THE DEBTOR'S DIGITAL AUTOPSY
OR
WHERE'S THE MONEY!

Trustee's answer: Find the "Pixie Dust"[1] – the recorded electronic data found on Computer Hard Disk Drives ("HDD"), PDA[2] and other Digital Devices[3].

Jack Seward
RosenfarbWinters, LLC
New York, NY 10016
JSeward@RWCPAs.com or
JackSeward@msn.com

Introduction

A trustee has the duty to investigate the financial affairs of the Debtor and to ensure that books and records are properly turned over to the trustee in accordance with Section 704. Furthermore, under Section 521(4) it is the duty of the Debtor 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". The Handbook for Ch 7 Trustees indicates that "Attorneys and accountants may not be compensated for performing the statutory duties of the trustee" and investigating the financial affairs of the debtor falls within the duties of a trustee "unless sufficiently documented to show that special circumstances exist". Most panel Trustees may not have the technical expertise to properly investigate in the modern financial world of computer technology. This article will demonstrate the need for qualified forensic accountants with specific computer forensic skills as it relates to the bankruptcy process.

How many millions of businesses and individuals have e-mail, Word Perfect, Word, Excel, QuickBooks, Quicken, Money, and accounting software applications[4] used to record and report on business and personal financial activities? (So did anyone mention keeping a second set of books or off the books accounting?) It is almost impossible for unscrupulous Debtors or their officers to escape from the trail of e-data left behind in today's digitized business environment.

Indeed this is the digital age, and in the Bankruptcy arena that means the Trustee has powerful resources available to sift through the electronic sand pit of the unscrupulous Debtor. To accomplish this, the Trustee will need the skills of the "eSleuthHound"[5], the forensic accountant for the 21st Century. The eSleuthHound is cognizant that business operates, and ultimately survives or fails, using digital information. After a failure, the eSleuthHound must be prepared to uncover and recover the Debtor's e-data[6] from any available data-storage source.

---

[1] "Pixie Dust" is a nickname that IBM gave to that thin layer of the element *ruthenium* sandwiched between the magnetic layers where the digital data is stored which has allowed more information to be placed onto a hard disk drive ("HDD").
[2] PDA is an acronym for Personal Digital Assistant that include Palm, Handspring Treo, iPaq, Jornada, Cassiopeia, Clie, Visor, or Windows CE and/or Pocket PC devices
[3] Digital Devices including but not limited to CD, DVD, Microdrive, CompactFlash, SmartMedia, SecureDigital, Memory Stick and MultiMediaCard.
[4] 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 and specific applications such as FRx, Timberline, Forefront, Keystroke Point of Sale, Supply Chain, CRM and Electronic Data Interchange (EDI) automated programs.
[5] "eSleuthHound" is used in this article to identify with forensic accountants who possess computer forensic skills related to the bankruptcy process.
[6] For purposes of this article references to e-data pertains to any information contained or stored in electronic, digital and optical format.

Computer Reality Check

Questions:

1. Let's assume that when you asked the Debtor at the Section 341 examination if the books and records were kept on computer, the Debtor answered "No". Did you then ask, "Ok, so how many computers were used in the business during the last six years and where are they now?"

2. Do you have the e-mail and website addresses from all your Debtor cases, including those of the insiders?

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

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

5. Does the Trustee have a plan to examine the all HDD, PDA, laptops and other digital devices?

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

7. 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 other digital devices?

8. Inasmuch as the computers and other digital devices are property of the Estate do you, as the Trustee, plan to sell the computers and other digital devices before the eSleuthHound makes an examination of the computer HDD, PDA and other digital devices?

9. Prior to any sale of computers or other digital devices belonging to the Estate, does the Trustee plan to take adequate measures to insure that no confidential personal and/or financial information resides in the Pixie Dust on the HDD (information such as credit card, personal identity, employee HR, customer history, financial, banking, and medical information etc.)?

10. Does the Trustee then plan to have the eSleuthHound first thoroughly examine and then sanitize those HDD prior to their sale?

Time is not on the Trustee's side

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

The Trustee would not want to learn after a case is closed that he/she did not find out that the insiders or employees of an unscrupulous Debtor slipped out the front door with the intellectual property of the Estate on a Microdrive, CompactFlash or HDD.

The ideal situation is for the Trustee to arrange for the eSleuthHound to immediately observe the computers and digital devices in place on site. Any hesitation on the part of the Debtor and/or insiders to allow that examination should be considered an indication that necessary financial and computer information is in jeopardy so long as controlled by the Debtor. Visiting the Debtor's facilities is key to being able to find things like passwords, the data backup schedules, private e-mail addresses, floppy disks, phone numbers and other information that might not be found by traditional techniques.

Exactly what are we talking about?

Promptly examining the Pixie Dust to find where the money went and who has the money now, before it is all gone, are obvious goals for both the eSleuthHound and Trustee.

What will the eSleuthHound do if the Pixie Dust does not contain the story about the Debtor's financial history and where the money went, and this information cannot be found in any of the electronic memos, documents, databases, spreadsheets, archives, presentations, graphics, accounting programs, or address books? What if this information was not recorded, revised, encrypted, deleted, backed up, copied, saved, pasted, printed and/or stored on the Debtor's computer HDD, digital devices[7] or the wide assortment of PDA that include Palm, Handspring Treo, iPaq, Jornada, Cassiopeia, Clie, Visor, or Windows CE and/or Pocket PC devices?

If the eSleuthHound cannot find the story in the e-mail messages or any of the arrays of other digital storage sources not already mentioned he may conclude, by deductive reasoning, that the insiders have the computers, PDA or other digital devices with the Pixie Dust, and that the insiders would not then be able to put back the Pixie Dust when that is finally documented. If warranted by the case, the eSleuthHound will be relentless in the pursuit of finding the money for the Estate and will continue searching the Pixie Dust for e-clues to the money trail for the Estate.

Valuable financial information including names, addresses, passwords, bank accounts, securities, taxpayer identification numbers, identifying related parties, insider transactions, financial statements, real estate, stock options, beneficial owners, joint ventures, insurance coverage, contracts, spreadsheets, or even a second set of books and other information about the unscrupulous Debtors or their officers can be hiding behind legitimate files on the HDD as invisible attachments[8]. This important information is not visible, unless one knows how to find it. Information stored on a computer HDD, PDA or other digital devices is often never printed on paper[9], so having the right skills to attain access to this data is key for any Trustee.

A wealth of information may be discovered in file slack[10] space, and ram slack or drive slack[11] space found on the HDD. In addition, most word-processing documents, spreadsheets, database files, presentation files and certain other files, contain information, including embedded information about the author, title of the document,

---

[7] Including but not limited to network servers, workstations, laptops, mini-towers, desktops, floppy disks, EIDE HDD, SCSI HDD, USB devices, FireWire devices, Network Attached Storage, RAID sets, CDs, DVDs, Microdrives, CompactFlash cards, Memory Sticks, PCMCIA HDD, MultiMedia Card, Zip Disks, Jazz Disks, external HDD, and tape backup systems.

[8] 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 Pixie Dust, because if the Debtor is hiding crucial e-data you should know about it.

[9] 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.

[10] 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.

[11] 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.

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 network 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 eSleuthHound should be any Trustee's dream.

During the examination of the Debtor's e-data, the Trustee is furnished with detailed summary and exception reports regarding the investigation of the Debtor's activities on a regular basis.

How will the eSleuthHound acquire the Pixie Dust?

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

It is important to recognize that the Trustee is not hiring the eSleuthHound to examine the Pixie Dust at this time. Rather the Trustee would initially engage the eSleuthHound to protect and secure the Pixie Dust by acquiring the Debtor's e-data for the Estate. The Trustee and/or the Court could always decide to use a different forensic accountant to examine the HDD, PDA and other digital devices, and in that case, the forensic images would be turned over to that forensic accountant.

The chances of the creditors receiving a dividend are improved when the Trustee engages the eSleuthHound to create and protect this e-data early on. The forensic images will permit the eSleuthHound 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 property of the Estate and the appropriate causes of actions for the Estate. Try as they may, the forensic accountant or others on the Creditors' team *should never* use the Debtor's computers and/or copy its computer files and then somehow hope to find the trail of money. In fact these types of actions likely will only compromise the integrity of the digital evidence in the Pixie Dust.

Why does a forensic image need to be created?

Before the forensic accountant can begin to do an examination of the Debtor's books and records, the Trustee needs to have a forensic image created of the computer HDD, PDA and other digital storage sources that are exact 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 eSleuthHound prepares an absolutely sanitized[12] or sterile HDD to receive the forensic image that will be created from the Debtor's HDD, PDA and other digital devices. The eSleuthHound will match (bit by bit) the e-data present on the Debtor's original source HDD, PDA and other digital devices with the forensic image being created during the acquisition process. As the forensic image is being created, it is sent to the destination drive awaiting verification that both the source and destination drives match. The eSleuthHound is not done until this match is verified.

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

The match of the digital information is verified using what is called a cryptographic Hash value[13]. The cryptographic Hash is a digest[14] 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[15] codes, and can be created for a single electronic 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 if the Trustee fails to have the eSleuthHound create the forensic image from the Debtor's computer HDD, PDA and other digital devices? The Debtor, or the insiders and/or others in an Adversary Proceeding, might allege that the digital information was nothing but some unsupported Pixie Dust and that the information obtained by the forensic accountant for the Trustee from the Debtor's computer HDD was unsubstantiated and could not be corroborated. Under those circumstances, would the documents supposedly found on the Debtor's computer HDD by the forensic accountant be admissible when challenged by the Defendant's eSleuthHound who made an examination of the Debtor's HDD, PDA and other digital devices and will testify that the Trustee and the forensic accountant failed to follow sound forensic practices and did not make a forensic image of the Debtor's HDD, PDA and other digital devices?

Would the Debtor, or Defendant(s) in an Adversary Proceeding, under the same circumstances mentioned above, more likely than not prevail if the Defendant's attorney produced excerpts of deposition transcript(s) taken of the Trustee and the forensic accountant at trial stating clearly that the Debtor's computer HDD, PDA and other digital devices were used after the filing of the Petition; the dates shown on the Debtor's HDD, PDA and other digital devices changed since the Petition date; hundreds of Debtor documents and files from the HDD, PDA and other digital devices were used, and neither the Trustee nor the forensic accountants could verify who used those documents, files and programs or why they were used; the Trustee was unable to provide the documents used, created, retained and/or destroyed by the forensic accountants subsequent to the filing of the Petition; the forensic accountants could not identify who had access to the Debtor's HDD, PDA and other digital devices; the forensic accountant failed to maintain chain of custody logs for the Debtor's HDD, PDA and other digital devices?

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

The real cost to the Estate could be enormous if the Trustee fails to authorize the creation of the forensic image copies, and instead allows the Debtor's computers, PDA and other digital devices to be accessed by someone who lacks eSleuthHound experience and the 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/servers, PDA and other digital devices may jeopardize the evidence. (So did someone again mention chain of custody?) The Defendants' eSleuthHound could destroy the Trustee's case as it relates to the e-data evidence.

---

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

[14] 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.

[15] 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.

In those cases in which the Trustee makes a referral regarding Bankruptcy fraud, the forensic images and the resulting e-data discovered will be crucial (one assumes that the forensic images and related digital information would greatly assist any prosecution of the unscrupulous Debtor).

What about PDA and Digital Devices

It is almost a certainty that several new Personal Digital Assistant (PDA) or other 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. The eSleuthHound always creates a forensic image and performs the Hash authentication as the e-data is acquired. Once the 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 eSleuthHound will recover during the acquisition process of creating the forensic image, including deleted files and the slack space found on the Palm. The Windows CE devices saves 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 eSleuthHound will not attempt to synchronize between the PDA and the Debtor's computer, and will access the devices directly.

Other Digital Devices:

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

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 the file, but the eSleuthHound will determine the method used and proceed accordingly with the examination of the Debtor's e-data.

The eSleuthHound 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 write files in disparate parts rather than contiguously on the disc, it makes searching for deleted files not a trivial matter. The eSleuthHound 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 eSleuthHound

The prudent eSleuthHound will make multiple 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 forensic image copies will be identical (just like the fingerprint) to the Debtor's source HDD, PDA or other digital devices.

These image copies are normally used as follows:

- One 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 Trustee's protection should any attempt be made to challenge the authenticity of the forensic image;

- Another 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, determining preference actions, fraudulent conveyances, creditor claims, printing Debtor's hard copy financial reports, spreadsheets, correspondence, memos etc.

- These "working images" will be used to find deleted electronic 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 for the Estate in that it will reduce the administrative costs associated with the e-forensic efforts during the term of the case.

What information will the Trustee gain from Pixie Dust?

The eSleuthHound maintains an extended collection of forensic software tools designed to assist and find the money for the Estate. The eSleuthHound 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 other digital devices from the forensic images created at the beginning of the case, and each of these media storage systems will require specific forensic tools.

Combined Digital DataSource:

This eSleuthHound will take all the Pixie Dust (using the 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 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, electronic commerce, phrase, business terms, acronyms, passwords, special purpose words 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 support tools, the eSleuthHound 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 eSleuthHound uses the powerful search capabilities, intuitive and fuzzy logic, to conduct unlimited[16] 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.

The eSleuthHound can search the combined Digital DataSource and locate practically anything that exists on Pixie Dust. 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 eSleuthHound created and used only the forensic images. The Debtor's computer HDD was never used, or turned on.

During the course of the case investigative results will continue to evolve. The eSleuthHound will provide the Trustee with updated reports.

Viruses:

The eSleuthHound needs to be careful of all e-mail and related attachments, inasmuch as this is the most common method for spreading viruses which are generally transported in e-mail attachments. Two of the leading Antivirus software programs are use to examine the Debtor's e-data, inasmuch as one cannot be too careful in protecting the Pixie Dust for the Trustee. Before the eSleuthHound begins to examine e-mail messages, all of the attachment files will be analyzed to determine if its name and/or file type matches any known virus (another reason to make additional forensic images).

Recovery of Debtor's deleted information:

This article does not attempt to comment on the effects of the Sarbanes-Oxley requirements relating or pertaining to electronic 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 eSleuthHound experience would benefit the investigation of white-collar crime in any setting.

Most participants in the Bankruptcy process are now aware, after the scandals of Enron, Andersen, WorldCom, and HealthSouth etc., that when you typically delete e-data, (documents, files, folders, directories and drives) that the computer only marks this information as deleted in the (computer) file system. The deleted e-data

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

while concealed[17] does remain on the HDD and will generally only be completely erased when the section of the HDD that had that information is overwritten with new e-data.

All Trustees must recognize that previously deleted e-data is extremely delicate from an evidentiary standpoint, and that allowing the use (other than by the eSleuthHound) of the Debtor's computer HDD, PDA and other Digital Devices during the administration of a case will overwrite information on those devices. This will jeopardize discovery.

Even in sophisticated corporate settings, using secure methods and adequate document retention policies, all of the Pixie Dust may not be eliminated. The relentless eSleuthHound 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 electronic documents may have already been saved or backed up to more than one computer, computer servers and/or tape drives (many times this is done automatically), external HDD, or other media. Documents can be on an individuals notebook or PDA. In those cases, the Pixie Dust still exists after the electronic shredding of specific documents and files. 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. This does not begin to take into consideration those nagging electronic footprints that are left behind by Debtors or their officers.

In many cases, it is likely that e-data files have been deleted, and the eSleuthHound will recover those deleted files and then electronically Bates stamp those files for further examination. The eSleuthHound will search the recovered deleted files and documents for specific excerpts of text using GREP regular expressions[18], logical expressions[19] and lightning fast multiple simultaneous text searches of the Debtor's e-mail messages, documents, and files. This includes familiar programs such as 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, QuickBooks, Quicken, Money, Access, Microsoft SQL Server, Databases[20], financial and accounting applications[21], and Macintosh files just to mention a few. The eSleuthHound has tools available for the quick search of files with metadata information[22], 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 Pixie Dust.

After the recovery of the Debtor's deleted e-data, and using the forensic images created to simulate the Debtor's computer, 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 resulting electronic footprints showing how it all fits together ought to be of enormous monetary value to the Estate (not to mention supporting possible denial of the Debtor's discharge resulting from the discovery of deleted, concealed and/or falsified recorded

---

[17] 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.

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

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

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

[21] See previous footnote number four (4)

[22] 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.

information). This additional information source created by the eSleuthHound may provide e-clues that could uncover fraudulent accounting activities and point to how and where to find the money trail for the Estate.

Steganography[23] and Encrypted e-data:

An extensive investigation is made of the Pixie Dust to locate encrypted documents, folders, directories, and drives, on the Debtor's HDD, PDA or other 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 recommended that the eSleuthHound perform a steganalysis[24] for the discovery of hidden embedded information inasmuch as steganography amidst the Pixie Dust poses a significant threat to the investigation of the Debtor's e-data. If the Debtor is hiding e-data, don't you want to know about it?

When encryption and/or steganography have been discovered on the Debtor's forensic images, and the passwords are not available, the eSleuthHound will utilize decryption and steganalysis software to attempt to discover and break the passwords and find the hidden and/or encrypted information.

Most often encrypted and hidden information will likely provide confidential information that the Debtor, insider or author is concealing. Accordingly, this information may provide extensive e-clues that could expose fraudulent accounting activities and point to how and where to find the money. This can be a lengthy process. It will be shortened if the eSleuthHound has the most current decryption software[25].

E-Mail and Instant Messages:

Sometimes it may be necessary for the eSleuthHound to find, recover and examine extensive e-mail and instant messages from HDD, PDA and other 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*[26], "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."

Once the e-mail and instant messages are found, it will be necessary to use 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. The eSleuthHound has forensic software for filtering and sorting of these messages. In addition, it is possible to search on very specific criteria, i.e. whole words, exact words, case sensitive, ignore case, sounds like, approximately, date or date range, GREP regular expressions, logical expressions, and search parameter commands.

---

[23] Taken from the Greek language, steganography means covered writing and has been used for centuries for the hiding of secret messages.
[24] Steganalysis is the inspection of digital files to detect steganography.
[25] Including but not limited to decryption software for 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.
[26] National Law Journal, November 4, 2002, Digital Discovery Starts to Work

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 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.

Most e-mail programs actually create a database using proprietary programs and it becomes no small task to extract information from computer servers that contain databases such as Microsoft Exchange Server. In conjunction with the investigation of the hard copy documents, the eSleuthHound will use extraction tools and techniques for e-mail messages and the related text from the e-clues contained in them

Hidden Assets:

The eSleuthHound can provide the Trustee with detailed, summary and exception reports on the Debtor's activities, insiders, divisions, subsidiaries, brother/sister companies, sales of property, customers, creditors, employees, products, inventory, 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. The true picture of the financial and business activities of the Debtor are to be found on the forensic images and this map and chronology cannot be logically compared to any other examination of the Debtor's business affairs.

The following is a small example of how the Pixie Dust can assist the Trustee and lead to the discovery of the trail of the money for the Creditors of the Bankrupt Estate.

- Uncover fraudulent accounting activities and theft of intellectual property, trade secrets, and customer information.
- Find hidden assets, including the ability to trace individual transactions from start to finish.
- Unusual insider transactions, including money and property transfers and complex related-party activities.
- Assisting in solvency and asset valuation.
- Discovery of the backdating of vital documents.
- Discovery of facts and circumstances relating to issues of substance over form that could not otherwise be documented.
- Determining compliance with Section 521(4) Re: Examination of the Debtor's e-data from all sources
- Section 727 abuses and the destruction and/or withholding of computer and e-data.

Computer Forensic Methodologies

One should take care and consider this section when making the appropriate decision to engage the eSleuthHound for a Debtor case.

Dealing with technical aspects of a case, the eSleuthHound must use established computer forensic methodologies. Each Debtor case needs to be tailored to the facts and circumstance related to the information technologies used and this cannot necessarily be pre-fabricated. Every circumstance needs to be examined on a case-by-case basis.

The following is a non-exhaustive list of the best practices for the acquisition of forensic evidence within the bankruptcy context:

General Rules:

- Do not turn on, start or use the Debtor's computers, PDA or other Digital Devices until the e-data has been safeguarded.
- Always document every step during acquisition, preservation and processing of the Debtor's e-data;
- Always gather and analyze the digital evidence in accordance with written polices and procedures, and allowing for flexibility as may be necessary for the individual case.
- Use current computer forensic hardware and software for examination of the Debtor's e-data;
- Be familiar with the forensic tools that you are using to gather or analyze digital evidence.

Chain of evidence:

- Use and maintain chain of custody records during the life of the case for all Debtor HDD, PDA and other Digital Devices;
- Keep a chronological diary with dates, times, and detailed notes as to the investigation process;

Acquisition of the Debtor's e-data:

- Do not allow the writing of any information to the Debtor's HDD or digital devices;
- Do not rely on write-protection software, and always use write protection hardware;
- Sanitize HDD prior to using for copying/storage of the Debtor's forensic image;
- Acquire and secure the forensic image using a cryptographic Hash digest value for the Debtor's HDD and other devices, always preserving the original Debtor's information;
- Should the forensic image fail, the destination drive will be wiped (sanitized) before re-use;
- Create multiple forensic images for expanded investigation if necessary;

Preliminary measures for processing the Debtor's e-data:

- Be prepared for confronting computer viruses and worms early in the case;
- Maintain adequate e-forensic software for locating and breaking encrypted information;
- Examine all media sources for possible steganography and/or encrypted files, folders and drives;
- Search forensic image for hidden disk partitions and disk areas early in the case;
- Examine date settings early in the case;
- Review possible file backdating early in the case;
- Create a time line analysis for the e-data found on the forensic images;

Processing the Debtor's e-data:

- Restore additional forensic image to another sterile drive to have a bootable clone;
- Filter e-mail and instant messages by name, subject, key information, text, dates, and multiple addresses;
- Create the combined DataSource forensic image for expanded investigation if necessary;
- Index the Debtor's combined Digital DataSource for each file type/signature;
- Create and regularly update the combined Digital DataSource for fast searches;
- Use electronic Bates numbers to identify case facts, files, and documents as necessary;

Preservation of the Debtor's e-data:

- Protect and secure the Debtor's HDD, PDA and Digital Devices for several years including providing for storage and related environmental safeguard and other conditions;
- Be prepared to protect and secure the "pristine" image of the Debtor's HDD, PDA and Digital Devices for several years including providing for storage and related environmental safeguard and other conditions;
- Use care when moving and examining the Debtor's electronic information, and document accordingly;

Forensic hardware and software:

The eSleuthHound can get to the Pixie Dust, the Debtor's e-data, using many different, alternative approaches. This necessitates maintaining an extensive forensic software and hardware library. Digital technologies are evolving at the speed of light, so the eSleuthHound must stay current with the latest advances in these areas. Because most complex situations are never exactly the same the eSleuthHound is always prepared to handle the next hurdle to find the e-clues.

Summary:

Digital devices, computer networks, e-mail and the Internet have utterly changed how business is conducted. A trustee is now faced with the enormous challenge of conducting a digital investigation on the Debtor's turf. How is that possible? The author is hopeful that you now understand that you have a solution for the digital age.

The eSleuthHound, the forensic accountant, experienced in bankruptcy, litigation, financial and accounting matters represents the best of breeds. Knowledgeable, with sophisticated computer accounting applications[27] and especially effective in the analysis of financial information, the eSleuthHound provides maximum results for the Trustee. The Trustee should always consider engaging the services of the eSleuthHound in those cases where the "smell" of money exists. The eSleuthHound is the Trustee's entrée into and solution for the digital 21st Century.

Golden Rule:

If you, the reader, retain anything from this article, it should be this:

"Never turn on (or off) the Debtor's computer or digital devices prior to the eSleuthHound's safeguarding the Pixie Dust" – "**NEVER**".

About the Author:

Jack Seward is a manager at RosenfarbWinters, LLC, a New York metropolitan area forensic accounting firm, and has, for many years, specialized in the recovery and analysis of digital information.

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.

[27] Please see footnote number four (4)