HELP! EMAIL IS TAKING OVER MY LIFE:
HOW TO TAME THE BEAST AND ORGANIZE THE MESSAGES

JASON SCOTT COOMER*, Austin*
Law Office of Jason Coomer

State Bar of Texas
BARTECH 05:
TECHNOLOGY STRATEGIES TO STAY
COMPETITIVE IN THE PRACTICE OF LAW
September 30, 2005
Houston

CHAPTER 11

Jason S. Coomer

Law Office of Jason S. Coomer
AbogadosdeTejas.com, LLC
406 Sterzing, Second Floor
Austin, Texas 78704
(512) 474-1477

Austin Lawyer, Jason Coomer, has been practicing law since 1995 and helps Texans that have been wrongfully injured or killed; that have lost their homes and possessions; or that have been wronged in a business transaction as a result of another's wrongful acts. **The Law Office of Jason Coomer** handles Personal Injury Claims including Residential Fires, Toxic Exposures (toxic mold, lead paint, black water), Automobile Collisions, Wrongful Death, Dangerous Conditions, & Construction Accidents. The Office also handles Consumer claims including Apartment Fire, Lemon Home, Negligence Construction, Construction Defects, Fraud and Misrepresentation, and Residential Fire & Toxic Tort claims. The Office also handles Computer Law including Domain & Intellectual Property Disputes, Business Development, & Breach of Contract.

AbogadosdeTejas.com, LLC, is an information technology consulting firm that provides Web Presence Development, Litigation Support, and Law Office Information Technology Consulting. Web Presence Development includes designing a Web presence that is tailored to the specific practice of a lawyer or law firm. Litigation Support includes development of presentations and demonstrative evidence with video, graphics, photos, sound and other multimedia. We can organize large amounts of data, prepare and respond to E-discovery, and assist at trial or ADR. Law Office Information Technology includes consulting in the set up networks, databases, and other information technology used in law offices.

Bar Tech '05

September 30, 2005

Houston, Texas Westin Oaks Hotel

Help E-mail is Taking Over My Life:
How to Tame the Beast and Organize the Messages

Presentation & Handout By:
Jason S. Coomer
Trial Lawyer and Technology Advisor
406 Sterzing, Second Floor
Austin, Texas 78704
e-mail: **BarTech05@texaslawyers.com**
Web: TexasLawyers.com
Office: 512-474-1477
Available at:
http://www.texaslawyers.com/BarTech05

Paper By:
Craig Ball
Trial Lawyer & Technologist
3402 Cedar Grove
Montgomery, Texas 77356
e-mail: **craig@ball.net**
Web: cybersleuthing.com
Office: 936-582-5040
Paper Available at:
http://www.ballpoint.org/emailpaper.pdf

Tips on How to Effectively Use E-mail

1. **Organize e-mail into useful categories for easy retrieval**
2. **Check your e-mail from multiple computers**
3. **Backup your e-mails monthly**
4. **Don't get sidetracked by spam (*spam filters*)**
5. **Virus Protection (*scan attachments*)**
6. **Don't put anything into an e-mail that you may regret (*Boeing & Microsoft*)**

Tips for proper e-mail etiquette

1. **Be professional, but get to the point**
2. **Do not attach large files or ask if its ok first**
3. **Include your name & e-mail address on all messages (*use a signature block*)**
4. **Word your Subject line carefully (*helps the recipient distinguish your message*)**
5. **Do not use all capitals (*sends the* MESSAGE THAT YOU ARE SCREAMING)**
6. **Proof your message before sending (*avoid misunderstandings & typos*)**

Bar Tech ‘05

September 30, 2005

Houston, Texas Westin Oaks Hotel

Help E-mail is Taking Over My Life:
How to Tame the Beast and Organize the Messages

e-mail Applications

1. **Outlook Express (download for free)**
2. **Netscape (download for free)**
3. **Mozilla (download for free)**
4. **Webmail (Yahoo, Gmail & other free webmails)**
5. **Outlook (included in Microsoft Office Suite about $200)**
6. **Eudora (download for about $50)**

Texas Lawyer’s Top 9 Web Sites

1. **Dogpile dogpile.com**
2. **MyTexasBar.com - State Bar Portal**
3. **Google google.com**
4. **Howard Nation's Information Library http://www.howardnations.com/nlli.html**
5. **The Texas Statutes http://capitol.tlc.state.tx.us/**
6. **Texas Legislature On-line http://www.capitol.state.tx.us/**
7. **WebMD http://www.webmd.com/**
8. **Tech Web http://www.techweb.com/**
9. **TexasLawyers.com http://www.texaslawyers.com**

Technology Tips

1. **Upgrade Internet connections**
2. **Go Wireless**
3. **Use the web for research**
4. **Use video/images/charts**
5. **Backup you data**
6. **Join an internet community**
7. **Use multiple computers**
8. **Learn to integrate software**
9. **Practice, practice, practice**

Jason Coomer
TexasLawyers.com

Craig Ball
Cybersleuthing.com

CRAIG BALL

Trial Lawyer & Technologist
Computer Forensic Examiner

3402 Cedar Grove
Montgomery, Texas 77356
E-mail: craig@ball.net
Web: cybersleuthing.com
Office: 936-582-5040
Fax: 936-582-4234
Home: 936-448-4321

Craig Ball is a Board Certified trial lawyer and computer expert with twenty-three years experience resolving a wide range of personal injury and products liability disputes. He's also dedicated his career to teaching lawyers about technology and trial tactics. Craig now limits his work to serving as a court-appointed special master and consultant in computer forensics and to publishing and lecturing on computer forensics, emerging technologies, digital persuasion and electronic discovery. Craig's monthly e-discovery column, "Ball in Your Court," appears in Law Technology News. While Chair of the State Bar of Texas' Technology Advisory Committee, Mr. Ball created the MYTexasBar web portal now used by over 45,000 Texas lawyers. Named as one of the Best Lawyers in America and a Texas Superlawyer, Craig is a recipient of the Presidents' Award, the State Bar of Texas' most esteemed recognition of service to the profession.

EDUCATION

Rice University (B.A., triple major, English, Managerial Studies, Political Science, 1979); University of Texas (J.D., with honors, 1982); Oregon State University (Computer Forensics certification, 2003); EnCase Intermediate Reporting and Analysis Course (Guidance Software 2004); WinHex Forensics Certification Course (X-Ways Software Technology AG 2005).

SELECTED PROFESSIONAL ACTIVITIES

Law Offices of Craig D. Ball, P.C.; Licensed in Texas since 1982.
Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization
Certified Computer Forensic Examiner, Oregon State University and NTI
Admitted to practice U.S. Court of Appeals, Fifth Circuit; U.S.D.C., Southern, Northern and Western Districts of Texas.
Member, Editorial Advisory Board, Law Technology News (American Lawyer Media)
Special Master, Electronic Discovery, Federal and Harris County (Texas) District Courts
Instructor in Computer Forensics, United States Department of Justice
Special Prosecutor, Texas Commission for Lawyer Discipline, 1995-96
Council Member, Computer and Technology Section of the State Bar of Texas, 2003-
Chairman: Technology Advisory Committee, State Bar of Texas, 2000-02
President, Houston Trial Lawyers Association (2000-01); President, Houston Trial Lawyers Foundation (2001-02)
Director, Texas Trial Lawyers Association (1995-2003); Chairman, Technology Task Force (1995-97)
Member, High Technology Crime Investigation Association and International Information Systems Forensics Association
Member, Texas State Bar College
Member, Continuing Legal Education Comm., 2000-04, Civil Pattern Jury Charge Comm., 1983-94,State Bar of Texas
Life Fellow, Texas and Houston Bar Foundations
CLE Course Director: E-Discovery A to Z (NY, Chicago, SF, Boston, Washington, D.C. and Minnepolis) 2004; Electronic Evidence and Discovery 2004, 2005; Advanced Evidence and Discovery Course 2003; 2002; Enron—The Legal Issues, 2002; Internet and Computers for Lawyers, 2001-02; Advanced Personal Injury Law Course, 1999, 2000; Preparing, Trying and Settling Auto Collision Cases, 1998.
Member, SBOT President's "Vision Council" on Technology, 1999-2000; Strategic Planning Committee Liaison, 2001-02; Corporate Counsel Task Force 2001-02

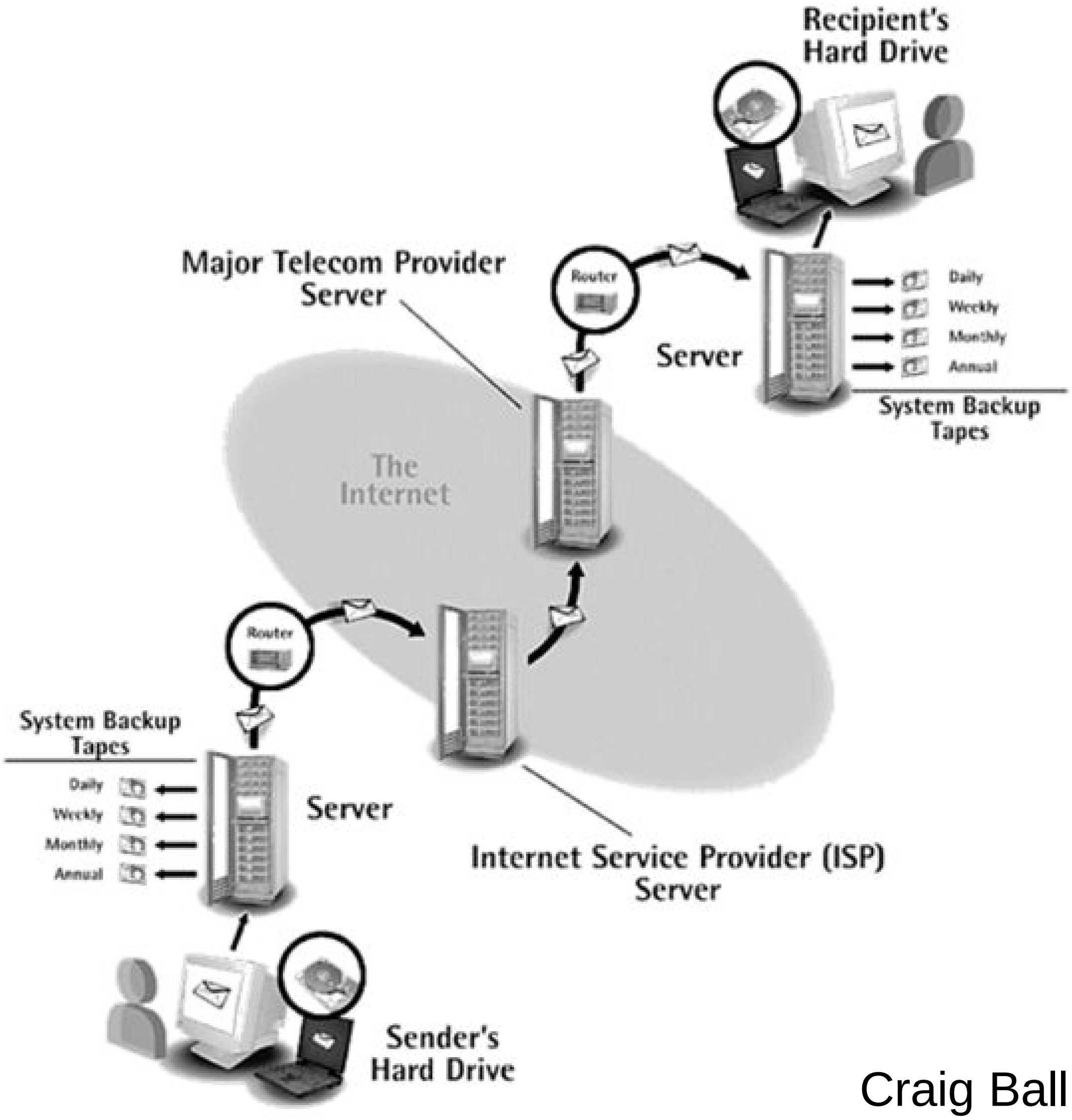
ACADEMIC APPOINTMENTS AND HONORS

The March 2002 CLE program planned by Mr. Ball and Richard Orsinger entitled, "Enron—The Legal Issues" received the Best CLE of 2002 award from the Association for Legal Education
National Planning Committee, Legal Works 2004 (San Francisco)
Recipient, State Bar of Texas Presidents' Award (bar's highest honor), 2001
Faculty, Texas College of Trial Advocacy, 1992 and 1993
Adjunct Professor, South Texas College of Law, 1983-88
Listed in "Best Lawyers in America" and Selected as a "Texas Super Lawyer," 2003 and 2004
Rated AV by Martindale-Hubbell

LAW RELATED PUBLICATIONS AND PRESENTATIONS

Craig Ball is a prolific contributor to continuing legal and professional education programs throughout the United States., having delivered over 350 presentations and papers. Craig's articles on forensic technology and electronic discovery frequently appear in the national media, including in American Bar Association, ATLA and American Lawyer Media print and online publications. He also writes a monthly column on computer forensics and e-discovery for Law Technology News called "Ball in your Court." The presentation, "Craig Ball on PowerPoint," is consistently the top rated educational program at the ABA TechShow.

Meeting the Challenge: E-Mail in Civil Discovery



Craig Ball
Trial Lawyer and Technologist
Certified Computer Forensic Examiner
Montgomery, Texas
Tel: (936) 448-4321
e-mail: craig@ball.net

Cover Illustration courtesy Kroll Ontrack

This Page
Intentionally Left Blank

Meeting the Challenge: E-Mail in Civil Discovery
Craig Ball

Table of Contents

© 2004 Craig Ball

All Rights Reserved

Understanding E-Mail in Civil Discovery

Introduction

Get the e-mail! It's the watchword in discovery today. Some label the press for production of electronic mail a feeding frenzy, but it's really just an inevitable recognition of how central to our lives e-mail has become. Lawyers go after e-mail because it accounts for the majority of business communications, and e-mail users tend to let their guard down and share things online that they'd never dare put in a memo. But if you're the lawyer on the receiving end of an e-mail discovery request, you not only have to be concerned about the contents of the messages, you may face a bigger challenge finding your client's e-mail, preserving it from spoliation and producing responsive items without betraying privileged or confidential communications. Meeting that challenge effectively takes effort geared to understanding the technology and formulating a winning strategy.

This paper seeks to equip the corporate counsel or trial lawyer with just about anything they might need to know to pursue or defend against the discovery of e-mail in civil litigation. Be warned that the paper—in particular pp. 5-17--is replete with technical information which I've tried to convey in manner that anyone reasonably comfortable with personal computers can grasp. If you don't enjoy technical topics, I urge you to plow through anyway because it's so important for a litigator to have a working knowledge of computer technology. Your "reward" will be the forty tips on pp. 29-32 for those seeking and defending against electronic discovery. Hopefully one or more of the tips, and the other information that follows, will aid you and your clients.

Not Enough Eyeballs

Futurist Arthur C. Clarke said, "Any sufficiently advanced technology is indistinguishable from magic." E-mail, like electricity, refrigeration and broadcasting, is one of those magical technologies most of use every day without really understanding how it works. But is there a judge who will accept, "I dunno, it's just magic," as an explanation of your client's e-mail system or as justification for a failure to preserve or produce discoverable e-mail?

A lawyer managing electronic discovery is obliged to do more than just tell their clients to "produce the e-mail." You've got to make an effort to understand their systems and procedures and be able to ask the right questions, as well as know when you aren't getting the right answers. To be sure, that's asking a lot, but 95% of all business documents are created digitally and most are never printed. *Fifty billion* e-mails traverse the Internet *daily,* far more than telephone and postal traffic combined, and the average business person sends and receives between 50 and 150 e-mails *every business day.* E-mail contributes *500 times greater volume* to the Internet than web page content. In discovery, it's increasingly

© 2004 Craig Ball

All Rights Reserved

infeasible to put enough pairs of trained eyes in front of enough computers to thoroughly review every e-mail. Much as we'd like, lawyers can't put their heads under their pillows and hope that it all goes away.

Test Your E.Q.

While I'm delivering bad news, let me share *worse* news: if you don't change the way your corporate clients do business by persuading them to initiate and enforce web- and e-mail usage restrictions with an iron fist, complete with Big Brother-style monitoring, you *will* fail to locate and produce a sizable part of your clients' electronic communications--and you won't even *know* you missed them until you see examples attached to opposing counsel's motion for sanctions. Of course, e-mail enabled cell phones, the Blackberry and other PDAs present pitfalls, but I'm also alluding to the digital channels that fall *outside* your client's e-mail server and back up tape system, like Internet Messaging, browser based e-mail and voice messaging.

Suppose opposing counsel serves a preservation letter or even a restraining order requiring your client to preserve electronic messaging. You confidently assure opposing counsel and the court that your client's crack team of information technologists will faithfully back up and preserve the data on the e-mail servers. You're more tech-savvy than most, so you even think to suspend the recycling of back up tapes. But are you really capturing all of the discoverable communications? How much of the 'Net is falling outside your net?

Can you answer these questions about your client's systems?

- Do *all* discoverable electronic communications come in and leave via the company's e-mail server?
- Does your archival system capture e-mail stored on individual user's hard drives, including company-owned laptops?
- Do employees ever use personal e-mail addresses or browser-based e-mail services (like Hotmail or Yahoo Mail) for any business communications?
- Do any employees use Internet Messaging on company computers or over company-owned networks?
- How do the company voice messaging systems store messages, and how long are they retained?

Troubled that you can't answer some of these questions? You should be, but know you're not alone. If your client runs a large network, capturing all the messaging traffic is a challenge akin to catching a spilled bucket of water in your bare hands. It's nearly impossible, and *you are going to miss something*.

Staying Out of Trouble

Fortunately, the rules of discovery don't require you to do the impossible. All they require is diligence, reasonableness and good faith. To that end, you must be able to establish that you and your client acted swiftly, followed a sound plan, and took such action as reasonable minds would judge adequate to the task. It's also important to keep the lines of communication open with the opposing party and the court, seeking agreement with the former or the protection of the latter where fruitful. I'm fond of saying that, "Even a dog knows the difference between being kicked and being tripped over." Likewise, it's hard to get much traction for a sanctions motion when it is clear to all concerned that the failure to produce electronic evidence was not part of an effort to conceal something or grew out of laziness, stupidity or arrogance.

…And You Could Make Spitballs with It, Too

Paper discovery enjoyed a self-limiting aspect in that businesses tended to allocate paper records into files, folders and cabinets according to persons, topics, transactions or periods of time, and did so throughout the business process. The space occupied by paper and the high cost to create, manage and store paper records served as a constant impetus to cull and discard them, or even to avoid creating them in the first place. By contrast, the ephemeral character of electronic communications, the ease of and perceived lack of cost to create, duplicate and distribute them and the very low direct cost of data storage has facilitated a staggering and unprecedented growth in the creation and retention of electronic evidence. At fifty e-mails per day, a company employing 100,000 people could find itself storing well over *1.5 billion* e-mails annually.

Did You Say *Billion*?

But volume is only part of the challenge. Unlike paper records, e-mail tends to be stored in massive data blobs. The single file containing my Outlook e-mail is almost a gigabyte in size and contains some 20,000 messages, many with multiple attachments, covering virtually every aspect of my life, and many other people's lives, too. In thousands of those e-mails, the subject line bears only a passing connection to the contents as "Reply to" threads strayed further and further from the original topic. E-mails meander through disparate topics or, by absent-minded clicks of the "Forward" button, lodge in my inbox dragging with them, like toilet paper on a wet shoe, the unsolicited detritus of other people's business. To respond to a discovery request for e-mail on a particular topic, I'd either need to skim/read all 20,000+ messages or I'd have to have a very high degree of confidence that a keyword search would flush out all responsive material. If the request for production implicated material I no longer kept on my current computer, I'd be forced to root around through a motley array of old systems, obsolete disks, outgrown hard drives, ancient back up tapes (for which I have no tape reader) and unlabeled CDs, uncertain whether I've lost the information or just overlooked it somewhere along the way.

Net Full of Holes

So what's a company to do when served with a request for "all e-mail" on a particular matter in litigation? Surely, I mused, someone must have found a better solution than repeating, over and over again, the tedious and time-consuming process of accessing individual e-mail servers at far-flung locations along with the local drives of all key players' computers? For this article, I contacted colleagues in both large and small electronic discovery consulting groups, inquiring about "the better way" for enterprises, and was struck by the revelation that, if there was a better mousetrap, they hadn't discovered it either. Uniformly, we recognized such enterprise-wide efforts were gargantuan undertakings fraught with uncertainty, and concluded that counsel must somehow seek to narrow the scope of the inquiry—either by data sampling or through limiting discovery according to offices, regions, time span, business sectors or key players. Trying to capture *everything,* enterprise-wide, is trawling with a net full of holes.

E-Mail Systems and Files

Michelle Lange of the national e-discovery firm Kroll OnTrack relates that Microsoft Exchange Server and Outlook e-mail account for nearly 75% of the e-mail Kroll encounters in its engagements, with Lotus Notes a distant second at 13%. Accordingly, the following discussion principally addresses the Microsoft e-mail applications, but be aware that each system employs its own twist on file structures and names. For example, AOL has long used a proprietary mail format incompatible with other common standards.

A Snippet about Protocols

Computer network specialists are always talking about this "protocol" and that "protocol." Don't let the geek-speak get in the way. An *application protocol* is a bit of computer code that facilitates communication between applications, i.e., your e-mail client, and a network like the Internet. When you send a snail mail letter, the U.S. Postal Service's "protocol" dictates that you place the contents of your message in an envelope of certain dimensions, seal it, add a defined complement of address information and affix postage to the upper right hand corner of the envelope adjacent to the addressee information. Only then can you transmit the letter through the Postal Service's network of post offices, delivery vehicles and postal carriers. Omit the address, the envelope or the postage--or just fail to drop it in the mail--and Grandma gets no Hallmark this year! Likewise, computer networks rely upon protocols to facilitate the transmission of information. You invoke a protocol—*Hyper Text Transfer Protocol*—every time you type *http://* at the start of a web page address.

Incoming Mail: POP, IMAP, MAPI and HTTP E-Mail

Although Microsoft Exchange Server rules the roost in enterprise e-mail, it's by no means the most common e-mail system for the individual and small business user. When you access your personal e-mail from your own Internet Service Provider (ISP), chances are your e-mail comes to you from your ISP's e-mail server in one of three ways, POP, IMAP or HTTP, the last commonly called web- or browser-based e-mail. Understanding how these three protocols work—and differ—helps in identifying where e-mail can or cannot be found.

POP (for Post Office Protocol) is the oldest and most common of the three approaches and the one most familiar to users of the Outlook Express, Netscape and Eudora e-mail clients. Using POP, you connect to a mail server, download copies of all messages and, unless you have configured your e-mail client to leave copies on the server, the e-mail is deleted on the server and now resides on the hard drive of the computer you used to pick up mail. Leaving copies of your e-mail on the server seems like a great idea, since you have a back up if disaster strikes and can access your e-mail, again and again, from different computers. However, few ISPs afford unlimited storage space on their servers for users' e-mail, so mailboxes quickly become "clogged" with old e-mails and the servers start bouncing new messages. As a result, POP e-mail typically resides only on the local hard drive of the computer used to read the mail and on the back up system for the servers which transmitted, transported and delivered the messages. In short, POP is locally-stored e-mail that supports some server storage.

IMAP (Internet Mail Access Protocol) functions in much the same fashion as most Microsoft Exchange Server installations in that, when you check your e-mail, your e-mail client downloads just the headers of e-mail it finds on the server and only retrieves the body of a message when you open it for reading. Else, the entire message stays in your account on the server. Unlike POP, where e-mail is searched and organized into folders locally, IMAP e-mail is organized and searched on the server. Consequently, the server (and its back up tapes) retains not only the messages but also the way the user structured those messages for archival. Since IMAP e-mail "lives" on the server, how does a user read and answer it without staying connected all the time? The answer is that IMAP e-mail clients afford users the ability to synchronize the server files with a local copy of the e-mail and folders. When an IMAP user reconnects to the server, local e-mail stores are updated (synchronized) and messages drafted offline are transmitted. So, to summarize, IMAP is server-stored e-mail, with support for synchronized local storage.

MAPI (Messaging Application Programming Interface) is the e-mail protocol at the heart of Microsoft's Exchange Server application. Like IMAP, MAPI e-mail is typically stored on the server, not the client machine. Likewise, the local machine may be configured to synchronize with the server mail stores and keep a copy of mail on the local hard drive, but this is user- and client application-dependent. If the user hasn't taken steps to keep a local copy of e-mail, e-mail is not likely to be found on the local hard drive, except to the extent fragments may turn up through computer forensic examination.

HTTP (Hyper Text Transfer Protocol) mail, or web-based/browser-based e-mail, dispenses with the local e-mail client and handles all activities on the server, with users managing their e-mail using their Internet browser to view an interactive web page. Although some browser-based e-mail services support local synchronization with an e-mail client, typically users do not have any local record of their browser-based e-mail transactions except for messages they've affirmatively saved to disk or portions of e-mail web pages which happen to reside in the browser's cache (e.g., Internet Explorer's Temporary Internet Files folder). Hotmail and Yahoo Mail are two popular examples of browser-based e-mail services, although many ISPs (including all the national providers) offer browser-based e-mail access in addition to POP and IMAP connections.

The protocol used to carry e-mail is not especially important in electronic discovery except to the extent that it signals the most likely place where archived e-mail can be found. Companies choose server-based e-mail systems (e.g., IMAP and MAPI) for two principal reasons. First, such systems make it easier to access e-mail from different locations and machines. Second, it's easier to back up e-mail from a central location. Because IMAP and MAPI systems store all e-mail on the server, the back up system used to protect server data can yield a mother lode of server e-mail. Depending upon the back up procedures used, access to archived e-mail can prove a costly and time-consuming task or a relatively easy one. The enormous volume of e-mail residing on back up tapes and the potentially high cost to locate and restore that e-mail makes discovery of archived e-mail from back up tapes a big bone of contention between litigants. In fact, most reported cases addressing cost-allocation in e-discovery seem to have been spawned by disputes over e-mail on server back up tapes.

Outgoing Mail: SMTP and MTA

Just as the system that brings water into your home works in conjunction with a completely different system that carries wastewater away, the protocol that delivers e-mail to you is completely different from the one that transmits your e-mail. Everything discussed in the preceding paragraph concerned the protocols used to *retrieve* e-mail from a mail server. Yet, another system altogether, called SMTP for Simple Mail Transfer Protocol, takes care of outgoing e-mail. SMTP is indeed a very simple protocol and doesn't even require authentication, in much the same way as anyone can anonymously drop a letter into a mailbox. A server that uses SMTP to route e-mail over a network to its destination is called a Message Transfer Agent (MTA). Examples of MTAs you might hear mentioned by IT professionals include Sendmail, Exim, Qmail and Postfix. Microsoft Exchange Server is an MTA, too. In simplest terms, an MTA is the system that carries e-mail between e-mail servers and sees to it that the message gets to its destination. Each MTA reads the code of a message and determines if it is addressed to a user in its domain and, if not, it passes the message on to the next MTA after adding a line of text to the message identifying the route to later recipients. If you've ever set up an e-mail client, you've probably had to type in the name of the servers handling your outgoing e-mail (perhaps *SMTP.yourISP.com*) and your incoming messages (perhaps *mail.yourISP.com* or *POP.yourISP.com*).

Anatomy of an E-Mail Header

Now that we've waded through the alphabet soup of protocols managing the movement of an e-mail message, let's take a look inside the message itself. Considering the complex systems on which it lives, an e-mail is astonishingly simple in structure. The Internet protocols governing e-mail transmission require electronic messages to adhere to rigid formatting, making individual e-mails fairly easy to dissect and understand. The complexities and headaches associated with e-mail don't really attach until the e-mails are stored and assembled into databases and post office files.

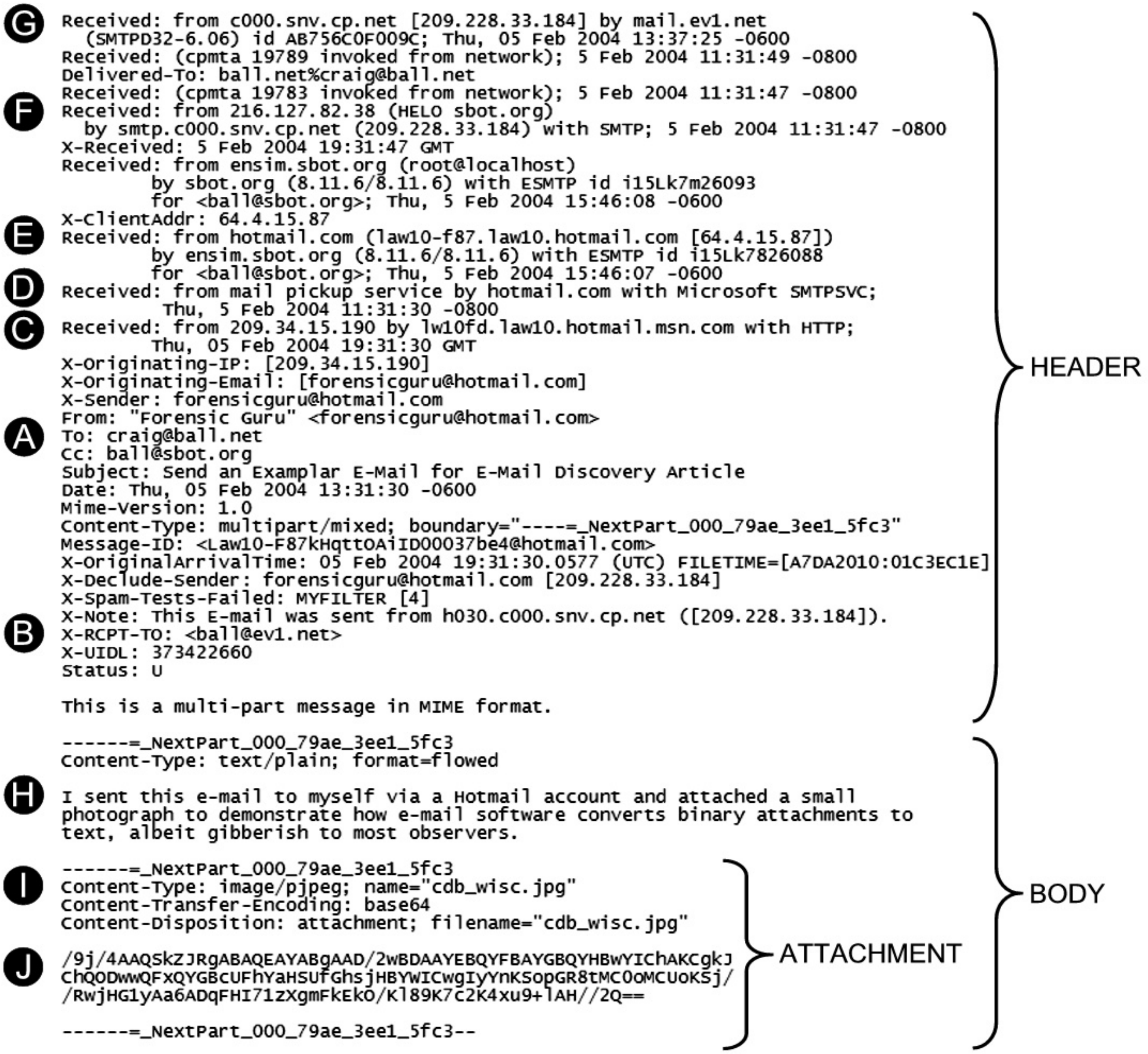
An e-mail is just a plain text file. Though e-mail can be "tricked" into carrying non-text binary data like application files (i.e., a Word document) or image attachments (e.g., GIF or .JPG files), this piggybacking requires binary data be encoded into text for transmission. Consequently, even when transmitting files created in the densest computer code, *everything in an e-mail is plain text*.

Figure 1 shows the source code of an e-mail which I sent using a browser-based Hotmail account. The e-mail was sent from forensicguru@hotmail.com and addressed to craig@ball.net, with a cc: to ball@sbot.org. A small photograph in JPG format was attached to the message.

Before we dissect the e-mail message in Figure 1, note that any e-mail can be divided into two parts, the header and body of the message. By design, the header details the journey taken by the e-mail from origin to destination; but be cautioned that it's a fairly simple matter for a hacker to spoof (falsify) the identification of all but the final delivery server. Accordingly, where the origin or origination date of an e-mail is suspect, the actual route of the message may need to be validated at each server along its path.

In an e-mail header, each line which begins with the word "Received:" represents the transfer of the message between or within systems. The transfer sequence is reversed chronologically; such that those closest to the top of the header were inserted after those that follow, and the topmost line reflects delivery to the recipient's e-mail server. As the message passes through intervening hosts, each adds its own identifying information along with the date and time of transit.

Figure 1.



```
Received: from c000.snv.cp.net [209.228.33.184] by mail.ev1.net
  (SMTPD32-6.06) id AB756C0F009C; Thu, 05 Feb 2004 13:37:25 -0600
Received: (cpmta 19789 invoked from network); 5 Feb 2004 11:31:49 -0800
Delivered-To: ball.net%craig@ball.net
Received: (cpmta 19783 invoked from network); 5 Feb 2004 11:31:47 -0800
Received: from 216.127.82.38 (HELO sbot.org)
  by smtp.c000.snv.cp.net (209.228.33.184) with SMTP; 5 Feb 2004 11:31:47 -0800
X-Received: 5 Feb 2004 19:31:47 GMT
Received: from ensim.sbot.org (root@localhost)
        by sbot.org (8.11.6/8.11.6) with ESMTP id i15Lk7m26093
        for <ball@sbot.org>; Thu, 5 Feb 2004 15:46:08 -0600
X-ClientAddr: 64.4.15.87
Received: from hotmail.com (law10-f87.law10.hotmail.com [64.4.15.87])
        by ensim.sbot.org (8.11.6/8.11.6) with ESMTP id i15Lk7826088
        for <ball@sbot.org>; Thu, 5 Feb 2004 15:46:07 -0600
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
         Thu, 5 Feb 2004 11:31:30 -0800
Received: from 209.34.15.190 by lw10fd.law10.hotmail.msn.com with HTTP;
        Thu, 05 Feb 2004 19:31:30 GMT
X-Originating-IP: [209.34.15.190]
X-Originating-Email: [forensicguru@hotmail.com]
X-Sender: forensicguru@hotmail.com
From: "Forensic Guru" <forensicguru@hotmail.com>
To: craig@ball.net
Cc: ball@sbot.org
Subject: Send an Examplar E-Mail for E-Mail Discovery Article
Date: Thu, 05 Feb 2004 13:31:30 -0600
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_NextPart_000_79ae_3ee1_5fc3"
Message-ID: <Law10-F87kHqttOAiID00037be4@hotmail.com>
X-OriginalArrivalTime: 05 Feb 2004 19:31:30.0577 (UTC) FILETIME=[A7DA2010:01C3EC1E]
X-Declude-Sender: forensicguru@hotmail.com [209.228.33.184]
X-Spam-Tests-Failed: MYFILTER [4]
X-Note: This E-mail was sent from h030.c000.snv.cp.net ([209.228.33.184]).
X-RCPT-TO: <ball@ev1.net>
X-UIDL: 373422660
Status: U

This is a multi-part message in MIME format.

------=_NextPart_000_79ae_3ee1_5fc3
Content-Type: text/plain; format=flowed

I sent this e-mail to myself via a Hotmail account and attached a small
photograph to demonstrate how e-mail software converts binary attachments to
text, albeit gibberish to most observers.

------=_NextPart_000_79ae_3ee1_5fc3
Content-Type: image/pjpeg; name="cdb_wisc.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="cdb_wisc.jpg"

/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAYEBQYFBAYGBQYHBwYIChAKCgkJ
ChQODwwQFxQYGBcUFhYaHSUfGhsjHBYWICwgIyYnKSopGR8tMC0oMCUoKSj/
/RwjHG1yAa6ADqFHI71zXgmFkEkO/Kl89K7c2K4xu9+lAH//2Q==

------=_NextPart_000_79ae_3ee1_5fc3--
```

Tracing an E-Mail's Incredible Journey

In this header, taken from the cc: copy of the message, section **(A)** indicates the parts of the message designating the sender, addressee, cc: recipient, date, time and subject line of the message. Though a message may be assigned various identification codes by the servers it transits in its journey (each enabling the administrator of the transiting e-mail server to track the message in the server logs), the message will contain one unique identifier assigned by the originating Message Transfer Agent. The unique identifier assigned to this message (in the line labeled "Message-ID:") is "Law10-F87kHqttOAiID00037be4@ hotmail.com."

In the line labeled "Date," both the date and time of transmittal are indicated. The time indicated is 13:31:30, and the "-0600" which follows this time designation denotes the time *difference* between the sender's local time (the system time on the sender's computer) and Greenwich Mean Time (GMT), also called Universal Time or UTC. As the offset from GMT is minus six hours, we deduce that the message was sent from a machine set to Central Standard Time, giving some insight into the sender's location. Knowing the originating computer's time and time zone can occasionally prove useful in demonstrating fraud or fabrication.

At **(B)** we see that although this carbon copy was addressed to ball@sbot.org, the ultimate recipient of the message was ball@EV1.net. How this transpired can be deciphered from the header data.

The message was created and sent using Hotmail's web interface; consequently the first hop **(C)** indicates that the message was sent using HTTP from my home network router, identified by its IP address: 209.34.15.190. The message is received by the Hotmail server **(D),** which transfers it to a second Hotmail server using SMTP. The first Hotmail server timestamps the message in Greenwich Mean Time (GMT) but the second Hotmail server timestamps in its local time, noting a minus eight hour offset from GMT. This suggests that the Hotmail server is located somewhere in the Pacific Time zone. The next hand off **(E)** is to the Ensim appliance on the SBOT.org server, where the message is designated for user ball@sbot.org. Note the erroneous timestamp affixed by the SBOT.org. Although the message has apparently come back into the Central Time zone, the receiving server's clock is some 135 minutes fast!

The message has reached its appointed destination at SBOT.org; however, its incredible journey is far from done. The header informs us that the SBOT.org server is set up to forward mail addressed to ball@sbot.org to another address, and so we follow the message as it heads to a server two time zones west, belonging to a company called Critical Path (cp.net). There, **(F)** the message is delivered to the address craig@ball.net. But it appears that mail addressed to craig@ball.net is also automatically forwarded to yet another address and server! The message skedaddled back to the Lone Star State, to a server operated by EV1.net, and **(G)** ultimately to the mailbox for ball@EV1.net **(B).**

Turning to the body of the message, notice how the content of the message **(H)** is set off from the header and the attachment **(I)** by a blank line and a boundary code generated by the e-mail client: **------=_NextPart_000_79ae_3ee1_5fc3**. Note, also, how the attachment, a photograph with the filename "cdb_wisc.jpg," has been encoded from non-printable binary code into a long string of plain text characters (J) able to traverse the network as an e-mail, yet easily converted back to binary data when the message reaches its destination. In order to fit the page, only three lines of the encoded data are shown. The encoded data actually occupied fifty lines of text.

Clearly, e-mail clients don't share onscreen all the information contained in a message's source but instead parse the contents into the elements we are most likely to want to see: To, From, Subject, body, and attachment. If you decide to try a little digital detective work on your own e-mail, you'll find that e-mail client software doesn't make it easy to see complete header information. In Microsoft Outlook Express, highlight the e-mail item you want to analyze and then select "File" from the Menu bar, then "Properties," then click the "Details" tab followed by the "Message Source" button. Think that sounds complicated? Microsoft's Outlook mail client makes it virtually impossible to see the complete message source; however, you can see message headers for individual e-mails by opening the e-mail then selecting "View" followed by "Options" until you see the "Internet headers" window on the Message Option menu.

Local E-Mail Storage Formats and Locations

Suppose you're faced with a discovery request for a client's e-mail, or you simply want to back up your own e-mail for safekeeping. Where are you going to look to find stored e-mail, and what form will that storage take? Because an e-mail is just a text file, individual e-mails could be stored as discrete text files. But that's not a very efficient or speedy way to manage a large number of messages, so you'll find that e-mail client software doesn't do that. Instead, e-mail clients employ proprietary database files housing e-mail messages, and each of the major e-mail clients uses its own unique format for its database. Some programs encrypt the message stores. Some applications merely display e-mail housed on a remote server and do not store messages locally (or only in fragmentary way). The only way to know with certainty if e-mail is stored on a local hard drive is to look for it. Merely checking the e-mail client's settings is insufficient because settings can be changed. Someone not storing server e-mail today might have been storing it a month ago. Additionally, users may create new identities on their systems, install different client software, migrate from other hardware or take various actions resulting in a cache of e-mail residing on their systems without their knowledge*. If they don't know it's there, they can't tell you it's not*. On local hard drives, you've simply got to know what to look for and where to look…*and then you've got to look for it.*

For many, computer use is something of an unfolding adventure. One may have first dipped her toes in the online ocean using browser-based e-mail or an AOL account. Gaining computer-savvy, she may have signed up for broadband access or with a local ISP, downloading e-mail with Netscape Messenger or Microsoft Outlook Express. With growing sophistication, a job change or new technology at work, the user may have migrated to Microsoft Outlook or Lotus Notes as an e-mail client. Each of these steps can orphan a large cache of e-mail, possibly unbeknownst to the user but still fair game for discovery. Again, you've simply got to know what to look for and where to look.

One challenge you'll face when seeking stored e-mail is that every user's storage path can be, and usually is, different. This difference is not so much the result of a user's ability to specify the place to store e-mail—which few do, but which can make an investigator's job more difficult when it occurs—but more from the fact that operating systems are designed to support multiple users and so must assign unique identities and set aside separate storage areas for different users. Even if only one person has used a Windows computer, the operating system will be structured at the time of installation so as to make way for others. Thus, finding e-mail stores will hinge on your knowledge of the User Account or Identity assigned by the operating system. This may be as simple as the user's name or as obscure as {721A17DA-B7DD-4191-BA79-42CF68763786}. Customarily, it's both.

***Caveat**: Before you or anyone on your behalf "poke around" on a computer system seeking a file or folder, recognize that absent the skilled use of specialized tools and techniques, such activity <u>will</u> result in changing data on the drive. Some of the changed data may be forensically significant (such as file access dates) and could constitute <u>spoliation of evidence</u>. If, under the circumstances of the case or matter, your legal or ethical obligation is to preserve the integrity of electronic evidence, then you and your client may be obliged to entrust the search only to a qualified computer forensic examiner.*

Finding Outlook Express E-Mail

Outlook Express has been bundled with every Windows operating system for nearly a decade, so you are sure to find at least the framework of an e-mail cache created by the program. However, since nearly everyone has Outlook Express but not everyone uses it (or sticks with it), finding Outlook Express mail stores doesn't tell you much about their contents.

Outlook Express places e-mail in files with the extension .dbx. The program creates a storage file for each e-mail storage folder that it displays, so expect to find at least Inbox.dbx, Outbox.dbx, Sent Items.dbx and Deleted Items.dbx. If the user has created other folders to hold e-mail, the contents of those folders will reside in a file with the structure *foldername*.dbx. Typically on a Windows XP/NT/2K system—and I emphasize that each situation is unique—you will find Outlook Express .dbx files in the path from the root directory (C:\ for most users) as follows: **C:\Documents and Settings\*useraccount*\Local Settings\Application Data\Identities\\{*unique identifier string*}\Microsoft\Outlook Express**. Multiple identifier strings listed in the Identities subfolder may be an indication of multiple e-mail stores and/or multiple users of the computer. You will need to check each Identity's path. Another approach is to use the Windows Search function to find all files ending .dbx, but be very careful to enable all three of the following Advanced Search options before running a search: Search System Folders, Search Hidden Files and Folders, and Search Subfolders. If you don't, you won't find any—or at least not all—Outlook Express e-mail stores. Be certain to check the paths of the files turned up by your search as it can be revealing to know whether those files turned up under a particular user identity, in Recent Files or even in the Recycle Bin!

Finding Netscape E-Mail

Though infrequently seen today, Netscape and its Mozilla e-mail client ruled the Internet before the browser wars left it crippled and largely forgotten. If you come across a Netscape e-mail client installation, keep in mind that the location of its e-mail stores will vary depending upon the version of the program installed. If it is an older version of the program, such as Netscape 4.x and a default installation, you will find the e-mail stores by drilling down to **C:\Program Files\Netscape\Users\*your profile name*\Mail**. Expect to find two files for each mailbox folder, one containing the message text with no extension (e.g., Inbox) and another which serves as an index file with a .snm extension (e.g., Inbox.snm).

In the latest versions of Netscape (e.g., Netscape 7.x), both the location and the file structures/names have changed. Drill down to **C:\Documents and Settings*Windows account name*\Application Data\Mozilla\Profiles\default\*p rofile*.slt\Mail** and locate the folder for the e-mail account of interest, usually the name of the e-mail server from which messages are retrieved. If you don't see the Application Data folder, go to the Tools Menu, pull down to Folder Options, click on the View tab, and select "Show Hidden Files and Folders," then click "OK." You should find two files for each mailbox folder, one containing the message text with no extension (e.g., Sent) and another which serves as an index file with a .msf extension (e.g., Sent.msf). If you can't seem to find the e-mail stores, you can either launch a Windows search for files with the .snm and .msf extensions (e.g. *.msf) or, if you have access to the e-mail client program, you can check its configuration settings to identify the path and name of the folder in which e-mail is stored.

Finding Outlook E-Mail

Microsoft Outlook is by far the most widely used e-mail client in the business environment. Despite the confusing similarity of their names, Outlook is a much different and more complex application that Outlook Express. One of many important differences is that where Outlook Express stores messages in plain text, Outlook encrypts messages, albeit with a very weak form of encryption. But the most significant challenge Outlook poses in discovery is the fact that all of its local message data and folder structure, along with all other information managed by the program (except a user's Contact data), is stored within a single, often massive, database file with the file extension .pst. The Outlook .pst file format is proprietary and its structure poorly documented, limiting your options when trying to view its contents to Outlook itself or one of a handful of .pst file reader programs available for purchase and download via the Internet.

To find the Outlook message store running Windows XP, NT or 2000, go to C:\Documents and Settings*windows user name*\Local Settings\Application Data\ Microsoft\Outlook\Outlook.pst. The default filename of Outlook.pst may vary if a user has opted to select a different designation or maintains multiple e-mail stores; however, it's rare to see users depart from the default settings. Since the location of the .pst file can be changed by the user, it's a good idea to do a search of all files and folders to identify any files ending with the .pst extension.

Finding E-Mail on Exchange Servers

125 million people get their e-mail via a Microsoft product called Exchange Server. Though the preceding paragraphs dealt with finding e-mail stores on local hard drives, in disputes involving medium- to large-sized businesses, the e-mail server is likely to be the principal focus of electronic discovery efforts. The server is a productive venue in electronic discovery for many reasons, among them:

- Periodic back up procedures, which are a routine part of prudent server operation, tend to shield e-mail stores from those who, by error or guile, might delete or falsify data on local hard drives.
- The ability to recover deleted mail from archival server back ups may obviate the need for costly and sometimes fruitless forensic efforts to restore lost messages.
- Data stored on a server is often less prone to tampering by virtue of the additional physical and system security measures typically dedicated to centralized computer facilities as well as the inability of the uninitiated to manipulate data in the more-complex server environment.
- The centralized nature of an e-mail server affords access to many users' e-mail and may lessen the need for access to workstations at multiple business locations or to laptops and home computers.
- Unlike e-mail client applications, which store e-mail in varying formats and folders, e-mail stored on a server can usually be located with ease and adheres to a common file format.
- The server is the crossroads of corporate electronic communications and the most effective chokepoint to grab the biggest "slice" of relevant information in the shortest time, for the least cost.

Of course, the big advantage of focusing discovery efforts on the mail server (i.e., it can deliver up thousands or millions of messages) is also its biggest disadvantage (someone has to *extract and review* thousands or millions of messages). Absent a carefully-crafted and, ideally, agreed-upon plan for discovery of server e-mail, both requesting and responding parties run the risk of runaway costs, missed data and wasted time.

Server-based e-mail data is generally going to fall into two realms, being online "live" data, which is easily accessible, and offline "archival" data, which may be fairly inaccessible. Absent a change in procedure, "chunks" of data shift from the online to the offline realm on a regular basis--daily, weekly or monthly—as selected information on the server is duplicated onto back up media and deleted from the server's hard drives. The most common back up mechanism is a tape drive, really just a specialized version of a cassette tape recorder or VCR. These back up drives store data on magnetic tape cartridges like the one shown in

Figure 2. As time elapses, the back up media may deteriorate, be discarded or re-used, such that older offline archival data entirely disappears (except, of course, from the many different places it may exist, in bits and pieces, on other servers and local systems).

Figure 2

When e-mail is online, it's an easy and inexpensive task to duplicate the messages and their attachments in their native form to a discrete file or files and burn those to CD or otherwise transmit the e-mail for review and production. When e-mail is offline, it can be no mean feat to get to it, and the reason why it's challenging and costly has to do with the way computers are backed up. The customary practice for backing up a server is to make a copy of specified files and folders containing data. Sometimes a back up will copy everything, including the operating system software and the date; but, more often, time and cost constraints mean that only the stuff that can't be reloaded from other sources gets copied. Another common practice is to only copy all the data every once and a while (e.g., monthly) and just record changes to the data at more frequent intervals. Let's try an analogy to make this clear.

Understanding Server Back Up, by Analogy

Imagine that all your work was done at your desk and that, to protect that work from being destroyed in a flood or fire, you had your assistant photocopy everything on your desk on the first of each month and store it, unstapled and unorganized, in the trunk of your car. Once a month, when the new copy is made, you move the old set from your trunk to your basement. This practice buys you some peace of mind, but realizing that you still stand to lose as much as a month's worth of work should your office burn on the 30th, you figure you need more frequent back up copy sets. Now, neither you nor your assistant can get much work done if everything on your desk is copied every day, so you come up with a shortcut: copy just the new stuff daily (that is, your latest work and your incoming correspondence). Now, on top of the monthly copy of everything on your desk, you add a daily copy of your latest changes. If the office goes up in smoke, it will take some effort to recreate your desktop, but the need to do that only arises in the event of a catastrophe, and you breathe more easily, confident in the knowledge it can be done.

Similarly, incremental server back ups are periodic and pervasive copies of selected datasets, augmented by more frequent recording of changes. Neither alone is complete, but together they comprise a complete dataset at each back up interval.

Coming back to the desktop analogy, some projects linger from month-to-month. Consequently, each monthly interval copy set is going to contain a lot of the same stuff from the month before. Likewise, a server's back up tapes tend to contain a huge volume of duplicate information, interval-to-interval. To forestall the need to wade through many identical copies of the same message, e-mail restored from server tapes must be de-duplicated or "de-duped" to remove repetitious material before review.

But what may be the biggest hitch in doing discovery from back up media is that offline information on back up media isn't accessible in the same way as is online information still residing on the server. Imagine the difference between trying to locate a particular document on your desk--where you are aided by folders, document trays, labels, sticky notes, locale and context--versus trying to do the same while rummaging through heaps of paper in the trunk of your car. Offline back up information usually must be returned to something resembling its former online environment before you can make much sense of it. That may not be a big deal if the systems where that data used to "live" are still around, but it can be a daunting task indeed if those systems were replaced three years ago. In the world of computers, change is constant, and obsolescence arrived yesterday.

You can't imagine how common it is for companies to diligently create back up tapes without ever testing a single one to see if it actually recorded any data. Even when the back up system works, some companies hang onto the tapes but dispose of all the hardware which can read them. In short, never underestimate the power of stupidity. Another point about data stored on tapes: it's fragile. For a host of reasons ranging from sloppy storage to bad hardware to physical deterioration, the usable data that can be successfully restored from a server tape is often less than 100%, and the percentage declines with the passage of time.

Each organization establishes at its own back up practices. Some take the server offline, halting file and e-mail access, while they copy everything. More commonly, incremental back up procedures are employed and may exclude back up of static data, like the server operating system software or packaged commercial applications that can be restored from the original product disks. All Exchange Server back up systems must, over some interval best-suited to the business environment, capture all dynamic data, including:

- System State, including the Microsoft Internet Information Services (IIS) metabase and the Registry;
- Web Storage System (WSS) databases and supporting files;
- Active Directory;
- Key Management Service (KMS) databases;
- Site Replication Service (SRS) databases; and

- Cluster quorum.

If you have no idea what this stuff means, join the club. I'm pretty fuzzy on some of it myself. But, unless you're the system administrator charged with protecting the data, all you may need to know is that back up procedures vary, but they are all geared toward hanging on to the mission critical data.

Brick Level Back Up

By all contemporary standards, e-mail is mission critical data. It's so critical, in fact, that system administrators may elect to back it up in two ways: the global back up touched on above and a mailbox- and message-level approach, commonly called "brick level" back up. If the party responding in discovery maintains a brick level back up system, it's easier and less costly to recover the e-mail of any particular user without having to restore the entire system structure to a recovery server (a spare server used as a target location for recovery operations). With a brick level back up, the system administrator can restore just a single employee's mailbox or an entire department's mailboxes, spitting them out as, e.g., Outlook .pst files for review in e-mail client software or ported into other applications for de-duplication and examination. That's the good news. The bad news is that not every enterprise runs brick level back ups because they take a whole lot longer to complete and use storage space less efficiently than their global counterparts. The lesson may be that, if your litigation needs dictate frequent access to the contents of individual mailboxes stored offline on server back up systems, a brick level back up strategy is best. Of course, if you're getting sued a lot and your opponents are seeking e-mail on your server back up tapes, you've got to also evaluate the strategic implications of making that a fairly easy, less-costly process. Recent trends in electronic discovery cost shifting suggest that getting everything you can into a relatively *in*accessible format may be advantageous to entities resisting discovery.

The Format Fight

Assuming that you've run the gauntlet and gathered all the e-mail files and databases, how are you going to review the fruits of your harvest for relevance, privilege and confidentiality? For any significant volume of data, printing it out and poring through stacks of paper is a terrible idea. You've got to be able to search the material electronically and to access each e-mail's metadata. Here is where the e-discovery world splits into warring tribes we'll call Natives and Missionaries: the Natives believe that e-mail and other electronic data should be searched and produced in its native format, arguing that it's quicker and less costly. The Missionaries preach the gospel of conversion…of data into images, typically TIFF or PDF files, facilitating review via a web browser-like application. For now, the Missionaries seem to predominate, but not for long. Information has simply moved too far beyond the confines of paper. How can the Missionary Model hope to do justice to spreadsheets with embedded formulae, audio content, animation or complex databases? Inevitably, the Natives will prevail; however, the idea of a universal viewer offering easy access to native data by emulating a wide range of common application software should stand the test of time.

For now, the choice of format is a tactical and financial decision. If you know your opponent will find one or the other format more daunting because, e.g., she lacks software to examine files in their native format, that hurdle may influence your choice…in favor of the *easier* format, no doubt. Likewise, if your firm or law department structure is geared to platoons of associates and paralegals conducting discovery reviews using Internet browser software and doesn't have staff capable of analysis in native format, the TIFF or PDF format may be the best choice.

What Format Do You Want?

If you are the party seeking discovery of e-mail, give some careful thought to the format you want to receive and ask for it in your discovery request. But always keep in mind the adage, "Be careful what you wish for, because you might get it." In deciding what to ask for you need to consider how you work and the structure and volume of the electronic information you seek. If you and your staff are incapable of tackling production in any format other than paper and the universe of electronic documents in your case is small (i.e., under 250,000 pages), then working with page image files or even having those images blown back to paper is a workable strategy. In that instance, just be sure that you obtain printouts of all the metadata for each electronic document. That means full headers for all e-mail, plus be sure that the production method will afford you a mechanism to pair attachments with transmittals and link individual messages to the data paths from which they were retrieved (i.e., whose mailbox was it in and what folder?).

Unless you command a platoon of skilled reviewers—or even if you do—once you get past about 250,000 pages, it just doesn't make sense to manage documents by reading each of them. Using my own e-mail stores as an example, I have nearly a gigabyte of e-mail online which, when printed out, might yield something in excess of 100,000 pages to review. If, on average, you can read through every page in thirty seconds, it's going to take around 800 hours to plow through it all. Even if you de-duplicate and cull out all the Viagra ads and Nigerian treasury scams, you're still looking at maybe ten 40-hour weeks of work…for one person…with one mailbox.

For my money, I want the e-mail produced in its native format--in a .pst file if it's Outlook or Exchange Server mail and as .dbx, files (e.g., Inbox, Sent Items, Deleted Items, etc.) if it comes from Outlook Express. Moreover, I'm going to look very closely at the privilege log to determine what has been removed from the mailbox and what relationship those excisions bear to the timing and content of other messages. I'm also going to seek deleted e-mail, whether by examination of server tapes, through discovery from others or by computer forensics.

Privilege and Confidentiality Considerations

If all the cost and trouble of electronic discovery stemmed only from the challenge to locate and restore e-mail, then improvements in technology and best practices could pretty well make those concerns evaporate. The cost of storage has never been lower and the storage capacity/per dollar is soaring. No, the greatest and growing cost of e-discovery stem from the legal services which must be devoted to the fight for access and the review of information before it can be produced. Plaintiff's counsel's fear of overlooking a smoking gun is nothing compared to defense counsel's fear of having unwittingly produced it! Though reprehensible, it's common for confidential e-mails from counsel and transmittals of sensitive trade secrets to rub shoulders with the electronic greeting cards, organ enlargement solicitations and routine matters that fill our electronic mailboxes. Then, there is the commingling of business and personal communications. If e-mail comes from an employee's spouse or physician, who will cull it from production? How do you produce something you haven't reviewed in detail without risking the waiver of privilege?

Claw Back and Quick Peek Arrangements

The inadvertent production of a privileged document following a diligent review and otherwise timely and careful assertion of privilege is not likely to be seen as a voluntary waiver; however, a broad expansion of that proposition---an emerging approach to e-discovery, called the "claw back" or "quick peek" method—offers a less-certain outcome. In a "claw back" production, documents are produced before or even without a review for privilege, confidentiality, or privacy. Instead, the parties agree—or, in rare instances, the court will order—that the party seeking discovery will be afforded broad access, but that the producing party may assert confidentiality and privilege to any of the materials reviewed. The notion is that the producing party may "claw back" any document it might otherwise have been permitted to withhold from production, without fearing a claim of waiver.

Claw back productions certainly have their appeal: make your opponent wade through everything and only focus on the items they indicate they might wish to use. But, even with an ironclad agreement, there is a greater potential for a producing party to waive a privilege or lose control of a confidential communication. There is also a question whether, in our adversarial system, a lawyer's duties are adequately fulfilled by "punting" the review process to one's opponent.

If a claw back or quick peek production is contemplated, one e-discovery think tank suggests that the Court enter an order that (1) indicates that the court is compelling the manner of production, (2) states such production does not result in an express or implied waiver of any privilege or protection for the produced documents or any other documents, (3) directs that the reviewing party cannot discuss the contents of the documents or take any notes during the review process, (4) permits the reviewing party to select those documents that it believes are relevant to the case, and (5) orders that for each selected document, the producing party either (a) produces the selected document, (b) places the selected document on a privilege log, or (c) places the selected document on a non-responsive log. *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery, Cmt. 10.d* (Sedona Conference Working Group Series 2004).

Preparing for E-Mail Discovery

If a request for production sought, "Jim Smith's Outlook Express e-mail from his Dell laptop, received or sent between March 23 and 30th 2004 and referencing the *Jones Project* in the subject line," electronic discovery would be a piece of cake! In reality, e-discovery requests rarely improve upon their paper discovery predecessors, with drafters opting instead to trot out the familiar "any and all" demand, while tacking "electronic data compilations" onto the litany of examples offered to define a "document."

A lawyer who appears quite savvy about electronic discovery published the following sample request for e-mail production on his website. Ordinarily, I'd credit the source, but since I'm going to savage a well-intentioned and unselfish effort to put something online to help other lawyers, the better part of valor is to let the publisher remain anonymous.

> *"Produce any and all information related to e-mail, including but not limited to current, backed-up and archived programs, accounts, unified messaging, server-based e-mail, Web-based e-mail, dial-up e-mail, user names and addresses, domain names and addresses, e-mail messages, attachments, manual and automated mailing lists and mailing list addresses."*

Now, let's translate it into a more-or-less equivalent request for paper documents:

> "Produce any and all information related to documents, including but not limited to the original and copies of any documents ever in your possession. Produce any documents you have at home, in your car or that you used to pack the old kitchen dishes you sold on e-Bay. Don't omit all those old compositions you wrote in the 4th grade that your Mom has stored in her attic or the Playboys you kept from college in that box behind the furnace. Produce your Rolodex, your diary, your Christmas card list and that list of the people who gave you wedding presents (your wife will know where it is). Be sure to include any mail you've ever sent or received, especially those blue envelopes with all the coupons in them and any letters from Ed McMahon indicating that, "You may already be a winner!" Produce any implements related to writing, including any

> pencils, pads, pens (especially those pricey MontBlanc ones and the ones with the squishy hold 'em thingies)."
>
> Or more succinctly:
>
> "Gimme everything."

Sooner or later, your client will get hit with a request like this--or one that isn't utter nonsense—and the reality of having to marshal and produce e-mail and other electronic records will set in.

The process that allows you to safely navigate the treacherous shoals of e-discovery begins *before* the preservation letter arrives. You need a plan. You need a policy. You need procedures.

According to a 2003 survey by the American Management Association, only a third of employers have written e-mail retention and deletion policies. Cohasset Associates, a consulting firm specializing in document-based information management, found that 39 percent of organizations have no formal policy regarding e-mail retention. Can this really be true after Enron, Frank Quattrone and all the other high profile e-mail self-immolations making recent headlines?

Planning and Policymaking

Companies get in trouble with e-discovery because they fail to keep something and create or retain something they shouldn't have. In a large, complex, far-flung organization, it's bound to happen despite best efforts, but it shouldn't occur because the law department doesn't know how to talk to the IT department or because no one ever told Dewayne that his Janet Jackson "wardrobe malfunction" video shouldn't have been e-mailed to the whole department.

Your client's electronic document retention policy has become a critical corporate policy. Having a sound retention policy and implementing it in a rational and consistent way is one of the best ways means of guarding against a charge of spoliation. Such a policy needs to be a collaborative effort between corporate counsel and the IT staff, with each seeking to understand the needs and constraints the other faces. The policy needs to be blessed by senior management and integrated into operations. It needs to be ingrained in the corporate culture by training, oversight and meaningful enforcement. Currently, most employers don't instruct their employees on proper handling of electronic records, and almost three out of four have no e-mail usage training. A policy without training and enforcement is just a piece of paper.

Dear David Duncan, Regards Nancy Temple

There's been plenty of ink spilled about the demise of accounting giant Arthur Andersen in the Enron mess, but one pertinent lesson is that Andersen didn't get in trouble because it lacked a document retention policy—in fact it had two pretty comprehensive document destruction policies. Andersen went down because it hadn't *followed* its policies and decided to play catch up and cover up while the Feds were pulling into the driveway. Few things spell "wrong" to a jury like a company's failure to adhere to its own policies. Some argue it's better to have no policy than one that's not followed.

To be effective, retention schedules have to be rigorously followed, but adaptable to lawsuits, government investigations and compliance obligations. The retention policy that only kicks into gear when the hoof beats of litigation approach waves the red flag of malfeasance. Yet more than a third of companies only follow their retention when it suits them.

Trust Everyone, but Cut the Cards

Even companies with sound e-mail usage and retention policies and employee training programs can't wholly rely upon their employees' good conduct. Employees must be disabused of the notion that they have an expectation of privacy in their use of company computers and reminded that their usage constitutes consent to monitoring of that usage. Monitoring of computer usage may be degrading and intrusive, but failing to monitor is an abrogation of responsibility that cedes trade secrets to those who steal them and vast digital conduits to those who use them for harassment and criminality. These threats are not imaginary. They occur in every large organization, and many small ones, from the board room to the mail room. Moreover, we must have the fortitude to look for the bad guys, inside and out. Though half of all companies claim to monitor incoming e-mail, less than one-in-five keep an eye on intra-company messaging.

Am I in Trouble? IM!

I used to call Instant Messaging "an emerging threat," but Punxatawney Phil already emerged and saw his shadow. Now we can look forward to six more years of S.E.C. investigations! Seriously, IM is in wide use throughout corporate America. Estimates of office usage range from 45%-90%, with an expectation that, whatever the real usage, it's getting bigger all the time. For the uninitiated, IM is a form of instantaneous, real time e-mail that doesn't come though normal e-mail channels, meaning it's largely invisible to those whose job it is to police such things. IM leaves little in the way of digital footprints, which may be desirable if you're using it to play footsie on company time; however, unmonitored and unrecorded communications pose an entirely different risk to financial institutions. For example, the National Association of Securities Dealers requires members to archive electronic communications for at least three years. NASD Vice Chairman Mary Schapiro recently said, "Firms have to remember that regardless of the informality of instant messaging, it is still subject to the same requirements as e-mail communications and members must ensure that their use of instant messaging is consistent with their basic supervisory and record keeping obligations." So, how come 61% of financial services firms surveyed by Security Industry News have no means of managing or archiving instant messaging, and 39% have no instant messaging policy at all? I forget, when the law says you must retain it and you don't, is that spoliation *per se* or just a felony?

> **Solution**: Firms must either bar IM usage altogether and monitor the Internet ports used by such applications to insure compliance, or allow such usage configured so as to permit monitoring and archival. Doing so won't be a one-time fix, because IM applications evolve rapidly, such that a message going out one port today will bust through the firewall an entirely new way tomorrow.

Training

I have an idea that might protect a company from employee e-mail gaffes. It involves putting a giant video screen in the company cafeteria and randomly displaying the contents of any e-mail going through the network. It's a bad idea, but it makes a point: Before they click on "Send," every employee needs to ask, "How would I feel if I had to read this in open court or if my kids heard it on the evening news?" Sensitivity to the perils of e-mail doesn't just happen—it has to be bred institutionally, and it needs to come from the people at the top and matter to the folks at the bottom. In 1945, people understood that, "Loose lips sink ships." In 2005, every employee needs to feel—and every co-worker should serve to remind them—that an inappropriate, illegal, misdirected or mishandled e-mail puts everyone's livelihood at risk.

> **Solution:** Just reminding employees that the company has an e-mail policy is not enough. There must be formal training on appropriate content. Retention policies must be spelled out, and employees should be made to understand why compliance matters—that when you don't do what the policy requires, you're betraying your co-workers. Teaching ways to avoid misdirection (e.g., turning off the auto complete feature for addressing e-mails) and encouraging the same level of reflection attendant to a written memorandum will help.

Social Engineering

Social Engineering is hacker-speak for tricking a person into revealing their password or launching a rogue program to open a back door into a system. I use it here to underscore the fact that the weakest security link in most systems isn't the software or the hardware. It's the "wetware," also called "liveware" or "meatware." That is, it's the people. The best planned systems are waylaid by the people that use them.

By way of example, since more than a third of companies store their e-mail solely on servers, system administrators are forced to limit mailbox size. In fact, three-fourths of companies surveyed by Kroll Ontrack impose such quotas, and a quarter of companies compel deletion as quotas are reached. When you tell employees that you are going to force them to delete what many view as essential information, not surprisingly some become quite resourceful at retaining e-mail despite company policy. Avoidance tactics take many forms, but whether it's forwarding older mail back to your own mailbox to circumvent time restrictions or burning private caches of CDs, such guerilla tactics jeopardize a company's ability to manage their e-mail systems and accurately respond to discovery. That's bad social engineering. An enterprise embroiled in litigation may vehemently deny the existence of responsive e-mail, only to find that an enterprising employee has a "private stash" of clearly-discoverable e-mail which does not come to light until the employee deems disclosure of that e-mail advantageous. As attorney Tom Watkins of Austin puts it, "E-mails are the cockroaches of litigation. You can't get rid of them, and they always manage to turn up when company comes to call."

> **Solution**: Build institutional awareness of the hazards of kamikaze computing. Train, monitor, audit and enforce. People try to get away with stuff because they can. Make it harder to cheat, and put real teeth in the policy. Help employees appreciate the risk to their company and their jobs posed by social engineering errors, and put peer pressure to work.

The E-Discovery Triage Plan

One of the earliest obligations of any litigant is to preserve evidence in anticipation of litigation. The duty to preserve is automatic, and doesn't hinge on suit being filed or even receipt of a preservation letter. Companies have to be prepared to retain evidence when litigation or government investigation is merely "in the wind." The role of harbinger often falls to corporate counsel, who must issue something of a "stop the presses" order to be sure that appropriate steps begin at once to preserve potential evidence.

If it fell to you to initiate the preservation of potential electronic evidence, would you know what to do? Would you even know everyone that must become involved? Would the IT department understand what they were required to do and have the resources and in-house expertise to do it?

If you're at all uncertain of your answers to the prior questions, you may need an e-discovery triage plan—the procedural equivalent of a big red button in your office you can push when you need to "stop the presses." An e-mail triage plan starts with knowing the systems and staying current on the nature and location of the servers, back up archives and other key data repositories. It requires having at hand the names and contact information for the persons in each department who have the authority and knowledge to preserve and protect potential evidence. It means knowing where the e-mail lives on the company's systems and halting activities that might destroy or alter those messages.

An e-mail triage plan needs to keep close tabs on all potentially significant sources of discoverable information. Who telecommutes and may have electronic evidence on a local hard drive in their home? Who's been issued a company-owned laptop, Blackberry or PDA that might hold e-mail or other evidence? How often is the e-mail server backed up? How complete is that back up? Do we need to temporarily implement brick level back ups? What is the rotation schedule for the back up tapes? What local hard drives need to be cloned immediately? What about Instant Messaging and voice mail?

Electronic data is fragile, and the cost of spoliation is high. To best serve your clients, you should stay abreast of how their IT systems retain electronic documents, and, if necessary, propose changes in procedures to support an e-discovery triage policy. The point at which the duty to preserve attaches is not the time to begin your education about the company's systems or start seeking management buy-in on a preservation plan. You must be fully prepared to preserve the status quo, to—as far as feasible—fix the company's data in amber for the near term, long enough to secure agreements with opposing counsel or relief from the court. The moment the duty to preserve attaches is likewise not the time to engage in a power struggle with the IT department. Make it your business to know who you will be dealing with and meet them. Discuss the e-discovery triage plan and inquire about potential conflicts or concerns. Though such a plan should have emerged as a collaborative effort, it's still a good idea to secure buy-in and solicit ways to improve the plan. In short, *communicate*.

Tips for your E-Discovery Triage Efforts:

1. Field an E-Discovery Triage Task Force and include:
    a. Corporate Counsel
    b. Outside Trial Counsel
    c. IT Officer(s)
    d. Records Custodian(s)
    e. Chief Financial Officer
    f. Operations Officer
    g. Electronic Discovery Specialist
    h. Forensic Specialist

2. Define the product of the Task Force: Are they drafting the company retention policy or a litigation action plan? What is each member's role and responsibility?

3. Identify all data storage locations and a mechanism to stay abreast of changes

4. Document existing procedures and schedules for creation, storage, retention, modification, securing, deletion and restoration of business data;

5. Identify likely candidates for discovery efforts and effective ways to delineate or "Chinese Wall" privileged, personal and confidential data, as well as to retain and retrieve.

6. Develop action plan procedures for particular events including employee departure, suspected theft of trade secrets, network intrusion, improper or unauthorized use of computer systems, government subpoena, FBI raid, employee destruction of data, litigation, etc.

7. Create a contact list of persons responsible for familiarity with and implementation of the action plan and insure a rapid and effective communication strategy. How will everyone "get the word" to act?

8. Secure support from top management to insure prioritization and avoid delay in implementation.

Enlist Help

Even with a well-conceived e-discovery triage plan, it's a good idea to get outside help on board to advise and assist. Why would a big communications or technology company need to bring in outside help to assist with electronic discovery? Do Microsoft or EarthLink or SBC really need outside expertise? The answer is often "yes;" not because an outsider necessarily brings more knowledge of the systems or mastery of the technology, but because a well-chosen outsider brings an independent voice to the table and speaks the language of the IT department at a time when clear communication is essential. Despite being paid by a party, an expert known to the court and enjoying a reputation for honesty and skill is simply more credible when stating, "We looked and it wasn't there," or "The items reviewed were not responsive to the request." Moreover, hiring outside talent helps demonstrate that discovery responsibilities were taken seriously and—let's be blunt here—it may serve to deflect responsibility if something should ultimately hit the fan.

Control the Channel and Capture the Traffic

As a forensic examiner, a common consequence of telling an employee that someone will stop by tomorrow to pick up their laptop is that they will be up most of the night running a Delete-O-Thon. Then, a case which might have been won is lost; not on the merits, but because of a failure to control the data channels and capture the traffic. You must be able to lock down your records into a full save mode upon the hint of litigation or investigation. You need to make users aware that not only must they keep their personal and sexual material off their company computers else they be content to hand it over when the time comes. Clients need to appreciate that those "evidence eliminator" programs that promise to cover their tracks don't do a very good job of it. Plus, covered tracks on a computer look just like—surprise!—covered tracks. Even if I don't find the erased item, chances are I'm going to find the crater it left behind.

"Controlling the channel" demands more than an occasional e-mail admonishment to "hang onto stuff." The average user has, at best, a hazy idea about how computers keep and lose information. You need to be explicit about what must be done or not done on desktop and laptop systems, and do it in such a way that it won't appear as a roadmap for running that Delete-O-Thon!

Consider hardware and software "solutions" that enable more centralized control of the retention process. Some of these will even image hard drives remotely to permit a "snapshot" to be taken of each user's hard drive during off hours. If it sounds a bit Big Brother, it is. But better Big Brother than O Brother, Where art Thou?

The Server Tape Conundrum

According to the market research firm Osterman Research, 67 percent of companies back up their e-mail systems to tape alone and recycle the tapes every 90 days. Suppose you know that your client's server data are backed up to tape and that those tapes tend to be re-used in a way that overwrites old data with new. When the time comes to swing into action and preserve potentially discoverable evidence, how are you going to deal with your client's tape rotation? The easy answer is, "I'll instruct them to stop re-using tapes until further notice." That's certainly not a wrong answer from the standpoint of protecting your client from claims of spoliation and even from the Delete-O-Thon initiatives of their own employees, but it's not always a practical or tactically sound one. It's the right answer according to 7 Moore's Federal Practice, which states that, "The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation." § 37A.12[5][e] (Matthew Bender 3d ed). But, it is not the *only* right answer, nor is it necessarily the right answer from beginning to end of the litigation.

Many companies are *always* embroiled in some phase of litigation, so an instruction to cease back up rotation during the pendency of a case is tantamount to saying, "Save everything forever." Back up tapes are expensive. Properly storing back up tapes is expensive. Hanging on to the obsolete hardware needed to read back up tapes from last year or the year before that is expensive. There are specialists who make a handsome living curating "Museums of Old Back Up Tape Drives" because no one thought to hang onto those tape drives from 1995 or the software than ran them. Even when the case from 1999 is over, do you have to retain the tapes because of the case filed last month?

What you advise your client to do and for how long should be based in part upon how they use their back up system. Companies tend to fall into two camps: those that use their back up systems as a means to recover from catastrophe—to get their systems "back up" and running again—and those that use back up as a means of institution memory--an archives of company activities extending beyond the minimum required to restore to the point of failure. If your client falls in the latter camp, they almost certainly *do* need to halt their tape rotation, since their usage is archival of business records and the start of litigation is an inauspicious time to start destroying business records, at least until you can fully ascertain the relevant scope of the matters in dispute. But if your client falls in the first camp and just uses back up to get back up, doesn't maintain an archive of old tapes and keeps the focus solely on catastrophic recovery, you may be fully justified in not halting back up tape rotation, assuming that you have taken other appropriate steps to preserve potentially relevant and discoverable data. Keep in mind that, absent a catastrophic failure, the most recent back up set is essentially a mirror image of the live system data, so restoring and searching the latest back up is usually of little value.

Before you decide in which camp your client falls, you'll need to do more than just ask the V.P. of IT whether there is a tape archive. You need to pose your questions as well to the person whose job it is to shove those tapes into the machine and keep track of them. The reality is that the manager may not always know what the technicians are doing "in the pits."

If you take the safe route and order a halt to rotation of back up tapes, recognize that there are costly consequences which follow upon that instruction and promptly explore whether there are less-costly alternatives. Perhaps the court will enter a discovery order making it clear that back up tapes need not be retained or an agreement can be reached with opposing counsel to the same end. A motion seeking cost allocation for back up tape retention costs can sharpen opposing counsel's focus on the issue. As plaintiff's counsel, I know I was very careful about what I sought in discovery when I thought it might come out of my pocket. Also, target follow up dates to advise IT about the need for continued retention. It would be embarrassing to find out that IT unnecessarily spent $22,000.00 this year on litigation-related back up activities because you forgot to tell them the case settled last year!

Confer, Confer, Confer!

Voluntarily sharing information with your opponent and seeking to work cooperatively in the electronic discovery process may not be your cup of tea, but it's certainly an effective way to protect your client from claims of spoliation and discovery abuse. Huge sums are spent on electronic discovery because of uncertainty—we're not sure what we must keep, so we keep everything.

The better way is to confer with your opponent early. Document the process well and seek to hammer out a discovery plan setting out what you are agreeing to preserve pending specific discovery requests. Be prepared to ascribe estimated volume and costs to more extensive retention efforts so that your opponent appreciates the costs occasioned by overbroad demands. Such a conference is less about agreeing to produce particular items as it is defining the universe of information to which future discovery will be directed. Why should your opponent agree to limit that universe and cede a tactical advantage? Because, if you've made your case that your opponent's demands are unreasonable and put your opponent on notice that money will be wasted as a consequence, you are better postured to shift that financial burden to the other side, or at least have it dangle over your opponent like the sword of Damocles.

The other reason to confer and seek agreements early is because limiting electronic discovery is a two-way street. Many discovery requests can be "boomeranged" back to your opponent, who will be hard-pressed to object to its scope. A common error of corporate counsel is to think that the cost, complexity and peril of electronic discovery are visited only on their side. Nearly everyone uses computers. Though the party litigating against your corporate client is an individual, they are likewise bound to preserve electronic evidence, a treacherous and costly obligation for the uninitiated, even for a single personal computer. A conference—and incisive questions about what steps the other side is taking to preserve evidence—may bring the parties closer to agreement.

If agreements can't be reached, seek a discovery conference with the court and help the judge appreciate the costs and perils of willy-nilly retention. Be prepared to discuss volumes of data, man-hours of work and associated costs. Few judges respond favorable to a plaintive, "It's too burdensome," but most, when made aware of the dollars and time at stake, are willing to use their power to prevent unfairness and waste. Help the court see alternatives—sampling, perhaps, or time limitations—to a global retention obligation. Even if you get no relief at all, you can better advise your client that the money and time being invested is indeed required, and you set the stage for a later cost allocation request should it appear that your opponent overreached or oversold.

Twenty Tips for Counsel Seeking Discovery

1. Get your preservation letter out early and be *both* specific and general. Assume that the recipients don't know their own systems and don't understand computer forensics. Educate them in the letter so they can't use ignorance as an excuse.
2. Do your homework: use the Net and ask around to learn about the nature and extent of your opponent's systems and practices. You're probably not the first person to ever pursue discovery against the opposition. Others might know where the sweet spots can be found.
3. Get your e-discovery out fast, with the petition if you're the plaintiff. Data is going to disappear. You're in a poor position to complain about it if you didn't ask while it was still around.
4. Force broad retention, but pursue narrow discovery
5. What they must keep and what they must give you are different obligations. Keeping the first broad protects your client's interests and exposes their negligence and perfidy. Keeping requests for production narrow and carefully crafted makes it hard for your opponent to buy delays through objection. Laser-like requests mean that your opponents must search with a spoon instead of a backhoe. Tactically, ten single, surgical requests spread over 20 days are more effective than 20 requests in one.
6. Be aware that your opponent may not understand the systems as well as you do, but may not want anyone—especially his client--to know it. Help your opponent "get it," so he can pose the right questions to his client.

7. Question the IT people. Avoid the managers and focus on the grunts. The latter are have spent less time in the woodshed and they know the *real* retention practices.
8. Seek a copy of any document retention policies and a complete inventory of system resources. You need to know where the data is stored and on what equipment.
9. Invoke the court's injunctive power early to force preservation. The agreement that can be secured to forestall a court order may be better than you'll get from the judge.
10. If you can't get make any headway, seek appointment of a neutral or special master.
11. Ask all opponent employee witnesses what they were told to do in the way of e-document retention and what they actually did.
12. Know how and when to check for authenticity of data produced. Digital data is easily forged.
13. Be sure to get metadata whenever it may be relevant.
14. Don't accept image data (TIFF or PDF) when you need native data.
15. Have the principal cases on e-discovery and cost shifting at hand. Tailor your requests to the language of the cases.
16. Set objections for hearing immediately. Require assertions of burden and cost to be supported by evidence.
17. Analyze what you get promptly after you get it and pin down that it is represented to be "everything" responsive to the request. Follow up with additional requests based upon your analysis.
18. Don't let yourself be railroaded into cost sharing but, if it happens, be sure you're protected from waste and excess by the other side, and leverage your role as underwriter to gain greater access.
19. Be prepared to propose a "claw back" production, if advantageous.
20. Don't accept assertions of cost or complexity unless you know them to be accurate. Have such claims independently evaluated and be ready to propose alternatives.

Twenty Tips for Counsel Defending Against E-Discovery

1. Respond immediately to any preservation letter and advise what you will and won't do without a court order and why. Don't enable your opponent to later claim, "I thought they were saving everything I asked for."
2. Act immediately to preserve potentially relevant data. Know the tape rotation schedule and decide whether to halt rotation. Communicate clearly and specifically what your client's employees must do and for how long. Don't rely on intermediaries if data destruction is in the offing. You may only get one shot to preserve some things, so don't just leave a voice mail for someone who's away on vacation. Implement your e-discovery triage plan, and be sure that management gets behind it unequivocally.
3. Confer with opposing counsel early and often. Document everything you proposed, agreed or declined to do.

4. Seek a discovery conference with the court if the retention or production obligations are onerous.
5. Meet with the IT staff and let them help you understand what must be done to respond to a request and whether it can be done. Have them propose alternatives. Treat them as "officers of the court" within their digital domain.
6. Prepare IT staff and records custodians for deposition--not just the department head. Be sure they know the retention policy and how it has been implemented. Engineering types tend to look for solutions, so caution them against helping your opponent solve her problem of getting what she seeks from your systems!
7. "Boomerang" your opponent's discovery where advantageous, serving it back on the other side. More importantly, ***push back with e-discovery****.* Responding to an electronic discovery request is a perilous undertaking even when you only have one computer (most Americans have more than one). Even if you are Goliath, the David suing you doesn't have an IT staff and may be unable to resist the temptation to sanitize his e-production. "David" may be no more inclined to share his e-mail with you than you with him. Moreover, home computers tend to reveal much more than their office counterparts, so consider computer forensics as well.
8. Document all efforts to identify responsive material. Should something be missed and you need to show good faith, it will take more than a global representation of, "We looked really hard." Quantify efforts in page equivalents, gigabytes or man-hours. This information will also be useful when seeking to demonstrate the burden imposed by future requests and when seeking to shift costs.
9. When appropriate, seek to shift costs to your opponent. A credible risk of paying your client's bills is a very big hammer, but be sure that the Court doesn't confuse cost shifting with broader access. Just because the opponent has to pay for the collection and search effort doesn't confer a greater right to see anything.
10. When claiming undue burden, be prepared to attach reasonable estimates of time and money to responsive efforts. Be sure the court understands that employee time isn't "free." Get quotes from outside vendors to support credibility. Don't forget the cost of review by counsel. It may not be shifted, but it is a major cost consideration capable of making an impression on the court. Help the court appreciate that a discovery request that costs you more than the settlement demand is a tactical ploy that doesn't serve the ends of justice.
11. Know the seven Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) cost shifting considerations, and be ready to apply them:
    a. *Is the request specifically tailored to discover relevant information?*
    b. *Is the information available from other sources?*
    c. *How does cost of production compare to the amount in controversy?*
    d. *What are the relative positions of the parties in terms of resources?*

   e. *Who is best able to control costs and has an incentive to do so?*
   f. *Are the issues in discovery key to the issues at stake in the litigation?*
   g. *What are the relative benefits to the parties of obtaining the data?*

12. Consider sampling as an alternative to broad production.
13. Be sensitive to undisclosed concerns stemming from private information on hard drives which may cloud judgment. The CEO may know that he has a porno collection hidden away on his office computer, but he's unlikely to admit it to counsel.
14. Be wary of forensic analysis of hard drives by the other side's expert. Almost everyone has something to hide, and a lot of them hide it on their computers.
15. A back up is just for getting the system "back up" after a crash. If your client doesn't need old back up tapes to get back up, then get rid of them! Keeping them tends to makes them discoverable as a business record. Being a digital pack rat is what gets so many companies into costly hot water.
16. Educate yourself about computer system and storage, so you can educate the court.
17. Protect your client by protecting the interests of third-parties. Raise claims of third-party privacy and privilege rights where such claims are genuine, material and will serve as grounds for non-production. Office e-mail oftentimes contains privileged attorney-client and spousal communications as well as confidential medical information. Complying with discovery may expose you to liability to third-parties.
18. Anticipate leaks in the net: Retired hardware, crashed drives, and employee pack rats are all places where you may find data all swear is gone forever. Look in drawers and on shelves!
19. Systematic retrieval starts with the sender. Encourage clients to train employees to use e-mail properly, label subject lines accurately and avoid threading.
20. Make sure your clients appreciate that failing to produce unfavorable electronic evidence—especially the smoking gun e-mail—is an invitation to disaster. You can't suppress all copies, and you can't be sure the other side won't get it from somewhere else. It a*lways* hurts more when it's introduced as something you tried to hide.