

“Delete” Doesn’t Mean Delete (Revisited) Computer Forensics and Doublespeak

By Kenneth Shear

Kenneth R. Shear has been the Vice President of Electronic Evidence Discovery, Inc (“EED®”) of Seattle since 1993. He enjoys a worldwide reputation as a leading legal authority on electronic evidence. Mr. Shear has published several articles on legal aspects of electronic evidence and delivered presentations to many groups, including the Electronic Mail Association, Harvard Law School, meetings of the ABA, American Corporate Counsel Association (ACCA) and the Association of Information Management Administrators (ARMA), among others. Mr. Shear worked extensively with assisting large and small corporations in dealing with the emerging issues of electronic discovery in litigation. Mr. Shear heads EED’s Technology and Law Division, which develops and tests new automated proprietary discovery tools.

Introduction - The Deleted E-Mail that Wasn’t, and Other Non-Issues

As computer evidence has become increasingly important in litigation, there has been a concomitant need for experts to explain how computer systems work and the significance of computer data. As a result, a whole new trade has started to emerge - computer forensic experts, who include both employees of law enforcement agencies and private practitioners. This is a discipline in its infancy. To date there are few standards for evaluating forensic computer work. As you would expect under these circumstances, the quality varies widely. Excellent work has been done in many cases - unfortunately, then there is the what I call Computer Forensic Misconduct. It is the latter that is the focus of this paper. Let’s start with an example.

The Case of the Non-Deleted Emails

Not long ago, the company where I work, Electronic Evidence Discovery, Inc., received a call from a company facing charges of trade secret theft. A new salesman - we’ll call him Arnold for this discussion — had come over from a competitor, who charged that he had violated a non-compete agreement and also had taken valuable contact lists and other competitive information in spreadsheets and email. The competitor had engaged a reputable computer forensic expert to go through Arnold’s laptop hard drive, and the expert claimed that Arnold had deleted hundreds of email messages after the law-

suit was filed in an effort to hide the original misappropriation of data.

We looked over the expert’s findings and all seemed to be in order. He used a standard diskimaging program used by many law enforcement agencies to reliably collect data from hard drives. He printed out deleted emails, all of which seemed to come from the competitor’s system, as well as carefully identifying spreadsheets and a big database of sales contact information taken by Arnold.

Adding to the bleak picture our client faced, Arnold admitted taking much of this data from his former employer by copying it onto an Iomega ZIP disk.¹ Arnold claimed that the sales database was mostly the contacts he already had developed before going to work for the competitor and that the email he took was mostly his personal messages. Arnold took the ZIP-disk, connected it to the laptop provided by our client company, copied the information over, and threw away the ZIP disk.

When the competitor filed the lawsuit and demanded production of anything Arnold took, he obtained a new ZIP disk, copied some data onto it, and gave it to our client’s attorneys. The new ZIP disk contained only a handful of email messages; the expert working for the competitor had found over 900 deleted on Arnold’s laptop hard drive. It looked very much like Arnold, and our client, were caught red handed, with Arnold taking data from his

Continued on next page

“Delete” Doesn’t Mean Delete (Revisited)

former employer, then covering his tracks by deleting the data after the lawsuit started. To make matters worse, Arnold couldn’t explain what was going on with his email, saying that he knew he’d taken more messages from his former employer, but they had mysteriously disappeared from his computer. As if Arnold’s confusion weren’t enough, our client’s outside counsel had given Arnold’s laptop to their internal law firm information systems department, which had proceeded to install programs on the laptop hard drive potentially overwriting substantial amounts of deleted data. The opposing side’s expert was of the opinion that not only Arnold but the law firm representing our client had destroyed evidence.

EED was engaged by Arnold’s new employer to tell them what he had actually taken from their competitor and what, if anything, they could do to address the charges of theft and concealment of evidence. Our first step was to make our own clone of the hard drive from Arnold’s laptop, where we found the same evidence of deleted e-mails that the other side’s expert had found, but when we looked a little deeper, we found a few other things that he had overlooked.

Deletion (n.) - Moving Something from One Place to Another

For one thing, the seemingly deleted email on the hard drive wasn’t really deleted. There were two electronic mail programs on the hard drive, both made by Microsoft, one, called Outlook Express, comes with the Internet Explorer web browser and is designed to be used primarily as an Internet mail provider. The other, called Outlook, is a more full featured program that is designed to be used both for Internet mail and for email over a network such as a typical corporate system. There’s a big difference between the ways that these two programs store data. Outlook Express saves messages onto a computer’s hard drive in “plain text” format, meaning that if you look at the raw data in the file, you can see messages containing readable text. The more full-featured Outlook program, by contrast, normally stores data in an encrypted format, meaning that if you look at the raw data in an Outlook file, you see mostly incomprehensible streams of data². You generally

need to use the Outlook program to decrypt the file so you can read the messages. And you can’t see messages in an Outlook file unless you have properly opened the file under Outlook, a process that’s somewhat more complicated than opening a word processing document or a spreadsheet. Essentially, you connect the Outlook file to the program, so that when Outlook is opened the user sees a set of folders from that file (called “personal folders” by default).

When we looked at Arnold’s hard drive we found that Outlook Express was installed, but there was no icon for the program on the Windows desktop and all the email stored by Outlook Express had been deleted. There were two different files of information in the Outlook format, a smaller one that Arnold seemed to be using and that contained the few messages from his former employer that he had turned over, and a larger Outlook file that contained a copy of every single “deleted” message that the opposing side’s expert had “recovered.” According to the file dates showing on the hard drive, the larger Outlook file had never been opened.

It was obvious to us that the “deleted” mail had in fact not been deleted at all, but moved from an Outlook Express file into an Outlook file. We confirmed by questioning Arnold who explained further that his Outlook Express mail had disappeared after he had sent his laptop to the corporate systems department because of problems with his screen display. He remembered that the systems department had worked on the email client on his computer. We tracked down the technician who did this work, and he confirmed that he had upgraded Arnold’s Outlook installation 3, and converted the Outlook Express mail to Outlook format. He had converted the data (without asking Arnold) because it was standard practice at the time for the corporate systems department to move users into Outlook, believed to be a more appropriate email client for the firm’s business.

The technician had set up two Outlook files - one to hold the old mail that was already on the computer, and one to hold new mail. This made clear why the Outlook file holding the converted mail had not been opened by Arnold. The file dates showed that it was last used when

the technician was working on Arnold’s laptop. The technician had sent the laptop back to Arnold with the new Outlook connected to the Outlook program, but had left the Outlook file holding the old mail without connecting it to the Outlook program. Arnold would have had no way to find the old mail, if he did not know that there even was a second Outlook file on his computer.

What accounted for Arnold having the handful of email messages that he did turn over on the second ZIP disk? These were the messages that he had saved or moved into Outlook before the upgrade. With older versions of Outlook and Outlook Express, while there were menu choices to move messages from one format to the other, results were sometimes surprising unless you are very familiar with the import / export messages features of the programs. The process would tend to create complex sets of sub-folders and would not always move all of the sub-folder structure quite the way you expected it to. When we examined Arnold’s Outlook file containing old mail, it seemed to contain some irrational folder structures that appear to have been created as the files were moved around. It wasn’t possible to determine at what point the handful of messages found their way into a separate Outlook file, however.

The Descent into the Maelstrom of the Registry

From our perspective, the most shocking thing about the situation was the failure of the other side’s expert – a reputable computer forensic examiner – to look at the contents of the Outlook file before rendering his opinion about deleted e-mail. And even more astonishing was his response when we pointed out that the mail had been moved, rather than deleted. The expert (who had plenty of time to inspect the laptop prior to issuing a report) declared that he had been misled, because Arnold had not described the upgrade of the email and creation of the Outlook files in his deposition, and further that it was suspicious that we at EED found the Outlook file so quickly! Actually, finding Outlook email is a very simple procedure, because the Outlook files must have a proper extension (PST or OST) to work with the program. It was, from our per-

“Delete” Doesn’t Mean Delete (Revisited)

spective, inexcusable for someone acting as a computer forensic expert to render opinions about email on a computer without checking for Outlook mail in these circumstances.

As if this weren’t enough, the competitor’s forensic expert decided to redouble his efforts after learning of the Outlook mail on the computer. He looked carefully at the computer’s registry - a place where a Windows computer keeps track of the computer’s configuration and also tracks information about programs, particularly those created by Microsoft, that are tightly integrated with the Windows operating system. One of the registry settings for the Outlook 98 program listed the last file imported into Outlook, and seemed to point to a file that Arnold had used to bring over data from the competitor which was no longer found on Arnold’s hard drive. Since this was an Outlook 98 registry setting the expert concluded that Arnold must have imported some of the data he took from the competitor after Outlook 98 was installed, and that, therefore, he had not thrown away the ZIP disk he used to transfer the data from the competitor to our client, or else that our client had a copy of the competitor’s email on our client’s network.

But the competitor’s expert had again overlooked a significant fact. When you upgrade a computer from Outlook 97 to Outlook 98, the registry settings from Outlook 97 are incorporated into the Outlook 98 setup. So the Outlook 98 registry settings did not necessarily show that data had been imported after Outlook 98 was installed, because an upgrade from Outlook 97 to Outlook 98 would preserve

the setting showing the file that was the source of the last import of mail under Outlook 97.

The Attorneys in the Dock (or, perhaps, in the Dark)

With regard to the expert’s claim that the information systems technicians of our client’s outside law firm had installed software on Arnold’s hard drive and caused changes in the hard drive, that claim was correct. The changes occurred prior to the competitor’s expert issuing his report, when our client’s law firm was trying to take reasonable steps to preserve the data but was not yet prepared to go to the expense of bringing in an outside computer expert. Changes therefore had occurred, but there was no evidence that they had been for the purpose of destroying evidence or that any relevant evidence had actually been destroyed.

The expert claimed that, by booting up the Windows system on the laptop, many files were modified or resaved on the hard drive. That is so, every time a Windows computer is booted from its hard drive. But it is very likely that any files overwritten by this activity were the same files that had been changed the last time the computer was booted. The issue in this case was what had happened historically with the data on the computer - not the precise state of the computer immediately before it was examined. The booting of the computer by the information systems department law firm had no significant effect from this perspective. Nor did the installation of a program on the hard drive. This installation may have overwritten some system data or even some of the Outlook

Express messages that the competitor’s expert was busily recovering. But it would not affect what was really at issue - what Arnold had taken from the competitor and what he had done to produce data when ordered to do so.

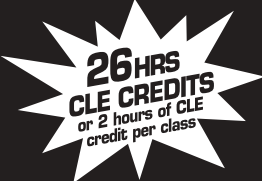
Raising the issue of relatively minor changes to the hard drive had little impact on the outcome of the case. But it did significantly increase the costs. Counsel for our client felt it was necessary to respond to these allegations to maintain credibility and to clear the air of yet another evidence destruction issue. So it was necessary to examine in some detail the changes on the drive in order to respond - even though there was no specific allegation of relevant evidence being destroyed, but only a general allegation that something had been done wrong.

All’s Not Well that Ends Well

The denouement of all of this made our client happy, but I was less so. The strategy of the competitor had been to focus on the allegations of destruction of computer evidence and seek to win the case by sanctions, rather than proving their claims. By answering these claims in detail, we altered this posture, leaving the Court with some fairly complicated computer technology to resolve. The Court basically disregarded these disputes in deciding the case on the merits - but then sanctioned Arnold for not having taken stronger steps to preserve what was on his computer after being ordered to do so. In effect, Arnold became responsible for innocent steps taken by a company computer technician to upgrade his system - steps that did not in fact result in any destruction of evidence. From our client’s perspective, however, it seemed that the sanctions were minor compared to the merits of the litigation.


From my perspective, this case was one of those that opened my eyes to a whole new emerging trend, which I call computer forensic misconduct. Increasingly, we are seeing cases where system information and computer data is misinterpreted, and where unjustifiable opinions are rendered. Arnold’s case illustrates several of these issues - incorrect identification of migrated data as “deleted”, misinterpretation of information from the sys-

Continued on next page



Are You Ready To Get Serious About Running Your Firm?

Join us for an intense, 13-week course covering the three software applications needed to run your business. Earn 26 CLE credit hours for the full 13-week course or attend individual classes for 2 CLE credit hours per class. Bright ideas. Great solutions. Call 601-992-6789.



“Delete” Doesn’t Mean Delete (Revisited)

tem registry, and unwarranted accusations of destruction of evidence. Yet judges and juries are rarely equipped to understand the technical complexities of information technology in this context. In Arnold’s case the competitor’s expert asserted that he had been sent on a “wild goose chase” by Arnold. Essentially the argument was that Arnold produced only a small amount of the email taken from his former employer saying it was all he had, but Arnold actually knew he had taken more. So Arnold was responsible for the expert thinking that Arnold had deleted the Outlook Express email and for the expert not looking at the Outlook file that the data was found in. From one perspective it’s understandable that the Court would hold Arnold responsible to disclose that some of his mail had disappeared - even if Arnold didn’t understand what had happened and might understandably be concerned about bad consequences if, as it appeared to him, his mail unaccountably disappeared when the computer was being serviced by his new employer’s technicians. But from another perspective, it is very distressing that the Court expressed no concern that someone holding themselves out as a computer forensic expert would go on a “wild goose chase” for deleted email without doing basic analysis that quickly made it obvious that the email had not been deleted at all.

Computer Forensic Misconduct - Misinterpretation of Data and Abuse of Authority

Unfortunately, the case discussed above is far from unusual in today’s world of computer forensics. Standards have not yet emerged for computer forensic work. Computer technology is changing rapidly, so that someone who has extensive experience in the field may have little actual knowledge of today’s technologies. On the other hand, programs are widely available that undelete files and have other “forensic” functions, so that it is possible to work with computer evidence without knowing very much at all about how the computer actually works - and without understanding the significance of what is being examined.

Deleted, Undeleted, and Non-Deleted

Recovery of deleted data is one of the main activities most people associate with

the idea of computer forensics. A lot has been written about the idea that delete doesn’t mean deleted - usually meaning that items which the user thought he or she deleted can be recovered in many instances. But there’s another side to all of this. What looks like deleted data on a computer - sometimes, even to a computer expert - often has gotten there by some other process besides deletion. But that doesn’t prevent some computer forensic evidence experts from leveling charges of destruction of evidence anyway. So practitioners need to be aware of some of the things that may masquerade as deletion:

Migrating files: As in Arnold’s story, the deletion process may be only one part of the whole story. You often find data that looks deleted on a drive, only because the information was moved into a different format. The data was “deleted,” but only after it had been saved somewhere else. It’s not fair to call this “deleted” data.

Moving files: Closely related to the migration process is what happens when you move a file from one location to another. The move process has two steps: copying the data to a new location, and deleting the listing showing the old location of the file (and sometimes the contents of the file as well). The second part of this process can look just like a deletion, when in fact it’s an artifact of copying the data to a different location.

Defragmentation: Disk or drive defragmentation is a process whereby data is moved around on a drive to store it

more efficiently. It’s needed because most computers use rules for data storage that permit files to be split up and stored in two or more locations, and place files in locations that are not the optimal for running the computer. Most systems have a special function called defragmentation that rearranges the files so that they are in contiguous chunks of disk space and optimize locations of the data. These defragmentation programs operate by moving the data to temporary holding areas, then recopying it to a new location. The process of relocating the data leaves residual data that looks, in many cases, very much like deleted data.

Temporary files: If the computer crashes or loses power while a file is open under an application, there is a substantial chance that the data in the file can be corrupted or lost. Many types of programs, such as those from standard office program suites, CAD files and data from other programs, create a temporary copy of a file when it is worked on. When the program is closed, these temporary or backup files are supposed to be automatically deleted, creating more information that can look like a “deleted” file, but actually had nothing to do with a user “deleting” data.

Compacting of files: Some types of data, such as email, are often found in files composed of more than one item. A single email file may hold thousands of messages. When a message is deleted

Continued on next page



Looking For Ideas On HIPAA Compliance?

Matrix Solutions will help your clients reach
HIPAA compliancy with an in-depth GAP Analysis
program. Bright ideas. Great solutions.
Call today at 601-992-6789.


Matrix
SOLUTIONS, INC.
www.matrixsolutions.com

“Delete” Doesn’t Mean Delete (Revisited)

ed, it remains in the file, but its content is marked as invalid data so the email program will no longer display it. Over time, if messages are being deleted, the file grows ever larger, with more and more space being taken up by deleted, “invalid” data. Not only does the file grow larger but its internal structure becomes more complex, increasing the chance that the data will become corrupt or flawed. In order to protect against this, most email programs have a “compacting” feature that rewrites the

email file essentially as a contiguous collection of “live” messages. This process can shrink the file substantially. It often overwrites the initial part of the file (however much data space it takes to hold the compacted file); the rest of the file remains present on the drive, but since it is no longer in the file, it is marked as invalid data. This left over data from the compaction process can look very much like deleted data - when it is often a copy of some of the messages that remain in the compacted file.

Renaming of files: In the Windows 95 system, when a file is renamed, the computer uses two steps (as in the case of moving files). First, a listing is written with the new file name; and second, the old file name is deleted from the directory listings. Most forensic examiners looking at the computer will list the old name of the file as a “deleted” entry, when it is only that the name of the file has been changed.

Swap File: Computers store data in “memory” and in “disk storage” on the hard drive. Data is stored in the computer’s memory while a file is open or processing is being done on the data. While the data is not being used, it is stored on hard drives or other data storage media, where forensic experts normally find files and “deleted data”. In order to increase the effective size of the computer’s memory, most operating systems including Windows and other systems “swap” data out of memory temporarily onto the hard drive. Often the computer will use a “swap file” for this data, and this file will grow and shrink depending on what processing is occurring on the computer at the time. Data formerly in a swap file that has subsequently shrunk can leave what looks like the footprint of deleted data on the drive.

Movement of Data from Networks: Some current models of data storage emphasize storage of data on networks where it can be accessed from different locations on a desktop or laptop computer. Data may be downloaded to the hard drive in a workstation while it is being worked on, then copied back to the network when the work is complete. This will again leave footprints resembling deleted data, where the “deletion” is an artifact of the networking process.

Forensic Misinterpretation of Data

A second major part of the computer forensics area is the interpretation of data. Here, the basic issue is whether or not the interpretation is supported actual evidence found on computer. And things are not always as they seem, as shown in the

Continued on next page

Your Clients Expect You To Know Everything.



From consultation to testimony, Koerber Turner, PLLC provides the financial counsel and litigation support you need to represent your clients in family law and other legal matters.

- Business Valuation Services
- Calculation of Damages
- Forensic Accounting
- Lost Profits Analysis
- Lost Earnings Analysis
- Shareholder Disputes
- Tax Issues Related to Settlements
- Consultation

KOERBER TURNER, PLLC

Tax, Valuation & Litigation Support Services

Jackson
(601) 960-0406

Hattiesburg
(601) 583-1000

Gulfport
(228) 868-7141

www.koerberturner.com

“Delete” Doesn’t Mean Delete (Revisited)

example above of the Outlook 98 registry entries that actually came from an earlier installation of Outlook 97. Computer systems rarely if ever are set up to save data for forensic purposes - the data is instead saved for the convenience of the user and to enhance the functionality of the computer system. The information is usually only as accurate as required for these purposes. A few examples where things can go awry in interpreting data found on computer:

Dates / times of files and messages: computer experts are sometimes called upon to provide opinions about the validity of dates and times of computer files and messages. We have seen experts render opinions that the date and time of an electronic mail message is accurate, or inaccurate, as represented on a computer - even where the question is meaningless. For example, dates and times in Outlook are stored in Greenwich Mean Time, and automatically change depending on the time zone setting for the computer. So the exact same message can appear with different dates. In these circumstances, you simply cannot say what the date and time of the message is, without information about the settings on the computer from which it was taken. But opinions are often rendered without reference to these settings.

Format of data: Data in computers is found in a variety of formats, and computer forensic experts often comment on the significance of the particular format in which it is found. A striking example: Files sent as attachments to email messages over the Internet must be put in a standard format, primarily because the files may be transmitted through different types of computer systems. The standard format is known as “Base64!” and involves conversion of the attachments to a format that looks meaningless to the human eye. In one case, where an individual was accused of stealing trade secrets, he had sent the file over email, and it was automatically Base64 encoded. The individual’s former employer hired a computer expert, who had three Ph.D.’s in computer science and taught at a major university - but most of his

experience was in older UNIX systems, where an archaic encoding program called “Uuencode” was used instead of the more effective Base64. The expert actually testified that the data was “hidden” intentionally by the user, when in actuality the data had automatically been encoded using the standard for transmitting information over the Internet.

Many Fish Bite When You’ve Got Good Bait

Perhaps even more important than the misinterpretation of evidence by computer forensic experts is the abuse of the legal process that has been fostered by “experts” who pay no attention to the normal limits of discovery, and offer services that, in the guise of computer discovery, in effect amount to litigation by dirty tricks. Consider the statements of one computer forensic practitioner:

In three quarters of cases I find porn on the machines, and attorneys use it however they can. That’s their job. We’re getting more and more calls to review the hard drives of employees who claim they were fired because of age, sex, or race discrimination. It’s a fishing expedition, but it works pretty well for most of our clients. The attorney usually goes back to the person filing the complaint and says: “We found some pretty outrageous material on your PC. That’s a violation of our company policy, so you could’ve lost your job anyway.”

In other words, the point of computer forensic examinations is not merely to establish relevant facts in the case. “It’s a fishing expedition,” plain and simple. Disturbingly, this practitioner reports that it works pretty well, to use the tools of computer forensics to come up with embarrassing information unrelated to the case, in order to pressure opponents. The discussion begins from a comment about pornography. But the interviewee goes on to state: “If the only way you can squeeze somebody’s shoes is to tell them you’re going to examine their home PC, sometimes that makes lawsuits go away.”⁶ The cited article is an excellent place to start, if one is looking for reasons that computer

forensic experts should not be allowed unrestricted access to the hard drives seized from parties in litigation or defendants.

Forensics, Doublespeak and Civil Liberties

A final word about a few civil liberties issues that the computer forensics area raises. A key issue is access to justice. Computer forensic work is expensive. Individual plaintiffs or criminal defendants may face ruinous expenses if they have to pay for expensive computer forensic experts. Costs of tens of thousands of dollars for going through a single hard drive are not unheard of. But imagine if Arnold in the case set forth above, had no forensic expert to rebut the charges leveled against him. Litigants faced with these types of allegations may be forced to choose between financial devastation or legal ruin. On the other hand, costs of computer forensic activity depend on factors that usually have nothing to do with the merits of a case. Should litigation be

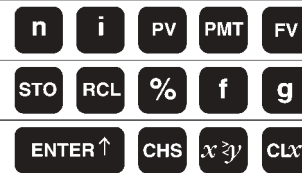
Continued on next page

Customized Asset Management

If you or your clients have \$250,000 or more to invest, we invite your inquiry as to our track record, background, and fee structure. Call us at 982-4123 or 1-800-844-4123.

Tim C. Medley, CFP
Cecil Brown, CPA/PFS
Kevin Anthony
Julius M. Ridgway, Jr.

Fee Only Financial Advisors



MEDLEY & BROWN FINANCIAL ADVISORS

P.O. Box 16725
Jackson, MS 39236-6725
795 Woodlands Parkway, Suite 104
Ridgeland, MS 39157
601/982-4123 • 1/800/844-4123
Fax 601-366-0013
www.medleybrown.com

“Delete” Doesn’t Mean Delete (Revisited)

more expensive and difficult, regardless of the merits, simply because a company or individual uses a computer system that presents problems for forensic analysis?

A second important issue is the quality of justice. The need to examine computer data leads to courts being confronted with more complex technical issues that judges and juries may not be equipped to deal with. This tends to make decision making more arbitrary. The increased emphasis on sanctions for destroying evidence means that more cases are focused on peripheral issues rather than the merits. All this tends to divert our legal system from attention to justice, rights and remedies, and into procedures and tactics.

Finally, computer forensic examinations tend to break down some of the barriers that have traditionally been used to protect privacy and individual freedom. Hard drive searches make information available to law enforcement authorities and attorneys that would have been much

more difficult to sweep into litigation in the past. Those who advocate this kind of activity often follow up by advising companies and individuals not to save data because of the danger it will be discovered. So does computer forensic work and electronic discovery mean the less information you have the better off you are? Hopefully not.

As our society’s information and knowledge has moved to computer systems, the legal system has struggled to keep up with the change. Our firm has wrestled with all of the issues and we always seek to find ways to target discovery on relevant data, keep costs within reason, and balance the needs for information with the practicalities of the legal practice. One of the great challenges of integrating legal procedures with the information age is to find ways to obtain data that do not undermine rights of privacy and freedom of expression, and do not disfavor the preservation of knowledge. ■

¹ A ZIP disk is a relatively common type of data cartridge that holds 100 megabytes or 250 megabytes of data and works like a big floppy diskette or small, slow hard drive. You need a ZIP drive to use the ZIP disk. A ZIP drive sometimes is found installed in the computer like the floppy disk drive or CD, or you can hook up a ZIP drive easily through a parallel port on your computer, where the printer is usually connected. Because it is easy to move the drive from one computer’s parallel port to another computer’s, ZIP disks have been a common way of moving data from one computer to another.

² If the Outlook program is set up using the default settings, the file storing the email will be encrypted. However, at the time the program is set up, or any time a new file is created for storing outlook data, the setting can be changed so that messages are stored under Outlook in plain text. It is relatively rare to find plain text Outlook files, and in the case discussed above, the Outlook files we found were encrypted.

³ The upgrade was from Outlook 97 to Outlook 98.

⁴ This is not a problem normally, because all popular email systems today automatically encode files in Base64 when they are sent and automatically decode the files when they are received. The user only sees Base64 code when something goes wrong.

⁵ U.S. News & World Report, “News You Can Use”, 10/2/00, quoting Ioan Feldman, President of Computer Forensics Inc.

■ LAW OFFICES OF BARRY J. WALKER ■



IMMIGRATION LEGAL SERVICES FOR BUSINESS,
INFORMATION TECHNOLOGY AND HEALTH EMPLOYERS

Barry J. Walker,
Member of the Mississippi Bar

M. Gabriela Ungo,
Member of the New York Bar

P.O. Box 1023
211 N. Madison Street
Tupelo, Mississippi

Telephone 662-841-0629
Facsimile 662-841-0620
Email immigration@msslawyer.com
www.immigrationpage.com

Foreign Languages: Spanish & French

Mark Your Calendars Now

The Mississippi
Bar’s

*Annual Meeting
&
Summer School*

July 5-10, 2004
Sandestin, FL