many computers can be accomplished in less than eight hours. The producing party and its counsel can observe the creation of the forensic image. The last step in creating a forensic image is to verify the image. Verification is the process that embeds into the image a “digital DNA marker”, termed an “MD5 Hash Value”. This value can be used to prove that the forensic image has not been altered in any fashion whatsoever from the time of its creation.

After forensic images are made of each of the relevant computers, these clones are then simultaneously connected to a forensic lab computer so they can be electronically searched. Electronic searching is conducted by the forensic expert using powerful searching software that identifies and extracts only relevant data. No “fishing expedition” is conducted by randomly opening files or folders hoping to stumble across something relevant. Because relevant data is identified electronically, no person will ever view any data that is not related to the litigation.

Once relevant data has been extracted, it can be compiled, parsed, and arranged so that the data intelligently reflects the issues in a case. At this point, the relevant data is usually placed into a Report that can be read using a word processor. The Report will contain exact copies of all relevant data, including all deleted email, letters, memos, instant messages, etc. The Report is then presented to counsel for the producing party so that counsel can redact the data for privileged matter. After redacting the data and creating any applicable privilege logs or reports as required by the court, the producing party provides the data to the requesting party.

The requesting party will receive all relevant data, including all data hidden, deleted, or otherwise rendered invisible to the computers of the producing party. The requesting party will receive, therefore, all the documents that would have been produced in the traditional manner, plus all documents and data that could not have been copied from the computers of the producing party.

This process is very quick. Imaging is usually accomplished in a matter of hours. Using software to electronically search and extract relevant data is completed within seven working days, including about 25-30 man hours to analyze, parse and compile the search results.<sup>5</sup> The Initial Report can be delivered electronically to counsel for the producing party, and is usually redacted in ten days. In almost all cases, litigators can have all the relevant facts within three to four weeks from the date of access to the computers. The process is very economical. The process usually results in reducing the time spent on discovery disputes, while costing about 10% of the total legal fee incurred in a case.

<sup>5</sup> This estimate is applicable to cases in which the computers are being searched to extract data; It is more complicated and therefore takes more time for cases in which artifacts must be analyzed to determine the manner in which the computer was used.



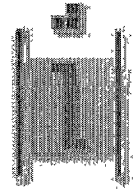
EXHIBIT C

CV FOR DAMON HACKER  
PRESIDENT  
VESTIGE, LTD



## Damon S. Hacker, MBA

---



### Present Position

**President/CEO**  
Vestige Digital Investigations  
Medina, Ohio

### Previous Positions

**Director (Managing Partner)**  
SS&G Technology Consulting LLC  
Solon, Ohio

**President/CEO**  
F1 Ltd, Cleveland, Ohio

**Sr. Business Analyst**  
Medical Life Insurance Company, Cleveland, Ohio

**Systems Manager**  
Case Western Reserve University,  
Auxiliary Services, Cleveland, Ohio

### Experience

#### SS&G Technology Consulting

Responsible for day-to-day and long-term strategic planning of technology consulting business.

Function as part-time **Chief Information Officer (CIO)** for several clients, including parent company, SS&G Financial Services.

Accountable for aligning Information Technology strategy with business objectives of four separate companies.

Oversee projects, practice development and human resource components of external consulting group, SS&G Technology Consulting.

Manage internal IT group, reviewing and prioritizing projects and acting as liaison between partner group and IT Specialists.

Developed, reviewed and implemented operational budgets for SS&G Technology, as well as internal technology component of SS&G Financial Services.

Designed and developed Managed Services platform for small- and mid-size businesses to address their on-going internal IT needs without hiring full-time IT department.

Developed SS&G Technology Consulting's Computer Forensic methodologies and head up that division of the practice.

Developed, recruited staff and directed the infrastructure for a leading technology consulting firm (from 2 to 11 FTE's)

## **Damon S. Hacker, MBA**

---

### **F1 Ltd**

Built service organization & consulting practice from the ground up. Successfully merged practice with large, independent financial service and business management consulting firm.

Responsible for day-to-day and long-term direction of company, human resources and financial management of company.

Obtained state-wide corporate sponsorship from Ohio Society of CPAs, as their preferred IT Solution Partner.

### **Medical Life Insurance Company**

Responsible for overseeing Information Technology needs of five out of eight functional departments within company.

Acted as internal consultant, interfacing with corporate management, functional department management and IT department to provide improved efficiencies, increased communication and better workflow through entire company.

Identified, designed and managed creation of an integrated billing system that provided Medical Life Insurance with an avenue to help lower overall administrative expenses by 3%. In addition to supporting the Self-Administered method of billing, it provided information back to MLI that further improved efficiencies in both the underwriting process and customer service process.

Developed system to automate marketing incentive plan administration. Reducing monthly effort from 60-80 hours per month to less than 1 hour on an on-going basis.

### **CWRU, Auxiliary Services**

Turned around failing department within the university's division that handled day-to-day amenities (Auxiliary Services).

Developed and managed team of 18 FTE's, including recruiting, mentoring, hiring and firing.

Increased annual sales from \$200,000 to \$1,800,000 in three years.

Instituted operating efficiencies and technology solutions to reduce standard job turnaround from 19-21 working days to 3-5 working days and instituted ability to handle emergency jobs immediately.

Opened 3 additional satellite offices of our division to provide service closer to the population using our services.



## Damon S. Hacker, MBA

---

### Education

#### Weatherhead School of Management

Master in Business Administration

Concentration in Information Technology & Marketing

Cleveland, Ohio

#### Case Western Reserve University

Bachelor of Arts in Chemistry

Cleveland, Ohio

### Affiliations

High Tech Crime Network

OSCPA-Technology Committee Chairman

### Publications

#### Authored the following articles

“Computer Forensics More Prevalent Means of Evidence in U.S. Courts”, The Edge, January 2003

“Whodunit? Ask your PC—Computer Forensics Combats Fraud, Complements Litigation”, The Contractor, November/December 2003 issue.

“Internet Fraud: It’s Getting Worse.”, Technology Matters, Spring 2004.

“The Seven Deadly Sins of Implementing Technology”, The Edge, October 2000.

“Factors to Consider when Evaluating Firm Management Software—A Nuts & Bolts Approach”, Ohio Lawyers Weekly, November 1999.

“Fed Up With Spam? Can It With These Smart Strategies”, Technology Matters, Summer 2003.

“Introducing the Technology Continuum: How To Get Up to Speed—and Stay There”, Technology Matters, Summer 2003.

“Look Who’s Talking: XML Promises Standardized Business Systems”, Technology Matters, Summer 2003.

“The Art of the Deal: 4 Steps to Cutting Your Telecom Costs”, Technology Matters, Summer 2003.

## Damon S. Hacker, MBA

---

"The Journey is just as important as the destination—How to evaluate software and vendors before you buy", Technology Matters, Spring 2004.

"From bucks to bytes and back again. 3 ways to evaluate your IT projects", Technology Matters, Winter 2004.

"Names, not numbers. Improve customer service with a CRM system.", Technology Matters, Winter 2004.

"Could a blog boost your business visibility?", Technology Matters, Winter 2004.

### In the News

"Electronic Data Discovery Gains New Ground", Crain's Cleveland, February 3, 2003.

"Solon Company Browses for Cyber Crime", The Solon Times, December 12, 2002.

"1-800-My-Computer's Crashed", Inc Technology, 1999, No. 4, p. 26.

"Charge IT", Inside Business, November, 1999, p. 73.

"The Answer to Your Technical Support Headaches", Ohio CPA Newsletter, Volume 35, No. 11, p.1.

### **Referenced In**

"The Shifting Sands of the IT Industry", The Edge (Lattimore, Black, Morgan & Cain ed.), Summer 2002, p.2.

## Damon S. Hacker, MBA

---

### Presentations

"Computer Forensics & Electronic Evidence", OSCPA Akron CPE Day, June 24, 2004.

"Computer Forensics & Electronic Evidence", OSCPA Columbus CPE Day, May 19, 2004.

"Cyberdiscovery" for the Cleveland Bar Association's The Litigation Institute—Hot Topics in Litigation, November 7, 2003.

"Computers & Crime", Ohio State Bar Association CLE, November 21, 2003.

"Computer Forensics: The Evidence Is Out There". OSCPA Business Valuation & Litigation Services Committee, Cleveland, Ohio. March 22, 2004.

"Computer Forensic Accounting", Ohio Society of Certified Public Accountants, John Carroll University & the National Association of Black Accountants, Spring Conference, May 22, 2003.

"What To Do If You're Hacked", Expert Panel, VigilantMinds, Pittsburgh, PA. May 21, 2003.

"SAS 94 from an IT Professionals Viewpoint"

"Managing Technology in an Advanced Practice"

"Long-Term Care in the New Millenium"

"Finding Funding for your Technology Projects – An Approach for Non-Profits"

"Benefits of Windows 2000"

"The QuickBooks Phenomenon"

"Intensive Course in Medical Record Keeping – An Introduction to Electronic Medical Records"

"An Update on Major Technology Issues Facing the Accountant in Industry"

## Damon S. Hacker, MBA

---

### Expert Witness Experience

*The following are court cases where I have been named as an expert and provided either testimony or an Expert Report.*

Apex Electrical Supply Inc v. American Electric Supply LLC, Summit County Court of Common Pleas, CV-2002-12-7500. Testified.

U.S. v. Bucheit International Inc, U.S. District Court, Cleveland, Ohio, 1:02CR004. Testified.

Sciarrino v. Tylinter, et al., U.S. District Court, Cleveland, Ohio, 03-CV-000125. Expert Report.

Stanners v. Al Root, U.S. District Court, Cleveland, Ohio, 1:01CV1269. Expert Report.

*The following are samples of cases that I have been named as an expert, but the case is either pending, has settled outside of court or I have been a consulting expert and have not been disclosed. To protect the privacy of these cases, only generalities have been presented. I can provide further information, within the confines of any privacy issues and non-disclosure agreements, should you deem it necessary to gain further information.*

Law Firm v. Law Firm: This case involved a dispute of the fees charged between the opposing counsel of two parties. Included behind-the-scenes analysis of the time & billing system of the law firm in question and reconciliation to supplied court fee invoices.

Criminal Defense: Alleged hack-in by former employee to employer's system. Analysis included review of log files, network activity and individual's home computer.

Former Employee v. Company: Wrongful termination suit that involved allegations that a document had been created ex-post facto. Analysis included determining document's authenticity.

Employer v. Former Employee: Intellectual property theft and trade secret violation of former employee to new employer. Analysis included search and retrieval of documents and e-mails highlighting the alleged actions.

Former Partner v. Partnership: Contract negotiation dispute. Alleged post-dating of documents. Included analysis of electronic documents to determine authenticity of date/time stamps.

Non-profit Organization: Internal administrative investigation against Accounting Manager to prove/disprove fraudulent transactions.

**Damon S. Hacker, MBA**

---

Individual v. Life Insurance Company: Case involved review of opposing expert's Expert Report, e-mail and Internet activity.

Benefits Fund/Non-profit Organization: Embezzlement investigation against former Controller of organization. Included analysis of e-mail, documents and the accounting system.

Child Custody/Divorce: Investigation of alleged "inappropriate household" claim from one parent against the other. Included analysis of Internet & e-mail activity of minors.

Medical Clinic v. former partners: Investigation of possible Trade Secret/Intellectual property. Involved analysis of servers and individual workstations, e-mail activity between former partners and other employees within clinic.

Divorce: Investigate e-mail, Internet and network activity to find hidden assets of spouse.

Accountant v. Former Partner: Investigation of claim of "negotiating in bad faith". Involved analysis of e-mail, documents and Internet activity surrounding the former partner's involvement with an outside organization.

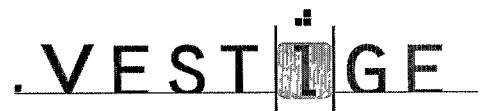


EXHIBIT D

CV FOR DONALD WOCHNA  
CHIEF LEGAL OFFICER  
VESTIGE, LTD





**Present Position**

**Chief Legal Officer**  
Vestige Digital Investigations  
Medina, Ohio

- Using teams comprised of forensically trained trial attorneys and computer experts, Vestige Ltd. provides attorneys with computer forensic services to extract, preserve, analyze, and present evidentiary data resident on electronic media in civil and criminal matters.
- Write articles, lectures, and consult in the area of search and seizure of electronic evidence in criminal and civil matters and general computer science issues.

**Experience**

**Chief Legal Officer**  
*Vestige Digital Investigations*  
March 2004, Medina, Ohio

- As the result of the merger of CI&E and F1, Ltd., I am the Chief Legal Officer of Vestige, Ltd. Provide computer forensic and legal analysis for Computer Analysis Teams assembled to image, extract, analyze and present evidence for our attorney clients.

**Chief Operating Officer**  
*Computer Investigation & Evidence*  
1998 – 2004, Hinckley, Ohio

- Founded Computer Investigation & Evidence, Inc. and negotiate license from Guidance Software to obtain and be certified in use of law enforcement software (Encase) to conduct forensic analysis of electronic media. Create search protocol for CI&E personnel, integrating legal requirements related to Rules of Evidence with unique character of electronic evidence. Establish testing protocol related to forensic tools to satisfy Daubert requirements.
- Test law enforcement forensic tools for accuracy and reliability to satisfy Daubert requirements.
- Prepare plan and requirements to initiate distributed computing paradigm for cpu-intensive forensic activities such as brute force password cracking or encryption de-coding.
- Prepare plan and incorporate procedures related to steganography and anti-forensic software, such as BC Wipe, Evidence Eliminator.
- Conduct on-going tests of the efficacy of anti-forensic software.
- Monitor state and federal judicial decisions and case law related to computer forensic issues, and to the search and seizure of computer evidence in criminal and civil matters. Revise CI&E protocol to reflect any changes.

## **Donald A. Wochna, Esq.**

---

- Create and maintain educational seminar for judges and attorneys related to the legal challenges to manage computer generated and computer stored information. Includes real time response to unauthorized computer access, computer files as evidence, and control of electronic data.
- Maintain membership and participate with CASPR\_ITCRIME Workgroup, part of the CASPR Project aimed at formulating Commonly Accepted Standards and Practices in Information Security. This workgroup concentrates on standards and practices relating to Computer Crime Prevention, Investigation, Forensics, and Digital Evidence.
- Participate in CFTT, Computer Forensic Tool Testing, a group dedicated to ensure that tools used by computer forensic examiners are providing accurate and complete results.
- Member Metropolitan Crime Clinic, a compendium of private and public law enforcement agencies organized to share information related to electronic crime
- Member Northern Ohio Information Technology Roundtable, an organization sponsored by the United States Secret Service, to share information related to technology issues and crime
- Participate in NOITR Electronic Crime Task Force organized under the U.S. Patriot Act

### **Chief Operations Officer**

*Lien Priority Insurance Agency*

1992 – 1998, Hinckley, Ohio

- Created Lien Priority Insurance, a financial service product underwritten by Great American Insurance Companies, that insured the proper perfection and priority of security interests in personal property anywhere in the United States. Developed the expert system computer programming using Borland's Dbase, to process, track, underwrite, and service LPI products delivered on an electronic network to end users comprised of lenders, attorneys, title insurance agents, and lessors. Created the marketing and distribution channels in the insurance and legal fields to bring LPI products to clients and provided the legal services support. Revised and updated the processing software to reflect changes in Article 9, filing offices, and judicial decisions

### **Partner, Attorney-at-Law**

*Baker & Hostetler*

1989 – 1992, Cleveland, Ohio

Partner in the Commercial Law, Bankruptcy Practice Area. Responsible for the proper, timely, and cost-effective handling of workouts, bankruptcies, and litigation. As part of the Revco bankruptcy team, successfully litigated the approval of a



Curriculum Vitae of

**Donald A. Wochna, Esq.**

---

- computerized point of sale system; implemented a litigation settlement strategy with the Creditors' Committee that saved the estate 39 million dollars, and the creation and implementation of a tax enhanced, self insured insurance program with off-shore reinsurance treaties.

**Associate, Attorney-at-Law**  
*Thompson, Hine & Flory*  
1983 – 1989, Cleveland, Ohio

**Juris Doctorate**  
1983, University of Chicago, Illinois

**Publications and  
Seminars**

- "Introducing Computer Forensic Files as Evidence in Civil Actions", Akron Bar Association's Law Expo, November 6, 2001. Discussed the use of law enforcement software to create and use forensic computer files in civil litigation cases.
- "Legal Issues and Challenges to Attorney and Client Strategies To Control the Creation, Extraction, and Use of Information Intentionally or Unknowingly written and Stored in Computer Systems: Real Time Response To Computer Incidents, Forensic File Audits to Find Evidence, Electronic Document Retention to Control Data". Ohio State CLE Institute, "Beyond Fingerprints October 16, 25, 2002.
- "Your client has a Question—Can you identify the computer issue and not harm your Client's Interest. Ohio State CLE Institute, "Computers and the Law: What you Don't Know Can Hurt You", December 19, 2002
- The Computer As Storage Device for Evidence—Why the "File Cabinet" or "Library" analogy leads to bad advice and bad law. Ohio State CLE Institute, "Computers and the Law: What you Don't Know Can Hurt You", December 19, 2002
- Forensic Analysis of Computers—Access, Preservation, Analysis, Extraction, and Presentation of Evidence. Ohio State CLE Institute, "Computers and the Law: What you Don't Know Can Hurt You", December 19, 2002.
- Level the Playing Field—use of Computer Forensics in civil cases by small firms and solo practitioners to extract evidence. Tri-C Community College, Corporate College Campus, Westlake, OH, November 5, 2003.

Curriculum Vitae of

**Donald A. Wochna, Esq.**

---

- Computer Forensics for Criminal Defense Attorneys—responding to law enforcement's use of forensic analysis. Tri-C Community College, Corporate College Campus, Westlake, OH, November 10, 2003.
- Computers—What you Don't Know can Hurt You. Ohio State Bar Association, Continuing Legal Education Institute, Columbus, OH, November 21, 2003.
- Computers-What you Don't Know can Hurt You. Ohio State Bar Association, Continuing Legal Education Institute, Cleveland, OH December 3, 2003.
- Family law Section, Lake County Bar Association. Presentation on Electronic Discovery and Computer Forensics in Family law cases. March 12, 2004.
- Computer Forensic Evidence, Don't Go to Court Without It. Akron Bar Association. April 8, 2004
- Computer Forensics for Law Students. Cleveland State School of Law. Invitational Speaker. April 19, 2004
- Buckingham Doolittle Litigation Practice Annual Retreat. Salt Fork, OH. May 2, 2004.
- Computer Forensics: Non-Adversarial Discovery. Dayton Bar Association. May 14, 2004.
- Various presentations to law firms and bar associations.

**Expert Witness  
Experience**

*I have been qualified as an expert witness in the following civil and criminal court cases:*

- State of Ohio vs Johnathon Steele, Hamilton County Common Pleas Court, Case No. unknown, (testified at suppression hearing)
- State of Ohio vs. David Frankowski, Summit County Common Pleas Court, Case No. unknown, (testified at trial).
- State of Ohio vs. Bryan S. Sparks, Summit County Common Pleas Court, Case No. 2002-12-3669 (testified at trial)
- State of Ohio vs. Kiwala, Medina County Common Pleas Court, Case No. 03 CR 0180 (testified in discovery hearing)
- State of Ohio vs. Roger L. Tooley Jr., Portage County Common Pleas Court, Case No. 03 CR 155

**Donald A. Wochna, Esq.**

---

- Mancan, Inc. DBA Manpower vs. Martha Crowder, Stark County Common Pleas Court, Case No. 2003 CVO 1230 (testimony pending)
- Tracy Mayle, et al v. Reverend Timothy R. King, et al, Trumbull County Common Pleas Court, Case No. 03-CV-35 (testified at discovery hearing, appeared in chambers to assist Judge)
- Julie Luft Signer vs. Benjamin Signer, et al., Cuyahoga County Common Pleas, Case No. D286746 (testimony pending)
- Larry Diemand, et al v. Laurel School, et al. Cuyahoga County Common Pleas Court, Case No. 496578 (testimony pending)
- Predictive Maintenance Corporation vs. Insight Serviceco, Inc., U.S. District Court, Northern District of Ohio, Case No. 1:02 CV 335 (testimony pending)
- DirecTV, Inc., vs. Michael Baumgardner, U.S. District Court, Northern District of Ohio, Case No. 5:03-CV-01484-JG. (did not testify; case settled after defendant given CI&E analysis or personal computer).
- DirecTV, Inc. v. Eugene Karpinsky, United States District Court, Eastern District of Michigan, Southern Division, Case No. 02-73929 (testimony pending)
- DirecTV, Inc. v. Dale Bearden, United States District Court, Northern District of Texas, Fort Worth Division, Case No. 4:03-CV-375-Y (testimony pending).

*The following are samples of cases that I have been named as an expert, but the case is either pending, has settled outside of court or I have been a consulting expert and have not been disclosed. To protect the privacy of these cases, only generalities have been presented. I can provide further information, within the confines of any privacy issues and non-disclosure agreements, should you deem it necessary to gain further information.*

- Assist disciplinary counsel investigate attorney malpractice by analyzing office computer
- Assist Ohio municipalities respond to wrongful termination suit by analyzing former employee computer four years after leaving, and after computer had been reformatted and placed into service with a different person.
- Assist Ohio safety services investigate potential wrongful use of computer equipment.
- Assist mortgagor to compel mortgagee identify all relevant computers used to create, store, process data relevant to loan in conversion and wrongful foreclosure action

Curriculum Vitae of

**Donald A. Wochna, Esq.**

---

- Assist company investigate unlawful copying of proprietary files immediately before former key employee left company to work for competitor
- Assist corporate official respond to allegations of child pornography by using computer data to prove pornography loaded onto computer on dates when official did not have possession of machine.

## Exhibit E

## Hypothetical Case and Cost Estimates

By way of example, a typically large engagement could be conducted as follows<sup>vi</sup>:

Assume Plaintiff and Defendant have, between them, identified 200 of their respective employees whose depositions were to be taken or who likely had information related to the hypothetical dispute. For each employee, the parties requested documents, including electronically stored information comprised, inter alia, of all communications (email, instant messages, memos, etc, whether deleted or not). Each employee had a computer and the parties, therefore, desired to interrogate 200 computers and four network servers used by these employees. Both parties were concerned that asking all 200 employees to search their computers would be wasteful because (1) such a search would necessarily be limited to the data visible to the operating system—thus no instant messages would be found, nor would any deleted data be accessed; (2) a protocol would have to be created to assist each employee identify responsive documents, and the accuracy of response could not be controlled using all 200 employees; (3) the disruption associated with searching all computers and servers was significant.

Vestige would assist the parties by suggesting the following strategy:

To minimize the downtime, Vestige would suggest that it perform the following services from 6:00 pm to 4:00 am each night for four consecutive nights;

- a. A Vestige Computer Analysis Team would create a forensic “clone” of each of the 200 computers and 4 network servers. A forensic clone is simply a hard drive on which has been written an exact copy of all visible and invisible data on the subject computer.
- b. On average 50 computers were estimated to be “cloned” each night
2. Once all the computers were cloned, the 200 clones would be mounted on a special laboratory computer and, using special software, electronically searched for data responsive to the discovery request. The searches would be conducted on all clones simultaneously, for all responsive data. Searching software automatically would identify all visible and invisible responsive data on all clones.
3. Estimated Cost of creating clones of 200 computers and 4 network servers would be approximately: \$60,000.00-\$80,000.

Computer forensic software and protocols have advanced so significantly in the last five years, that each clone is embedded with a “digital fingerprint” that ensures the clone is an exact copy of the subject media. The digital fingerprint guarantees the accuracy and authenticity of the clone. Moreover, the creation of the clone “freezes” all the data (visible and invisible) in all the physical areas (allocated and unallocated) of all types of media and devices.



## ENDNOTES

- 
- <sup>i</sup> We have appended to these comments two articles that Donald Wochna has written regarding the Non-adversarial nature of computer forensic analysis (Exhibit A), and the ineffectual use of Requests for Production of Documents (Exhibit B). We have also included our CV (Exhibits C and D).
- <sup>ii</sup> Vestige Ltd., for example, is licensed to use Encase software, a computer forensic tool currently used by over 14,000 law enforcement agencies around the world.
- <sup>iii</sup> See Exhibit E for hypothetical case, involving 200 computers and servers, and breakdown of estimated time and costs.
- <sup>iv</sup> If there is any doubt in the minds of any member of the Committee of the ease with which visible and invisible data, resident on several different electronic media, can be simultaneously searched for relevant data, Vestige Ltd would gladly demonstrate this capability.
- <sup>v</sup> However, if there is a sufficient need to be able to recover overwritten data, the firms such as Vestige Ltd will develop the technology and deliver the capability to read overwritten data
- <sup>vi</sup> Cost estimates do not include cost of media nor costs related to archiving forensic images

