Information Security Journal: A Global Perspective, 19:118–123, 2010

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393550903074135

Taylor & Francis
Taylor & Francis Group

eDiscovery versus Computer Forensics

David R. Matthews
Office of Information Security,
City of Seattle, Washington, USA

ABSTRACT The contents of this article are similar to a chapter in an upcoming book by Steve Hailey and Mike Chapman, for which the author of this article will be a contributing author. This new book on computer forensics will be about the forensics process and will contain excellent guidelines for both professionals and laypersons to help them understand the right ways to access that information that might be hiding in the depths of those mysterious computer brains. Look for it soon in a bookstore or online distributor near you.

KEYWORDS eDiscovery, Electronic Evidence, Forensics, Computer Forensics, Digital Forensics, Digital Investigations, Forensic Process, Discovery, Data Preservation, Records, Management

In this article we will consider electronic discovery, often referred to as eDiscovery. We'll talk about the what, when, why, where and how of discovering, recovering and preserving electronic evidence, as well as discussing the difference between eDiscovery and Computer Forensics.

Let's start with a definition. What exactly is electronic discovery? Electronic discovery or eDiscovery, is simply the process of locating, collecting, and organizing relevant electronically stored information (aka ESI), usually for litigation. Forensics tools are often used in this process when the ESI has been deleted or is otherwise difficult to acquire. Good forensic practices can also ensure quality chain of custody for electronic evidence which can be hugely important to a legal case.

So, where do we find electronic evidence? Electronic evidence surrounds us like an ever-deepening fog. Look around yourself right now as you sit reading this article. If you're reading it on-line, you are of course immersed in the most obvious world of electronic information, the computer, and the immense worldwide network we call the Internet.

Even if you are reading it on old-fashioned tree fiber, I bet you can find several items within your immediate vicinity that are storing electronic data. Go ahead, I will wait . . .

OK, welcome back – how many did you find? Here are a few I can see from here. My cell phone, my telephone, my watch, USB thumb drives, CDs, DVDs, and (yes I still have them) floppy disks. Of course, I also know that in my drawer I have a laptop and an external drive that contain a bunch of data. And that is only talking about the physical locations within my reach.

Now, because of my work I may be more inundated than you are by these devices. But I can safely say that within reach of my desk I have immediate near-line access to terabytes of electronic information, and that is not counting the

Address correspondence to David R. Matthews, Office of Information Security, City of Seattle, 700 Fifth Avenue, Suite 2700, Seattle, WA 98124-4709.
E-mail: david.matthews@seattle.gov

Internet or my organization's network, backup tapes, and so forth. That is just what I can literally touch.

When you add in the rest of the online universe, the numbers are staggering and growing exponentially.

As a citizen in this electronic universe we all need to understand where this data lives and how to find it, especially if we are responsible for managing that data or preserving it for legal or compliance reasons. To completely document all of those different sources of electronic data would take a much longer article, but I encourage all of you to consider them carefully.

Electronic discovery and computer forensics are related practices that enhance and complement each other. Though they sometimes overlap, the procedures and best practices for each are different in some essential ways.

Let us use a metaphor to help make this clearer. Think of this as the difference between learning to playing a guitar for fun and learning classical guitar. That is not to say that eDiscovery is not as important or serious a pursuit as the forensic side of things, but just that with forensics you have to get deep into the details.

You can pick up a guitar, learn a few chords, and be off and running – playing songs around the campfire. With a little practice and maybe some lessons you can have a lot of fun and maybe even play in a garage band. Similarly, if you understand the basics of electronic evidence and the places to find it, you can begin to help your organization or clients winnow out the relevant data and gather, store, and organize it for litigation. As you get better at these procedures you can ensure that your clients or the organizations you work for are following best practices and right procedures so they are properly prepared for litigation. You can also act as an expert witness once you have studied and gained enough experience to really understand the sources and correct ways to recover and store electronic evidence.

However, there is a whole different concentration and effort involved if you want to learn classical guitar. To do that well, you have to know your instrument intimately. You have to understand the history and the theory of music, tonality, rhythm, dynamics, and style. You have to practice, practice, practice! The depth of knowledge and experience needed to do this well and with recognized expertise is exponentially greater than that required of the garage band musician.

Again, this is not to demean the practitioner of electronic discovery, but rather to point out the difference in the concentration and depth of understanding required. While a person who is an expert in eDiscovery must be well versed in the sources of electronic data, the forensics expert must be able to take those sources apart right down to the bits and bytes. The forensics expert needs to understand in detail how file systems are created, accessed, deleted, and changed. When those systems have broken down, he or she must be able to pick out those pieces and put them back together again if at all possible, or explain why it cannot be done. That is classical music to a geek's ears. The best of these experts can play that music in such a way that even the most unschooled listener can understand and appreciate its beauty and clarity.

Both the eDiscovery and the forensics expert have an important part to play. The classical guitar sounds best when it is backed up by the basic chords of the rhythm guitar. Both practitioners are at their best when they can communicate their expertise in plain, clear, and simple terms. When played right, that music will appeal to any audience. When communicated well, the expertise of either of these practitioners will add value and clarity to court cases or investigations.

So, both eDiscovery and forensics have an important place in this practice. To help make this even clearer, the next section gives some specific examples of eDiscovery cases.

eDISCOVERY CASE EXAMPLES

Electronic discovery is most often thought of in reference to litigation processes. However, sometimes it can be useful in preparation for possible litigation, records management, or public disclosure. With that in mind here are three examples of actual cases that involved recovery and organization of electronic data.

Let us start with public disclosure. Virtually all government organizations are subject to what are called "sunshine laws." These laws are intended to keep your public servants honest with your taxes and fees, by providing transparency into how those monies are spent, and by offering insight into your government's activities. To ensure that is the case, there are public disclosure rules that require governments to provide citizens with any public records requested within a reasonable amount of time and in a reasonably usable and complete state.

As someone who has worked in local government I can tell you that these requirements are not always easy to fulfill. Think about your own records. Your mortgage papers or rental agreements, maintenance warranties, your will, your tax records, bank records, and so forth. If you are very well organized you could probably put your hands on any of the above pretty quickly as long as someone was asking for relatively current records. But what if they wanted records from seven years ago? Many of the records retention laws require that public sector records be maintained for seven or more years. If you multiply your quantity of files by literally thousands of government entities, departments, functions, and employees you can begin to imagine the complexity of storing, organizing and accessing those files on demand.

Of course, when you add in the electronic records component of the last couple of decades, you have created an exponentially rising curve of records in a vast array of formats and media. All of those add another level of complexity that is orders of magnitude above what it was when it was simply paper media. A statistic I saw recently said that the world generates a petabyte of new data every hour and that amount is growing. A petabyte is essentially a thousand terabytes, and if you do not know what a terabyte is, look it up – we are talking lots of data!

So for those in local government or any government organization the demands of public disclosure can be extremely challenging and at times overwhelming. One case I am familiar with asked for the entire human resources database of a major city. The eDiscovery experts, the owners of the databases, and the public disclosure officers and attorneys met to go over the disclosure request and were able to work with the requestor to narrow that down to specific parts of the database. In that case, the eDiscovery expert, through his understanding of database structure and theory, was able to assist the lawyers in finding the actual relevant data that responded to the disclosure request. He was also able to act as liaison between the lawyers and the database administrators to help the lawyers ask for the fields and queries necessary to allow the administrators to recover and store the correct information.

Next, let us consider records management. As mentioned above, all government records are subject to records retention law. This is also true in the private sector in many cases. Depending on the regulations that affect your organization, those of you in private sector enterprises probably know that you are subject to records retention rules about how long you must keep certain types of records.

Those rules can be complex and difficult to understand, much less follow correctly. There are whole industries dedicated simply to the interpretation and compliance with records retention law. To follow the retention rules it is necessary to understand both what records you have and where and how they are stored.

Once again, the eDiscovery expert can be of assistance. In one case, an eDiscovery practitioner was asked to assist a large corporation in the recovery and organization of years of stored data on backup tapes. To do so, she started by interviewing the organization's management and staff to better understand its business model and the regulations to which the organization was subject. She then used recovery tools to carefully copy and index all of the data on the backup tapes. Using her knowledge of the business and its regulatory requirements, and with the help and feedback of subject matter experts from the different business lines in the organization, she was then able to assist them in organizing those records and storing them appropriately with the required retention schedules.

This can be extremely valuable both for compliance with regulations and in possible litigation. If you are found to have destroyed data that by law you were required to retain, it can result in fines or other sanctions both in court and by regulatory agencies. On the other hand, if you have saved data that you could have destroyed, that data is still discoverable in a court case. If it is data that you would rather not have introduced, you obviously have not done yourself or your organization any favors by retaining that data past the required retention schedule.

Finally, let us look at a prelitigation eDiscovery case. This looks very much like a case in an actual litigation, so it will suffice as an example for both, although we will also talk about some of the possible differences.

In this case, an employee was being let go for what was considered good cause. Without going into detail, suffice it to say that he had violated the organization's acceptable use policies on his company computer. This was not the first time, nor was it the only problem this employee had had; rather, it was only the latest problem and the most egregious so far and thus led to his termination. The company's eDiscovery expert, who we will call John, was contacted by the

employee's supervisor on advice from the law department. He went to her office and interviewed her about the employee and type of work that he did. In that interview he found out the employee had access to and did daily input for a financial database. He was also in charge of investment information for the organization. He used a laptop, sometimes worked from home over Virtual Private Network (VPN), used external storage devices, and had a BlackBerry smartphone.

Immediately, John contacted the database, email, and network administrators to ensure that the user's authentication credentials were disabled. This was to ensure that the terminated user was no longer able to access the database or the network to make any changes to the records he had access to.

Next, they visited his office, and John, with the assistance and permission of the supervisor (which he documented), searched the office for any and all digital media. They found boxes of CDs and DVDs, two USB flash drives, the user's BlackBerry, an external hard drive, a laptop, and two desktop computers. John carefully documented everything they had found, including recording the date and time and even taking pictures of where everything was found and how it looked when they found it.

One of the computers was running, so John left it running, took a picture of the opening screen, and documented all of the open applications.

Now, John moved into forensics mode, or at least into the beginning of good forensics procedures. Since the eDiscovery process and the forensics process can interweave at times, it is important for eDiscovery experts to understand and practice correct forensics procedures.

John used a special USB stick with forensic tools on it to plug into the running computer and capture all of the memory and services that were currently running. Only then did he shut that computer down. Then he pulled hard drives from both desktop computers and the laptop and carefully stored them in antistatic bags for eventual forensic analysis.

Finally, John finished documenting all of the types of media and hardware that he had acquired (specific information about when and where and how of each) and had the supervisor sign off on a chain of custody form so he could take them all with him.

As a next step, John contacted the database administrator for the database the employee was working with and asked for copies of all available access and activity logs. He also contacted network administrators and requested logon/logoff data for the individual, as well as a copy of his home drive where he stored his entire work product on the network. Finally, he contacted the email administrators and requested they back up the user's email data and provide him with a copy.

John was careful to document every step of this process and to record dates and times and sources of all the data that he gathered for this case. All of the data copies and sources were stored in locked and/or protected file space in case they were needed.

In fact, approximately six months later, John was contacted by the law department and notified that the employee in question had filed suit for wrongful termination. The carefully stored information was recovered. John did some forensic analysis on some of that data and the attorneys did their own analysis of some of the other data. When they presented their information to the plaintiff's attorneys the case was dropped as it was clear that the evidence against the employee was overwhelmingly in favor of the organization.

This was a case where the eDiscovery procedures took place simply because there was a likelihood of litigation. In fact it is thought by many in the legal profession that the duty to preserve evidence is triggered by the mere possibility of future litigation, so it was good practice by this organization to do so. As is obvious from the story, it turned out to be to their advantage.

However, in many cases eDiscovery does not begin until there is an actual case filed. The procedures should be similar to those above. However, in many organizations there will be an official process called a "litigation hold." This is required by the courts in nearly all jurisdictions. It simply means that the parties in a case have a duty to preserve any and all data relevant to the case at hand from that point forward. The "hold" part of it refers to the fact that you not only hold all data, but you put any recycling or destruction of media, deletion, or other destruction, or any changes to data, on hold until you can ensure that all relevant data have been recovered and stored. The idea of discovery in a legal case is that both sides find and reveal all relevant information to each other so that the case can be tried fairly with all the facts available to all parties. eDiscovery addresses that requirement in the electronic side of data recovery.

The litigation hold process must include notification of everyone who might be in possession of relevant data. In the case of John's organization, they gather anyone who might have relevant data in a meeting with information technology staff, supervisors, and the attorneys on the case. John, the eDiscovery expert, facilitates the discussion ensuring that all possible digital media or electronic data sources have been considered. The information technology staff are the subject matter experts who can ensure the required data are accessible and who may well be responsible for actual acquisition and storage of the data. During this meeting, the attorneys explain the responsibilities of all staff who might hold relevant information and get them to sign documentation that they understand their responsibility to preserve, locate, and report or store any and all relevant data.

Again, the eDiscovery expert adds value by being the liaison between the technicians and the employees and attorneys. His job is to translate the geek and ensure that the technicians understand what is required of them and that the employees and attorneys understand their part in the process. His part in this process is extremely important, and in a mature organization there should always be at least one person who can perform this service.

As you can see from these examples, the eDiscovery expert can be a valuable member of the legal, information technology, and/or management team in any organization. The cases we looked at above give you a good idea of the different ways that eDiscovery procedures can be utilized in an organization to assist with compliance, records management, and/or litigation. In the next section we will walk through how that process works in one organization.

THE eDISCOVERY PROCESS

Like anything else, eDiscovery is done best when it is done consistently and follows established best practices. Since the work of eDiscovery is often part of litigation or compliance, the ramifications of doing a poor job can be extremely embarrassing at best, or expensive at worst.

Let us walk through a typical procedure in one organization during a specific event to give you an idea of the different elements required in a quality eDiscovery process.

For instance, assume someone slipped on their way into this organization's store and broke their ankle. There is every reason to believe this could result in litigation. A staff person or manager immediately contacts their legal counsel. Their legal counsel immediately starts the litigation hold process. This process includes a notification that is sent to everyone who was present at the time or who had any responsibility for the maintenance of the facilities. The company's eDiscovery expert or perhaps a senior network or information technology manager is notified with a written request to assist in the identification and preservation of any electronic evidence. That person initiates a meeting with all of the affected staff and their management, the information technology experts, and the attorneys.

In that meeting they discuss the different types of records that are relevant and need to be preserved. They put a hold on deletion of email for any of the affected employees. They ask the information technology staff to create backup snapshots of all affected staff's network drives, desktop or laptop drives, and email accounts. They ensure that video tapes from the surveillance cameras are carefully preserved. They ask for records of phone calls that might be relevant, such as the call to 911.

The technology staff that are responsible for preserving electronic data from computers will need to use accepted forensic practices to ensure that data is copied and stored in its original configuration and that no data is changed or lost. To do so, they will need to be familiar with correct and accepted tools and practices.

Someone in the organization needs to be responsible for keeping track of what will be recovered and preserved, who will acquire it, when and how it will be acquired, and where and how it will be stored and organized. That may be the eDiscovery expert, someone in the legal department, or another staff member. This is an essential part of a quality eDiscovery process and should not be neglected.

That person or persons will need to document all of the above and carefully track the process as it unfolds. Their job will include follow-up with technical staff and the affected users and their management to ensure that no relevant data is missed, lost, or changed. They may also be called upon to help users locate and recover data or to explain to technicians exactly what is required. Finally, they may be required to analyze the acquired data to assist the legal personnel with winnowing out the relevant information and possibly help with organization and storage of the data.

All of these steps and processes must be carefully documented in case they are questioned later. Again, this is a part of the process that the eDiscovery expert is responsible for and should be careful to do well. Cases have literally been won or lost based on the practices of preservation and recovery followed by organizations.

As you can now understand, eDiscovery is an extremely important and involved practice. It is imperative for an organization of any size or type to understand what is required of them under electronic discovery rules and best practices. Creating and practicing these procedures before they are actually required will save you and your organization resources, time, and money. It behooves everyone to ensure they have procedures in place and employees who understand and follow them.

As you continue learning about eDiscovery and forensics and developing procedures in your organization, remember that the foundation you are building upon will be the established procedures for electronic data recovery that we have illustrated here. You have to learn the basic chords before you can begin to move into the techniques, challenges and rewards of classical guitar music. So never forget or neglect the basics.

REFERENCES

Cohen, A.I., and Kalbaugh, G.E. (2009). *ESI Handbook Sources, Technology, and Process* (1st ed.). Frederick, MD: Aspen Publishers.

Cohen, A.I., and Lender, D.J. (2009). *Electronic Discovery Law and Practice* (3rd ed.). Frederick, MD: Aspen Publishers.

Contoural. (2007, November 17). Taking control of your information: What every legal department wants from IT. Contoural, Inc.

Hagy, D.W. (2007, January 1). Investigations involving the Internet and computer networks. *U.S Department of Justice, National Institute of Justice*. U.S. Dept. of Justice. Retrieved April 3, 2007, from <http://www.ojp.usdoj.gov/nij>

Microsoft. (2007, January 11) Fundamental computer investigation guide for Windows. *Microsoft Technet*. Retrieved February 14,2007, from <http://technet.microsoft.com/en-us/library/cc162846.aspx>

Nelson, S.D., Olsen, B.A., and Simek, J.W. (2006). *The Electronic Evidence and Discovery Handbook, Forms, Checklists and Guidelines* (1st ed.). American Bar Association.

Rothstein, B.J., Hedges, R.J., and Wiggins, E.C. (2007, February 11). *Managing discovery of electronic information: A pocket guide for judges*. Federal Judicial Center.

Shinder, D. (2008, July 16). Documenting authenticity of evidence for the e-discovery process. WindowsSecurity.com. Retrieved July 21, 2008, from <http://www.windowsecurity.com/articles/Documenting-Authenticity-Evidence-E-Discovery-Process.html>

Wiles, J. (2007). *Techno Security's Guide to E-Discovery and Digital Forensics* (1st ed.). Burlington, MA: Syngress Publishing, Inc.

BIOGRAPHY

David Matthews is currently the Deputy Chief Information Security Officer for the City of Seattle. He has worked in the Information Technology field since 1992. He began working for the City of Seattle as the Technology Manager for the Legislative Department (City Council) in 1998. In early 2005 he was selected to be the first Deputy CISO for the City. In his work for the City he has developed and created a NIMS/ICS compliant incident response plan; updated and extensively re-written the City's Information Security Policy; and created and taught training courses on information security and forensics. He has most recently created an IT primer for the City's Law department as part of his collaboration with them on eDiscovery issues.

He is a participant and leader in regional information security organizations. He is the public sector co-chair of the US-Cert/DHS sponsored North West Alliance for Cyber Security (NWACS). With NWACS he has worked with the Pacific Northwest Economic Region non-profit (PNWER) to sponsor information security training for SCADA operators and managers; a risk management seminar; a regional cyber response exercise; four Blue Cascades disaster scenario exercises; and is the creator and editor of a portal Website with local information security and forensics activities; a library of best practice documents and links to information security and forensics Websites.

Matthews is also an active participant in many local, national and international information security, forensics, and e-discovery organizations. He participates on the local Critical Infrastructure Protection sub-committee of the Regional Homeland Security team, and also is a member of the American Bar Association's Science and Technology and Electronic Discovery committees. He has published an article on Active Defense in the ISSA journal, and has presented at many emergency management and information security conferences. His most recent presentation on eDiscovery called "Translating Geek for Attorneys" has been presented to records managers, information technology and security audiences in corporations such as REI and Starbucks, presented as a Peer to Peer session at RSA, and was given as a continuing legal education course for the U.S. Attorney's office in Seattle and the City of Seattle's Law department.

He holds the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and a Certification in Forensics Investigation.