The Debtor's Digital Reckonings

Introduction

Every bankruptcy professional understands that the Ch 7 trustee has the duty to investigate the financial affairs of the Debtor and to ensure that books and records are properly turned over in accordance with Section 704. The Debtor has the obligation, under Section 521(4), to "surrender to the trustee all property of the estate and any recorded information, including books, documents, records, and papers relating to property of the estate, whether or not immunity is granted under Section 344 of this title". Ch 11 trustees and Debtors have similar duties and responsibilities.

Environment

Millions of individuals and businesses use electronic banking, computers, personal digital assistants, digital devices, have e-mail, word processing, spreadsheets, and accounting software applications[1] used to record and report on personal and business financial activities.

Bankruptcy statistics are devoid of information regarding the number of business Debtors using computers and digital devices. Unfortunately for the creditors, most trustees do not have the understanding and technical expertise necessary to properly investigate digital technology in the modern financial world. This e-illiteracy can be fatal to creditors trying to recover assets from Debtor's and insiders. It is almost inconceivable that, in 2003, bankruptcy trustees are conducting financial investigations without the benefit of this expertise. How can any trustee investigate the Debtor and recover assets for the creditors without initiating a digital forensic accounting investigation?

Solution

Nowadays it is practically impossible for unscrupulous Debtors or their officers to escape from the trail of e-data[2] left behind in today's digitized business environment. Yet, little or nothing is being done by the trustees to protect the rights of creditors. When creditors suspect the existence of significant assets - a comprehensive risk (cost) - reward (recovery) analysis is necessary.

Trustees and creditors need the skills of the digital forensic accounting technologist[3] ("forensic technologist") for the 21st Century. The forensic technologist is cognizant that business operates, and ultimately survives or fails, using digital information. After a bankruptcy filing, the trustee and forensic technologist must be prepared to immediately begin to uncover, recover and analyze the Debtor's e-data from any available digital data-storage source for the benefit of creditors.

The forensic technologist understands this is not inexpensive, and it may need to be funded by creditors, but the bottom line is the rewards can be enormous. This article will explain the process necessary to facilitate change and how to get the money back for creditors.

Bankruptcies Digital Reality

This is about understanding how digital evidence, the Debtor's e-data found on computer hard disk drives ("HDD"), PDA[4] and digital devices[5] can directly benefit creditors.

Queries:

1. When did you last hear a trustee ask the Debtor at the Section 341 examination if the books and records were kept on computer? Did the Debtor answer "No"?

2. Did the trustee then ask the Debtor, "Ok, so how many computers were used in the business during the last six years and where are they now?"

3. Did the trustee obtain the e-mail and website addresses from the Debtor, including those of the insiders?

4. In larger cases the Debtor often fails to immediately file the Schedules and Statement of Financial Affairs with the Petition. The creditors can be assured that those Debtors will have used more than one computer in their business.

5. Did the Debtor document for the trustee exactly how many computers, PDA, laptops and digital devices were used and where they are now?

6. Does the trustee then plan to have the forensic technologist thoroughly examine those HDD prior to their sale?

7. Did the Debtor sell or dispose of any desktop systems, laptop computers, PDA or digital devices during the two years prior to the filing?

8. Does the Debtor have leased computer equipment containing the business and financial records, including e-mail and word processing files on HDD, PDA, laptops and digital devices?

9. Does the trustee plan to use an auctioneer to dispose of the computers and digital devices that are property of the estate?

10. Do the creditors intend to STOP the trustee from having the auctioneer dispose of computers and digital devices before the forensic technologist

has completed his preliminary examination? (Auctioneers may immediately begin the process of having the computers HDD "wiped" clean of all the e-data.)

Time is not on the creditors side

Time is all-important and the trustee should consider obtaining access to all the Debtor's HDD, PDA and digital devices before the Section 341examination. Obviously, in any bankruptcy case today, computers and digital devices contain the critical information necessary to obtain money for creditors.

The creditors would not want to learn after a case is closed that the trustee did not find out that the insiders or employees of an unscrupulous Debtor slipped out the front door with the intellectual property on a Microdrive or computer HDD.

The ideal situation for the creditors is for the trustee to arrange for the forensic technologist to immediately observe the computers and digital devices in place on site. Hesitation on the part of the Debtor and insiders to allow that examination may be considered an indication that necessary digital financial information is in jeopardy so long as controlled by the Debtor and insiders. A visit to the Debtor by the forensic technologist may facilitate locating passwords, the data backup schedules, hand-written notes, private e-mail addresses, floppy disks, phone numbers and other information.

Exactly what are we talking about?

Promptly examining the e-data to find where the money went and possibly who may have the money or property now, are obvious goals for the creditors. Examination of the e-data would not encompass merely a cursory glance at the computerized records of the Debtor's business.

A proper digital forensic accounting examination includes, but is not limited to, a review of the computerized accounting records, e-mail messages, instant messages, digital memos, word-processing documents, databases, spreadsheets, archives, presentations, graphics, and address books or other contact management data contained in the wide assortment of computers, digital devices or PDA used by the Debtor or insiders but only after the digital evidence has been protected by the technologist. Most interesting is the fact that a digital forensic accounting examination of a computer whose use was disclosed by the Debtor may reveal the use of other computers or digital devices or media.

If warranted by the case, the forensic technologist will be relentless in the pursuit of finding assets for the creditors and will continue searching for the e-clues to the money trail.

How is information stored on the HDD?

A wealth of information may be discovered to benefit creditors in the Debtor's file slack[6] space, ram slack or drive slack[7] space found on the HDD. In addition, most word-processing documents, spreadsheets, database files, presentation files and certain other files, contain information, including endogenous embedded information about the author, title of the document, actual date and time created, edit or lapsed time, actual date and time modified, file last saved by whom, number of pages, and software program version used.

Examination of computer logs will provide a history of files and documents accessed, including those printed, backed up, downloaded and/or shared between users. Surveying Internet history may provide further insight into the financial affairs of the Debtor. Having this information provided by the forensic technologist should be any creditor's dream.

How will the forensic technologist protect and acquire the e-data?

The first step in maintaining the best practices for protecting the integrity and validity of the Debtor's digital information for the benefit of the creditors is for the forensic technologist to create what is called a digital forensic image (sometimes technically referred to as low-level bit-stream image) from the Debtor's computer HDD, PDA, and digital devices.

The digital forensic images will permit the trustee to assess the Debtor's activities with a greater degree of completeness and this, in turn, allows the trustee to promptly ascertain the location of any hidden property for the creditors. Try as they may, the trustee or others should never use the Debtor's computers and/or copy its computer files and then somehow hope to find the trail of money or property for the creditors. These actions may only succeed in compromising the integrity of the digital forensic evidence.

Why does a digital forensic image need to be created?

Before the trustee can begin to do an examination of the Debtor's financial information and the books and records, the trustee needs to have a digital forensic image created of the computer HDD, PDA and digital storage sources that are exact digital forensic image copies that will be admissible as evidence in court. The "trail of evidence" must be proven unbroken from the Debtor's digital data sources to the witness stand.

Using forensically sound hardware and software, the forensic technologist prepares an absolutely sanitized[8] or sterile HDD to receive the digital forensic image that will be created from the Debtor's HDD, PDA and digital devices. The forensic technologist will match (bit by bit) the e-data present on the Debtor's

original source HDD, PDA and digital devices with the digital forensic image being created during the acquisition process.

The match of the digital information is verified using what is called a cryptographic Hash value[9]. The cryptographic Hash is a digest[10] value that establishes that the e-data does match exactly. A digest value is a characteristic number value used for verification of data authenticity. However, digests are more than that, as they are exceedingly strong one-way cryptographic Hash[11] codes, and can be created for a single digital file or document, or an entire HDD. The digest value is a digital signature that is unique and cannot be replicated, except when the algorithm is applied to the same identical e-data, just like a fingerprint.

What is the harm to the creditors if the trustee fails to have the forensic technologist create the digital forensic image from the Debtor's computer HDD, PDA and digital devices? The Debtor, or the insiders and/or others might allege that the digital information was nothing but some unsupported e-data and that the information obtained by the trustee was unsubstantiated and could not be corroborated. Under those circumstances, would the documents supposedly found be admissible when challenged by the Debtor's forensic technologist who will testify that the trustee failed to follow sound digital forensic practices and did not make the digital forensic images?

The trustee's best answer should be that the e-data found on the Debtor's computer HDD, PDA and digital devices **"**was obtained in accordance with established digital forensic practices; that the trustee's forensic technologist preserved the Debtor's computers, and the evidence, including the digital forensic images, has been made available to the Debtor for inspection at reasonable times; and to the best of his or her knowledge the Debtor has not challenged the authenticity of the e-data discovered and preserved by the trustee**"**.

The real cost could be enormous for the creditors if the trustee fails to obtain the digital forensic image copies, and instead allows the Debtor's computers, PDA and digital devices to be accessed by someone who lacks forensic technologist experience and skills necessary to conduct a forensically sound examination. One must seriously consider that merely starting up and/or just turning on or off the Debtor's computer, PDA and digital devices may jeopardize the evidence.

In those cases in which the trustee makes a report regarding bankruptcy fraud, the digital forensic images and the resulting e-data discovered will be crucial in the prosecution of the unscrupulous Debtor.

What about PDA and digital devices

It is almost a certainty that several new Personal Digital Assistant (PDA) or digital devices have hit the marketplace since the completion of this article. However, the more popular ones need to be addressed here as to their characteristics.

PDA and hand held devices:

Generally these devices have operating systems that save information using memory (RAM and ROM). This includes the Palm, Handspring Treo, iPaq, Jornada, Cassiopeia, Clie, Visor, or Windows CE and Pocket PC devices. Once the digital forensic image is acquired from the PDA, the particular hardware and software specification then becomes available. Practically all items found on Palm PDA are saved and stored in databases in some form. It is these database files, the Debtor's e-data, that the forensic technologist will recover during the acquisition process of creating the digital forensic image, including deleted files and the slack space found on the Palm. The Windows CE devices save the e-data using similar methods found in Windows and this image is sent to the destination drive.

Since the Debtor's e-data is stored in memory, it is imperative that the battery be properly charged. If the PDA were to lose power, the e-data would generally be lost. Most Palm and related PDA rely on synchronizing with big brother, the desktop computer. The forensic technologist will not attempt to synchronize between the PDA and the Debtor's computer, and will access the devices directly.

Digital devices:

These include, for purposes of this article, CDs, DVDs, USB storage devices, FireWire storage devices, PCMCIA HDD, Microdrives, CompactFlash cards, digital hand held devices of every type and quite literally, hundreds of other computer electronic/digital/optical storage devices. Generally, if the e-data is stored on a digital device, then the probability exists that the forensic technologist will acquire, recover, examine, search, and review the information discovered for the benefit of creditors.

When e-data is written to a CD-RW, DVD-RW or DVD+RW and thereafter deleted, exactly what happens to the e-data is dependent on the specific software application being used to create this media. Many of the software applications will add the area occupied by the files that were deleted to the available free space. That space will not be used until the entire disc has been written to once. Only then will this freed space be reused.

It is unfortunate that some of the software for CD-RW, DVD-RW or DVD+RW will immediately reuse the space occupied by deleted files, but the forensic

technologist will determine the method used and proceed accordingly with the examination of the Debtor's e-data.

The forensic technologist will find the deleted and now orphaned files (when they have not been immediately overwritten) and acquire the e-data still present on the CD-RW, DVD-RW or DVD+RW. Because the most common form used with re-writable media actually writes files in disparate parts rather than contiguously on the disc, it makes searching for deleted files not a trivial matter. The forensic technologist will find and locate the Debtor's e-data that has been deleted on CD-RW, DVD-RW or DVD+RW searching the entire media source looking for any e-data, including slack space and the contents of deleted files.

Alternatives for the digital forensic accounting technologist

The prudent forensic technologist will make multiple digital forensic images at the time of the original acquisition of the Debtor's e-data. The ideal number will vary depending upon the particular facts and information technologies used by the Debtor. In every case the digital forensic image copies will be identical (just like the fingerprint) to the Debtor's source HDD, PDA or digital devices.

These digital forensic image copies are normally used as follows:

- One digital forensic image is always kept for safe keeping, remaining pristine during the life of the case. It will always agree with the Debtor's computers as they initially were examined (using the MD5 Hash digest discussed previously), for the creditors' protection should any attempt be made to challenge the authenticity of the digital forensic image;

- Another digital forensic image will be used during the examination, to recreate the live computer environment of the Debtor's system. This can be used by the trustee (for example) for the collection of accounts receivable, fraudulent conveyances, printing Debtor's hard copy financial reports, spreadsheets, correspondence, memos etc.

- These "working images" will be used to find deleted digital documents and files, locate altered financial records, search e-mail files, examine books and records and consequences regarding the confirmation of substance over form issues.

The costs associated with the purchase of HDD have decreased and this approach is economical in that it will reduce the administrative costs associated with the digital forensic efforts during the term of the case for the creditors.

What about viruses and worms?

The forensic technologist needs to be careful of all e-mail and related attachments, inasmuch as this is the most common method for spreading viruses and worms which are generally transported in e-mail attachments. Multiple AntiVirus software programs will be used to examine the Debtor's e-data, inasmuch as one cannot be too careful in protecting the e-data for the creditors.

What about the examination of E-mail?

Sometimes it may be necessary for the forensic technologist to find, recover and examine extensive e-mail and instant messages, including deleted e-mail files and attachments, from HDD, PDA and digital devices. E-mail messages could number from 10,000 to 10,000,000 or more (no limit). As published in the *National Law Journal*[12], "Ken Withers, a research associate at Washington D.C.'s Federal Judicial Center, who speaks and writes frequently on electronic discovery, estimates that a hypothetical company of 100 employees will generate a total of 7,500,000 messages a year."

Most e-mail programs actually create a database using proprietary programs such as Microsoft Exchange Server. Once the e-mail and instant messages are found, it will be necessary to use digital forensic extraction tools to carve out specific lists of e-mail addresses (removal of duplicates is automatic) and identify, if necessary, the original server that sent the message.

Digital forensic software tools allow for the identification of the location of attachments to the e-mail message that will generally identify the source of the documents or files, the software application used to create the document, the author of the document and the exact date and time of creating the document or files, including any changes and modification to that document or file. This is most beneficial for the creditors in examining financial transactions between the Debtor, insiders and/or others to determine substance over form issues related to financial information that may be part of an all-pervasive accounting fraud.

In conjunction with the investigation of the hard copy documents, the forensic technologist will use digital forensic extraction tools and techniques for e-mail messages and the related text from the e-clues contained in them. The forensic technologist will develop and organize during the digital investigation the e-mail and related attachments based on relation cliques, the circle of people with an apparent common purpose.

What information will creditors gain from the e-data?

The forensic technologist maintains an extended collection of digital forensic software tools designed to assist and find the money for the creditors. The forensic technologist will examine the e-data found on the Debtor's computer

HDD, external HDD, backup media, floppy disks, Zip drives, Jazz drives, tape drives, CDs, DVDs, PDA and digital devices from the digital forensic images created at the beginning of the case, and each of these media storage systems will generally require specific digital forensic tools.

Combined Digital DataSource:

This forensic technologist will take all the e-data (using the digital forensic image copies) and create the Debtor's combined Digital DataSource to be used in connection with the examination of the e-data. The combined Digital DataSource adds enormous data mining capabilities for both trustee and the creditors. It is important to recognize that this image is in addition to the digital forensic image copies previously discussed.

The Debtor's combined Digital DataSource constitutes a complete universe of the digital alpha/numeric indexed text from all available sources. This database will contain every word, number, digital commerce, phrase, business term, acronym, password, special purpose word that relate to the Debtor's and/or the insider's business, addresses, personal and business assets, lifestyle activities, and any and all dates and times that pertain to any document or actions by the Debtor and/or insiders, business affiliates or related parties. Also, using multi-language digital forensic support tools, the forensic technologist will search and locate documents and files that may contain evidence of foreign languages. These will be documented and electronically Bates stamped for further examination.

The forensic technologist uses the powerful search capabilities, intuitive and fuzzy logic, to conduct unlimited[13] and simultaneous searches of the Debtor's combined Digital DataSource. Looking for e-clues from the positive "hits" found in the e-data can possibly uncover fraudulent accounting activities and point to how and where to find the money for the creditors.

The forensic technologist can search the combined Digital DataSource and locate practically anything that exists on e-data. In summary, what can be defined, can be found and the following are just a few examples:

- Find any documents or files for any given date, or any range of dates;
- Locate specific types of documents or files pertaining to any select number of days or dates for spreadsheets, correspondence, e-mail, memos etc.;
- Locate any document or files based on the original date created, date modified and date last accessed;

- Find all documents or files from any source using any number of specific words, phrase, addresses, and/or names or numbers;

As a reminder the forensic technologist created and used only the digital forensic images. The Debtor's computer was never used, or turned on.

If the Debtor is hiding e-data, don't you want to know about it?

Invisible attachments:

Valuable financial information including names, addresses, passwords, bank accounts, taxpayer identification numbers, related parties, insider transactions, financial statements, real estate ownership, stock options plans, beneficial owners, joint ventures, insurance coverage, contracts, spreadsheets, or even a second set of books and other information about unscrupulous Debtors can be hiding behind legitimate files on the HDD as invisible attachments[14]. The trustee must find the second set of books for the creditors.

This important information is not visible, unless one knows how to find it. Information stored as e-data on a computer HDD, PDA or digital devices is often never printed on paper[15], so having the right skills to attain access to this data is key for the creditors. The trustee should not allow this to be overlooked during the examination of the e-data, because if the Debtor is hiding crucial e-data, the creditors should know about it.

Steganography[16] and encrypted e-data:

An extensive investigation of the digital forensic image is made to locate encrypted documents, folders, directories, and drives, on the Debtor's HDD, PDA or digital devices. Once these encrypted files are identified, indexed and electronically Bates stamped, it will be necessary to decrypt those files using passwords provided by the Debtor. In addition, it is strongly recommended that the forensic technologist perform a steganalysis[17] for the discovery of hidden embedded information inasmuch as steganography amidst the e-data poses a significant threat to the recovery of money for the creditors.

When encryption and/or steganography have been discovered on the Debtor's e-data, and the passwords are not available, the forensic technologist will utilize decryption[18] and steganalysis software to attempt to discover and break the passwords and find the reveal hidden and/or encrypted information. Most often encrypted and hidden information will likely provide confidential information that the Debtor is concealing. This evidence may provide extensive e-clues that could expose fraudulent accounting activities and point to fraudulent conveyances that can be recovered for the creditors.

Recovery of deleted information:

This article does not attempt to comment on the effects of the Sarbanes-Oxley requirements relating or pertaining to digital document retention and the destruction of financial information for publicly held companies, their respective accounting firms and corporate counsel (Sections 802 and 1102 of the Act). Nor is 18 U.S.C. Section 1020 dealing with fraud and related activity in connection with computers cited in this article. However, that being said, the forensic technologist experience would benefit the investigation of white-collar crime, accounting fraud and commercial litigation in any setting.

Most participants in the bankruptcy process are now aware, after numerous and repeated scandals, that when you typically delete e-data, (documents, files, folders, directories and drives) the computer only marks this information as deleted in the (computer) file system. The deleted e-data while concealed[19] does remain on the HDD and will generally only be completely erased when that section of the HDD is overwritten with new e-data.

Previously deleted e-data is extremely delicate from an evidentiary standpoint. Allowing the use (other than by the forensic technologist) of the Debtor's computer HDD, PDA and digital devices during the investigation of a case will overwrite information on those devices. This will jeopardize discovery that could benefit the creditors.

Even in sophisticated corporate settings, using secure methods and adequate document retention policies, all of the e-data may not be eliminated. The forensic technologist may still have a chance of finding the e-data that existed even after the Debtor and/or others attempted to completely delete it. Many software programs create numerous temporary files and several versions may still exist with different names.

The digital information and documents may have already been saved or backed up, but not limited to, more than one computer, computer servers and/or tape drives (many times this is done automatically), external HDD, CD, DVD or other media. Sometimes the e-data has been copied to an individual's or insider's personal laptop or corporate computer and numerous "pieces" of documents from other sources may be found. In those cases, the e-data still exists after the digital shredding of specific documents and files. This does not begin to take into consideration those nagging digital footprints that are left behind by Debtors and their officers.

In many cases, it is likely that e-data files have been deleted, and the forensic technologist will recover those deleted files and then electronically Bates stamp those files for further examination. The forensic technologist will search the recovered deleted files and documents for specific excerpts of text using GREP regular expressions[20], logical expressions[21] and lightning fast multiple

simultaneous text searches of the Debtor's e-mail messages, documents, and files. This includes familiar programs, such as, but not limited to, WordPerfect, Word, Excel, PowerPoint, Visio Drawings, Publisher, Project, Photo Draw, Adobe PageMaker, PDF documents, Text documents, Rich Text Format, HTML, Compression Archives, Multimedia, Crystal Reports, Access, Microsoft SQL Server, Databases[22], financial and accounting applications, and Macintosh files just to mention a few.

The forensic technologist has digital forensic tools available for the quick search of files with metadata information[23], which provides for the identification of more than six thousand (6,000) programs, documents, spreadsheets, databases and a monumental list of file extensions if indeed they exist amidst in the Debtor's e-data for the benefit of creditors.

After the recovery of the Debtor's deleted e-data, and using the digital forensic images created to simulate the Debtor's computers, the recovered deleted e-data can be combined with the simulated restored computer providing a view of what was on the Debtor's computer prior to any deletions.

The forensic technologist examines the Debtor's e-data searching for anomalies. After the recovery of the Debtor's deleted e-data the trail of digital footprints ought to be of enormous value to the trustee and this evidence may lead to the recovery assets for the benefit of the creditors.

Finding assets for the creditors

The following is an example of how the digital forensic accounting technologist can benefit the creditors:

- Find hidden assets, including the ability to trace individual transactions from start to finish.
- Identify and reveal digital evidence related or pertaining to possible claims against Board of Directors for breach of fiduciary duty, fraud, theft, conversion and unjust enrichment.
- Detect and uncover unusual transactions, including money and property transfers and complex related-party activities.
- Identify and reveal digital evidence related or pertaining to possible claims against Preferred Shareholders for breach of contract and fraud.
- Expose facts and circumstances relating to issues of substance over form that could not otherwise be documented.

- Uncover fraudulent accounting activities.

- Discover undisclosed business or business activities to which assets may have been shifted.

- Detect hidden documents, including the ability to trace related activities.

- Identify and expose digital evidence related or pertaining to possible claims against Auditors for breach of contract, breach of fiduciary duty, aiding and abetting a breach of fiduciary duty, fraud and negligent misrepresentation, professional negligence, and securities fraud.

.

- Discover and expose digital evidence related or pertaining to possible claims against Underwriters for breach of fiduciary duty, aiding and abetting a breach of fiduciary duty, claims of breach of contract, fraud and negligent misrepresentation, and securities fraud.

- Detect the backdating of vital documents leading to possible fraudulent conveyance actions.

- Reveal abuses, concealment and destruction of computers and e-data leading to § 707(a), 707(b) and § 727 referrals by the trustee.

The forensic technologist will provide the trustee with detailed, summary and exception reports on the Debtor's activities, insiders, related companies, sales of property, and for any subject matter, place or circumstances, allowing for the creation of a relative time-line analysis as it relates to any of the above for the benefit of the creditors.

Dealing with the technical aspects of the digital forensic accounting investigation, the trustee and creditors need the forensic technologist to follow established digital forensic methodologies.

Please contact the author directly to receive a non-exhaustive list of best practices for the acquisition of digital forensic accounting evidence within the bankruptcy context for the uttermost recovery for creditors.

Summary

Computers, digital devices, e-mail and the Internet have utterly changed how individuals and businesses operate today. It is time for bankruptcy professionals to become more e-literate in these matters. The author is hopeful that you now understand that creditors have the solution available for the digital age.

Trustees, attorneys, examiners, and forensic accountants that conduct financial investigations of the Debtor's books and records without the benefit of digital forensic accounting technologist expertise and neglect to follow established digital forensic methodologies should seriously consider the attendant risks from failing to do the following: (a) protect the Debtors e-data; (b) create digital forensic images of the Debtors HDD, PDA and digital devices; (c) examine for invisible attachments, encryption, steganography, multi-languages, unallocated file space, drive slack space, file slack space, ram slack space and numerous other digital forensic methodologies discussed; (d) discover, recover and analyze digital forensic accounting evidence for recovery of assets for creditors.

Conducting a digital forensic accounting investigation to find assets for the creditors amidst the e-data is not an easy or an inexpensive task. It is however necessary in those instances where the creditors and trustee suspects the Debtor may be hiding assets or the "smell" of money exists.

The trustee and creditors needs the skills of the digital forensic accounting technologist, experienced in bankruptcy, litigation, financial and accounting matters. Knowledgeable, with computerized financial and accounting applications and especially effective in the analysis of financial information, the forensic technologist provides maximum results for the creditors.

About the Author:

Jack Seward has, for many years, specialized in bankruptcy, insolvency, litigation support and the discovery, recovery and analysis of digital forensic accounting information for attorneys, creditors, trustees, stockholders and other interested parties.

The author is a consultant and has an association with RosenfarbWinters, LLC, a New York metropolitan area forensic accounting firm.

With special thanks to Stuart L. Fleischer, Managing Partner of the New York Office for his encouragement and suggestions and Mary Schlager, New York Office Manager for her editing assistance.

Jack Seward is the author of **"**The Debtor's Digital Autopsy or Where's The Money?©**"**, published by the National Association of Bankruptcy Trustees in the summer 2003 issue of NABTalk® as the feature article.

If you have comments, questions or requests please contact the author at JackSeward@msn.com or JSeward@rwcpas.com. You may contact Jack Seward at his New York Office 212.686.0220 or his Cell 917.450.9328.

Footnotes:

[1] Accounting applications including but not limited to Great Plains, Sage, Best, MAS 90/200, Solomon, DacEasy, J.D. Edwards, Peachtree, SAP, Lawson, Simply Accounting, Business Works, Net Ledger, Oracle , Platinum, e Epicor, Pro Series, PeopleSoft, ACCPAC, Ross Systems, Intentia, Cougar Mountain, M.Y.O.B., Agresso, Macola, Navison, Siebel, Easy Accounting, QuickBooks, Quicken, Money and specific applications such as FRx, Timberline, Forefront, Keystroke Point of Sale, Supply Chain, CRM and Electronic Data Interchange (EDI) automated programs.

[2] For purposes of this article the term "e-data" pertains to any information contained or stored in electronic, digital and optical format.

[3] The term "forensic technologist" is used in this article to identify with the digital forensic accounting technologist and his or her necessary role to protect, expose, recover and analyze the digital accounting evidence, the e-data, during the insolvency and bankruptcy process.

[4] PDA is an acronym for Personal Digital Assistant that include, but not limited to Palm, Handspring Treo, iPaq, Jornada, Cassiopeia, Clie, Visor, or Windows CE and/or Pocket PC devices.

[5] Digital Devices for purposes of this article include, but are not limited to CD, DVD, Microdrive, CompactFlash, SmartMedia, SecureDigital, Memory Stick, USB Flash Drives, and MultiMediaCard. In addition, when specific digital devices are not described the term is intended to include, but not limited to computers, including network servers, workstations, laptops, mini-towers, desktops, floppy disks, EIDE HDD, SCSI HDD, USB devices, FireWire devices, MP3 HDD, Network Attached Storage, RAID sets, PCMCIA HDD, Zip Disks, Jazz Disks, external HDD, and tape backup systems.

[6] File Slack space exists at the end of computer file to the end of the last "cluster" and this space may contain valuable information. Since file slack may contain randomly dumped information from computer "memory" such as passwords, bank account numbers, and other confidential information this is not an insignificant item.

[7] RAM slack relates to the last "sector" of a file and comes from the dump of computer "memory". Drive slack space retains the information that was previously stored and this space may contain valuable scraps of previously deleted files.

[8] According to U.S. Department of Defense (DoD) standards for HDD sanitization and disposal as specified in Section 5220.22-M

[9] For further information see Bruce Schneider, Applied Cryptography, Wiley, 1996. This texts is considered one of the most comprehensive and useful texts on cryptography.

[10] Using: 128-bit MD5 cryptographic Hash, 160 bit Secure cryptographic Hash Algorithm or SHA1, or the SHA2, a 256, 384 or 512 bit cryptographic Hash.

[11] In cryptographic terms, the Hash is said to be "collision free". Please see "The MD5 Message-Digest Algorithm", R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc. April 1992.

[12] National Law Journal, November 4, 2002, Digital Discovery Starts to Work

[13] Allowing for the simultaneous search using more than 3,500 six (6) character words and/or numbers.

[14] The Microsoft NTFS file system provides for Alternative Data Streams (also referred to as Multiple Data Streams) and ADS will hide the Debtor's e-data. ADS should not be overlooked during the examination of the Debtor's e-data, because if the Debtor is hiding crucial e-data you should know about it.

[15] According to a study conducted by the University of California at Berkeley, 93% of all information generated in 1999 was generated only in digital form.

[16] Taken from the Greek language, steganography means covered writing and has been used for centuries for the hiding of secret messages.

[17] Steganalysis is the inspection of digital files to detect steganography.

[18] Decryption software for programs including but not limited to Encrypt Magic Folders, Source Safe, BestCrypt, PC-Encrypt, Microsoft Office, Word, Access, Pocket Excel, dBase, FoxBASE, Windows XP, Windows 2000, Windows NT, Outlook, Outlook Express, Microsoft Exchange Server, WinZip, PKZip, ZIP, General Zippers, VBA Visual Basic, Internet Explorer, Adobe Acrobat, Quicken, QuickBooks, Lotus 1-2-3, Lotus Organizer, Lotus WordPro, Microsoft Project, MYOB, Paradox, ACT!, Microsoft Mail, Schedule+, Microsoft Money,

WordPerfect, Filemaker, Peachtree Accounting, Quattro Pro, Ami Pro, Backup, Bullet Proof FTP, Cute FTP, Data Perfect, File Maker Pro, My Personal Check Writer, Norton Secret Stuff, Palm, Q&A, WinRAR, Symphony, Versa Check, Adobe PDF, Window95 and Window98 PWL Files, and Netscape Mail.

[19] Deleted e-data remains in the "unallocated file space" and this space potentially contains entire documents, spreadsheets, accounting transactions and databases, hidden software programs, e-mail messages, bank account numbers, online banking information, Electronic Data Interchange transactions, passwords, file histories, hidden temporary files, spool folders, remnants of documents, Internet histories and caches, and entire files and folders, subdirectories and other temporary files which were produced by the program applications and operating system.

[20] Regular expressions are derived from the UNIX utility GREP and enable powerful text searches using special characters.

[21] Logical expressions (Boolean) allows for searching using two or more search strings in a variety of ways.

[22] Including but not limited to ORACLE, Sybase, Informix, DB2, Interbase, Paradox, Microsoft Visual FoxPro.

[23] Metadata information is invisible unless you can find it and includes the Application name, Title, Subject, Keywords, Template, Comments, Revision number, Number of pages, Number of paragraphs, Number of lines, Number of words, Number of characters, Number of notes, Number of slides, Manager, Company, Category, Security flags, Creation date, Last accessed date, time, e-mail and messaging.