`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2023

Technology Track – Session 6

Digital Forensics for the Digitally Fearful

Presented By:
Brett Burney, Burney Consultants, Cleveland, OH
Matthew Stippich, Digital Intelligence, Milwaukee

About the Presenters...

Brett Burney helps law firms and corporate legal departments navigate their e-discovery challenges as the VP of eDiscovery Consulting at Nextpoint Law Group and the eLaw Evangelist at Nextpoint software. Brett's passion lies in educating lawyers and legal professionals on the duties and responsibilities around collecting, reviewing, and producing electronically stored information. Brett served as the Chair of the 2015 ABA TECHSHOW Planning Board and regularly speaks around the country to lawyers and legal groups on a wide variety of technology-related topics. You may contact him at bburney@nextpointlawgroup.com.

Matthew J. Stippich is an owner, General Counsel and President of Professional Services for Digital Intelligence, an industry leader in providing digital forensic and eDiscovery equipment, training and services. He advises, implements and performs ESI strategies for clients ranging from emerging growth companies to Fortune 100 companies, law firms and government agencies with a focus on managing costs associated with the preservation, searching and production of ESI as well as internal investigations. Mr. Stippich works extensively with corporate legal and IT teams to develop proactive best-practices for managing ESI issues associated with litigation, employment and security events. Past projects have included developing and implementing ESI strategies in response to SEC and US DOJ investigations of potential FCPA violations across more than 40 countries. Among other civic activities, Mr. Stippich currently serves as Alderman for Wauwatosa's 1st District. Mr. Stippich Frequently writes and speaks on topics related to e-discovery and digital forensics. He is a Charter Affiliate Member of the Association of Certified E-Discovery Specialists, and maintains a CEDS certification. He is also a partner in the Milwaukee based law firm of Stippich Selin & Cain, LLC. Mr. Stippich earned his undergraduate degree from Grinnell College and his J.D. degree from Marquette University.

State Bar of Wisconsin
Friday, October 20, 2023

Digital Forensics for the Digitally Fearful

Brett Burney
Vice-President, eDiscovery Consulting
2375 East Camelback Road, Suite 600
Phoenix, AZ 85016
bburney@nextpointlawgroup.com

Atty. Matthew J. Stippich
General Counsel / Pres. Prof. Services
1841 North Prospect Avenue
Milwaukee, WI 53202
Direct (414) 420-2120
mstippich@di4n6.com

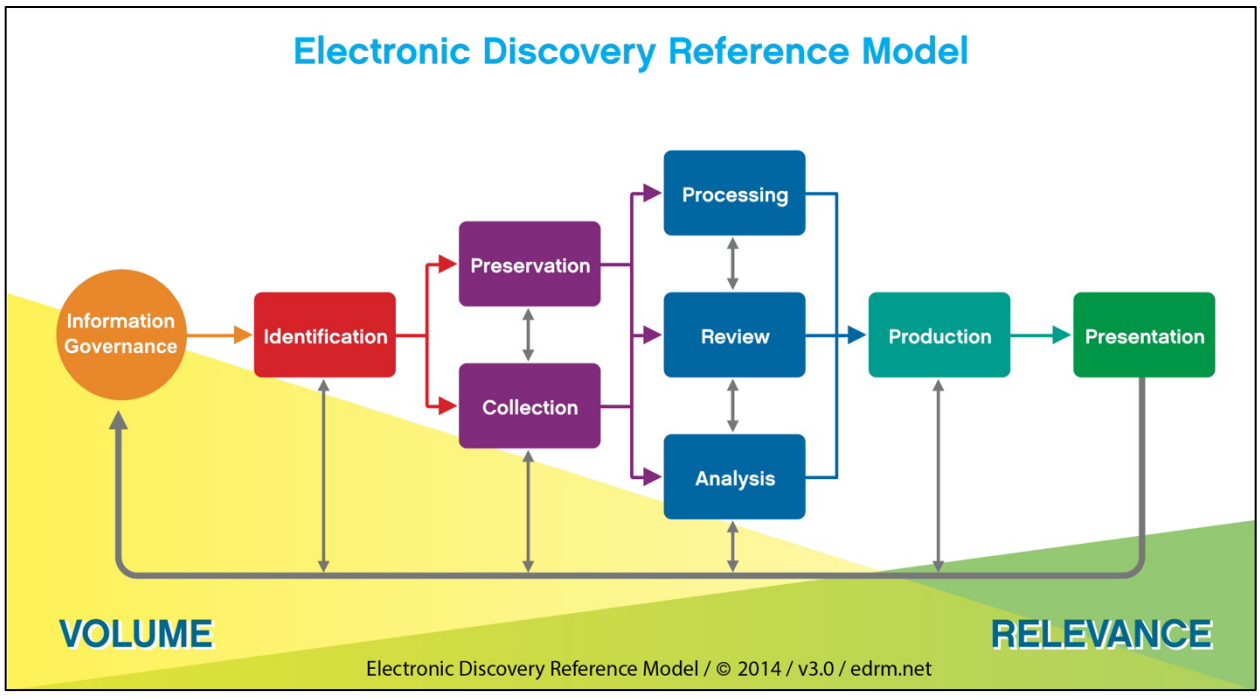
I. Background

A. Not every case requires the use of computer forensics professionals, but when computer systems and data must be preserved for litigation purposes, it's imperative to employ professional help as soon as possible.

B. Computer forensics can be scary – professional examiners can literally scrape information from your computer about e-mails you've sent, websites you've visited, and old documents you thought you deleted. This session will inform you what computer forensics professionals can do for you and your client, and also help you obtain the electronic evidence you need from the other side.

C. The Electronic Discovery Reference Model (EDRM)

In 2005, right when e-discovery first stared becoming a thorn in the side of many litigators, the Electronic Discovery Reference Model was developed to provide a visual construct for the "workflow" involved with e-discovery in litigation matters. The diagram serves as a cornerstone today for any conversation regarding e-discovery.



Each box represents a specific "phase" in e-discovery that carries certain duties and responsibilities. But also notice the yellow and green triangles in the background - they represent the concept that you will start off with a much larger volume of documents and information in the beginning which is whittled down to a smaller sub-

set through the entire process. Again, this is no different than what happens in traditional discovery.

In addition, take note of the multiple arrows that point back and forth among the boxes. The arrows are attempting to indicate that this entire process is iterative - i.e. that it's not a one-time process from start to finish. In many cases, there will be multiple collection phases, and multiple production phases. You may need to repeat certain steps in the EDRM depending upon the data collected or the demands of opposing counsel. The EDRM has been updated to place additional emphasis on Information Governance at the beginning of the diagram.

II. Differences Between Forensic Analysis and E-Discovery

A. Electronic discovery

1. Focuses on gathering potentially responsive electronic documents and data.

2. Interested in the message or content of the documents produced.

B. Computer Forensics

Computer forensics can be defined broadly or narrowly. But it is generally accepted that the science of computer forensics involves the identification, preservation, examination, and interpretation of magnetically-stored information (e.g. computer hard drives).

The identification phase does involve some technology, but it really begins at the physical level. Before you retain the services of a computer forensics professional, it's important to already have a good idea of which computers and/or external hard drives need to be copied or "imaged." The computer forensics professional isn't going to be able to help identify the key players in the litigation, but once they hear the facts of the matter, they can usually make some important suggestions as to where to look on the computer to find relevant electronic data.

Computer forensics essentially covers the following areas:

1. Autopsy of a document or data

2. Analyzes not only the what, but also the where, who, how and why

3. Scientific approach with defensible processes

4. Can be investigative in nature

5. May result in an opinion and/or expert testimony

6. Background, training and techniques should be closely scrutinized.

C. Electronic discovery should nonetheless utilize sound “forensic procedures”

D. There are three main types of data that can exist on a computer that can be evidence.

1. *Active Data*: Active Data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction.

2. *Archival Data*: Archival Data is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

3. *Latent Data*: Latent data includes deleted files and other non-logical data types such as memory dumps, swap files, temporary files, printer spool files, and metadata that can be retrieved. This data is generally inaccessible without the use of specialized tools and techniques.

One of the best types of evidence that can exist in all three types of data from above is the date and time stamps of the files themselves. Date and time stamps are recorded by Last Accessed Date, Last Modified Date, and Date Created. In some case date deleted is also possible.

E. **Deleted Information**. Most users have a basic understanding that a file is not "really" deleted when you press the delete key. In most situations, only the file entry in the File Allocation Table is altered, but the file "data" still exists until it is overwritten by another file. An analogous situation would be to remove the label from a VCR tape when you're finished viewing the program that you recorded. The information is still on the tape and will remain there until you decide to record a new program.

1. *The delete myth*. Most users have a basic understanding that a file is not "really" deleted when you press the delete key. In most situations, only the file entry in the File Allocation Table is altered, but the file "data" still exists until it is overwritten by another file. An analogous situation would be to remove the label from a VCR tape when you're finished viewing the program that you recorded. The information is still on the tape and will remain there until you decide to record a new program.

2. *The delete myth #2*. Not all deleted information can be retrieved. (see above regarding Volitility of data).

3. Deleted electronic data is fully discoverable. *Dodge, Warren and Peters Insurance Servs. v. Riley*, E031719, 2003 WL 245586 (Cal. App. February 5, 2003); see also *Simon Prop. Group LP v. my Simon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000) ("Computer records including records that have been 'deleted' are documents discoverable under Fed. R. Civ. P. 34").

F. **Unallocated Space**. Computer operating systems also routinely make backup copies of documents or drafts without the user's knowledge to allow recovery in case of a power failure or other incident that might result in lost work. Microsoft Windows-based computer operating systems utilize a special file to write data when additional random access memory is needed. In Windows, Windows 95 and Windows 98, these are called Windows Swap Files. In Windows NT and Windows 2000 they are called Windows Page Files, but both have very similar characteristics. Swap files are potentially huge (20 million to 200 million bytes) and most computer users are unaware of their existence. These files can contain remnants of word processing files, e-mails, Internet browsing activity, database entries and almost any other work that may have occurred during past Windows work sessions. Windows Swap Files can actually provide access to information that was not intended or expected to be saved.

G. Threshold required for use of forensic analysis

III. PRESERVATION OF DATA

A. Forensic preservation vs. forensic analysis

Preservation is the most important job of a computer forensics professional. The main reason one calls a computer forensics professional is to ensure that sensitive and relevant data on a computer is protected against accidental or unauthorized deletion (spoliation). Preserving the electronic data for future examination is the ultimate goal of every computer forensics project.

"The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Zubulake v. UBS Warburg*, (Zubulake IV) 220 F.R.D. 212 (S.D.N.Y. 2003) The role of a computer forensics professional helps an attorney appropriately accomplish the duty to preserve relevant evidence when it is located on individual computers. While the Zubulake IV opinion states that a party is obviously not required to preserve "every shred of paper or e-mail," they must actively preserve important, relevant data that may easily be found "hiding" in computers. While it may not be easy for a non-technical person to find "hidden" information in a computer, a skilled computer forensics professional can quickly and easily discover many details that are not readily apparent to a normal computer user.

B. **Chain of custody**. A process for demonstrating data integrity from preservation/collection to production.

C. Failure of Proper Preservation. The failure to utilize proper preservation methods can lead to:

1. Loss of data
2. Alteration of data
3. Challenge to data integrity

D. Method of Preservation

1. *Forensic backup*. A forensic copy (also referred to as a "mirror copy", "image" or "clone") involves the process of a bit by bit copy of all data on a storage device. A forensic backup is typically recommended because it will preserve all potentially relevant data.
2. *File Based Backup (logical image).* File based backup involves the identification, selection and preservation of specific files or folders on a file system. Current technologies allow a file based backup that preserves the integrity of the data. Unallocated space, deleted files, etc. are not preserved with a file based backup method.
3. *Ghost Images.* Ghost is a type of back-up utility that will create a "backup" of the files on the system and store the disk "image" in a proprietary format. While Ghost can be configured to create a full forensic image, the default configuration only copies active file data.

E. Common Mistakes

In civil litigation, computer forensics professionals are routinely called upon to ensure that electronic evidence is pristinely preserved, and then to retrieve relevant evidence from the images of the hard drives. Both parties to a civil litigation have to understand, however, that they are must engage in several balancing acts in regard to the hard drive images. For example, taking the hard drive out of a computer renders the computer useless, and so it can be a crippling situation for someone's business to image the hard drive during working hours. Additionally, many computer hard drives will contain a vast mix of both personal and business-related information. While an opposing party may have a right to see the business-related data, precautions must be taken so that non-relevant personal information is adequately protected. Common mistakes include:

1. ***Searching before preserving:*** The first and most important thing to remember is to NOT TOUCH a computer that you have determined must be imaged to preserve the data it holds. Electronic data is very

volatile and although it can remain in a fixed state for a long time (i.e. on a backup tape, hard drive, etc.), it is possible to change many files just by turning on the computer. It's always tempting to turn on a computer just to get a "quick peek" at the contents; but in so doing, relevant information can be erased or modified. The best thing to do is keep the computer turned off and physically secured, and call a computer forensics professional as soon as possible.

2. ***Failure to utilize a complete preservation***: A skilled computer forensics professional understands more than just how to push a button on a software package – they have studied the intricate details of how data is saved, organized, and managed on a computer. Computer hard drives allocate space for data based on very logical rules. It's important to understand the intricacies of how the technology works in order to know where to look for deleted data - which usually turns out to be where the juiciest and most revealing information is found. Terms like "slack space" and "unallocated space" are regularly mentioned in regard to the "hidden" areas of the hard drive where computer forensics professionals commonly find old, deleted information.

IV. FORENSIC ANALYSIS: UNDERSTANDING THE POSSIBILITIES

Examination and interpretation are important in communicating what is found on a computer to attorneys. A computer forensics professional will examine the data collected from a computer with the goal of retracing the steps of the computer user. The goal of this phase is to “give voice” to the digital evidence that exists on computers and digital devices. The following are some examples of digital forensic methods:

A. **Registry Analysis**. The windows registry is a database that stores settings and options for the operating system, hardware, software, users and preferences on a particular operating system. Information that may be retrieved from the registry include:

1. List of hardware and devices connected to the computer.
2. User preferences
3. Application and Internet history

B. **Internet Cache**. Browser caches and Internet caches store copies of Web pages retrieved by the user for some period of time in order to speed up retrieval the next time the same page is requested. This information may be maintained in a quasi-active state for extended periods of time, depending on the software settings on the computer. Deleted internet cache can be

recovered. Examples of information that can be discovered through internet cache include:

1. Internet activity (unauthorized use, intranet activity, etc).
2. Web based mail
3. Online chats
4. Evidence of theft of intangibles

C. **Data Carving**. Data carving involves the process of searching and extracting data from a storage device (typically from unallocated space) that may no longer be recognized through the file allocation table. Data carving may result in full or partial pieces of files that can then be reconstructed or analyzed. Data carving is often thought of as an advanced level of deleted data recovery. Types of cases where data carving is useful includes:

1. Carving for web based email
2. Carving for documents that may have been deleted or altered
3. Carving for html document to show internet activity
4. Carving for specific data strings or content
5. Carving for images

D. **Event Logs**. Event logs track or receive information related to "major events" that may occur on a computer system. Depending on the type of system or system configuration, event logs may contain detailed information that can demonstrate user activity. Event logs may not be known by a user or system administrator (default settings), and may be turned off completely to increase efficiency of a system. Types of data that can be recovered from event logs include:

1. Show changing of clock – alteration of dates/times on documents
2. File activity on a file server
3. System access to a computer network
4. Application activity

E. **Wiping Programs**. The process of obliterating data on a storage device by writing or overwriting data on the device. Systems may commonly be wiped to remove sensitive information. Wiping may demonstrate activity intended in destroying or hiding information.

1. Presence in registry
2. Case law
    a. *Arista Records, LLC v. Tschirhart*, 2006 WL 2728927 (W.D. Tex. Aug. 23, 2006). Court entered default judgment as

discovery sanction where forensic evidence showed that defendant deliberately used “wiping” software to permanently remove data from her hard drive and stated: "The sanction in the present case is to deter other defendants in similar cases from attempting to destroy or conceal evidence of their wrongdoing."

b. *Anderson v. Crossroads Capital Partners, LLC,* 2004 WL 256512 (D. Minn. Feb. 10, 2004). Plaintiff's use of Cyberscrub data wiping software prior to court-ordered inspection of her computer and after agreeing on the record that she would not purge her hard drive or delete any documents, and her misrepresentations about age of hard drive, were not sufficiently egregious to warrant dismissal but did warrant an adverse inference instruction

F. Detecting Data Hiding Techniques

1. *Steganography*. The process of hiding data within other data. Commonly used for hiding contraband within innocuous documents.

2. *Use of removable media.* Removable media will commonly be connected to a computer system to either move, remove or store information. Without an directed examination of the specific computer system, this activity may go undetected.

3. *Password protection.* Use of password to prevent access and/or modification of a file or system.

4. *Encryption.* May include one of multiple methods for encoding electronic data so that it can only be opened or viewed with knowledge of the encryption method and/or key.

G. **Metadata**. Metadata is data about data. Typical metadata may include:

1. Date and time information related to when documents were created, last saved, printed, edited, etc.

2. Applications may maintain application specific metadata (photo information, document editing time, author, etc.)

3. Metadata may also provide insight as to information that has been manipulated in a document.

4. **File System (external) Metadata.** Information stored by the file system typically for management of the files on the computer system. Types of information may include: CREATED DATE/TIME, LAST ACCESSED TIME/DATE, LAST MODIFIED TIME/DATE.

5. **Host File (internal) Metadata.** Type of metadata is dependent on the computer application used. Typical fields may include: AUTHOR, CREATION DATE, EDITING TIME, DOCUMENT TEMPLATE, CUSTOM FIELDS, APPLICATION NAME, FILE TYPE, ETC.

V. Benefits of Early Case Assessment

A. Pre-Preservation Assessment / Scoping

1. What type of information will be relevant to the dispute?

a) **Background**: Types of discoverable information[1]

(1) *Active Data*. Active Data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction.

(2) *Archival Data*. Archival Data is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

(3) *Backup Tapes.* Backup of data not specifically organized for retrieval of individual documents or files.

(4) *Latent Data*. Latent data includes deleted files and other non-logical data types such as memory dumps, swap files, temporary files, printer spool files, and metadata that can be retrieved. This data is generally inaccessible without the use of specialized tools and techniques.

b) **Assessment**. Early in the litigation process, it is important to determine what information would be relevant and responsive based upon the merits of the case, and what is known about the claims. Potential data sources will vary depending on the nature of the case. FOR EXAMPLE:

[1] *Zubulake I* broke down electronic data into five categories outlined in this section. *Zubulake v. UBS Warburg* ("*Zubulake I*"), 217 F.R.D. 309, 321-322 (S.D. N.Y. 2003). The Sedona Conference has extended these categories to 12 "complexity" factors that identify the relative complexity of accessing such information.

(1) Employment (sexual harassment, wrongful termination, discrimination, etc.)

(2) Business disputes (contract formation, theft of trade secrets, unfair competition, etc.)

(3) Family law (divorce, T&E, custody, etc.)

(4) Intellectual property

(5) Personal injury

(6) Malpractice

(7) White collar crime

2. Tools to Identify Potential Locations

a) ***Federal Rule 26(f) (and Form 35)*** – ***Meet and Confer /*** Wis. Stat. 804.01(e) – Limitations on Discovery (Confer Requirement).

(1) Consistent with past practice, meet and confer (Rule 26(f) conference) must be held at least 21 days before a scheduling conference under Rule 16(b). The parties must "discuss any issues relating to preserving discoverable information." Note that this discussion does not trigger the obligation of preservation – such obligation arises much earlier. See discussion of preservation below.

The parties must also develop a proposed discovery plan that includes: "any issues relating to disclosure or discovery of electronically stored information including form or forms in which it should be produced" and "any issues related to claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to include their agreement in an order."

b) PRACTICE TIPS:

(1) 804.01(e) and 26(f) conference provides an opportunity for a well-informed attorney to establish preservation and production standards that can manage client costs.

(2) To narrow scope, propose time constraints (based on technical issues as well as case specific factors), keyword search processes, form of production.

(3) To expand scope, consider testing procedures, use of neutral party and cost-shifting proposal.

(4) The Wisconsin Supreme Court Note to 804.01(e) states that, "The rule ***does not require parties to confer before commencing discovery under ss. 804.05 (Depositions upon oral examination), 804.06 (Depositions upon written questions), 804.08 (Interrogatories to parties); or 804.11 (Requests for admission).*** These discovery devices, if employed before serving a request for production or inspection of electronically stored information, may lead to more informed conferences about the potential scope of such discovery." This is commonly referred to as "discovery about discovery."

c) ***30(b)(6) Deposition (Wis. Stat. 804.05(2)(e)).*** If IT personnel are not involved in the meet and confer conference, the 30(b)(6) / 804.05(2)(e) deposition can be one of the most effective ways to obtain an understanding of the potential sources of discoverable information. This can also be effectively used to demonstrate justification for a motion to compel (see case examples).

d) ***Interrogatories.*** See sample interrogatories.

B. UNDERSTANDING POTENTIAL INFORMATION SOURCES

1. DESKTOPS AND LAPTOPS

a) **Type of data**. Desktop and laptop computers will often be the best source of electronically stored information. These machines not only contain the most "active" data for the particular custodian, but will also contain residual data (deleted files, etc.) in the hard drive's unallocated space. Undoubtedly, computers of key custodians should be preserved.

b) **Type of case**. Virtually any.

c) **Cost of preservation**. Forensic preservation of a computer/laptop hard drive can typically be accomplished for $150 - $500. Factors that will impact the price of preservation include:

i. Size of the hard drive

ii. Age of the hard drive

iii. Working vs. non-working drive

iv. File/folder backup vs. forensic backup

d) Other considerations.

i. Due to the relatively low cost of preserving electronic data on a laptop/desktop computer, it should be done by an expert that can testify as to process and chain of custody.

(1) Laptop/desktop computers are a frequently used storage device. Therefore, data is changing continuously on these machines. Early preservation of these machines will ensure maximum retention of file information as well as unallocated space.

(2) Do not forget about on-going preservation.

(3) Depending on the nature of the case, it is possible to perform a file or folder specific preservation. Time required to locate and segregate the specific data must be considered.

(4) Does the responding party utilize Citrix, terminal services, or other type of system that would prevent data from being stored locally.

2. SERVERS

a) **Type of data**. A server is part of a network of computers that controls access to particular shared resources. The following are typically server types:

(1) *Mail server*. Microsoft Exchange Server, Lotus Notes Server, etc.

(2) *File server*. Will typically contain individual user storage areas as well as group file repositories.

(3) *Application server*. In larger enterprises, separate applications (SAP, Peoplesoft, Oracle, etc.) may be operated on separate servers. Depending on the nature of the case, this application server data may be relevant and necessary to preserve.

b) **Type of case**. Due to the ease of implementation, it is common that a server will exist in any situation where multiple users need to collaborate and share applications, data or otherwise.

c) **Cost of preservation**. Unlike backup tapes, server data does not generally need to be "restored" or reprocessed to complete the preservation process. Preservation of server data may be more time consuming and costly than desktop/laptop computers due to the size of the storage typically attached to a server. Factors that will impact the cost of preserving server data include:

(1) Size of server

(2) Ability to have exclusive connection to server (vs. continued operation of server)

(3) Whether a complete preservation will be performed vs. file/folder specific preservation

(4) Server operating system

d) Other considerations.

(1) In addition to the actual information included in the "documents", a server may maintain "server logs" that detail user activity, access, etc.

(2) Scope of collection

(3) Forensic vs. file based production

(4) Amount of data relative to issue in question

e) Cases

(1) *Tilberg v. Next Mgmt. Co.*, No. CIV.04-7373, 2005 U.S. Dist. LEXIS 24892, at *2-4 (D.N.Y. Oct. 24, 2005). The Court allowed the employee full access to search the employer's e-mail server, central server, and individual workstations.

3. BACKUP TAPES

a) **Type of data**. Backup tapes can be useful is certain cases because the tapes may contain an historical preservation of data. Backups are often performed on a systematic or periodic basis, thus potentially providing a timeline of active data. Types of backups include the following:

(1) *Full backup*. A complete backup of a particular data source as of a particular date. If a full backup is performed weekly on an a file server, this backup should contain ALL active files from the specific server as of the date of the backup. The backup will not typically contain files deleted prior to the backup.

(2) *Incremental backup*. Due to the storage space and time required to make frequent full backups, companies will often implement an incremental backup procedure. An incremental backup starts with a baseline "full backup". Each incremental backup includes only those files changes between the last incremental backup and the current

incremental backup. While an incremental backup can save time when the backups are created, restoration can be time consuming. **PRACTICE NOTE:** if a party utilizes an incremental backup procedure, a complete set of the backup tapes will be required to ensure complete preservation. Restoration/analysis can be costly.

(3) *Selected file backup*. As the name suggests, a selected backup is performed on specific files of folders. This type of backup is typically done "on-demand". On-demand backups may also be performed by individual users to backup a completed project, desktop computer, etc.

b) **Type of case**. Backup tapes are typically at issue in larger civil cases; however, backups may exist in virtually any case. Possible uses of backup tape data may include:

(1) To demonstrate deletion, modification or spoliation of data

(2) When "active data" does not represent a complete set of relevant and responsive data for the time period

c) **Cost of preservation**. Backup tapes can either be "preserved" by pulling a set of tapes from normal backup rotation or by creating a restoration/copy of the data. Recovery and analysis of data from backup tapes can be costly. Pricing for processing tapes can range from $500 to $5,000 per backup tape, depending on the following factors:

(1) Availability of hardware for restoration of tapes

(2) Size of tape storage

(3) Level of analysis required

d) **CAUTION:** Before agreeing to a preservation process, you must understand the type and contents of the backup. A set of backup tapes from an incremental backup rotation may not include a complete set of data.

e) Other considerations.

(1) Before requesting backup tapes, consider how they will be restored/processed

(2) Residual data (unallocated space) is not transferred to backup tapes. (Note: some backup software such as Ghost can be configured to capture residual data).

(3) Sampling of larger backup sets may be advised. See *McPeek v. Ashcroft* (McPeek I), 202 F.R.D. 31 (D.D.C. 2001)

f) **Basis for production**. Backup tapes by their very nature contain archival data that is not immediately accessible. Production/preservation is therefore more costly and time consuming. Rule 26(b)(2) will likely be looked to in determining whether backup tapes should be preserved and produced. Rule 26(b)(2) builds on a two-tier structure of discovery scope suggested in Rule 26(b)(1), applying the structure to the burden of discovery of electronically stored information. In essence, a party must provide discovery of relevant reasonably accessible electronically stored information without a court order, but a party need not review or provide discovery of electronically stored information that it identifies as not reasonably accessible. If the requesting party moves for discovery of purportedly inaccessible information—the second tier—the responding party must show that the information sought is truly not reasonably accessible. The court would then balance the burden or expense of the proposed discovery against its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery, in resolving the issues as set forth in Rule 26(b)(2)(i), (ii), and (iii).

g) Objections to production

(1) Cost and burden

(2) Duplication of active data

h) Cases

(1) *McPeek v. Ashcroft* (McPeek I), 202 F.R.D. 31 (D.D.C. 2001). The court found that retrieval of specific records from computer backup tapes was not within the ordinary and foreseeable course of business, but ordered the restoration of a small sample of the backup tapes to determine whether the backup tapes contained relevant discoverable information not available from any other source.

(2) *Hagemeyer North American Inc. v. Gateway Data Sciences Corp.,* 224 F.R.D. 594 (E.D. Wis. 2004). In a commercial dispute between two corporations, deposition testimony of one of the defendant's top executives indicated that computer backup tapes might contain e-mail files and accounting records. The plaintiff moved for production of the backup tapes, which had already been

made available as part of a larger, virtually unfettered warehouse production of all of the defendant's business records, and upon which the plaintiff had already performed some cursory searches, resulting in no relevant documents. The court refused to compel production of all the backup tapes without a more substantial showing of a likelihood that responsive documents would be found. Adopting the approach of *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), the court ordered the defendant to restore three sample backup tapes and for the parties to make additional submissions on the benefits and burdens of the proposed discovery, based on the results. The court also announced that it would adopt the factors set out in *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) to consider whether costs for any further production should be shifted to the plaintiff.

(3) *Byers v. Ill. State Police*, 2002 WL 1264004, 53 Fed.R.Serv.3d 740 (N.D. Ill. 2002). Plaintiffs in sex discrimination suit moved to compel defendants to produce email stored on backup tapes created daily over an eight-year period. Based on the cost of the proposed search and plaintiffs' failure to establish that the search would likely uncover relevant information, the court concluded that plaintiffs were entitled to the archived emails only if they were willing to pay for part of the cost of production. 2002 WL 1264004, at *12.

(4) The court thus granted plaintiffs' motion to the extent they would bear the cost of licensing the email program no longer in use by the defendant but required to read much of the requested email. The defendant would continue to bear the expense of its review for responsive documents and for privileged or confidential material. Id. It was expected that requiring plaintiffs to share in the cost would provide them an incentive to narrow their requests.

(5) *Williams v. Spring/United Mgmt. Co.*, 230 F.R.D. 640, 650 (D. Kan 2005). The court ruled that metadata was discoverable and in dicta noted that residual data may also be discoverable depending on the circumstances of the caser.

4. OFF-SITE/THIRD-PARTY STORAGE

a) **Type of data**. Often the electronic data that is sought will reside with an outsourced third-party. This is quite common with large entities that outsource their IT function. It is becoming more common for small business that are large enough to justify a full-blown internal IT

infrastructure. Any data that may be found on a server may be outsourced to a third-party. Email is another example of off-site storage (AOL, Yahoo, Hotmail, etc.).

b) Type of case. Any dispute has the potential to include third-party/off-site storage. Particularly interesting cases may include:

(1) Employee use of web-based email

(2) Spouse use of web-based mail

(3) Investment accounts

(4) Activity on internet accounts (travel agent sites, eBay, Google, etc.)

(5) ASP based services

c) **Cost of preservation**. The cost of preserving off-site storage will vary, depending on the type of data that is sought. Typically the large scale outsourcing of IT functions will result in a preservation process that is similar to preservation in-house. The servers and applications are typically dedicated to a single business entity or user. Small and medium sized outsourcing can be more difficult because the data that is sought is commingled with other user data.

d) Other considerations.

(1) Amount of data to be processed

(2) Commingling of data

(3) Need to comply with third-party processes

(4) Need to obtain subpoena for non-party production

(5) Ability to freeze or close account by mutual agreement

5. PORTABLE PHONES AND DIGITAL ASSISTANTS

a) Type of data.

(1) Email

(2) Personal contacts

(3) Calendar information

(4) Documents

(5) SMS Messages

(6) Phone activity

b) Type of case.

(1) Theft of IP.

(2) Divorce/family law

(3) Employment harassment

c) **Cost of preservation.** Depending on the level of data extraction required, preservation and analysis of phones and PDAs can be expensive relative to the amount of data. Often proprietary hardware, tools and/or software may be required to preserve data from the device. As with most devices, the method of preservation will be dictated by the facts of the case. Often (with PDAs), the data will reside in another location (the computer).

d) Other considerations.

(1) Replication of data

(2) Agreement regarding contesting collection process

(3) Volatility of information

e) Cases

(1) *Mathias v. Jacobs*, 197 F.R.D. 29 (S.D.N.Y. 2000), *vacated on other grounds*, 197 F. Supp. 2d 606 (2001). Court ordered production of a Palm Pilot where defendant had requested production of calendars, electronic organizers, schedules, diaries, etc. from the plaintiff.

6. OTHER MEDIA

a) ***Thumb drives***. A small, lightweight, USB-based, removable storage device. May store multiple gigabytes of information on a single device.

b) ***CD/DVDs***. Often overlooked, but may contain periodic user backups of data.

c) ***Removable hard drives***. May contain periodic user backups of data. Connection of device to computer will typically be tracked within registry.

d) ***Voicemail***. Often overlooked, but may be relevant. Preservation of system may require traditional data preservation or transcription.

e) ***GPS.*** Depending on the nature of the case, GPS data from an automobile, phone, PDA, etc. may provide relevant information. Collection methods from these devices are not standard, and may require proprietary software and/or hardware.

f) ***Copier/printer***. Many modern copiers and printers contain an internal storage device to speed the copying process. Images of the

pages to be printed are stored temporarily, and may be recovered in certain situations.

g) ***Digital cameras***. Memory from digital cameras are similar to other mass storage devices. They may contain active and latent data that indicates what images were on the memory device.

h) ***iPod/portable music players***. When connected to a computer, these devices can act as a portable hard drive or storage device. More frequently, we are seeing these devices used to copy data from a computer system.

7. METADATA - Metadata is defined as data about data. Typical metadata may include:

a) ***Date and time information*** related to when documents were created, last saved, printed, edited, etc.

b) Applications may maintain application specific metadata (photo information, document editing time, author, etc.)

c) Metadata may also provide insight as to information that has been manipulated in a document.

d) ***File System (external) Metadata.*** Information stored by the file system typically for management of the files on the computer system. Types of information may include: CREATED DATE/TIME, LAST ACCESSED TIME/DATE, LAST MODIFIED TIME/DATE.

e) ***Host File (internal) Metadata.*** Type of metadata is dependent on the computer application used. Typical fields may include: AUTHOR, CREATION DATE, EDITING TIME, DOCUMENT TEMPLATE, CUSTOM FIELDS, APPLICATION NAME, FILE TYPE, ETC.

VI. WHEN TO UTILIZE FORENSIC ANALYSIS: CASE EXAMPLES

A. Early identification of electronically stored information

B. Development of defensible strategy for collecting, analyzing and producing electronically stored information – effort to minimize scope and cost

C. Preservation and collection of data

D. Forensic analysis of data you control

1. No threshold required to permit analysis

2. Recovery of information may nonetheless contain information that is covered by privilege (employment situation).

E. Forensic analysis of data controlled by third parties

1. Forensic data not a presumed discovery deliverable
2. Must be showing that forensic data is relevant (i.e. bad faith, document manipulation, etc.).
3. Sneak peek/sampling
4. Court appointed special master

F. Use of Neutral Third Party. Increasingly, a third party will be engaged to facilitate electronic discovery. Under this process, the third party will preserve and then search the responsive data with terms or in accordance with a procedure agreed to by the parties. The results will then be tallied, and the responsive documents are first produced to the responding party for privilege review. A privilege log is created, and the responsive documents (less any privileged documents) are then turned over to the requesting party.

G. Cases

1. *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000). ***Held:*** Requesting party permitted to attempt to recover deleted computer files from computers used by the four named individuals, whether at home or at work. Requesting party to cover cost of analysis. Forensic expert was appointed as neutral officer of the court.
2. *Bro-Tech Corp. v. Thermax, Inc.,* 2008 WL 724627 (E.D. Pa. 2008). ***Held:*** no evidence of intentional violation of order by producers as would warrant full disclosure of forensic copies of hard drives.
3. *Scotts Co. LLC v. Liberty Mut. Ins. Co.*, 2007 WL 1723509 (S.D. Ohio 2007). ***Held:*** Federal Rules of Civil Procedure do not require forensic computer search as a matter of course.
4. *Orrell v. Motorcarparts of America, Inc.*, 2007 WL 4287750 (W.D. N.C. 2007). ***Held:*** former employer entitled to inspect plaintiff's home computer where plaintiff claimed she had forwarded offensive e-mails from co-workers to her home computer.
5. *Benton v. Dlorah, Inc.*, 2007 WL 2225946 (D. Kan. 2007). ***Held:*** finding that defendants did not sustain burden of showing that plaintiff had failed to comply with requests for production, plaintiff's hard drive contained any additional information subject to discovery, or that plaintiff had spoliated evidence and denying motion that plaintiff produce hard drive).
6. *Balfour Beatty Rail, Inc. v. Vaccarell*, 2007 WL 169628 (M.D. Fla. 2007). ***Held:*** plaintiff's request for defendants' computer hard drives denied, where plaintiff did not provide any information regarding what it sought to discover from the hard drives or make any

contention that defendants had failed to provide requested information contained on hard drives.

7. *Williams v. Massachusetts Mut. Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass. 2005). ***Held:*** plaintiff in employment discrimination suit not allowed to conduct forensic study of employer's electronically stored information in attempt to locate e-mail between company officials allegedly reflecting discriminatory practice and policy, where employer had already undertaken its own search and forensic analysis and had sworn to its accuracy, and employee provided no reliable or competent information to show employer's representations were misleading or substantively inaccurate.

8. *Ukiah Automotive Investments v. Mitsubishi Motors of North America, Inc.,* 2006 WL 1348562 (N.D. Cal. 2006). ***Held:*** where numerous financial statements were missing from responding party's computer records, court ordered responding party to produce computer on its own using an agreed-upon neutral inspector with expenses paid by producing party unless producing party produced information on its own.

9. *AutoNation, Inc. v. Hatfield*, 2006 WL 60547 (Fla. Cir. Ct. Jan. 4, 2006). ***Held:*** Forensic analysis permitted of third party computer.

In connection with its order granting temporary injunctive relief based upon the defendant's alleged theft of trade secrets, the court ordered the forensic inspection of a personal computer:

> Within thirty (30) days Hatfield unless and until further ordered by the Court, shall make Julie Anderson's personal computer available to AutoNation so its contents can be examined by a forensic computer expert to determine whether the emails Hatfield sent to Ms. Anderson's email address have been forwarded or otherwise altered or used, and to determine whether any other AutoNation material exists on the computer. The forensic expert is authorized to copy any AutoNation material on the computer, including the January 26, 2005 emails, and to then delete all AutoNation material from the computer. Hatfield and Anderson are authorized to have an independent forensic expert available and in attendance at the inspection.

10. *Advante Int'l Corp. v. Mintel Learning Tech.*, 2006 WL 1806151 (N.D. Cal. June 29, 2006). Motion for forensic examination of opposing party's computer hard drives denied where movant failed to provide any details about how the examination would be conducted and did not present specific, concrete evidence of concealment or destruction of evidence sufficient to justify the relief requested.

11. *Curto v. Med. World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006). ***Held:*** The magistrate concluded that plaintiff had not waived her right to assert the attorney-client privilege and work product protection with regard to any of the documents retrieved by defendants from the two laptop computers owned by the defendants (as employer of plaintiff), and directed defendants to return all such material.

In this opinion, the district court denied defendants' objections to a magistrate's discovery order which concluded that plaintiff had not waived any attorney-client privilege or work product protection as to documents originally created on (but subsequently deleted from) two employer-provided laptops.

Plaintiff had worked for the defendant ("MWC") out of her home office and was assigned company-owned equipment to use in her home, including company-owned laptop computers. Specifically, plaintiff was assigned a company-owned Macintosh ("Mac") laptop computer until May 2003, when she was told that she would be converting to a Dell laptop computer. As a result, plaintiff had her files from the Mac laptop transferred to the new Dell laptop. Prior to this transfer, plaintiff deleted her personal files from the Mac laptop, including notes and e-mails she had sent to her attorneys regarding this action. The Mac laptop was then returned to MWC.

In May 2003, plaintiff was assigned a Dell laptop computer to use in her home office. Plaintiff used the Dell laptop until she was terminated in October 2003, at which time she was instructed to return the Dell laptop to MWC. Before plaintiff returned it, she again deleted all personal files and written communications to counsel.

Almost two years later, MWC hired a forensic consultant to inspect the Mac and Dell laptops that were assigned to plaintiff. The consultant was able to restore portions of the computer files and emails that had been deleted by plaintiff. On July 1, 2005, MWC produced these restored documents to plaintiff's counsel. By letter dated July 8, 2005, plaintiff's counsel asserted that many of these documents were protected from disclosure by the attorney-client privilege and attorney work product immunity. Plaintiff demanded that the files be returned and not disclosed by defendants. When the parties could not resolve the dispute, MWC moved for an order to determine whether the documents were protected.

The magistrate began his analysis by noting that, while the voluntary disclosure of protected communications generally results in a waiver, inadvertent production does not waive the privilege unless the producing party's conduct was so careless as to suggest that it was not concerned with protecting the asserted privilege. To determine whether there had

been a waiver, the magistrate balanced four factors: (1) the reasonableness of the precautions taken by the producing party to prevent inadvertant disclosure of privileged documents; (2) the volume of discovery versus the extent of the specific disclosure at issue; (3) the length of time taken by the producing party to rectify the disclosure; and (4) the overarching issue of fairness. The magistrate added a further factor or "subfactor" - "whether or not there was enforcement of [any computer usage] policy."

As for the relevant four factors, the magistrate found that: (1) plaintiff had taken reasonable precautions to prevent inadvertent disclosure in that she sent the e-mails at issue through her personal AOL account which did not go through the defendants' servers and she attempted to delete the material before turning in her laptops; (2) the case involved limited items that were recovered from a computer as opposed to "a tremendous volume of paperwork"; (3) plaintiff immediately sought to rectify the disclosure; and (4) the "overarching issue of fairness" weighed in plaintiff's favor because clients should be encouraged to provide full disclosure to their attorneys without fear that their disclosure will be invaded. With regard to the "subfactor," the magistrate noted that the following facts were undisputed: MWC had a computer usage policy which prohibited the personal use of computers. Plaintiff signed the employee handbook containing this policy, and plaintiff did use the computer for personal use. However, the magistrate stated that this did "not end the issue" because the lack of enforcement by MWC of its computer usage policy created a "false sense of security" which "lull[ed]" employees into believing that the policy would not be enforced. More specifically, he indicated that there were approximately four instances in which MWC monitored the computer use of its employees and that they occurred under very limited circumstances, viz. "when there was a request by either a manager or supervisor or by someone else at [MWC]." For example, one instance involved an employee who allegedly downloaded pornographic materials, another involved an employee allegedly playing poker on the internet, and another involved an employee allegedly using the computer to conduct an outside business. The magistrate further noted that at least two of these cases occurred in Chicago and California, respectively, which would not have provided plaintiff with any notice that the company monitored computer usage.

Accordingly, the magistrate concluded that plaintiff had not waived her right to assert the attorney-client privilege and work product protection with regard to any of the documents retrieved by defendants from the two laptop computers, and directed defendants to return all such material.

He reserved decision as to whether the documents at issue were protected by the attorney-client privilege or work product immunity.

> The district court found that the magistrate's ruling, which considered the governing four factors as well as the subset of enforcement, was not clearly erroneous or contrary to law. It further directed that any applications regarding whether the documents at issue were actually protected by the attorney-client privilege or work product immunity should be submitted to the magistrate.

12. *Kaufman v. SunGard Inv. Sys.*, 2006 WL 1307882 (D.N.J. May 10, 2006) (Unpublished). ***Held:*** Deleted email to employee's attorney found on employee's computer system was fully discoverable because employee did not make an effort to segregate the information and was fully aware of employer's computer use policy, thus resulting in a waiver of attorney-client privilege.

This case is similar to *Curto*, but it reaches a different result. Kaufman and OSI, a financial software company owned by Kaufman, initiated suit action against SunGard, alleging, among other claims, breach of contract in connection with SunGard's acquisition of OSI's assets and hiring of Kaufman as a senior executive. In its answer and counterclaim, SunGard asserted state law claims against Kaufman based on the alleged disclosure of SunGard confidential information.

In May 2005, SunGard brought an Order to Show Cause against Kaufman for several items of relief relating to files Kaufman copied from two laptops that she returned to SunGard in January 2005. SunGard asserted that some or all of the copied files were proprietary and confidential. SunGard utilized a computer technician to determine the files that were copied, as well as to recover and restore certain files that were deleted by Kaufman prior to returning the two laptops. Among the deleted files that were recovered were emails between Kaufman and her attorneys. These emails were sent from and received on SunGard's email system during Kaufman's employment with SunGard. The relevant emails exchanged with counsel fall into two categories. First, email communications (including hard copies) exchanged prior to the November 8, 2002 closing and SunGard's purchase of OSI's assets ("Pre-Closing Communications") - these emails remained on OSI computers after closing because OSI continued to operate at the same location. The second group included emails between Kaufman and her attorneys after the November 8 closing date ("Post-Closing Communications"). In opposition to the order to show cause, Kaufman asserted that the restored emails were protected by the attorney-client privilege.

SunGard argued that Kaufman "waived the attorney-client privilege as to Pre-Closing Communications by failing to delete same," and that the

Post-Closing Communications exchanged after November 8, 2002 were not protected based on SunGard's employment policies governing email communications.

The magistrate ruled that all of the communications were discoverable because Kaufman had waived the attorney-client privilege. As to the Pre-Closing Communications, the magistrate found that Kaufman's actions in transferring the disputed emails were "deliberate." The record showed that Kaufman had confirmed that she did not remove or segregate communications with her counsel at the time of the closing, nor did she take steps to protect or segregate the existing communications after the closing.

As for the Post-Closing Communications, the magistrate relied on provisions of SunGard's employment policy which provided that all information and emails stored on SunGard's computer systems was SunGard property and that all emails were subject to monitoring. The magistrate held that any applicable privilege was waived because Kaufman knowingly utilized SunGard's network with the knowledge that company policy provided that SunGard could search and monitor email communications at any time.

In this unpublished letter opinion and order, the district court affirmed the magistrate's rulings.

13. *Nat'l Econ. Research Assocs., Inc. v. Evans*, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006). ***Held:*** If an employer wishes to read an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet, the employer must plainly communicate to the employee that: 1. all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and 2. the company expressly reserves the right to retrieve those temporary files and read them. Only after receiving such clear guidance can employees fairly be expected to understand that their reasonable expectation in the privacy of these attorney-client communications has been compromised by the employer.

14. *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002). Plaintiff sued former consultant and competing company for copyright infringement and unfair competition. Prior to any pretrial conference or entry of a scheduling order, and before any formal discovery had commenced, plaintiff moved for the entry of a preservation order, expedited discovery, and the appointment of a neutral computer forensics expert for the purposes of copying defendants' hard drives.

The basis for all three motions was the plaintiff's belief that the defendants may destroy relevant documents, inadvertently or intentionally. 210 F.R.D. at 649. The defendants had appeared pro se, and plaintiff noted that they might not appreciate their duty to preserve evidence under the rules of procedure. Plaintiff also presented some evidence that the defendants might be going out of business in the near future.

The court entered a preservation order, which the defendants did not oppose, and ruled that expedited discovery was appropriate in part to ensure that computer records were preserved. Id. at 650. The court also granted plaintiff's motion to appoint a neutral computer forensics expert to make copies of defendants' hard drives and retrieve deleted data. It noted that plaintiff had proffered "some evidence that the Defendants use e-mail as a form of communication for their business," and that the defendants had not denied that use. Id. at 651. The court also highlighted the affidavit of plaintiff's expert, in which he testified that "data which is deleted from a computer is retained on the hard drive, but is constantly being overwritten by new data, through the normal use of the computer equipment." Id. From these submissions, the court concluded:

> 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 Plaintiff's claims, or Defendants' defenses. This information may be in the form of stored or deleted computer files, programs, or e-mails, on the Defendants' computer equipment. Id. at 652.

In its discussion of legal precedents, the court noted that "it is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable." Id. Without discussing any specific evidence alleged to have been deleted, and apparently not requiring any such particularized showing from plaintiff, the court concluded that deleted information on defendants' computer equipment "may well be both relevant and discoverable." Id. It ruled that the plaintiff "should be able to attempt to resurrect data which has been deleted from the Defendant's computer equipment," and granted the motion to appoint an expert. Id. The court's order applied only to deleted information on defendants' computer equipment; the defendants remained responsible for producing computer information otherwise accessible from their computers. Id. at 653 n.7. The plaintiff would bear the cost of recovering the deleted computer data. Id. at 652 n.6.

The court went on to fashion a protocol based on those employed in *Playboy Ent., Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D. Cal. 1999) and *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000): The plaintiff would select an expert in the field of computer

forensics, and defendants would make their computer equipment available to the expert at defendants' place of business at a mutually agreeable time. The expert was to use his best efforts to avoid unnecessarily disrupting defendants' business operations. Only the expert and expert's employees would be allowed to inspect or handle the equipment, and they would maintain the information in the strictest confidence. Within ten days of the inspection and copying, the expert would prepare a report as to what computer equipment was produced and the actions taken by the expert with respect to each piece of equipment; the expert would maintain the chain of custody for any copies or images. Id. at 653.

The expert would then produce two copies of the data retrieved from the hard drives, one for the court and one for the defendants. "Thereafter, once [plaintiff] propounds any discovery requests, the Defendants will sift through the data provided by the Expert to locate any relevant documents." Id. The court directed the parties to meet and confer on an appropriate time for the expert to access defendants' computer equipment.

VII. USING FORENSIC TO ADDRESS ESI "NOT REASONABLY ACCESSIBLE" AND LIMIT THE SCOPE OF DISCOVERY

A. Use of Search Terms

1. Search Term Limitations
2. Other factors

B. Custodian Based Discovery

C. Date Restrictions.

1. Email Dates
2. File Dates
   a. Internal vs. External Metadata
   b. Date Created. Date the file was first written to the file system.
   c. Last Modified. Last date that the contents of the file was "modified", or when a "save" was performed on the file. Note that the last modified date can be earlier than the Date Created date.
   d. Last Accessed. Last time the file was accessed. This may be caused by opening the file to view it (without saving the file), scanning the file (virus scan), etc.

D. Data "not reasonably accessible." Rule 26(b)(2)(B) – Framework for "undue burden and costs" analysis.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

* * * * *

(b) Discovery Scope and Limits.

(1) Scope in General. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is **relevant to any party's claim** or defense and **proportional to the needs of the case**, considering the importance of the issues at stake in the action**, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit**. Information within this scope of discovery need not be admissible in evidence to be discoverable.

(2) Limitations on Frequency and Extent.

* * * * *

(B) ***Specific Limitations on Electronically Stored Information.*** A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

---

1. ***Overview***. Rule 26(b)(2) and builds on a two-tier structure of discovery scope suggested in Rule 26(b)(1), applying the structure to the burden of discovery of electronically stored information. In essence, a party must provide discovery of relevant reasonably accessible electronically stored information without a court order, but a party need not review or provide discovery of electronically stored information that it identifies as not reasonably accessible. If the requesting party moves for discovery of purportedly inaccessible information—the second tier—the responding party must show that the information sought is truly not reasonably accessible. The court would then balance the burden or expense of the proposed discovery against its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery.

2. ***Caution***. It is not sufficient simply to claim a source of information is "inaccessible" because of undue burden or cost without a supporting statement of the estimated cost to access the information. Furthermore, inaccessibility for discovery or production purposes **does not relieve a party from preserving the information**. If preservation costs affect a party's ability to preserve information from a relevant and responsive source, the parties should address this issue at their mandatory pre-discovery conference. (*See* Wis. Stat. 804.01(2)(e)).

Practice Tip: If you are presented with a claim by opposing counsel that certain information is "inaccessible", consider requesting an opportunity to test or sample materials to verify the potential evidentiary value of particular information sources.

3. Representative Cases:

In *Zubulake v UBS Warburg* (S.D.N.Y), Laura Zubulake sued UBS Warburg LLC, UBS Warburg, and UBS AG, alleging gender discrimination and illegal retaliation. The plaintiff contended that key evidence was contained in various emails exchanged among UBS employees which subsequently existed only on backup tapes and perhaps other archived media. She requested that the defendant produce "[a]ll documents concerning any communication by or between UBS employees concerning plaintiff." When the defendant produced only 350 pages of documents, the plaintiff, having already produced 450 pages of emails alone, requested that the defendants produce the email from archival media. The defendant, citing Rowe, asked the court to shift the cost of production – estimated at $175,000 – to the plaintiff.

Zubulake filed a motion to compel UBS to provide these emails. Noting that the 8 factors cited in Rowe might result in disproportionate cost shifting away from large defendants, Judge Shira A. Scheindlin set forth a new 7-factor test for cost analysis, drawing from *Rowe* and *McPeek v. Ashcroft*. Judge Scheindlin is explicit that the factors should be weighted according to order:

a. The extent to which the request is specifically tailored to discover relevant information;
b. The availability of such information from other sources.
c. The total cost of production, compared to the amount in controversy.
d. The total cost of production, compared to the resources available to each party.
e. The relative ability of each party to control costs and its incentive to do so.

f. The importance of the issues at stake in the litigation.

g. The relative benefits to the parties of obtaining the information.

In the order handed down, Judge Scheindlin emphasized the need for parties to be fully informed of the technology and cost issues and confirmed that the test employed is a qualitative one in which all relevant factors must be considered in resolving issues on allocating costs and determining whether and how the presumption that the producing party pays should be altered. The presumption is still that the producer pays, especially in situations where data is considered accessible.

Zubulake v. UBS Warburg LLC (*Zubulake III*), 216 F.R.D. 280 (S.D.N.Y. 2003 Opinion and Order dated July 24, 2003). Following the May 13, 2003 Opinion and Order above, the defendants restored and reviewed five backup tapes selected by the plaintiff at a cost slightly over $19,000. Six hundred e-mail messages were deemed to be responsive to the plaintiff's discovery request. The defendants estimated that the cost for production of the entire seventy-seven-tape collection would be $165,954.67 for restoration and $107,694.72 for review. Analyzing each of the seven factors announced by the court in the previous decision, the court determined that the balance tipped slightly against cost shifting, and that requiring the defendants to bear 75% of the costs would be fair. However, the court determined that none of the costs for attorney review of the data, once they had been made accessible, should be borne by the requesting party.

E. Wisconsin State counterpart is Wis. Stat. 804.01(3).

804.01 **GENERAL PROVISIONS GOVERNING DISCOVERY.**

* * * *

(3) **PROTECTIVE ORDERS**. (a) Upon motion by a party or by the person from whom discovery is sought, and for good cause shown, the court may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including but not limited to one or more of the following:

1. That the discovery not be had;

2. That the discovery may be had only on specified terms and conditions, including a designation of the time or place;

3. That the discovery may be had only by a method of discovery other than that selected by the party seeking discovery;

4. That certain matters not be inquired into, or that the scope of the discovery be limited to certain matters;

* * * *

VIII. KEEPING DOWN THE COSTS

A. Preserve broadly

B. Utilize forensic reports and summary data

C. Seek agreement on scope of documents to be searched

1. Active documents?

2. Custodian Based?

3. Date limitations

D. Use testing/sampling approach

E. Consider use of third-party protocol

IX. Definitions

A. **Application**: A program or set of programs designed to perform a specific function. Common examples of applications found on a computer include word processors, web browsers, database programs, and editing and drawing programs. Additionally, the term "App" (short for "Application") is used in the common vernacular to refer to software designed to perform a specific function on a smartphone, tablet, or other mobile device.

B. **Cache**: Space on a hard drive that is used to store recently accessed data so that the same data can be accessed quicker on subsequent requests, and the computer can run faster and more efficiently. Cloud Computing: The delivery of hosted computing services over the Internet, which allows users to share resources such as storage, applications, and networking tools instead of owning, managing, and storing these utilities locally.

C. **ESI (Electronically Stored Evidence)**: Documents and files such as e-mail, databases, text messages, spreadsheets, word processing files, digital images, metadata, and any other type of file stored in a computer or other digital media storage device.

D. **Forensic Image: (also called "bitstream image" or "forensic copy")**: A bit-by-bit copy of a hard drive that is an exact duplicate (or mirror image) of the original hard drive copied, including both active and unallocated space.

E. **Hash Value**: A string of characters assigned to a set of data created as a result of a mathematical algorithm that acts like a digital "fingerprint." Hash values are routinely used by forensic examiners and eDiscovery professionals to identify identical files and to verify the integrity of a bitstream image.

F. **HTML**: A computer language used to create websites. Acronym for HyperText Markup Language.

G. **Internet Service Provider (ISP)**: A company that provides customers with access to the Internet.

H. **IP Address**: A unique number that serves as an identifier for every computer connected to a network.

I. **Logical Image**: The forensic imaging of specific files on a hard drive or other device. Commonly used by forensic examiners to copy portions of a server or other hard drive when only certain files are at issue. This process does not, however, capture deleted files or unallocated space.

J. **Metadata**: Data that describes electronically stored information. Metadata commonly found for user created files on a hard drive includes the date created, the last date modified, and the last date saved.

K. **Native Format**: The file format in which a document was created.

L. **Operating System**: A set of programs that manages all of a computer's hardware, software, memory, and other processes. Examples of common operating systems include Microsoft Windows, Mac, Linux, and Android.

M. **Server**: A computer (usually very large in capacity) that can provide centralized services to other computers over a network. Common examples of servers found in business environments are file servers, email servers, database servers, and web servers.

N. **SQL**: A programming language designed to interface with databases. Acronym for Structured Query Language. (Pronounced "sequel").

O. **Unallocated Space**: The portion of a computer's hard drive that is not being used to store active user files and/or operating system data. Unallocated space often contains deleted content which, while no longer visible to the computer user, can be recovered by a forensic examiner using special tools.

P. **Whole Disk Encryption**: Technology used to encrypt an entire hard drive, including all files as well as unallocated space. For computers with whole disk encryption present, it is necessary to get the applicable passwords or credentials necessary to decrypt the device before it can be imaged and analyzed.

Q. **Wiping**: A method of erasing the contents of a hard drive (or certain portions of a drive) that renders the data permanently unrecoverable from the drive. Many common wiping utilities can be acquired online and downloaded to a computer via the internet.