December 2003

Computer Forensics and Electronic Evidence

Linda Volonino
Canisius College

COMPUTER FORENSICS AND ELECTRONIC EVIDENCE

Linda Volonino
Canisius College
volonino@canisius.edu

Abstract

When electronic documents are used as evidence, they are referred to as electronic evidence, or e-evidence. Broadly defined, e-evidence is any electronically-stored information on any type of computer device that can be used as evidence in a legal action. A computer forensics investigation is the search for e-evidence by analyzing electronic devices (e.g., computers, PDAs, cell phones, iPAQs, voice-mail, servers, disks, zip drives, or backup tapes) and communication media (e.g., instant messaging or chat rooms.) In 1995, a U.S. District Court stated that "the law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced."

By 2000, email had become the most common type of e-evidence. In 2003, email evidence had become so prevalent it became known as evidence-mail. According to Garry Mathiason, whose law firm defends major corporations in employment cases, almost every case they handle has a "smoking email" component to it (Varchaver, 2003).

In legal actions where evidence-mail or other e-evidence is used, it is as powerful as a smoking gun or DNA evidence, and as hard to deny or refute.

In 2002, President George W. Bush pledged that the Justice Department would "hold people accountable" for mismanaging their companies through "deceit and corruption" (Gordon, 2002). With the government's efforts to reassure the public, it is beyond question that company emails and other electronic documents will be sources of evidence for all sides of a dispute (Tambo and Redgrave, 2002).

Information Security and Discoverability of E-Evidence

The escalating role of e-evidence made the discoverability of email and electronic records an information security issue. Given today's technology and legal forces, companies face potentially serious risks if the courts subpoena their electronic records.

The purpose of this tutorial is to alert IS faculty to specialized cyber security issues. Computer forensics is the discovery and recovery of e-evidence. That e-evidence may be of a hacker's stealth attack, employee's disclosure of confidential data, or email evidence of corporate misconduct. The tutorial covers the discovery and admissibility of e-evidence in legal actions, such as those involving theft of intellectual property, identity theft, civil rights violations, electronic-fraud or extortion, information security breaches, breach-of-contracts, or Internet or email abuse. Also covered are ways to mitigate potential legal landmines, which are the risk of loss, liability, or litigation for inappropriate or rogue email and the most severe risk—spoliation (destruction of evidence).

E-Evidence Risks

Companies' information assets can be exposed by hackers, disgruntled or corrupted employees, or as a result of legal actions. Legal actions include civil disputes, criminal cases, class action lawsuits, employment grievances, and government or homeland security investigations. Unfortunately, the risk of e-evidence in legal actions does not receive adequate attention despite the

sharply increasing role of computer forensics in litigation. "There is going to come a time when there isn't a single criminal case that doesn't involve some electronic evidence" (Zuckerman, 2002).

In February 2003, *Forbes* magazine reported that "email has become a prosecutor's No. 1 weapon and the surest way for companies to get sued." Legal experts predict that e-evidence will be used in 100% of civil and criminal lawsuits, labor relations cases, and regulatory compliance cases. It is also central to government and homeland security investigations. Discovery of email in federal civil litigation cases is becoming broader and more common (Burke, 2002). Email is specifically targeted for evidence because highly-placed executives and employees discuss issues candidly, even if they are discussing confidential, incriminating, or criminal issues.

New York Attorney General Eliot Spitzer issued subpoenas to Merrill Lynch and five other Wall Street firms. He suspected they might have deliberately misled investors by making fraudulent stock recommendations in exchange for lucrative investment banking business. The focus of another investigation was Henry Blodget, Merrill's former star Internet analyst. At issue for investigators was whether Blodget or Merrill was criminally or civilly liable for securities fraud based on some of his stock recommendations under New York's Martin Act (Gasparino, 2001). However "…an analyst's bad call coupled with an investment banking relationship between the analyst and the issuer does not in and of itself suggest criminal activity" (Arkin, 2002). The distinction between "intent to defraud" and "intent to mislead" Is important. And absent strong circumstantial evidence of intent, analysts' bad recommendations do not amount to criminally fraudulent misrepresentation even if the analyst or brokerage had a financial interest with the issuer.

In light of this distinction, the Securities and Exchange Commission (SEC) and Spitzer investigated the firms' electronic records looking for evidence of fraud. Spitzer discovered many incriminating internal emails written by Merrill's analysts. In these messages, analysts disparaged companies they were publicly recommending, describing them as "crap" or "junk." Key evidence against Merrill was Blodget's email in which he slammed stocks that he was maintaining bullish ratings on (Knox, 2002). Furthermore, several analysts had complained about the pressure they felt from the banking division. One typical statement: "I think we are off base on how we rate stocks and how much we bend backwards to accommodate banking," to cite a discovered email (Loomis, 2002). In 2002, Merrill paid $100 after incriminating email was discovered containing evidence of intent to defraud. In total, the Wall Street brokerages paid over $1.5 billion in settlements—in large part because of the evidence-mail.

Federal Rules Pertaining to E-Evidence

In 1970, Rule 34 of the *Federal Rules of Civil Procedure* (FRCP) was amended to address changing technology and communication. The amendment to Rule 34 made electronically stored information subject to "subpoena and discovery" for use in legal proceedings (Rasin and Moan, 2001). This rule has far-reaching implications for electronic records and communications. They are breeding grounds for evidence of company activities and conduct. And every computer-based activity—whether it is sending email, invoices, viruses, or hacker attacks—leaves an electronic trace.

Electronic traces may be the actual content of emails or files or audit trails of the activity or attack, which are contained in log files or meta-data. Meta-data are descriptions or properties of data files or email, examples of which are dates/times an email or file was created or accessed. Meta-data is the "invisible information" attached by programs like Microsoft Word, Excel, and Outlook. For example, Outlook meta-data might include who was bcc'd (blind copied) on an email, when, and to whom an email was forwarded. "Obviously, this can be very important in setting up a *who knew what and when* type of scenario" (Jones, 2002). Traces of these scenarios can be revealed with computer forensics tools and techniques.

Email Defined by as a Business Record by Federal Rules

Email is not simply communication, but may also be considered a business record under Federal Rule of Evidence 803(6). Email qualifies as a business record if all five conditions are met. Those five conditions as stated in Federal Rule of Evidence 803(6) are:

(1) The record must be kept in the course of a regularly conducted business activity.
(2) The particular record at issue must be one that is regularly kept.
(3) The record must be made by, or from, information transmitted by a person with knowledge of the source.
(4) The record must be made contemporaneously. (That is, the document or file must be created at the same time as the business activity).

(5) The record must be accompanied by foundation testimony. (That is, someone must be able to validate that the record was made at the time of the activity.

With very few exceptions, all email communication and business documents are business records. Business records include computer records or printouts created as part of an organization's operations or transactions. Common examples of business records are purchase orders, human resource files, vendor reports, sales reports, and inventory/production schedules.

Computer Forensics

Computer forensics is used to gather evidence for human resource and employment proceedings, trade secret and anti-trust violations, fraud, sexual and racial harassment cases, discrimination suits, and civil lawsuits.

Computer forensics can reveal what users did on the company network, including:

- Theft of intellectual property, trade secrets, confidential data.
- Defamatory or revealing statements in chat rooms, usenet groups, or Instant Messaging (IM)
- Sending of harassing, hateful, or other objectionable email
- Downloading of criminally pornographic material
- Downloading or installation of unlicensed software
- Online gambling, insider trading, solicitation, drug trafficking
- Files accessed, altered, or saved.

Computer forensics also offers important benefits. It can reveal what users did on the company network, including:

- Recovery of lost client records, which were deleted by an employee who was stealing funds from the company.
- Proof that an ex-employee stole company trade secrets for use at a competitor.
- Proof of violations of non-compete agreements.
- Proof that a supplier's information security negligence caused costly mistakes.
- Proof of a safer design of a defective in a product liability suit.
- Recovery of an earlier draft of a sensitive document or altered spreadsheets to prove intent in a fraud claim.

Thus, deleted or not, there is a good probability that email, drafts and revisions of documents, spreadsheets, or messages can be retrieved. Computer forensics will play a major role in legal cases as new legislation is passed to combat cyber crimes, fraud, and terrorism. The most notable acts are the Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, and Sarbanes-Oxley Act of 2002. Congress passed the Sarbanes-Oxley Act, an investor protection bill, after financial scandals at Enron, WorldCom, and other companies sent stocks plummeting (Anderson and Black, 2002). This Act orders the SEC to issue rules requiring disclosure of financial transactions. Companies will no longer be able to hide their debt. Lynn Turner, former chief accountant at the SEC commented that "For the first time ever, we are going to find out about how much people are really hiding, and I think the world is going to be shocked when they see that" (Reason, 2002).

The use of computer forensics is increasing by law enforcement for criminal cases and by lawyers in civil cases. In the Computer Security Institute's *Alert* newsletter, Zuckerman [2002] stated that "There is going to come a time when there isn't a single criminal case that doesn't involve some electronic evidence." And in order for e-evidence to be admissible, it must be recovered and handled in a way that complies with the rules of evidence.

Handling E-Evidence: The 3 Cs

IS staff may be able to easily find and retrieve computer-data. However, retrieving and preserving e-evidence for use in a civil case is more complex than simply finding the e-evidence. For example, to use e-evidence in court, it might be necessary to create an exact duplicate copy of the files for proof that the e-evidence was not altered. Thus, an expert may be needed for computer forensics investigations. If the e-evidence of an employee's activity is being collected, an objective, outside investigator should be hired to prevent accusations, such as the company deliberately tried to frame the employee.

Legal protocols must be followed to ensure that the e-evidence is admissible. The operations used to collect, analyze, control, and present e-evidence cannot modify the original item in any manner. Any alteration to the primary source of evidence could contaminate it and render it inadmissible in court. Like all other types of evidence, the handling of e-evidence must follow the 3 Cs of evidence: Care, Control, and Chain of custody.

Care and Control

The first steps that are taken in collecting evidence are the most important. Everyone who touches the e-evidence can contaminate it. To ensure that care and control of the e-evidence are maintained, those who are investigating the digital media and content must know what they are doing before they do it. Also, the files and digital audit trails must be kept safe and secured.

Chain of Custody

Chain of custody is a legal guideline to ensure that the evidence presented at court or for evidence is the same as that which was seized. It requires documentation that the evidence is still in its original state. Maintaining the chain of custody of e-evidence is more difficult than for physical evidence because it is more easily altered.

Electronic Discovery

In a legal action, if the opposing party submits a discovery request for the company's emails and other electronic information, the company is required by law to retrieve and produce that evidence. The cost of responding to a discovery request can be huge if the company must sort through several years' worth of email and files to remove confidential material. And courts now impose severe sanctions, including criminal penalties, for improper destruction of electronic documents.

High-profile legal cases have been determined by the discovery and introduction into evidence of defendants' email or digital files, including those that users believed, incorrectly were private, secure, or gone.

Since every action taken by a computer user leaves a telltale trail, even the act of deleting documents can itself be revealing. Thus, not only do computer forensic techniques recover documents, they can inform investigators when and how they were deleted. It is possible to determine if a deletion is an innocent act pursuant to a corporate document retention policy or if there is an illegal motive.

Most computer users do not realize the huge strides in computer forensics that make it remarkably difficult to hide data from a determined investigator, such as a U.S. Attorney General or the Security and Exchange Commission.

Every day hundreds of U.S. companies face electronic discovery requests that they must comply with or face additional legal problems (Melnitzer, 2003). As a standard practice, lawyers and investigators are adding email to the list of records and documents they demand during the discovery process of cases. Companies had better be able to respond to a discovery request by the required date—or risk even more serious legal problems. One risk is a charge of obstruction of justice, a crime punishable by prison time. A related risk is spoliation, which is the intentional destruction of evidence. Spoliation is such a serious offense that most lawyers would rather face a smoking gun than spoliation.

Electronic Records Management (ERM)

Electronic records management (ERM) practices are important because irresponsibly managing the use and storage of electronic records can have expensive consequences or court sanctions. Any comprehensive document retention policy or plan must attempt to predict consequences of litigation. The cost of responding to discovery requests may turn on how information is stored. For example, a policy that requires separate servers for business documents will expedite the identification of privileged material in case of the need to produce documents in a legal action as required by Rule 34 (Scheindlin and Rabkin, 2002)

To avoid the risk of indiscriminately retaining or destroying information that may be requested as evidence, companies should implement and enforce ERM practices. ERM's two main components are electronic record retention and destruction.

According to the law, companies cannot destroy what they can reasonably expect will be subpoenaed. That is, they must retain all relevant documents and e-documents when they know, or should have reason to know, that they might become necessary as evidence in the future. Not surprisingly, this is a major dilemma for companies. They are required to retain records including emails that might be destroyed when backup tapes are reused.

Discovery Request Leads to Incriminating Email Evidence and $92.5 Million Fine

In October 1997, Boeing, the world's largest aircraft manufacturer, announced a $1.6 billion write-off because of production problems earlier that year. When this news was released to the public, the value of the company's shares dropped so sharply that a class-action lawsuit for securities fraud was filed against Boeing (Melnitzer, 2003).

During the pre-trial investigation, the attorney for the plaintiffs (the party that is suing) learned that Boeing stored 14,000 email backup tapes in a warehouse in Washington, D.C. The attorney filed a discovery request for all Boeing's email related to their production problems. Company officials had to produce those tapes for use as evidence in the case. Boeing faced serious problems because they could not figure out whose emails were on which tapes without restoring and searching all 14,000 of them. They did not have an ERM system in place.

Tapes are rarely configured so that they can be easily searched. Tapes are the most common backup media, but they are designed primarily for disaster recovery, in which the entire tape is simply reloaded. However, regardless of how difficult or expensive it is to retrieve files from backup tapes, companies must comply with discovery requests and produce the emails or records that are requested. Boeing had no choice. It had to restore all tapes, which took thousands of hours of employee time. In addition to the huge cost of responding to the discovery request, the emails that Boeing produced for the plaintiffs' attorney contained so much damaging evidence that the company paid $92.5 million to settle the class-action case.

Cases on Point: Computer Records of Andersen, Enron, and Wall Street

The House Energy and Commerce Committee asked Enron's accounting firm, Arthur Andersen, to turn over hundreds of documents from the firm's audits of Enron. The Senate's Permanent Subcommittee on Investigations went beyond "asking" for documents and issued 51 subpoenas to Enron and Andersen demanding the documents. Within the mountain of records that investigators looked at were *hot documents*—spreadsheets, invoices, contracts, memos—that showed a pattern of wrongdoing (Iwata, 2002). Before the Enron cases, electronic records retention and destruction were not a main concern. But after watching members of Congress on CNN or C-SPAN asking accountants and oil executives about their document-retention practices, that changed (Doerner and Milton, (2002). The Enron and Andersen cases clearly focused attention on e-evidence, the risks associated with a poorly structured or implemented document-retention management, and computer forensics.

In the billion-dollar insurance investigation of J.P. Morgan Chase & Co.'s financing of Enron (J.P. Morgan, 2002) , the determining factor was Judge Jed S. Rakoff 's ruling to allow "explosive" email into evidence. Eleven insurance companies were suing Chase, claiming that the bank knew that Enron's futures contracts for oil and gas were really loans. On Dec. 23, 2002, the Judge ruled that internal bank emails written over nine months be admitted as evidence (Anonymous, 2003). In one of the emails, a senior Chase official allegedly called the transaction a "disguised loan." J.P. Morgan tried to refute the evidence-mail unsuccessfully by claiming that the emails did not refer to the Enron transactions in question. Other internal emails suggest J.P. Morgan Chase officials were shocked to learn in October 2001 just how much Enron had outstanding. "$5B in prepays!!!!!!!!!" wrote one employee. The response was: "shutup and delete this email." (Reason, 2002).

References

Anderson P. J., and Black, A. R. "Accountants' Liability After Enron," *S&P's The Review of Securities & Commodities Regulation* (35: 18) October 23, 2002, p. 227.

Anonymous. "Explosive' E-Mails Allowed into Evidence in Enron Loan Trial," *Digital Discovery and e-Evidence* (3:1), January 2003, p. 14.

Arkin, S. "Analysts' Conflict of Interest: Where's the Crime?," *New York Law Journal.* February 14, 2002, p. 3.

Burke, P. J. "Learning from Wall Street's E-Mail Nightmare: Discovery and Admissibility of E-Mail," *The Metropolitan Corporate Counsel,* September 2002, p. 48.

Doerner, S., and Milton J. C. "Document Retention after Enron: When Should I Press 'Delete'?," *Oklahoma Employment Law Letter* (10: 6) May 2002.

Gasparino, C. "State Inquiry to Follow Close on Heels of Departing Merrill Lynch Analyst," *Wall Street Journal,* December 10, 2001.

Gordon, M. "WorldCom Stock Drops to 6 Cents," *AP Wire Story*, July 1, 2002.

Iwata, E. "Enron Case could be Largest Corporate Investigation," *USA Today,* February 18, 2002 (available online at **http://www.usatoday.com/life/cyber/tech/2002/02/19/detectives.htm**).
Jones, A. "Discovery Becomes Electric," *New York Law Journal* (226). March 11, 2002.
J. P. Morgan Chase Bank v. Liberty Mutual Insurance Co., 01 Civ. 11523.
Knox, N. "5 More Wall Street Firms Subpoenaed., *USA Today,* April 11, 2002, p. B1.
Loomis, T. "Electronic Mail: A Smoking Gun for Litigators," *New York Law Journal* (227), May 16, 2002.
Melnitzer, J. "Keeping Track of the Invisible Paper Trail: What Legal Departments Can Learn From Boeing's Experience," *Corporate Legal Times.* February, 2003. p. 15.
No. 94 Civ. 2120 (1995) U.S. District (S.D.N.Y. Nov. 3).
Rasin, G. I., and Moan, J. P. "Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace," *Missouri Law Review* (66 Mo. L. Rev. 793) Fall 2001.
Reason, T. "Reporting: See-Through Finance?" *CFO Magazine*, October 2002.
Scheindlin, S. A., and Rabkin, J. "Retaining, Destroying and Producing E-Data: Part 1" *New York Law Journal.* (227) May 8, 2002.
Tambe, J. W., and Redgrave, J. M. "Electronic Discovery Emerges as Key Corporate Compliance Issue," *Metropolitan Corporate Counsel.* October 2002.
Varchaver, N. "The Perils of E-Mail," *Fortune*, February 3, 2003.
Zuckerman, M. J. "A Letter from Washington, DC," *Alert: Computer Security Institute (CSI) Newsletter*, September 2002.