## Contents

**Foreword** ix  
**Preface** xi  
**Acknowledgments** xiii  
**Author** xv  

### Chapter 1: What Is Electronic Information, and Why Should You Care?  
1.1 Introduction 1  
1.2 Electronically Stored Information and the Federal Rules of Civil Procedure 1  
1.2.1 Changes to the Federal Rules of Civil Procedure 3  
1.2.1.1 Rule 1: Scope and Purpose 3  
1.2.1.2 Rule 16(b)(5) and (6): Pretrial Conferences; Scheduling Management 3  
1.2.1.3 Rule 26 4  
1.2.1.4 Rule 37 Safe Harbor 11  
1.2.1.5 Rule 34(b) Producing Documents Procedures 13  
1.2.1.6 Rule 33(d) Interrogatories to Parties 15  
1.2.1.7 Rule 45 Subpoena 15  
1.2.1.8 Form 35 15  
1.2.2 Federal Rules of Evidence 16  
1.2.2.1 FRE 502 17  
1.2.2.2 FRE 901 17  
1.2.2.3 FRE 802 18
Chapter 4  Who’s in Charge Here? Allies, Owners, and Stakeholders  
4.1 Introduction  
4.2 The (Long) List of Stakeholders  
  4.2.1 Information Technology Professionals  
  4.2.2 Legal Staff  
  4.2.3 Records Managers  
  4.2.4 Auditors  
  4.2.5 Human Resources  
  4.2.6 Department Heads, Vice Presidents, and Executives  
  4.2.7 Physical and Information Security Personnel  
4.3 Ownership of Data  
4.4 Data Control Considerations  
4.5 Required Skill Sets and Tools  

Chapter 5  The Hunt: Recovery and Acquisition  
5.1 Introduction  
5.2 Where, Oh Where, Has My Data Gone?  
  5.2.1 Applications as a Vital User Interface  
  5.2.2 Hidden or Restricted Access Data  
  5.2.3 Encrypted Data  
  5.2.4 Deleted or Corrupted Data  
  5.2.5 Proprietary Data or Data Stored on Obsolete Media  
5.3 Privileged, Sensitive, and Inaccessible Data Management  
5.4 Proving Ownership and Integrity  
5.5 Marking Time: How Time Is Recorded and Ensuring Integrity  
5.6 Legal and Forensically Sound Acquisition  

Chapter 6  Keeping Your Treasures: Preservation and Management  
6.1 Introduction  
6.2 Securing the Data  
6.3 Access Control and Management  
6.4 Organization and File Management Techniques  
  6.4.1 Day-to-Day Organization  
  6.4.2 Management of Data over Time  
  6.4.3 Response to Litigation or Audits  
6.5 Safe Storage Issues and Considerations  
6.6 Litigation Hold  
6.7 Spoliation: The Loss of Relevant Data  
6.8 Automated Technical Solutions  

Electronically Stored Information, Second Edition  
https://www.crcpress.com/9781498739580  
for IT Business Edge
# Contents

**Chapter 7**  
**Sharing Is Good: Dissemination and Reporting**  
7.1 Introduction  
7.2 Format Issues: Original or Usable?  
7.3 Mediums for Transfer  
7.4 Creating Readable Reports  
7.5 Tips for Depositions and Expert Witness  
7.6 Conclusion  

**Appendix I: Links and References for More Information**  

**Appendix II: Forms and Guides**  

**Appendix III: Links to Technical Software Solutions**  

**Index**
Foreword

Matthews has approached e-discovery from a fresh, new perspective—one that is understandable to the layperson as well as the technologist. *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval* will guarantee that you know more about e-discovery than you thought possible. A must read for anyone in the information technology and legal professions, the book provides invaluable information to be proactive or reactive in responding to requests of electronically stored information. The flow of the book from the first chapter to the last is clear, simple, and thorough—any attorney who desires to become a technically savvy advocate for his or her corporate legal department or law firm will have this book at hand. This book goes a long way in removing the intimidation factor between IT, the corporate legal department, and outside counsel. This book should be required reading for anyone in a computer science, information technology, or law-related program, and is now part of the Digital Forensics and the Law course I instruct. If you want to get up to speed on e-discovery and actually understand what you read, you’ll buy this book.

Steve Hailey
President/CEO
CyberSecurity Institute
Digital Forensic Examiner and Educator
7

Sharing Is Good
Dissemination and Reporting

7.1 Introduction

In this final chapter, we will discuss the reasons and the methods for sharing the data we have so carefully acquired, preserved, and managed. There are several reasons that we will consider, and each may engender different approaches or procedures appropriate to the specific needs of those situations.

These approaches will include the format in which the data are produced, the content, the timing of release, and the actual physical media and process for delivering the electronic information (Figure 7.1). We also discuss reporting protocols and suggest some ideas to ensure that the reports you create are clear and concise.

Finally, we end this chapter with some tips for participating in depositions or as an expert witness.

7.2 Format Issues: Original or Usable?

One of the first considerations in sharing the data you have collected will be in what format you want to produce the data.

Think about it in terms of your reasons for producing the data in the first place, and this should guide you in your formatting decisions (Figure 7.2). For instance, one reason for producing data is for dissemination to colleagues, relatives, or friends who simply have a nonadversarial interest in the information. In that case, there is little likelihood of their using the data or its metadata in any way that would be harmful to your interests. There will also be no legal or regulatory rules compelling you to ensure the integrity of the data.

If that is the case, you might simply create copies of the pictures, documents, spreadsheets, and so forth, and send them via standard
Figure 7.1  Consider the procedures that you will put into place for disseminating the evidence you collected.

Figure 7.2  The format of the evidence you produce should be decided early on.
e-mail, mail them on a DVD, or store them online on a file sharing tool. You have no responsibility to ensure the data are secure and uncompromised. You do not need to be concerned about what metadata are attached to the data as it is very unlikely that any of those people will even know or care about its existence.

Another reason for producing data could be for a tax audit required by the Internal Revenue Service (IRS) or other taxing authority. You might consider this a somewhat more adversarial situation, and you are legally required to produce any and all relevant records and to be able to prove their integrity. It is unlikely that the IRS would require specific metadata, but if questions arise about the integrity of your records, you could be required to prove the legitimacy of those records. That proof is likely to be enhanced by your ability to refer to metadata and to your careful data handling processes. If this is the case, you will most likely be creating copies of documents, spreadsheets, and so forth, with accompanying metadata or other means of proving their integrity as we discussed earlier (e.g., hashing).

The IRS or other legal auditing authority will be specific about the format in which they expect your documentation to be delivered. It will be to your advantage to not only comply with those requests, but to do all you can to ensure good procedures and data management, including chain of custody and data security practices. That will allow you to address any issues of data integrity with well-documented management practices.

Another likely scenario is the need to produce data for a legal matter. For the most part, as we discussed in Chapter 1, a meeting will be conducted between the parties to discuss the data that will be produced. In that meeting, your legal counsel will make decisions with the other side about specific electronic and physical evidence required to adjudicate the case. The sides will agree in what format they want the evidence produced.

In some cases, they will decide that they want the data produced in its original format, including all metadata. Or they might decide that graphic copies such as TIFF files are appropriate. If that is what they decide, they might also ask for graphic copies of metadata for each file, or they might not require metadata.

Depending on the specific types of data, producing them in original format can have advantages and disadvantages. For instance, if the
original data were in a Microsoft Word file, that is relatively common and most organizations will have the applications and tools to be able to read both the document and its attached metadata. Therefore, as long as you are careful not to compromise the document when you transfer it in that Word document format, it will be a simple and relatively secure production of the electronic evidence.

However, if the original data were stored as a Lotus 123 spreadsheet created many years ago, it may be very difficult, first to preserve any metadata when you produce the copy, and second for the recipient to open it with current existing tools. The recipient might also have a hard time being able to access the metadata without specialized tools.

This becomes even more difficult when the original form of the data is in a proprietary database. Database applications can be expensive, and data stored therein might be difficult or impossible to extract or even to view. Without having the correct version of the database software (including required licensing), specific information about the design of the original database, and expertise to re-create the original database architecture, it might be impossible to actually view data in the original context.

All that said, it can be a daunting task to be able to actually gain relevant electronic evidence that will stand up to evidentiary requirements in court. The most important thing that you and your legal counsel can do is to be aware of these issues up front and be specific when requesting data from the other parties during your pretrial meetings.

Being aware of these issues as they relate to your own data will also help to inform you and your legal counsel as to your capabilities for producing relevant electronic evidence in either its original format or in some other format that might be requested.

At times, it may be to everyone’s advantage to create different data formats in order to ensure that the evidence is consistent, uncompromised in any way, and most effectively and easily used by all sides. The sides might decide to have all evidence stored in a database online so that it is accessible by all concerned. There are some new online services that offer that possibility.

In the end, it is most important to consider the goals of everyone involved for the production of the data and find the most efficient and effective method to accomplish those goals.
7.3 Mediums for Transfer

The actual physical or logical medium used to transfer produced electronic data will depend on both the goals of the producing parties and any agreements made between them. In many cases, electronic evidence can be copied onto physical media such as DVDs, CDs, tape, or USB devices such as hard drives or flash drives. As long as this copying is done in a forensically sound manner that ensures the integrity of the data, that should be sufficient for most situations (Figure 7.3).

The ways you can ensure a forensically sound copying of data to these media are as follows:

- Create and document at least two different hashes of the data before and after copying (see Chapter 5 for more details).
- Maintain a chain of custody, documenting where the data were originally, who was the custodian, who copied the data, when, and for what purpose.
- Document the tools used to copy the data including their version numbers.

Appendix II includes some sample logging and chain of custody documents.

In other cases, the parties involved might decide on transferring the data using e-mail or an online service. In these cases, you can ensure the integrity of the data by using hashes and maintaining good

Figure 7.3 The type of media on which you store or deliver the evidence will depend on many factors.
logging of all activities involved in copying the data. This should be agreed upon up front between all of the parties.

If you decide to use e-mail as a means of transferring data, you should consider the classification of the information. If it is sensitive in any way, you should look at the possibility of encrypting the e-mail transmissions or possibly encrypting the documents. Most e-mail applications have the capacity to encrypt their contents, or there are third-party add-ins that will allow you to do so. Encrypting the documents or other evidence can also be accomplished with commonplace tools, several of which are referenced in Appendix III.

Should you decide to use an online service, you should ensure that the service provider contract includes the following:

- Information security policies that address the confidentiality of your data, its availability, and its integrity
- Backgrounding of its employees who will have access to your data
- Well-defined procedures for access to the data
- Defined and practiced authentication protocols to ensure data are accessed only by those with the correct and current rights
- Disaster recovery and business continuity policies and practices that are both well documented and auditable
- 24/7/365 access to support and priority assistance
- Effective and timely notification procedures in case any issues affect the confidentiality, integrity, or availability of your data
- Data management, access, retention, and archiving procedures that meet your requirements

These contractual requirements are important in any service that you use online, but when you decide that this is how you are going to disseminate legally relevant electronic evidence, they become paramount to ensuring your data are there when you need them, and that the integrity of the data is unsullied.

Whatever medium makes the most sense to achieve the goals of sharing your data with another party, the most important consideration will always be ensuring the integrity and availability of the data to all concerned. As you consider which solution makes the most sense, always keep this in mind.
7.4 Creating Readable Reports

As the person in your organization who has taken on the task of learning about electronic evidence, or just due to your interest in better managing your own data, you may be in the position to create reports in this regard. These might include data management and retention reports, audit information, or evidence investigation and acquisition reports.

One of the most important things you can do for the sake of your audience is to create reports that are understandable, concise, and complete (Figure 7.4).

The first step in ensuring that your report is complete and contains all of the relevant information is to keep excellent records of everything you do in relation to the data in question. The foundation of that record keeping and of your eventual ability to document your actions will always be a good records retention policy. That policy means little or nothing if it was not properly disseminated and carefully followed by you or your organization.

Beginning with your records management policy, you should have some record or log that illustrates your or your organization’s compliance. It should document how you follow the correct records management procedures, where and how the data are preserved, and your process for archiving or destroying the data according to your documented and audited schedules.

Next, you need to carefully log any and all activities undertaken to locate, acquire, and secure any relevant electronic evidence. Using...
the samples we give you in Appendix II, or something similar that is appropriate for your organization, you should carefully document all of the following:

- The owner(s) and custodian(s) of the data in question
- The physical and logical locations of the data
- The tools and methods used to acquire the data, including names and versions of acquisition applications and types of hashes or other integrity assurance tools used
- The time and date of acquisition
- The movement of data to or from any type of storage (chain of custody), including who moved it and why
- The security procedures, both physical and logical, used to ensure the data could not have been compromised or accessed by anyone without the correct authority
- The physical and logical medium on which the data is stored or transferred to or from, including the name or type of media and a unique identifier such as a serial number, model number, or label

If you are investigating or analyzing electronic devices or systems to find relevant evidence, you should also log every step of your investigative process. You should include the time and date of each part of the investigation as well as the tools you used and the results of your analysis.

There is an easy way to do this if you are using the Windows operating system. Every Windows OS includes a simple text application called “Notepad.” Start up Notepad and create a new file with the first line: ‘LOG’ (without the quotes) and then close the application. Then when you open it up again it will “automagically” insert a date and time stamp.

I have all of my investigators use this simple tool to log every step of their analyses of devices for forensics investigations or acquisition of data for e-discovery. As they are working they simply open the file, note everything they did, the tools they used, and the results and then close the file again. By doing this we get a nice time-stamped record that is extremely useful in depositions or court appearances by assisting in our recollection of what we did in an investigation.
Depending on the physical and logical location of the evidence in question, you may also need to gather up system or database event logs, ingress and egress records, application logs and metadata, or other detailed information related to the data in question.

Once you begin your reporting process by gathering or creating all of the documentation above, your next step is to winnow it down to the important information for your intended audience.

Take the time to understand who that audience will be and their level of expertise. For instance, perhaps you are creating a report to present to your manager who has a very good understanding of the technical details and language related to the electronic data. In that case, you can use known acronyms and more technical language to describe the work you did, what you found, how and where it was acquired and preserved, and so forth.

However, if you are creating a report to be used in court or for an auditing authority, you should avoid the use of technical terms or acronyms. Instead, create a document that you could easily explain to your grandmother. In Chapter 2 we discussed in detail the idea of translating geek. This is where this skill is most important.

If you need to explain a technical process, try to come up with simple and easy-to-understand metaphors or examples. In Appendix I, we offer some great resources that explain how technical things work in easy-to-understand language.

Should you need to create a report explaining something technical such as how Internet information is stored on a computer, or how data can be fingerprinted using hash algorithms, I recommend reviewing sections in this book that address those ideas or taking the time to research some of the resources offered in Appendix I. These can give you great ideas of ways to make these technical details understandable to people without a technical background.

When creating a report, always begin by having all of the information you need, then consider your audience and tailor your presentation to their level of understanding. In every case, you want to be sure all of the important points are covered while not digressing into information that is not important, not required, or simply too esoteric or technical for the audience.

Very few jurists, judges, or lawyers have studied computer science, so they will neither appreciate nor understand your in-depth
explanation of the advantages of the latest version of Linux over the Windows operating system, for example (unless that is germane to your analysis of the evidence).

With written reports, be sure to do a good spell check and reread the report to ensure it is clear and covers all of the important information. There are sample reports in Appendix II.

If you are presenting an oral report, it is important to be comfortable with public speaking. We discuss that in the following section.

7.5 Tips for Depositions and Expert Witness

One of the most challenging and also most rewarding activities that might come from your having used this book and other resources to become an expert in electronic evidence will be the opportunity to share your knowledge as part of a legal matter (Figure 7.5).

This might take the form of simply assisting your legal counsel or your management in understanding the relevant electronic evidence and all of the details and issues that we discussed in this book. In that case, you will probably be dealing with one or only a few people at a time, and it should not be too daunting. Having done a great job in creating the written report as we discussed above, you will simply need to help them understand all of the pertinent details.

However, should you be called upon for a deposition or as an expert witness in a court case, or asked to present your findings to a larger audience, that can be a frightening proposition for some people. The first recommendation I would make is to spruce up your public

Figure 7.5  Delivering your information in court or a deposition can take some special skills.
speaking skills. There are classes and organizations available, some of which are referenced in Appendix I, which can help you with speaking and presentation skills and practice sessions. There are also some online resources with good ideas for creating presentations.

The same ideas apply here as with a written report. Make sure you understand your audience and have all of your information at hand. The actual information you present will depend on the specific requirements and level of expertise of your audience. However, I recommend bringing along any logs or other documentation that you might be questioned about as reference for yourself.

Be concise and ensure you are able to answer any question that might be asked of you. It can be very valuable to sit down with your legal counsel and rehearse possible questions and answers that might be brought forward during the case or deposition.

An important caveat, especially in a court setting, is to only answer the question you are asked. It is not your job to try to figure out what else the questioner might want to know, or to give details that were not specifically requested. It is a common mistake for someone in the witness stand or during a deposition to try to be helpful and to expound on their deep knowledge of a subject without having been asked. This might confuse the actual issue or give opposing counsel information that is not relevant or might even be used against your side. It can lead to your counsel’s inability to control the case to their advantage.

Another important tip for appearing in court: Do not allow your questioners to paint you into a corner by insisting on an answer. It is perfectly legitimate for you to reply that you do not know an answer, or that you have provided them with all the information you have. It is a relatively common tactic to try to get the answer they want by insisting that you tell them, “Yes” or “No,” or give some other response that leads to the conclusion they want. You can usually avoid this trap by being very careful to answer only with what you know for sure and being ready to say, “I don’t know.”

Take the time to review all of your data and to go over the possible issues with your own legal counsel beforehand. A mock deposition or trial rehearsal is a great idea if you have the time. It can help to bring up any areas where you might need more information or research. It can also be a way for you and your legal counsel to decide
what information is truly relevant and what might be privileged or unnecessary.

Finally, remember that there are specific rules and protocols for expert witnesses and evidence. We discussed those in more detail in Chapter 1, and your legal support will understand and apply those rules as appropriate.

Your responsibility is to be honest, prepared, and respectful. That will mean dressing appropriately, speaking clearly, and being polite and respectful to everyone present. The more prepared you are ahead of time, the less nervous you will be in your presentation.

Presenting to any audience, whether a group of managers, attorneys, a judge and jury, or any other group can be intimidating. However, if you are prepared, have practiced, and have taken the time to hone your presentation skills, you will come off as knowledgeable and reliable.

If it is your job to assist your side of a case, everything might depend on the impression you make. A confident, well-spoken, and clear speaker will be much more believable than someone who is reserved, nervous, and difficult to understand. Even if that nervous person is telling “the whole truth and nothing but the truth,” he or she is much less likely to be trusted by a jury or any other audience.

7.6 Conclusion

Well, you made it through to the end. I hope that whether you used this as a reference and skipped around, or worked your way through all seven chapters, you have found this useful in helping to better understand and manage electronically stored information.

The appendices that follow offer many resources for learning more or for further enhancing your understanding of this important subject.

By taking the time to read this book and to better understand these ideas, you have become a more unique and valuable person than you already were, whether just for your own knowledge or for the betterment of your organization. I encourage you to keep learning and to pass on this knowledge to ensure that more people are aware of the data fog we all live in today and all of the important means we have to manage and control that electronically stored information.
Appendix I: Links and References for More Information

The following resources can offer you a vast amount of information that you can use to further enhance your study and expertise about electronically stored information (ESI).

*Advice from a Risk Detective*, “How can we handle the commonest risks at home, at school, at work, online and on the road?,” written by Annie Searle and published by Tautegory Press—This is a very easy to understand book on risk. http://www.advicefromariskdetective.com/.

*Considering Third Generation eDiscovery? Two Approaches for Evaluating eDiscovery Offerings*—This is another, very inexpensive ($0.99) e-book available in a Kindle version from Amazon. http://www.amazon.com/Considering-Generation-eDiscovery-Approaches-ebook/dp/B002JCSUTK/ref=pd_sim_kinc_3?ie=UTF8&m=AG56TWVU5XWC2.

Discovery Resources—This is another great site with up-to-date information, resources, and news about electronic discovery. http://discoveryresources.org.

e-Discovery for Dummies—This provides a beginner resource for anyone looking to understand the rules and implications of e-discovery policy and procedures, available from Amazon.
EDRM, the Electronic Discovery Reference Model Project—This organization has done a lot of the work to better understand and document the procedures we discuss in this book. http://www.edrm.net/.

Electronic Discovery Law—This is an excellent resource published by the law firm K&L Gates for tracking and understanding the evolution of case law. http://www.ediscoverylaw.com/.


LexisNexis® Zimmerman's Research Guide—This resource on federal court rules covers all of the different rules and has references to other court rule sources. http://law.lexisnexis.com/infopro/zimmermans/disp.aspx?z=1458


*The Applied Discovery® Black Letter Book* (fourth edition of the Discovery Book)—This is a relatively inexpensive book that can be purchased in electronic format (Kindle) and “provides readers with an essential guide to the latest cases, rules of
APPENDIX I

269


The Legal and Economic Implications of Electronic Discovery: Options for Future Research—This is a relatively inexpensive e-book available for Kindle that provides an overview of the issues involved and outlines five avenues for future research on the legal and economic implications of e-discovery. http://www.amazon.com/Economic-Implications-Electronic-Discovery-ebook/dp/B001FB68AY/ref=pd_sim_kinc_6?ie=UTF8&cm=AG56TWVU5XWC2.

The Sedona Conference—This organization of attorneys and experts in evidential law has extensive references on interpretation of court rules. http://www.thesedonaconference.org/.

Truth to Power, Information Governance Research Community—This is a site with a comprehensive library of documents and guidelines on information security, governance, and auditing. Some are free and others require membership and payment before you can download them. But they are all excellent. http://www.t2pa.com/.

Windows Incident Response Blog—This excellent blog by Harlan Carvey holds a wealth of knowledge for anyone who needs to delve into the forensic analysis of Windows computers. http://windowsir.blogspot.com/.

Wikipedia is of course an excellent source of information on many different subjects and you will note that it was often referenced in my footnotes. Here are two specific Wikipedia articles that reference issues discussed in the book in much more detail:


The following are good resources for understanding how computers work and keeping up with the latest technologies.

Electronically Stored Information, Second Edition
https://www.crcpress.com/9781498739580
for IT Business Edge
Several different websites and books are great references to help you understand computer technology.

http://www.ehow.com/how-computers-work/
http://computer.howstuffworks.com/


For news and updates on computers and technology, I recommend the following websites:

http://news.cnet.com/
https://www.computerworld.com/
http://gcn.com/
https://www.zdnet.com/
http://www.computerweekly.com/
http://www.pcmag.com/
http://www.theregister.co.uk/
https://www.infoworld.com/
http://www.networkcomputing.com/
http://www.v3.co.uk/
https://www.sans.org/newsletters/

For good resources on presentation skills and tools and expert witness/deposition training, consider the following:

http://www.presentation-skills.biz/
http://www.effective-public-speaking.com/
http://www.presentation-skills.org/
http://prezi.com