

As Featured in the NYC Bar Center CLE Program

MATRIMONIAL PRACTICE IN THE DIGITAL AGE

Deconstructing Electronic Evidence: What Is It in Layperson's Terms; Sources of Evidence and Electronic Evidence Procedure.

©Copyright 2010 – 2011 Nicholas G. Himonidis, all rights reserved.

Digital Evidence - Introduction

Computers as we know them today have been in our homes and offices for several decades. During this period, technology has expanded exponentially. The “Digital Revolution” has reached a fever pitch, and the changes that affect almost every aspect of our lives have been dramatic. The way we think about the practice of law must change to keep pace. This is no longer a question of embracing new technology as a means to facilitate our practice or increase efficiency in our offices. This is about the realization that everything our clients and adversaries are doing, the subject matter of what we are litigating, and the forms and location of the vast majority of evidence in the world is now created, stored, exchanged and / or replicated **DIGITALLY**.

Over 95% of all information created in the world is now created or stored digitally. This change is qualitative & quantitative at the same time. Not only is the VOLUME of information much greater than anything the world has ever experienced, but the very manner in we think and act has changed in fundamental ways.

Qualitative: E-mail and texting have replaced talking on the telephone as a primary means of communication. Just about everyone you know has a cellular phone (and they are ALL digital). Try “calling” someone under the age of 25 on the phone – it’s likely they won’t answer, and you’ll get a text message in response. Do not over simplify the significance of this change. SMS (text messaging) is limited to 160 characters. If texting has replaced “talking” as the primary means of communication for most people under 25 (and believe me, it has) an entire generation is now “programmed” to abbreviate and truncate their language and thoughts into 160 character “sound bytes.”

Over 90% of banking transactions are now conducted electronically – without anyone ever entering a bank branch, and without a single piece of paper being generated.

On the quantitative level, information is being created and stored on a scale never before seen - and one which is difficult to comprehend.

The SCALE of the Change: Statistics

Over 280 EXABYTES of data (a/k/a information, a/k/a potential evidence) was created, stored and / or replicated digitally in 2007 alone. That figure is estimated to exceed 1800 EXABYTES in 2011. This is the volume of digital information being created in a SINGLE YEAR – not the total volume of digital information in existence!

Put these numbers in Context: All printed material in every library in the world would fit in less than **one (1) Exabyte** and five (5) Exabytes is sufficient to record every word ever spoken by every human being who ever lived.

All recorded “information” is potentially evidence. Therefore, digital evidence already dwarfs, by sheer volume, all other forms of evidence in the world. The impact of this change on criminal and civil litigation and the justice system is pervasive and cannot be ignored. Not only should it not be ignored, but in some states it literally CANNOT be ignored by any practicing attorney. In New York, for example, the Uniform Court Rules for NYS Trial Courts (PART 202.12) now contain language mandating the items that SHALL BE considered at the Preliminary Conference which include “the manner and scope of any electronic discovery.” (NYCRR 202.12(c)(3)).

Digital Evidence - Key Terminology & Concepts

“Electronic” vs. “Digital” – What is “ESI” Really?

Electronic: Electronic is a term that is properly used to describe a device, not information. Electronic refers to devices that operate by controlling the flow of electronically charged particles. Your laptop computer is “electronic”. The Microsoft Word document you create on it is DIGITAL.

Digital: Information which is stored using numerical values to represent the information itself. Information can be “digital” and it can be created and / or stored by an electronic device. However, information itself cannot accurately be described as “electronic.”

Computers and other electronic devices that store data DIGITALLY, do so using Binary Code, a series of 0’s and 1’s, to represent the information in question. Whether that information is a

digital photograph, a text message, a web page, a word document, a digital audio recording or a map display on a GPS device, they all break down, ultimately, to a string of 0's and 1's.

“**Digital Evidence**” therefore, is any information which is created or stored digitally (i.e. using numerical values to represent the information) which tends to prove or disprove any fact in controversy.

As we see, the term “Electronic Evidence” is a misnomer, unless you are referring to a DEVICE or MACHINE. New York Courts now use the term “**Electronically Stored Information**” or ESI as the term of art to refer to what we call “Digital Evidence.”

Electronic Discovery v. Computer Forensics:

Electronic Discovery (more properly referred to as Discovery of ESI) is the process of requesting and producing digital information (or the new term “ESI”) through the formal legal discovery process. Everything from a subpoena to a non-party to produce stored data in digital form, to a Notice for Discovery and Inspection demanding production of a party’s computer hard drive to be imaged and examined, is “Electronic Discovery” or Discovery of ESI.

Computer Forensics is the process of examining digital information for use in investigations or litigation. It may be conducted in connection with electronic discovery, or completely outside of same.

Native Format:

Native Format is the format in which a digital file (a group or “string” of digital data) was originally created and stored. The “Native Format” of a Microsoft Word document is a .doc file or .docx file (depending on the version of the program).

Every digital file has a Native Format and it is critical to have an item in its Native Format if we seek to obtain the relevant Metadata (see below) and to allow for proper forensic evaluation of the file if necessary.

All digital evidence has a Native Format by definition. **Examples include:** Digital Video Files, Digital Audio files, Digital Photos, Emails, and Documents. In the case of emails and certain other items, the Native Format may be slightly more complicated, such as an individual email message which is contained within a Microsoft Outlook .pst or .ost file. In such case, the email is only truly in its Native Format if the entire host or container file is intact.

Some Native Formats are proprietary or custom, and the source code of the application which created the file is not known. Therefore, when requesting files in Electronic Discovery it is important **to consider** requesting they be produced in their Native Format, but NOT to knee jerk and make blanket demands that EVERY item of Digital Evidence demanded be produced in its Native Format without consideration of what those items might be.

Requesting that Items be produced in “Electronic” or in “Digital” form is not the same as requesting them in their Native Format. The Native Format of a Microsoft Excel Spreadsheet is .xls (or .xlsx). That spreadsheet may be printed out, then scanned and turned into a .tiff or .pdf file and produced as such. To be sure, the item produced is in “Digital Form” but is certainly not in its Native Format. Upon receipt of the spreadsheet in its “new format”, there will be “Meta Data” (see discussion below) but the Meta Data will not be relevant as it will not relate to the original creation, modification or accessing of the spreadsheet, it will only relate to the creation of the file in its current format.

As noted above, consideration must be given before requesting every file in its Native Format. Some files, for example complex database files and files in proprietary and / or custom file formats, may be of little value in their native format, unless the recipient has the application that created them or the “front end” through which they were designed to be accessed. ***Although every computer file can ultimately be broken down in Binary Code, a tremendously long series of 0's and 1's is of remarkably little value if it cannot be properly interpreted as the information it is supposed to represent.***

Meta Data (and beyond):

Meta Data is data about data. It is additional information created by the operating system or device which is creating / storing the substantive or primary data, to help keep track of and provide additional information about that data (usually a digital file). The most basic form of Meta Data is referred to as MAC Dates or the date(s) and time(s) a computer file was created, last accessed and last modified. Nearly every operating system embeds its files with such Meta Data. Depending on the application used to create the data or file in question, Meta Data could also include the Author, the Version Number, the Machine Name of the computer used to create the file and a variety of other items.

Meta Data can be very valuable in providing additional information about a computer file. However, you must have the file in its NATIVE FORMAT in order review and analyze the RELEVANT Meta Data. (See example above regarding production of a Microsoft Excel Spreadsheet which has been printed, scanned, saved as a PDF and produced. The file is in

digital form but the RELEVANT meta-data as relating to the original spreadsheet will no longer be available).

Although Meta Data contains difficult to alter dates, times and other information about the file(s) and the user or system that created the file, Meta Data can be manipulated. For example, MAC dates & times (discussed above) are based on the Windows (or other operating system) internal clock. This clock can be manipulated by a savvy user. For example if the user sets the Windows clock back to a date in the past, and then creates an exculpatory letter in Microsoft Word, the Meta Data of that Microsoft Word file, when obtained and examined in its Native Format, will corroborate the “false” date the user has typed in the body of the letter. As easy as it may be to engage in such a manipulation, however, it is extremely difficult to do so without leaving significant evidence of the manipulation elsewhere on the system. The evidence of the manipulation will NOT likely exist within the file itself, NOR even within the “relevant meta data.” It will only be found in OTHER places on the hard drive of the system or device that was used to create the “false” evidence.

Therefore, you MUST have access to the system / hard drive in question to analyze “beyond the four corners” of the file itself, and beyond the “Meta Data.” This is one of the best arguments for demanding production of entire computer(s) for inspection and “imaging” through discovery, OR obtaining images of relevant computer hard drive(s) outside formal legal discovery where same can be done legally. (For a more thorough treatment of this issue, see the T&M White Paper: “Clandestine Imaging of a Spouse’s Computer(s) Outside Formal Legal Discovery”)

With access to the system which created the file or evidence/item in question, we have access to **secondary / indirect evidence such as:** Created by System (OS) or Application Files, Internet Temporary Files, Application Temporary Files, System Logs and Registry Files. This type of evidence can tell us about what the computer in question was used for, what programs were run and when, and a variety of other potentially relevant information we might otherwise never know. For example, in one forensic examination we found an Application Temporary File called “wipeinfo.lgc” This is a file that would never have been asked for, or produced, as part of any “standard” or even “extensive” ESI discovery request. The existence of that file however, proved that: 1) a program known as Norton System Works had been installed on the subject computer; and 2) one of that program’s utilities, known as “Wipe Info” had been run on the subject computer – the Wipe Info utility being a known “data wiping” utility used to permanently delete data and make same unrecoverable. We then determined that the Norton Program had been installed AFTER the owner of the computer, a party to the litigation, had been served with the Summons and Complaint. This fact, coupled with the lack of information

recovered from the subject computer (as compared to what would reasonably have been expected to be there) resulted in an “adverse inference” by the court against that party. Had there been only a discovery demand for specific ESI responsive to certain issues, the “truthful” yet misleading response could well have been “a thorough search of the ESI in defendant’s possession and control have yielded no such documents” and the inquiry might have ended at that.

The discussion of having access to the actual computer, system or device which created the digital evidence in question actually begs the question: ***“when can I get the other party’s computer in discovery?”***

It is beyond question that discovery of ESI in matrimonial cases is vital. “Fault” is now effectively gone from the matrimonial litigation equation, and even before that development, it was settled (at least in some jurisdictions like the First and Second Department in New York), that discovery on issues of grounds was not permitted. However, discovery regarding the opposing party’s finances is not only permitted, it is often ***the central issue*** in a matrimonial case. In addition, where custody is an issue, discovery of material relevant to the character and fitness of each party, and any conduct relevant to the issue of custody is properly discoverable (see Bill S. v. Marilyn S., Slip Op 51093 (Sup. Ct. Nass. 2005)) and it goes without saying that a computer used by the opposing party may be an excellent source of such evidence.

All this notwithstanding, access to an opposing party’s computer(s) in a matrimonial case, as opposed to merely obtaining discovery of specific documents / files, is not guaranteed, and the cases determining when such access is appropriate are far from uniform. One of the seminal New York cases on this issue is Etzion v. Etzion, 7 Misc.3d 940 (Sup. Ct. Nass. 2005), in which the author was the lead computer forensic consultant for the Plaintiff. In Etzion, Judge Stack ruled that Plaintiff Wife was entitled to have her computer forensic experts clone (or image) each and every hard drive in use at the defendant husband’s business, as well as his personal computers, which he used for business purposes. The court did hold that privileged communications and certain “non relevant personal communications and data” was not discoverable and the Plaintiff Wife was ordered to bear the cost of having the hard drives cloned or imaged. In addition, the court set forth a detailed protocol for processing and review of the information on said hard drives. As a result, the Plaintiff Wife would be in a position to not only obtain “direct” evidence, such as documents and emails, but potentially critical “indirect” or “secondary evidence” such as system files and other data even beyond the basic Meta Data attached to specific digital files in question. (Following the Court’s decision in Etzion, the parties settled the matter.)

Contrast the Etzion case with *Schreiber v. Schreiber*, 2010 NY Slip Op 20271 , 904 N.Y.S.2d 886, Supreme Court Kings County, 2010, where the court actually cited Etzion, but held that wife's requests to have her expert image and examine the hard drive of Husband's office computer were unwarranted.

Forensically Sound:

As with any other form of forensic / scientific evidence, the evidence is only considered to be Forensically Sound, and therefore, admissible, assuming other evidentiary standards are met, if the evidence has been Properly Collected, Authenticated (in this case digitally) and an appropriate Chain of Custody is maintained / documented.

Digital Information on a hard disk or other media is difficult to destroy or eliminate entirely, however, it is easily tampered with or corrupted. Therefore, proper collection, authentication through "hashing," (explained below) and chain of custody are extremely important for purposes of admissibility.

Although some cases have apparently dispensed with chain of custody as a pre-condition to admissibility of digital evidence (see UNITED STATES v. WERNICK, 03CR0189 (DRH) U.S.D.C. (E.D.N.Y. 2010)), most cases hold that some proof of a Chain of Custody is a condition of admissibility. (See: People v. Pena, 169 Misc.2d 366, 642 N.Y.S.2d 807 (Sup. Ct. 1996) (chain of custody was relevant and chain of custody was proven by showing that cellular telephones and computers seized were the same items offered into evidence: also CA, Inc. v. Simple.com, Inc. et al., 02 Civ. 2748 (U.S.D.C. E.D.N.Y. 3-5-2009)).

The Wernick case, above, is an interesting divergence, but the full picture cannot be understood from the published decision(s) alone. One must also review other filed documents in the case, including letters from counsel and motion papers, to understand the full import of what occurred. Basically, the defendant was charged with possession of Child Pornography and related offenses. It appears from the letters and motion papers filed by the prosecution and the defense, that certain hard drives (on which the Child Pornography was located) were seized by local authorities when the defendant was initially arrested. Sometime later, those hard drives were released by the local police to the custody of a third party (relative of the defendant) by mistake, when the federal government took over the prosecution. It further appears that these hard drives then made their way to the defendant's counsel, who assumed they were irrelevant and contained no evidence, hence their release by the authorities and in whose office the hard drives sat for almost a year. When the authorities finally realized the mistake, and recovered the drives from defendant's counsel, under threat of arrest for possession of Child Pornographic Material, the "chain of custody" of the drives had been irretrievably broken – and

in no insignificant manner. Nonetheless, the evidence recovered from the drives was apparently deemed admissible, as the defendant was convicted at trial, and his conviction upheld on appeal notwithstanding his many objections to the admissibility of this evidence.

Authentication through Digital Verification (a/k/a “Hashing”):

“Hashing” is a process by which a mathematical formula known as a Cryptographic Algorithm is used to obtain a unique alphanumeric value (like a fingerprint or DNA profile) for a digital file or volume of digital information. This “digital fingerprint” can then be used to authenticate that file or volume of information, and to verify an original to a copy, a copy to a copy, etc. This commonly misunderstood process is mathematically complicated, but in practice, very simple and straightforward.

In order to “Hash” (i.e. obtain the Hash Value) of a digital file or volume of digital data (such as a hard disk, memory card etc.) the file or volume of data (which is actually just a string of binary code – i.e. 0’s and 1’s) is subjected to the Cryptographic Algorithm. The two most commonly used and accepted Cryptographic Algorithms for this purpose are known as the “Md-5” and the “SHA-1” Algorithms. These Algorithms are referred to as “cryptographic” because they can be used to calculate a unique alphanumeric value for that file or volume of data, **which cannot be calculated in reverse**,¹ and therefore cannot be manipulated.

When a digital file or volume of data is subjected to the Md-5 Algorithm or the SHA-1 Algorithm, the product is an alphanumeric value which is highly unique (more unique in fact than a “DNA Profile”) for the digital file or volume of data in question. The Md-5 and SHA-1

¹ The Md-5 and SHA-1 Hashing Algorithms have come under significant scrutiny in recent years. Since approximately 2004 there have been a growing number of theoretical and actual documented exceptions to the uniqueness of these hashes, known as “collisions.” In the field of digital security, where for example the Md-5 Algorithm has been relied upon to generate “keys” based on a supplied string (a phrase or password), such collisions are admittedly very serious, especially as the ability to create them has become more prevalent due to publication of the research regarding the collisions and the availability of greatly increased computing power to the general public. **However**, in the area of authenticating digital files or data volumes as evidence, and verifying the integrity of copies or “duplicate originals” the issue of “collisions” and the ability to purposefully generate them, is greatly overstated. While it is possible to generate an identical Md-5 Hash Value using a different input string than the original (i.e. generating a “collision”) it is quite another thing to make a contextually meaningful change to a source file or “string” (such as Word Document or Spreadsheet) and then calculate the “balancing” changes that would have to also be made to cause the Md-5 or SHA-1 Hash of the now altered document to be the same as the Md-5 Hash of the original un-altered document.

Algorithms are so sensitive, that ***altering even a single letter or punctuation mark in a Word document*** or other file, causes the resulting hash value to change radically.

For example, the Md-5 Hash Value of "*The quick brown fox jumps over the lazy dog*" is **9e107d9d372bb6826bd81d3542a419d6**. Observe what happens if we simply add a period (.) at the end of the sentence: "*The quick brown fox jumps over the lazy dog.*" The Md-5 Hash Value is now: **e4d909c290d0fb1ca068ffaddf22cbd0**. One punctuation mark is changed, and the hash value is radically different. Calculating what else would need to be changed in order to have the now altered string produce the same Md-5 Hash Value as the original would be extraordinarily difficult, and this is an ultra simple example. Imagine trying to make meaningful changes to a document and then calculating the required changes to offset them, then apply those balancing changes in a manner that does not create obvious irregularities in the document or photo, etc.

The value of hashing and obtaining these values when evidence is collected can be explained as follows. Assume we collected a Word document as evidence. Upon collecting it, we obtain its Md-5 Hash and exchange not only the document, but its hash value, with the other parties involved. If different "versions" of that document are later presented by one party, and a dispute arises as to which is the "original" version, the question can be simply and irrefutably answered by re-hashing the questioned versions. Whichever one matches the original hash value is the "authentic" original document.

Despite recent "challenges" from the tech world to the Md-5 and SHA-1 Hash Algorithms (primarily as they are used in digital security and encryption applications) (See FN 1 above) they remain the "gold standard" in authentication of digital files and data volumes for litigation purposes, as evidenced by cases as recent as 2009 and 2010 which tout their value and reliability for such purposes. For example:

Uniloc USA, Inc. v. Microsoft Corp., 640 F.Supp.2d 150,167-8 (U.S.D.C. D. R.I. 2009) (At trial, the parties agreed MD5 and SHA-1 are algorithms and there was little, if any, dispute over their operations. MD5 is a well-known, publicly available, complex, cryptographic program code (also described as a cryptographic checksum or hashing algorithm) that produces a 128-bit output from its inputs, or the equivalent of 16 characters of information (the SHA-1 output is 160-bits)"... It is undisputedly a "one-way" algorithm; that is, from its 16-character output it is impossible to go backwards or "go back and get the information" forming the input.

State v. Tremaine, WD70670 (Mo. App. W.D. 7-27-2010) Limewire verifies that it is accessing pieces of the correct file by means of a Secure Hash Algorithm (or 'SHA-1') value which uniquely corresponds to an individual computer file. (Footnote: A SHA-1 value is an alphanumeric signature which identifies an individual computer file, regardless of how the file is named on an individual computer. Besides being used by the search function of the Gnutella network, and by LimeWire, law enforcement agencies track the distribution of files containing known child pornography using the files' SHA 1 value, and can identify the Internet Protocol (or "IP") address downloading particular files by the same means.

U.S. v. Wellman, 1:08-cr-00043 (U.S.D.C S.D.W.Va 1-7-2009) (Footnote 2: a hash value is a "digital fingerprint" that is unique to a particular file. Because each hash value is unique, an algorithm, the Secure Hash Algorithm-1 (SHA-1) can be used to show to a 99.99 percent certainty that a file with the same hash value is an identical copy of the same file.

State v. Garbaccio, 214 P.3d 168 (Wn. App. 2009) (footnote 2: [The Detective] was able to determine that a known video of child pornography was available for download from [defendant's] computer by examining the video file's "SHA-1" value, a lengthy alphanumeric code unique to each computer file available for transmission over file-sharing networks, such as Gnutella, which is the network that [defendant] used in this instance.)

Imaging vs. Cloning:

The terms "Imaging" and "Cloning" are often used interchangeably – but they are NOT the same. Both are methods of duplicating a volume of data on a hard drive or other media in a forensically sound manner (i.e.: such that the Hash Value (Md-5 or otherwise) of the duplicate matches that of the original). However, aside from the technical distinctions (discussed below) there are serious practical differences which directly affect the conduct of computer forensic operations and / or electronic discovery engagements. Among these differences is that only one (1) physical clone can be made on a "target" (forensically "sterile" receptacle hard drive) hard drive, whereas several, or in some cases, many, "Images" can be placed on a single "target" drive. This distinction alone, in the context of a large scale forensic data collection, could amount to thousands or tens of thousands of dollars in additional cost, if for example a Stipulation or Court Order directs that a group of hard drives be "Cloned" and makes no provision or discretion for "Imaging" them instead.

Cloning a hard disk, or other data storage medium means the creation of a **physical duplicate** of the original media (sometimes referred to as a “Mirror Capture”). The defining characteristic of the CLONE, as opposed to a FORENSIC IMAGE (discussed below), is that while both may be forensically sound, the Clone is a working (bootable) duplicate of the original. That is to say, if the original was a bootable hard drive, then the clone will be a bootable hard drive. If we remove the hard drive from a desktop computer, obtain its Md-5 Hash, and then CLONE that hard drive, the result will be a second working hard drive, with a MATCHING Md-5 Hash to the original, which when placed into the host computer, will boot up, and operate as if it were the original. ***(NOTE: immediately upon the booting up of either the original or the clone, its Md-5 hash will change radically, as a result of the numerous files within the operating system and registry which are changed every time the computer is powered on or “booted”).***

“Imaging” or creating a “Bit Stream Image” or “Image” of a hard drive or data volume refers to the creation of a single data file (or series of files) which represent a verifiable bit for bit “copy” of the entire sequence of digital information on the original hard disk or other storage medium. Unlike a “Clone” an Image File or “Image” of a hard drive, despite being a “forensically sound copy” and having an identical “Hash Value” as the original drive, cannot be “booted up” because it is not a physical duplicate. Unlike clones, Images may be stored on Target Drives along with other Images and / or related data (such as logs or photos of the imaging process) without affecting the forensic integrity of the image file itself.

Recovery of “Deleted” Material:

The operating systems (OS) which run the computers we use today are LAZY – that is to say they are designed to provide maximum output with as little work as possible. The less work they have to do, the faster they run – and in the computer world, SPEED is everything.

“Erasing” data is time consuming and resource intensive. Therefore, there is no functional equivalent of an “eraser” in the OS of a computer. There is also no truly “blank” or “empty” space on a hard drive. There is only that space which the OS recognizes as “occupied” and that which is recognized to be “free.” The key here is that “free” does NOT mean empty – it simply means free to be used by the OS as needed, because whatever may be in this space is NOT designated as part of the contents of the hard drive.

In order for something on a hard drive to actually become the equivalent of “erased” requires that the data in question be “overwritten” as discussed below. Overwriting takes work. Work that would slow the OS down if it had to be performed every time you clicked “delete” so its simply not done by default.

What actually occurs when the user clicks “delete” is that the OS removes the reference to, and information about, the file or files in question from the “index” (the Master File Table or MFT in Windows-based NTFS file systems). The result is NOT an erasure of data from the drive. In fact, the digital information which made up the file(s) in question remains entirely intact, exactly where it was before it was “deleted” – until something else changes that. That “something else” is the overwriting of the digital information making up those file(s), either through continued use of the computer in the ordinary course, the purposeful overwriting of that specific location on the hard drive (in order to make the “deleted” files unrecoverable), or the “wiping” of the entire hard drive, to accomplish the same result.

Unless and until “deleted” data is overwritten it is often readily recoverable through simple computer forensic operations. Once the data is in fact completely overwritten, it becomes unrecoverable by commercially available forensic tools and methodologies.²

Overwriting can and does occur in a number of ways. First, it occurs in the ordinary course of continued use of a computer after a particular item is deleted. When you create new data, it has to be written to someplace on the hard drive. When the space occupied by a deleted file becomes the next “logical” choice of the OS as to where it will write some new piece of data, the deleted file will become partially or wholly overwritten and, as discussed above, unrecoverable.

For this reason, you should consider sending a PRESERVATION LETTER to your adversary regarding preservation of ESI at the inception of a case, and not even wait for the preliminary conference. Furthermore, if you believe that specific, discoverable information may have existed on an opposing party’s computer, and may have recently been deleted, you should consider a motion by OTSC, for an Order directing the party to cease and desist from using the computer in question, since each and every time it is used there is a risk that the deleted, discoverable information may be overwritten and become unrecoverable by commercially available forensic means.

Where on the hard drive the OS chooses to write new data is not a “linear” function. That is to say, it is not always the next “numerically” empty space. Modern Operating Systems use

² There are believed to be methods of recovering data that has been deleted **and overwritten**. These methods primarily involve examination of the magnetic platters of the hard disk under an electron microscope. These methods, which many industry experts believe are in use by government intelligence agencies, are not commercially available, and would cost hundreds of thousands of dollars per hard drive to be examined if they were. Published data on these supposed methodologies is scare. One published research paper, entitled, ***Data Remanence in Semiconductor Devices*** by Peter Gutmann, of IBM’s T.J.Watson Research Center, suggests the technology is viable.

complex formulas to determine where to write the new data based on size, content, etc. It might seem that making such calculations would take up more time than they are worth, but comparatively speaking, computers make CALCULATIONS at lightning speed, compared to the physical process of writing data to a hard disk, and reading it back when needed. ***Therefore, it is impossible to say with any certainty, how long a particular deleted file may remain intact, and recoverable, after it is deleted.*** Although the volume of use of the computer, the overall size of the hard drive, the size and makeup of the deleted file will all effect the answer, there is no way to calculate same with any degree of certainty as there are simply too many variables.

Hard drives are divided into sections. When a file is written to a hard disk, it must begin at the starting point of a new sector, never in the middle of one. Often, the new file being written to the sector in question is smaller than a “deleted file” currently occupying the space. The space between the end of the new file and the beginning of the next sector is called slack space. Where the size of the older deleted file exceeds that of the new file, a portion of the older deleted file will not be overwritten, and will remain in the space between the end of the new file and the end of the sector which the old “deleted” file occupied. This space is known as “**File Slack**” space, and the fragment of data, which is part of the old “deleted file” although no longer in its original form or “Native Format,” is known as a “**file fragment.**” This file fragment will likely remain for a long time, undisturbed (not overwritten) if the ‘new file’ remains undeleted, because additional new files must begin at the beginning of a new sector and therefore the computer cannot “chose” to write any additional “new data” to the space occupied by the “file fragment” remaining the in the “file slack” space described.

Overwriting can also occur PURPOSEFULLY, of course. Overwriting all or a portion of a hard disk, a procedure known as “**wiping,**” is the accepted method of sanitizing and “permanently deleting” data from hard disk. The process of “wiping” can be accomplished with any number of free or inexpensive software tools designed for this purpose. In essence, all these tools do the same thing. They write random data or “0’s” to the entire hard drive, or designated portions thereof, thereby overwriting whatever data was there before and making same unrecoverable.

Wiping tools designed to wipe entire disks tend to be extremely effective, as their job is quite simple. Tools designed to “surgically” wipe only selected portions of a hard disk, leaving the Operating System and selected user files unaffected, are often not nearly as effective.

In any event, material that is successfully “wiped” will not be recoverable – but evidence of the fact that the drive, or portions of it, have been “wiped” is usually easy to recover, and extremely difficult for the other party to explain, especially if that party has been noticed with a

preservation letter, or better yet, is subject to a preservation Order. (This is an excellent reason to send a Preservation Letter to opposing party's counsel or the party themselves if unrepresented, immediately upon inception of the matter.)

Digital Evidence - Sources of Evidence:

By far the most sought after category of "Digital Evidence" through electronic discovery in litigation is Electronic Communications. Primarily E-mail, electronic communications also consist of IM (Instant Messaging), postings to electronic message forums such as Twitter, online bulletin boards or "Blogs," Social Networking Sites such as Facebook and MySpace and text messages (SMS data transmissions.)

All of the above represent sources of hugely important potential evidence. What can be obtained forensically, what can be obtained legally, (inside or outside formal discovery,) and how can we ensure its admissibility are all questions to be addressed.

Any discussion of Electronic Communications as evidence must begin with a discussion of the SOURCE, i.e.: ***where do we obtain the evidence of the communication and a copy thereof.***

"Device vs. Carrier" Particularly in the case of E-mail and text messages, and to a lesser extent in the case of social networking sites, and 'blogs,' we have two theoretical options. From a technical point of view, we can attempt to obtain the evidence in question (a copy of the communication or "post") from the DEVICE which sent or received the communication (or from which it was posted), or we can attempt to obtain it from the Carrier through whose network the communication was sent or on whose service it was posted. The former poses various technical challenges, and the latter, some serious legal obstacles.

"Carrier"

The legal obstacle first. The Federal Electronic Communications Privacy Act (ECPA 18 U.S.C. § 2510 et seq) and specifically, Title II thereof, referred to as the "Stored Communications Privacy Act" (18 U.S.C. § 2701) provides that an Internet Service Provider (which would include web mail hosts and account providers) may not release **the SUBSTANTIVE CONTENT** of stored electronic communications (i.e.: emails, text messages, and possibly, postings on social network pages, etc.) of their customer / user, ***absent a Court Order obtained by a governmental entity or the consent of the originator or an intended recipient.*** (NOTE: This only applies to the Substantive Content of Communications. ***Information regarding who***

owns a particular email address, the date such address / account was created and / or the IP Address from which the account was created, are examples of information that can usually be obtained with a Subpoena to the ISP / Mail Host or “Carrier”.)

As a practical matter, this means we have two choices in civil litigation. We either obtain the email (or text message) in question from the sender or receiver’s DEVICE, legally of course, or we must obtain an authorization from the originator or an intended recipient to obtain same from the ISP. Since we presume such consent will not be forthcoming, we would fall back on requesting the court to order the originator or intended recipient to execute an authorization for same, PRESUMING the originator or an intended recipient is a party to the case, or subject to the jurisdiction of the court. (See e.g.: Romano v. Steelcase, Inc., 2233-2006 (Sup. Ct. 09-21-2010)) where upon determination that the demand by Defendants for “access to Plaintiff’s current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information” was appropriate and within the scope of discovery, the Court ordered Plaintiff to furnish counsel for the Defendant’s with such “properly executed consent and authorization as may be required by the operators of Facebook and MySpace” to effectuate such discovery.)

In any situation where it is contemplated that Electronic Communications evidence may be sought from a Carrier (ISP, Social Network Operator etc.) ***it is imperative to prepare and send a Preservation Letter to the Carrier as soon a possible*** upon discovery that such evidence might exist. It may take a substantial amount of time to procure the necessary authorizations / releases and make the subsequent demand to produce on the Carrier. During such time, there is a significant risk that deleted communications, postings, pages etc. may become unrecoverable by the Carrier, for the same basic reasons discussed above in “Recovery of Deleted Material”.

Sample Preservation Letters, along with a reference chart providing the contact information for major ISP’s, Social Networking site operators, and wireless carriers is available on our website or by contacting the author.

In the case of “Blogs,” Social Networking Sites, web sites and other online sources of evidence that may be legitimately accessible to the public, or to someone who is willing to facilitate access to same on our behalf. (For example, most “blog” sites are accessible to the public, and in the case of a Facebook page, portions of that “page” may be available to all Facebook members, and other portions or “pages” may be available to those Facebook members designated as “Friends” by the “owner” of the page.) Assuming we can VIEW / access the

page(s) in question, which represent or contain the “evidence,” we can “capture” that evidence for use in a variety of ways which are surprisingly “non-technical” and quite simple.

Photographs or “screenshots” of the above described page(s) have been deemed admissible in many cases (See, “**Authenticating Web Pages as Evidence**,” M. Anderson Berry and David Kiernan, *Internet Law & Strategy*, January 21, 2010). Simple but effective techniques, such as using a program called “Snag-it” to make high quality, complete “border to border” screen captures of online evidence, complete with date and time stamps, and showing the URL (web address) being viewed should be considered. Generally speaking, the resulting “photograph” of the web page which constitutes the evidence can be introduced just as a photograph would, by the sponsoring witness testifying that they saw the webpage in question at the date and time the “screen capture” was made, and that the screen capture is a “fair and accurate representation of what they observed.” (See e.g.: Toytrackerz LLC v. Koehler, 2009 WL 2591329, at 6 (D.Kan. Aug. 21, 2009); see also, Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., 2007 WL 4563875, at 5-6 (N.D. Ga. May 11, 2007)).

In the case of web pages obtained from the Internet Archive, also known as the “Way Back Machine,” which archives pages from websites on an ongoing basis, most courts have determined that such pages are admissible as evidence. (See “**Authenticating Web Pages as Evidence**,” *supra*.) At least one New York District Court has held that screen shots from the Wayback Machine may be “authenticated by a knowledgeable employee of the website.” (Audi AG v. Shokan Coachworks, Inc., 592 F. Supp. 2d 246, 277-78 (N.D.N.Y. 2008)).

Device:

Our other option is to obtain the evidence from the sender or receiver’s computer (or cell phone / PDA as the case may be.) This may be possible (and perfectly legal and acceptable) outside formal discovery if our client has legitimate / legal access to the device in question (see e.g. Byrne v. Byrne, 168 Misc. 2d 321, 650 N.Y.S.2d 499 (Sup. Ct. 1996)), or through formal discovery demand to produce the device in question for discovery and inspection (or for an expert to “clone” or image same (See e.g.: Etzion v. Etzion)).

Whether we can recover the evidence in question, from a technical perspective, varies greatly depending on the form of evidence, the type of system or device on which it has been created, the length of time which has elapsed since its creation and / or deletion and many other factors.

Email Evidence: There are many forms of email, but basically speaking, there is “Web Mail” or internet based email, where the user’s email data is stored on the server of a “Carrier” or web

mail host, and “client based mail” such as Microsoft Outlook or Outlook Express, where the user’s mail is stored locally on their machine, or on a network account, which they access through their machine. In the case of client based mail, the ability to recover copies of email messages sent or received by the user in question determined by the user and/or network settings. Generally, the chance of recovery of such mail is extremely high, assuming the mail has not been deleted by the user and many times even if it has. In the case of webmail, the chances are less, but we can recover entire mail messages, or substantial portions of mail messages, in many situations, even in situations where the user did NOT purposely “download” or save copies of such mail messages to their machine. In either case, “deleted” emails can very often be recovered, but when and to what extent varies greatly depending on the circumstances.

It is important to keep in mind that MULTIPLE SOURCES may exist to obtain the same email message. For example, an email may be recovered from the SENDER’s machine, from any Recipient’s machine, and / or from any number of intermediate servers. Servers owned and maintained by a party to the case, or their employer, are NOT governed by the Stored Communications Privacy Act unless the party hosting such mail or communications server(s) provide such services to the public. Therefore, a subpoena maybe all that is required to obtain a copy of an email from the employer of a party, if same cannot be readily recovered from another source.

SMS Data (Text Messages):

These are short messages (up to 160 characters). The content of SMS messages, like email, is governed by the Stored Communications Privacy Act, but here we face an even more difficult problem. Assuming you are willing to make a motion to compel the opposing party to provide the necessary authorization to obtain the evidence, ***unless you get a preservation letter delivered to the Carrier within three (3) to seven (7) days of the message being sent and delivered*** (less if the sender and receiver DELETE the message), ***the evidence will no longer exist*** at the Carrier when you eventually obtain such authorization.

As of this time, the following carriers no longer “log” SMS data on their servers at all: AT&T, Sprint / Nextel, T-Mobile, Cricket, Boost Mobile. Other carriers, such as Verizon Wireless, do currently maintain SMS data on their servers, but as noted above, for only a very brief period of time.

Therefore, the only truly practical method of obtaining SMS data as evidence is to obtain it from the sending or receiving device. NOTE: recovery of deleted SMS data from sender or receiver devices is a HIGHLY DEVICE SPECIFIC endeavor.

Some devices, such as the I-phone and Droid, are excellent sources of evidence and a great deal of data, including deleted data can be recovered from them due to their robust operating systems. (For example, we can recover SMS Data, Emails, GPS coordinates, photographs, history of websites visited etc. from an iPhone in much the same way as we do from a computer.)

iPhones – Examples of Recoverable Data

- Photos taken with camera which may also contain EXIF data showing GPS coordinates where a photo was taken
- Google Maps searches / routes
- Skype calls produce NO “third party” record – but proof of “calls” exists within the device
- Raw GPS Data to prove where phone has been
- Emails / Text Messages
- Call Histories
- Calendars / Address Books (with photos!)

BLACKBERRY DEVICES

Devices engineered and manufactured by Research in Motion, a Canadian firm. They are in use on most major wireless carriers, and SECURITY / ENCRYPTION is VERY TOUGH. Blackberry Devices can yield a great deal, or very little, in terms of recoverable data, depending on whether security features are enabled, and whether we have been provided the password if they have been. Unlike most other devices, if security features are enabled and we are NOT provided with the password(s), we may we may not be able to access the data on the device at all.

Digital Evidence – Collection, Preservation and Presentation

The hard disk inside a desktop, laptop or server, is the most common source of digital evidence. A 40 GB hard drive (very small by today's standards) can contain 3.5 million pages of text. In addition to hard drives inside desktops, laptops, servers, and other systems, there are many forms of **removable media** such as portable / external hard drives, "thumb drives" (small USB drives now capable of holding up to 128GB of data), CD's, backup tapes, off site / remote backup storage services. All of these are sources of digital evidence, all of which pose unique collection and preservation issues. In addition, consider other, less thought of sources of digital evidence, such as:

- Video Security Systems (Homes & Businesses)
- Electronic Access Control Systems
- GPS Devices: (Vehicle Based, Portable, Incorporated into PDA)

Digital evidence can be collected (extracted) and preserved from all of the above sources. However, in order for that evidence to be admissible, and equally important, in order for it to withstand scrutiny as to its weight / reliability, it must be collected and preserved in a forensically sound manner. The basic tenets of this "forensic soundness" were discussed above. In addition to those basic principles of: Proper Collection, Authentication (through "hashing") and Chain of Custody, we must now add detailed procedural steps, the presence of which will help to ensure admissibility, and bolster the WEIGHT of the digital evidence, and the lack of which will provide excellent impeachment material on cross examination if the opposing counsel is so inclined and / or prepared.

- Collection and Preservation Methods must not only be forensically sound, meaning commonly accepted as such by the relevant technical community, but they must be WRITTEN, in the form of Standard Operating Procedures, for ALL persons conducting the forensic work (collection, processing, examination of evidence) to follow. This ensures uniformity, and REPEATABLE RESULTS, which is one of the hallmarks of "proper scientific procedure."
- Detailed Logs, screenshots and / or photographs of EVERYTHING should be maintained. Every item handled, processed and from which evidence is collected should be photographed. Every imaging event should be accompanied by a CONTEMPORANEOUS "acquisition log" including all relevant forensic details

such as hard drive serial numbers, sector counts, makes, models, and verification data.

- Written Standard Operating Procedures should be in place, and followed, for everything from field acquisitions of single computer hard drives to acquisitions, processing and examinations which occur in the forensic lab. LOGS, screenshots and photographs should be maintained, again, to document compliance with all written operating procedures.
- The qualifications of ALL persons collecting, handling, processing and examining the digital evidence should be known and available, NOT just the individual who may show up to testify in court.
- Forensic hardware and software utilized for collection and processing must be generally accepted as “forensically sound” AND validated regularly. If any “custom” or “proprietary” forensic hardware or software tools are used, the user and COUNSEL must discuss this, and must be prepared to validate that they are forensically sound, again through control validation / testing.
- LAB Conditions: Digital forensic work, like any other forensic science, must occur in a controlled environment. Although a digital forensic lab need not be a “clean room” it must be ACCESS CONTROLLED and there should be LOGS of all entries to the Lab, including dates and times.

THE TOUGHEST QUESTION ... WHO WAS AT THE KEYBOARD?

Forensic evidence can be extremely compelling due to its scientific “objective” nature. Digital evidence is no different in this regard than fingerprints, DNA or ballistic evidence for example. But while DNA and Fingerprint evidence are quite often used to conclusively prove the “WHO,” other forms of forensic evidence, such as ballistic microscopy and digital forensics are more adapted to proving the “WHAT”. Within these forensic disciplines, i.e. those which are not focused on PERSONAL IDENTIFICATION, there is a tendency to over-emphasize the value of the forensic proof of **WHAT HAPPENED** (i.e.: this bullet came from this gun) and not enough focus on “who pulled the trigger”? In the digital forensic world this is a problem as old as the discipline itself, and the issue is quite literally “who was at the keyboard.”

A Digital Forensic Examination of a hard drive or other system can often prove to a “reasonable degree of scientific certainty” if not to a virtual certainty, that a specific activity was engaged in using the computer in question, often at a specific date, at a specific time. Proving however, **who** was sitting at the computer at that date and time, is NOT something that can usually be proven SCIENTIFICALLY. Proof of that issue usually requires a resort to circumstantial evidence. That circumstantial evidence may include such items as:

- whoever did the activity in question at that date and time, was logged onto the computer under a password protected user account with a complex password;
- Immediately before, or immediately after (perhaps within minutes or less) the person suspected of doing the activity in question logged onto their email account, online banking, or other “secure” account from the subject computer, and would need passwords and other information to do so;

Ultimately, however, such proof is circumstantial and quite often, it will not rise to the degree of scientific certainty required for an expert witness to properly and honestly say to a judge or jury that they KNOW to a “reasonable degree of SCIENTIFIC certainty” that a particular person is responsible for creating the digital evidence in question.

CONCLUSION

Every litigated matter in this day and age must certainly include consideration of what relevant digital evidence may exist, and how we can, within the bounds of what is legal, and technologically feasible, obtain such evidence and preserve it for use at trial. Matrimonial practice, with its intense focus on communications between parties and on financial information is at the forefront of these developments.

ABOUT THE AUTHOR

Nicholas G. Himonidis, J.D., CFE, CCFS, is a Vice President at T&M Protection Resources, LLC (“T&M”) and the head of T&M’s Private Investigations Division. Prior to joining T&M, Mr. Himonidis was the President and Chairman of The NGH Group, private investigation and forensic consulting firms operating throughout New York and Florida. Mr. Himonidis has an extensive background in investigations, computer forensics and law. Over the past decade, he has directed the investigative phase(s) of some of the largest matrimonial litigations in New York State. He has worked with trustees appointed by the United States Bankruptcy Court to recover fraudulent asset transfers in cases involving millions of dollars of diverted funds and fraudulent schemes perpetrated directly against the United States Government. He has litigated cases, and been an expert witness, in both state and federal court in a variety of matters, including domestic relations cases.

Mr. Himonidis has a B.S. in Criminal Justice from St. John's University and his J.D. from St. John's University School of Law, where he graduated Magna Cum Laude. He began his career as a Private Investigator in 1990 and subsequently worked as an attorney at several prestigious law firms prior to returning to Private Investigations full time in 1997.

Mr. Himonidis is a ***Certified Computer Forensic Specialist (CCFS)***, with extensive training and expertise in computer forensics, data recovery, electronic discovery and digital evidence handling procedures. He is widely recognized for his computer forensic work, in matrimonial cases among others. He is also a ***Certified Fraud Examiner (CFE)***, the only professional certification formally recognized by the FBI as encompassing a critical skill set for investigators. Mr. Himonidis lectures frequently on topics including digital evidence, electronic discovery and computer forensics as well as legal and ethical issues for attorneys working with investigators and consultants.

About T&M Protection Resources, LLC

For nearly three decades, T&M Protection Resources has been providing a growing portfolio of seamlessly integrated security and investigative services, including state-of-the-art security technologies, to leading corporations, organizations and private clients. Its capabilities include Security Consulting, Executive Protection, Security Officer Services, Explosive Detection, Data Forensics & Information Security, Technical Security Solutions, Private Investigations and Global Investigations and Risk Management. T&M also has security business affiliates in Israel including Saar Security, Ltd., Goshen Security Services Ltd., technology based Shamor-Israel Service Center, and B-Protect Online Ltd., making T&M one of the largest security firms in Israel. T&M employs over 4,500 security personnel and has annual revenue in excess of \$120 million.

For more information, please contact T&M Protection Resources at 212-422-0000 or visit our website at www.tmprotection.com

For further information contact:

Nicholas G. Himonidis, J.D., CFE, CCFS
T&M Protection Resources, LLC
(646)445-7800
PI@tmprotection.com
www.tmprotection.com