



IDENTIFY

MATCH

Digital Archaeology

The Art and Science of Digital Forensics

SCAN

MICHAEL W. GRAVES

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Digital Archaeology

This page intentionally left blank

Digital Archaeology

THE ART AND SCIENCE OF
DIGITAL FORENSICS

Michael W. Graves

◆◆ Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States, please contact:

International Sales
international@pearsoned.com

Visit us on the Web: informit.com/aw

Library of Congress Cataloging-in-Publication Data
Graves, Michael W.

Digital archaeology : the art and science of digital forensics / Michael W. Graves, MSDIM.—First Edition.

pages cm

Includes bibliographical references and index.

ISBN 978-0-321-80390-0 (pbk. : alk. paper)

1. Computer crimes—Investigation. 2. Forensic sciences—Data processing. I.

Title.

HV8079.C65G7293 2013

363.250285—dc23

2013020221

Copyright © 2014 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to (201) 236-3290.

ISBN-13: 978-0-321-80390-0

ISBN-10: 0-321-80390-6

Text printed in the United States on recycled paper at Edwards Brothers Malloy in Ann Arbor, Michigan.

First printing, August 2013

Editor-in-Chief
Bernard Goodwin

Development Editor
Michael Thurston

Managing Editor
John Fuller

Project Editor
Elizabeth Ryan

Copy Editor
Teresa Wilson

Indexer
Infodex Indexing, Inc.

Proofreader
Carol Lallier

Editorial Assistant
Michelle Housley

Cover Designer
Chuti Prasertsith

Compositor
Graphic World, Inc.

I guess I'm just a regular guy after all. In spite of the fact that my daughter's assignment to draw a picture of one of her parents consisted of a silhouette of my head against a computer monitor—despite the fact that I learned that my son got a blue ribbon in marksmanship by seeing the award hanging on the wall—even though my wife had to remind me twice of anniversaries and dozens of times about birthdays—my family always stuck with me. This book is for them.

This page intentionally left blank

CONTENTS

Preface	xiii
About the Author	xxi
1 The Anatomy of a Digital Investigation	1
A Basic Model for Investigators	2
Understanding the Scope of the Investigation	8
Identifying the Stakeholders	12
The Art of Documentation	13
Chapter Review	21
Chapter Exercises	21
References	22
2 Laws Affecting Forensic Investigations	23
Constitutional Implications of Forensic Investigation	24
The Right to Privacy	29
The Expert Witness	31
Chapter Review	32
Chapter Exercises	32
References	33

3	Search Warrants and Subpoenas	35
	Distinguishing between Warrants and Subpoenas	36
	What Is a Search and When Is It Legal?	37
	Basic Elements of Obtaining a Warrant	40
	The Plain View Doctrine	43
	The Warrantless Search	44
	Subpoenas	50
	Chapter Review	51
	Chapter Exercises	52
	References	52
4	Legislated Privacy Concerns	55
	General Privacy	56
	Financial Legislation	59
	Privacy in Health Care and Education	62
	Privileged Information	64
	Chapter Review	67
	Chapter Exercises	68
	References	68
5	The Admissibility of Evidence	71
	What Makes Evidence Admissible?	71
	Keeping Evidence Authentic	76
	Defining the Scope of the Search	84
	When the Constitution Doesn't Apply	84
	Chapter Review	89
	Chapter Exercises	89
	References	89
6	First Response and the Digital Investigator	91
	Forensics and Computer Science	91
	Controlling the Scene of the Crime	96
	Handling Evidence	100
	Chapter Review	109
	Chapter Exercises	109
	References	110

7	Data Acquisition	111
	Order of Volatility	112
	Memory and Running Processes	112
	Acquiring Media	121
	Chapter Review	128
	Chapter Exercises	128
	References	129
8	Finding Lost Files	131
	File Recovery	131
	The Deleted File	141
	Data Carving	145
	Chapter Review	149
	Chapter Exercises	150
	References	150
9	Document Analysis	151
	File Identification	151
	Understanding Metadata	157
	Mining the Temporary Files	172
	Identifying Alternate Hiding Places of Data	176
	Chapter Review	183
	Chapter Exercises	183
	References	183
10	E-mail Forensics	185
	E-mail Technology	185
	Information Stores	191
	The Anatomy of an E-mail	196
	An Approach to E-mail Analysis	203
	Chapter Review	210
	Chapter Exercises	211
	References	211

11	Web Forensics	213
	Internet Addresses	213
	Web Browsers	215
	Web Servers	233
	Proxy Servers	238
	Chapter Review	244
	Chapter Exercises	244
	References	245
12	Searching the Network	247
	An Eagle's Eye View	247
	Initial Response	248
	Proactive Collection of Evidence	250
	Post-Incident Collection of Evidence	262
	Router and Switch Forensics	268
	Chapter Review	275
	Chapter Exercises	275
	References	276
13	Excavating a Cloud	277
	What Is Cloud Computing?	277
	Shaping the Cloud	279
	The Implications of Cloud Forensics	284
	On Virtualization	291
	Constitutional Issues	300
	Chapter Review	303
	Chapter Exercises	304
	References	304
14	Mobile Device Forensics	307
	Challenges of Mobile Device Forensics	307
	How Cell Phones Work	308
	Data Storage on Cell Phones	313
	Acquisition and Storage	317
	Legal Aspects of Mobile Device Forensics	322

Chapter Review	324
Chapter Exercises	325
References	325
15 Fighting Antiforensics	327
Artifact Destruction	328
Hiding Data on the System	336
Covert Data	347
Chapter Review	354
Chapter Exercises	355
References	355
16 Litigation and Electronic Discovery	357
What Is E-Discovery?	358
A Roadmap of E-Discovery	358
Conclusion	377
Chapter Review	377
Chapter Exercises	377
References	378
17 Case Management and Report Writing	379
Managing a Case	379
Writing Reports	389
Chapter Review	393
Chapter Exercises	394
References	394
18 Tools of the Digital Investigator	395
Software Tools	395
Working with “Court-Approved” Tools	410
Hardware Tools	413
Nontechnical Tools	418
Chapter Review	421
Chapter Exercises	422
References	422

19	Building a Forensic Workstation	423
	What Is a Forensic Workstation?	424
	Commercially Available Forensic Workstations	425
	Building a Forensic Workstation	
	From Scratch	429
	Chapter Review	440
	Chapter Exercises	440
	References	440
20	Licensing and Certification	441
	Digital Forensic Certification	441
	Vendor-Neutral Certification Programs	442
	Vendor-Specific Certification Programs	449
	Digital Forensic Licensing Requirements	452
	Chapter Review	454
	Chapter Exercises	454
	References	454
21	The Business of Digital Forensics	457
	Starting a New Forensics Organization	458
	Maintaining the Organization	466
	Generating Revenue	478
	Organizational Certification	481
	Chapter Review	483
	Chapter Exercises	483
	References	483
A	Chapter Review Answers	485
B	Sample Forms	505
	Glossary	511
	Index	521

PREFACE

In performing an investigation that explores the use of computers or digital data, one is basically embarking on an archaeological expedition. To extract useful artifacts (information, in our case), one must be exceedingly careful in how one approaches the site. The similarities between a digital investigation and an archaeological excavation are much closer than you might imagine. Data, like physical artifacts, gets dropped into the oddest places. The effects of time and environment are just as damaging, if not more so, to digital artifacts as they are physical mementos.

WHY THIS BOOK?

Archaeologists are fully aware that, due to the passage of time, there are things they can never recover. The skin that once covered a skeleton long buried in the desert can never be found and analyzed. Likewise, data that was once stored in active memory on a computer can't be recovered once the computer is switched off. However, in each example, it is possible to uncover evidence that both existed. When you first begin a digital investigation, you are undertaking a modern archaeological dig. Just like the shards of broken pots tell the anthropologist a lot about the culture that once used the vessel, the data you dig out of the computer can tell you volumes about the people who used the system.

This book takes the concepts of archaeology and applies them to computer science. It is a tutorial on how to investigate a computer system to find evidence of a crime or other misbehavior, and to make sure that evidence will stand up in

court. While there are numerous other books that cover the whys and wherefores of digital forensics, this one will go into some detail on how to accomplish the task.

We've all watched the TV programs where the good guys figure out everything the bad guys did just from examining a piece of hair. (Is this why the bad guys are always called "hairballs"?) In modern-day investigations, the role of the computer plays as big a part as the star witness in many cases. In fact, the computer often *is* the star witness. Many cases have been solved or settled on the basis of what trained professionals were able to discover while examining *electronic evidence* (e-evidence).

However, the courts take a dim view on just anybody digging around in somebody else's computers. They generally insist that legal process be followed, and that only a trained professional attempt the examination. The extraction and analysis of e-evidence is all part of what we call *computer forensics*. So what is forensics? The word itself originated from the Latin word *forum*, which described a place where people could assemble publicly and discuss matters of interest to the community. In that context, the word was derived from the strict rules of presentation applied to such discussions. In the context of this book, the word best means *application of science or technology to the collection of evidence for the purpose of establishing facts*. The vast majority of references specify that forensic science is targeted at criminal investigation. However, in the real world, digital investigations are commonly used in civil cases and within organizations to identify members engaged in illicit activities.

A crime scene investigator might have DNA from samples of hair found at the scene analyzed to prove that a specific individual was on the scene at least once. Chemical analysis of soil can identify a geographical origin. The process of computer forensics is a series of steps by which professionals can prove the following:

- Data exists.
- Data once existed.
- Data originated from a specific source.
- A particular individual either created or had access to the data in question.
- The data is relevant to the case.
- The data has not changed in any way from acquisition to analysis.

While it is not always necessary to prove all of the above statements are true, in order to secure a case it is best if as many as possible can be locked down. Even when all of the above are proven, a slick lawyer can always point out the fact that e-evidence is almost always circumstantial and press for reasons why the investigation team has presented insufficient corroborating evidence to demonstrate relevance or authenticity. (Both of these terms will be discussed in greater detail in the course of this book.) Even if you can prove beyond a shadow of a doubt that Tammy Sue created the letter

you found on Billy Bob's computer, can you prove that Billy Bob actually acquired the letter illegally? Probably not—which is why, as an expert witness, you don't even try. You simply collect the evidence and state the facts. The more incriminating evidence that you can find, the better the chances are that your side wins the battle.

WHO WILL BENEFIT FROM THIS BOOK?

This book is primarily targeted at the reader who is preparing for a career as a professional investigator. It will not server as a legal tome for the prosecutor but will provide the background needed to efficiently and accurately collect evidence that a prosecutor can use. It will also prove handy to the IT professional who is occasionally called upon to perform e-investigations.

In addition, while the book's primary goal is not to show people how to hide their tracks, understanding the processes discussed in this book can help an individual or organization prepare for a hostile demand for the delivery of electronic information (*e-discovery*). Properly identifying the bits on your computer can go a long way in preparing a defensible stance. If you know the garbage they are likely to find, you can be ready with an explanation. Foreknowledge also stops you from making the legally indefensible mistake of deliberately destroying evidence in advance of e-discovery. Such bad behavior doesn't just result in a slap on the wrist. It can result in fines ranging into the millions (or even billions) of dollars.

WHO WILL NOT BENEFIT FROM THIS BOOK?

Before attempting to fully understand this book, a wise reader will already have fulfilled a few prerequisites. He or she already knows a computer inside and out. Swapping out hard disks is second nature, and she finds it easier to work from the command prompt than a GUI. And he doesn't have to ask what a GUI is. Operating systems and file systems aren't a foreign language. Opening a registry editor doesn't induce spasms of panic, and most of all, exploring new areas of technology is a form of entertainment—not a nightmare.

There will be terms used in this book that I assume the reader already knows from previous experience or learning, because they are more relevant to general computer technology than to digital forensics. While it is not necessary to be a networking guru, it is certainly essential that you have a firm understanding of the concepts of networking, including principles of TCP/IP, network hardware, and communications.

HOW THIS BOOK IS ORGANIZED

The book starts out by introducing the reader to various things that must be clear before an investigation is ever initiated. The key differences between civil and criminal investigations are covered. What are the rules of the game? What laws affect us? Tools of the trade and minimum levels of training are a topic of discussion. What are the basic procedures of performing a computer forensic investigation?

From there on, the book describes tools and techniques that the average investigator will use on a day-in, day-out basis. The chapters are set up in approximately the order that the tasks will be accomplished in the real world. Finally, some of the humdrum aspects of the profession are discussed. Documentation, certification, and business aspects of digital forensics aren't that much fun. But they are necessary aspects of the profession.

UNDERSTANDING THE BOOK'S FORMAT

In order to present information in an orderly fashion, this book follows a scheme that will help the reader learn the material more quickly:

- **Bold:** A new term that will appear in the glossary
- *Italics:* A definition
- Monospace type: Code or commands to be typed into the computer
- Command Syntax:

```
copy {filename.doc} {PATH:\newfile.doc} is the syntax used in  
the text to represent the command copy novel.doc c:\temp\docs\  
novel.doc. Brackets will not be used at the command prompt.
```

- Sidebars: Anecdotes or examples that relate to the current text

THE NEED FOR PROFESSIONALS

Sadly enough, this is a litigious world we live in. If you run a business, chances get better every day that you will find the need to sue someone—or will be on the wrong end of the need. Some people want to retain a rosy outlook on life and go into computer forensics because they think it is a way to bring the bad guys to justice. I'm delighted to report that sometimes, they are actually right. Just don't forget that the other side always has their team of professionals ready to refute everything you say or write. That's why so many computer investigators are needed.

A sign of how strong the field is can be seen in the Great Recession of 2008. When nearly six million people in regular walks of life all lost their jobs, openings couldn't be filled for practitioners in the black arts of digital forensics. To top things off, scanning a listing of job offerings showed the lowest offering salary (that was stated) at \$46,000 per year. The vast majority of starting salaries listed ranged from the high fifties to the mid-sixties per year. And this was starting salary.

With recent laws such as Sarbanes-Oxley and the new Federal Rules of Civil Procedure, along with venerable old laws like HIPAA and Gramm-Leach-Bliley, putting more pressure on business, health, and nonprofit organizations, it is a certain bet that the number of investigators needed will only increase. The key to getting one of these jobs is training and certification. And compliance has become a huge issue for many organizations.

CERTIFICATION PROGRAMS FOR FORENSICS PROFESSIONALS

As of this writing, there are several certification programs dedicated specifically to forensic investigation of digital data sources. In order to impress a potential client with your qualifications, it is not only necessary to demonstrate your competence with digital forensic tools, but you must also show that you have a satisfactory knowledge of operating systems, networks, and computer hardware. The following list is by no means comprehensive, but offers a glimpse of what the industry offers. In addition to certification programs, a number of colleges have begun to offer computer forensics as a degree program, including a handful that offers master's degree programs in the subject.

GENERIC FORENSICS CERTIFICATIONS

- Certified Computer Examiner (CCE): International Society of Forensic Computer Examiners
- Certified Electronic Evidence Collection Specialist (CEECS): International Association of Computer Investigative Specialists (offered only to law enforcement officials)
- Certified Forensic Computer Examiner (CFCE): International Association of Computer Investigative Specialists
- Certified Information Systems Security Professional (CISSP): (ISC)²
- Global Information Assurance Certification (GIAC) Certified Forensic Analyst
- GIAC Certified Forensic Examiner

VENDOR-SPECIFIC FORENSICS CERTIFICATIONS

- AccessData Certified Examiner (ACE): Certification of proficiency with the AccessData Forensics Toolkit
- EnCase Certified Examiner: Guidance Software
- Paraben: Various certificates of completion

NONFORENSIC CERTIFICATIONS

- Microsoft Certified Systems Engineer (MCSE): Microsoft certification of professional excellence in managing Microsoft servers
- Cisco Certified Network Engineer (CCNE): Proof of mastery of Cisco router and switch management
- A+: Vendor-neutral certification of expertise in computer hardware installation and maintenance offered by the Computing Technology Industry Association (CompTIA)
- Network1: Vendor-neutral certification of expertise in network infrastructure and administration offered by CompTIA

A PERSONAL NOTE ON CERTIFICATION PROGRAMS

Many years ago, I earned my daily bread in a completely different field. I sold computer hardware and systems to businesses and schools. As it was, the company for which I worked was unwilling to hire telephone support staff to assist customers with hardware issues. Instead, they expected the sales staff to field support calls. I got very good at that task. So much so that my boss started dispatching me to perform actual repairs any time the service call was close enough to justify the travel.

I discovered that I liked repairing computers a whole lot more than I did selling them. So I started distributing my resume to a variety of potential employers—and didn't get a single response. On a whim, I self-studied for the A+ certification from CompTIA, took the exams, and passed with flying colors. As soon as I had those letters behind my name, I started circulating my resume again and got three invitations to interview on the first pass. Of those, I was offered a position that paid approximately 35% more than I earned in my best year as a sales rep. For me, that was a very powerful lesson on the value of certification. Getting a master of science in digital investigation management hasn't hurt either.

ACKNOWLEDGMENTS

A book of this nature is not the product of a single individual. I get my name on the cover because it was my idea and I did most of the writing—on the first go-around, anyway. However, there are some people who might go completely unnoticed for their patience, knowledge, skill, and understanding if I don't point them out.

First of all, I would like to thank Robert J. Sherman for his help in mobile phone technology. Okay, to be precise, he didn't just help . . . he wrote the whole chapter on mobile device forensics. He is an expert in this field, and my knowledge pales in comparison. So in the face of a lot of begging and pleading, along with promises of fame and fortune (sorry, bud . . . this is all the fame and fortune you're likely to get out of this deal), he caved and agreed to help me. In the end, he turned out an excellent chapter. So if, after reading that chapter, you wonder why it reads so much better than the rest of the book, now you know.

Next, I'd like to give credit to two amazing reviewers whose comments turned a marginal first draft into a profoundly better final manuscript. Jay Lightfoot and Ruth Watson both provided chapter-by-chapter comments on my first effort, suggesting numerous improvements in both structure and content. Without those reviews, I don't think this book would be as good as it is (however good that may be).

Naturally, I'm saving the best for last. My publisher actually made me *complete* the book! What's with that? Michelle Housley, Michael Thurston, and Bernard Goodwin at Addison-Wesley all refused to give up hope on either me or the project (although I'm sure there were times it was tempting) and got me through that inevitable mid-book crisis where I felt I couldn't possibly write another page without insanity setting in. This book is proof that I was wrong about the former, but I cannot with certainty attest to the latter.

Michael W. Graves
April, 2013

This page intentionally left blank

ABOUT THE AUTHOR

Michael W. Graves has worked as an IT professional for more than 15 years—as a network specialist, a security analyst, and most recently as a forensic analyst. He holds a master of science in digital investigation from Champlain College, where he spent several semesters as an adjunct professor of computer science. His publications include a number of certification manuals for several of the CompTIA certifications, as well as two novels. When not poking around in computers or writing books, he carts around an 8x10 view camera and makes black-and-white landscape photographs with a nod toward the F64 school of photography.

This page intentionally left blank

THE ANATOMY OF A DIGITAL INVESTIGATION

This chapter will deal with the structural aspects that are common to most, if not all, digital investigations. Most current texts on the subject refer to a common investigation model, although there is some disagreement on how many components make up the model. This book will use a six-part model, which will be covered in more detail later in this chapter.

It is essential to understand at the outset precisely what the scope of the investigation entails. The type of investigation dictates the level of authorization required. Generally, there are three types of investigation. **Internal investigations** are sponsored by an organization. They generally start out as a deep, dark secret that the company doesn't want getting out. Therefore, courts and state and federal agencies are rarely involved at the outset. The other two types—**civil** and **criminal**—both require involvement by the courts, but on different levels.

There will never be an investigation that does not have multiple stakeholders. In all court cases, there is the **plaintiff** and the **defendant**. In civil cases, these are the two litigants asking the courts to settle a dispute. In criminal cases, the defendant is the person accused of a crime and the plaintiff is the one making the accusation, which will always be some level of government authority. In addition to these obvious players, there are those on the sidelines whose interests must be considered. Lawyers will almost always be involved, and in cases that are likely to end up in court, be assured that the judge will take an active interest.

With people's finances, freedom, or even lives at stake, the necessity for accurate and thorough reporting cannot be emphasized enough. It is so critically

important that the subject of documentation will be discussed several times and in several places in this book. This chapter will start the reader off with the basics of good documentation.

Please be aware that this chapter deals only with the process of investigation. In Chapters 2 and 3, there will be detailed discussions of the various legal issues that the digital investigator must face on a daily basis. Consider the legal issues to be the glue that binds the model, but not the actual model. You can perform any number of investigations with no regard for the law. The results will be very revealing, but useless. Failure to be aware of legal aspects will cause the most perfectly executed investigation to fall apart the instant the case is picked up by the legal team.

A BASIC MODEL FOR INVESTIGATORS

Today's teaching methods require everything to be broken down into a simplified structure that you can put into a diagram. Computer investigations are no different. Even though there will probably never be any two cases that are identical, they should always be processed in accordance with a standard investigative model. Kruse and Heiser (2001) laid out the basic computer investigation model in their book entitled *Computer Forensics: Incident Response Essentials*. Their model was a four-part model with the following steps:

- Assess
- Acquire
- Analyze
- Report

As shown in Figure 1.1, the four steps are further broken down into more granular levels that represent processes that occur within each step. A more thorough study expands the model to six steps, as follows:

- Identification/assessment
- Collection/acquisition
- Preservation
- Examination
- Analysis
- Reporting

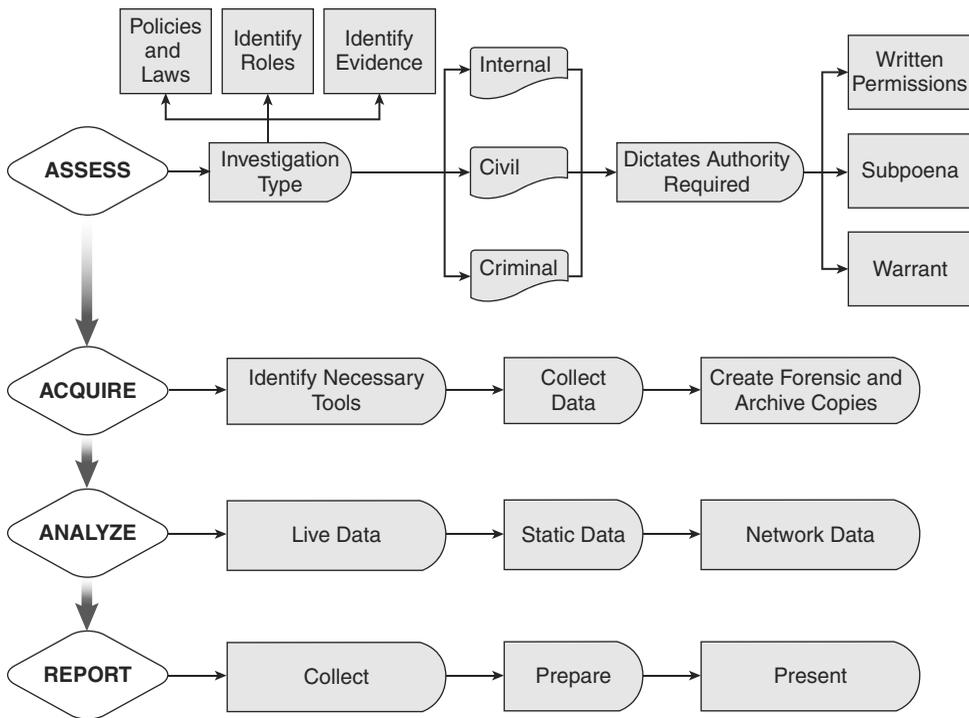


Figure 1.1 The steps of a digital investigation

The six-step model (Casey 2001) as seen in Figure 1.1 emphasizes the importance (and process) of preserving the data. It also distinguishes between the process of examination and analysis, whereas Kruse and Heiser considered them to be two parts of a single process. Experience has shown that acquisition and preservation are not the same, and while it might be an easy enough procedure to extract and examine data, accurate analysis is as much an art as it is a science.

From a management standpoint, each of these steps must be carefully monitored. Through a process of careful documentation of the history of each case, the various processes can be constantly reassessed for efficiency and reliability. When it becomes necessary, knowing what works and what doesn't allows the observant manager to tweak the steps in order to improve organizational effectiveness.

Figure 1.1 emphasizes just how detailed these seemingly simple steps can actually be. The assessment phase alone has a multitude of steps involving people, hardware, environment factors, political implications, and jurisdiction. Acquisition of evidence cannot begin until all potential sources of evidentiary material

are identified, collected, inventoried, and catalogued. All of this must be done according to strict legal guidelines, or any subsequent investigation will be a waste of time. Legal and internal regulations regarding privacy must be followed at all times, or any information collected will not be admissible as evidence should the case ever make its way to court. In the case of internal investigations, adherence to corporate guidelines will generally be sufficient.

IDENTIFICATION/ASSESSMENT

Before beginning any investigation, the general rules of engagement must be established in advance and from the very start be strictly followed. Those rules can be very different between criminal and civil cases. It is essential that the investigator know what regulations apply to a specific investigation in order to not damage or destroy a case by failure to abide, either flagrantly or inadvertently.

In a criminal investigation, it is almost always necessary to obtain a warrant before seizing systems, media, or storage devices. In order to obtain that warrant, the investigating entity must provide a judge sufficient evidence that a crime has been committed, is about to be committed, or is in the process of commission. The specific type of information sought by the investigation must be identified; general fishing expeditions are never approved by a reputable judge—at least not for the purpose of issuing warrants.

Civil cases have more lenient guidelines. Internal investigations sponsored by an organization can be even more lenient. Federal guidelines regarding invasion of privacy are not as strictly enforced on civilian investigators looking into civil infractions as they are on agents of a government—state, federal, or local—who are investigating criminal complaints. Internal investigations can be made even easier when employees or members have signed a statement outlining an organization's policies and guidelines.

No case should be accepted by an investigator directly. An executive-level decision, based on a set of predefined guidelines (to be discussed later), must be made on whether to accept or decline each individual case presented to the organization. While it falls upon a law enforcement agency to accept any case assigned that involves violation of state or federal statutes, a private organization can refuse to accept cases for a variety of reasons. The organization's leadership must identify the criteria for case acceptance and stick to those criteria. It does the company's reputation no good to be associated with a pedophile after publicly stating that its motives are to defend the community.

Make a list of all legal documentation that will be required. Warrants will be required in criminal cases. Court orders or subpoenas will be needed in civil

matters. Signed agreements outlining the scope of the investigation should be required in all internal investigations.

Once the ground rules are established, it is time to identify potential sources of evidence. The obvious place to look is on the local system, including hard disk drives, removable media that might be lying about, printers, digital cameras, and so forth. Less obvious sources of information might be PDAs, external hard disks or optical drives, and even system RAM if the data processing systems are still running when the incident is reported. Knowing in advance what must be acquired can prevent the investigator from making critical errors during the process of acquisition.

COLLECTION/ACQUISITION

This is the most technical part of the investigation and can also be the most critical time for making errors. If the case under scrutiny should ever come to trial, the investigator presenting the case must be able to prove the following:

- The data is authentic.
- The copy of the data used for analysis is reliable.
- The data was not modified during acquisition or analysis (chain of custody).
- The tools used to analyze the data are valid tools.
- Sufficient evidence, both **incriminating** and **exculpatory**, has been acquired and analyzed to support the proffered conclusion.
- The conclusions drawn are consistent with the data collected and analyzed.
- People involved in the collection and analysis of the data are properly trained and qualified to do their job.

This doesn't sound easy, and it isn't. Details on how to assure that all of these requirements are met are covered in greater detail in later chapters. For now, suffice it to say that it is essential that they be fulfilled.

PRESERVATION

A cardinal rule of digital investigation is that the original data must *never* be touched. For many years, the standard rule has been that a forensically sound copy of the original be made and that the examination and analysis of data be performed on the forensic copy. In terms of nonvolatile media, such as hard disks, removable media, and optical disks, this is still the rule. Devices should always be

mounted as read-only in order to assure that no data is modified or overwritten during the process of mounting the device. Hard disk duplicators are designed specifically for this purpose, and in Windows systems, a simple modification of the registry allows USB devices to mount read-only.

Legal issues might arise if there is any possibility that media used to store images may have been contaminated. Be aware of that possibility and either have new media available for collection or be certain that previously used media has been forensically wiped.

In many cases, it becomes essential that copies of data be acquired through a process of live acquisition. This is the case when it becomes necessary to capture the contents of memory from a running system, to acquire log files from network devices that cannot be brought down, or to archive information from network servers or storage appliances that defy the making of a forensic copy. If it is not possible, for any reason, to create a forensically sound copy, it is essential that the investigator document the reasons such a copy could not be made and record as accurately as possible the state of the evidentiary source before and after acquisition.

Storage of preserved information becomes part of the chain of custody process, and care must be taken that all data and devices collected during this phase are properly documented and tracked. Be able to verify that there was never a possibility for evidence to become tainted through outside tampering, corruption, or improper procedure.

EXAMINATION

The process of examining data increases in scope and complexity every year. Whereas 1.44MB floppy disks were once the repository for stolen and illicit data, investigators these days are presented with flash drives the size of key fobs that hold 64 or more gigabytes of data and hard disks that store in excess of a terabyte. To make matters worse, the data is not likely to sit on a porch swing in plain view for anyone to see. Investigators will find it necessary to look for evidence in **unallocated space** left behind by deleted files. Hidden partitions, **slack space**, and even registry entries are capable of hiding large quantities of data. Steganography can hide documents inside of an image or music file. So essentially, the investigator is given an archive the size of the Chicago Public Library and asked to find a handwritten note on the back of a napkin tucked somewhere inside of a book.

Data carving tools and methods of looking for evidentiary material have evolved, and depending on the nature of the case, the investigator's tool kit will require having several utilities. For criminal cases requiring forensically sound

presentation, it is critical that the tools used to examine data be those considered valid by the courts. There are a few commercially available software suites approved for evidentiary use. Among these are Encase by Guidance Software and the Forensics Tool Kit (FTK) from Access Data Corporation. A suite of tools running on Linux that is not “officially” sanctioned but is generally considered acceptable by most courts is The Sleuth Kit, designed by Brian Carrier.

Keeping up with technical innovations in the industry is most critical in this area. As new technology emerges, new tools will be needed to examine the accumulated data it creates. The organization that follows the cutting edge of technology will always be two steps behind those that help develop it. The balancing act comes when management must defend the use of a new tool to which the courts and lawyers have not yet been exposed. Be prepared to defend the tool along with the conclusions it helped you formulate.

ANALYSIS

Here is where the process of digital forensic investigation leaves the realm of technology and enters that of black magic. It is up to the investigator to determine what constitutes evidence and what constitutes digital clutter. A variety of tools exist that assist the investigator in separating OS files from user data files. Others assist in identifying and locating specific types of files.

Technique is as critical as the selection of tools. For example, when searching an e-mail archive for messages related to a specific case, string searches can bring up all those that contain specific keywords. Other utilities can detect steganography or alternate data streams in NTFS file systems. Collecting the data necessary to prove a case becomes as much art as it is science. One thing that the investigator must always keep in mind is that exculpatory evidence must be considered as strongly as incriminating evidence.

REPORTING

Documentation of the project begins the minute an investigator is approached with a potential case. Every step of the process must be thoroughly documented to include what people are involved (who reported what, who might be potential suspects, potential witnesses, or possible sources of help), as well as thorough documentation of the scene, including photographs of the environment and anything that might be showing on computer monitors. Each step taken by the investigator needs to be recorded, defining what was done, why it was done, how it was done, and what results were obtained. **Hash** files of data sources must be generated before

and after acquisition. Any differences must be documented and explained. Conclusions drawn by the investigating team must be fully explained. On the witness stand, it is likely that an investigator will be required to prove his or her qualifications to act as an investigator. A meticulously investigated case can be destroyed by inadequate documentation. While commercial forensic suites automate much of the documentation process, there is still much manual attention required of the investigator.

UNDERSTANDING THE SCOPE OF THE INVESTIGATION

As mentioned, there are three basic types of investigation. With each type, the rules get tighter and the consequences of failure to comply get progressively stricter. A good rule of thumb is to pretend that the strictest rules apply to all investigations. However, as you might imagine, there are some role-specific requirements that don't apply to all of them.

INTERNAL INVESTIGATIONS

Internal investigation is the least restrictive of the inquiries you might make. From a standpoint of professional courtesy, internal investigations are more likely to be the least hostile type you'll ever do. You work directly with management, and the target of your inquiries probably won't even be aware of your activities until you are finished. You don't have courts and lawyers combing every word you say or write, hoping to find the smallest mistake.

That is not to say that there aren't laws that apply to internal probes. There most certainly are. State and federal laws regarding privacy apply to even the smallest organization. Also, different states have different laws regarding how companies deal with employment matters, implied privacy issues, and implied contracts. This isn't intended to be a law book, so for the purposes of brevity and clarity, understand this. It is important to review any relevant regulations before you make your first move.

Most corporations have formal guidelines for such matters. In addition to a written employee handbook, it is very likely that a company has documented guidelines regarding issues leading to termination, use of company infrastructure (including computers, e-mail systems, and network services), and so forth. In every step of your process, make sure that you adhere to the law and to corporate policy. If there appears to be a conflict between the two, get legal advice. At the very least, make sure you have written authorization to perform every step you take. Management needs to be aware of your process and every step involved in

the course of investigation, and they must sign off, giving approval. Document everything you do, how you did it, and what results you obtained. In digging into the source and impact of any internal security breach, your foremost concern is the protection of your client. However, should your probe uncover deeper issues, such as illegal activity or a national security breach, then it becomes necessary to call in outside authorities.

CIVIL INVESTIGATIONS

Civil cases are likely to be brought to the organization in situations where intellectual property rights are at risk, when a company's network security has been breached, or when a company suspects that an employee or an outsider is making unauthorized use of the network. Marcella and Menendez (2008) identify the following possible attacks:

- Intrusions
- Denial-of-service attacks
- Malicious code
- Malicious communication
- Misuse of resources

An investigator involved in a civil dispute should be cognizant of the Federal Rules of Civil Procedure. Although a legal degree is hardly necessary, a strong background in civil law is invaluable. Additionally, experience in business management is useful, in that a good understanding of standard corporate policy is necessary. Good communications skills are required. Management needs to be able to feel equally comfortable dealing with a CEO or a secretary.

When working with large repositories of data connected to many different users and devices, it becomes more difficult to assess who actually committed an infraction. Proving that a specific user was accessing the network at a specific time (and possibly from a particular machine) can be critical to winning a case. Anson and Bunting (2007) point out the difficulties of generating an accurate **timeline** and recommend some good tools for simplifying the matter. A good manager will keep abreast of changing technology and make sure that the organization is equipped with the proper tools.

Tools required for examining large networks or performing live data capture are substantially more expensive than those used to search individual data sources. Generally, it is not possible to bring down a corporate network while the investigative team captures images of thousands of drives. Costs in time and materials

would be prohibitive, as would be the negative impact of downtime on the company. Specialized software is needed to capture, preserve, and document the data. Additional tools are needed for data reduction. Filtering out the general network chatter and unrelated business documents can be a time-consuming process.

Keeping up with newer technology is essential, as is constant refresher training. The organization must continually assess its current capabilities and apply them to what imminent future needs are likely to be. As technology advances, investigative tools and techniques need to advance as well. Cases are won and lost on the ability of investigators to extract evidence. If a forensics team finds itself faced with a technology it doesn't understand, there will be no time for on-the-job training.

CRIMINAL PROCEDURE MANAGEMENT

Defining precisely what constitutes computer crime is very difficult to do. Fortunately, it is not up to the investigator to determine what is and what is not criminal activity. However, some definitions have been presented by various experts. Reyes (2007) states that a computer crime will exhibit one or more of the following characteristics:

- The computer is the object, or the data in the computer are the objects, of the act.
- The computer creates a unique environment or unique form of assets.
- The computer is the instrument or the tool of the act.
- The computer represents a symbol used for intimidation or deception.

Generally speaking, computer crimes are little different from conventional crimes. Somebody stole something, somebody hurt somebody else, somebody committed fraud, or somebody possessed or distributed something that is illegal to own (contraband). While not an exhaustive list of possible computer crimes, the following is a list of the most commonly investigated:

- Auction or online retail fraud
- Child pornography
- Child endangerment
- Counterfeiting
- Cyberstalking
- Forgery

- Gambling
- Identity theft
- Piracy (software, literature, and music)
- Prostitution
- Securities fraud
- Theft of services

Prosecution of criminal cases requires a somewhat different approach than do civil cases. Legal restrictions are stricter, and the investigator is more likely to be impacted by constitutional limitations regarding search and seizure or privacy. Failure to abide by all applicable regulations will almost certainly result in having all collected evidence suppressed because of technicalities. Many civil investigations are not impacted as severely by constitutional law because there is no representative of the government involved in the investigation. To assure that the investigation succeeds, management of a criminal division needs to have someone with a strong legal background. Courts will use the **Federal Rules of Evidence** to decide whether or not to allow evidence to be admitted in an individual case.

For the same reasons, reporting procedures and chain of custody must be rigorously followed by each person involved in an investigation, whether they are involved directly or peripherally. Even a minor departure from best practice is likely to be challenged by opposing counsel. Because of this, selection of personnel becomes a greater challenge. A technical whiz with little or no documentation ability is likely to fail in criminal investigation. Anyone who demonstrates a disregard for authority is a poor candidate for investigating criminal cases.

Tools used in criminal cases are subject to a tighter scrutiny than those used in civil cases. When a person's life or liberty hangs in the balance, judges and juries are less sympathetic to a technician who cannot verify that the tools used to extract the evidence being presented are reliable. Software and hardware tools used by the organization must be recognized by the court for use, and the techniques used by investigators must be diligently documented to show there was no deviation from accepted standard procedures.

Funding is likely to be more limited in criminal work than in civil investigations. Money will be coming from budget-strapped government entities or from law offices watching every dime. In some cases, courts will apply the *Zubulake* test to determine if costs should be shifted from one party to the other. This test is based on findings from the case *Zubulake v. UBS Warburg* (217 F.R.D. at 320, 2003) where the judge issued a list of seven factors to be considered in ordering

discovery (and in reassigning costs). These factors are to be considered in order of importance, the most important being listed first:

1. The extent to which the request is specifically tailored to discover relevant information
2. The availability of such information from other sources
3. The total cost of production compared to the amount in controversy
4. The total cost of production compared to the resources available to each party
5. The relative ability of each party to control costs and its incentive to do so
6. The importance of the issues at stake in the **litigation**
7. The relative benefits to the parties of obtaining the information

IDENTIFYING THE STAKEHOLDERS

In any investigation, there are going to be a large number of people with a vested interest in the outcome. These people are the **stakeholders**. Stakeholders vary in each investigation, depending in part on the scope of the investigation and in part on the raw size of the organization and the data set involved. Sometimes it is easy for the investigator to become overwhelmed by the sheer number of people involved. In all cases, it is safe to assume that there are two primary stakeholders with a greater investment than any other. Those are the accused and the accuser.

The accuser is the easiest to identify. This is the person or the organization that initiated the inquiry to begin with. As simple as that may seem, all too often the actual accuser gets left in the wake of bureaucracy and procedure. This is particularly true in cases that are destined to be presented before a court. Lawyers suddenly take the place of the stakeholders, and the assumption becomes that suddenly they *are* the primary stakeholders. A good investigator never lets this happen. Communications may be with these attorneys as representatives of the stakeholders, but the primary stakeholders remain the accused and the accuser.

Depending on the magnitude and the scope of the case, there might be a wide variety of secondary stakeholders—or none at all. To be a stakeholder of any kind, an individual or organization must have something to gain or lose from the outcome of the investigation. In spite of possible arguments to the contrary, this does not include the news media. Key stakeholders include

- Decision makers: Those who have the authority to initiate or to cancel an investigation or to reassign personnel.

- Mediators: Judges or third-party arbitrators who are responsible for deciding the outcome of the case or issue decisions pertaining to procedure.
- Customers: People or organizations downstream from the accused or accuser who will be directly impacted by the decision. For example, in *i4i Limited Partnership v. Microsoft Corporation*, virtually every reseller of Microsoft Word was impacted (*i4i v. Microsoft Corporation*, 6:07VC113, 2009).
- Process owners: People or organizations whose actions may have contributed to the case or whose operations were or will be impacted by the case.

Extraordinary circumstances can lead to unexpected stakeholders. The Exxon-Valdez incident in 1989 started out as the accidental grounding of an oil tanker that resulted in Exxon's launch of an investigation into the actions of the ship's captain. Before it was over, there were more than 38,000 litigants, including individuals, agencies, and environmental organizations, and three different sets of judges involved in a variety of decisions (Lebedoff 1997). That's a lot of stakeholders.

THE ART OF DOCUMENTATION

Any individual who lacks organizational skills or who finds it difficult to keep accurate notes as he works is not a likely candidate for the position of digital investigator. The vast majority of work the investigator does is documentation. There are five levels of documentation that must be either maintained or created during the course of each case study:

- General case documentation
- Procedural documentation
- Process documentation
- Case timeline
- Evidence chain of custody

Every one of these is important to winning a case should it make its way to court. Faulty, incomplete, or missing documentation can destroy an otherwise meticulously prepared case. In addition to these items, there is also the final report, but that will be covered elsewhere in this book.

THE CRAFT OF PROJECT MANAGEMENT

While this book is not intended to be a treatise on what makes a good project manager, it should be pointed out that good project management practices can

facilitate the smooth completion of an investigation from beginning to end. Virtually all of the principles defined in the Project Management Institute's (PMI) *Project Management Book of Knowledge* (PMBOK) apply directly to the investigatory process. Wysocki (2009) defines a project as "a sequence of unique, complex, and connected activities that have one goal or purpose and that must be completed by a specific time, within budget, and according to specification."

Like all other projects, a digital forensics investigation involves multiple stakeholders and a defined scope, and has specific objectives that must be pursued. Multiple people will be involved, requiring the project leader to manage people's time, to assure that tasks are assigned to the person most skillful in performing the work involved, and to keep everything in budget and on time.

GENERAL CASE DOCUMENTATION

Case documentation begins the moment you are asked to consider investigating an incident. Even if an investigator or agency chooses not to accept a case (assuming that possibility exists), it may later become necessary to explain why the case was turned away. Another thing the investigator needs to keep in mind is that anything recorded during the case is **discoverable**. To be discoverable means that opposing counsel has the right to examine and analyze data collected during the process. If an investigator takes written notes or uses a digital voice recorder to make verbal observations, copies of the notes and audio files must be made available to the opposition if requested. Therefore, great care should be taken in the creation of documentation.

A number of factors need to be addressed in the basic case documentation:

- What is the name and contact information for the organization involved in the incident? Record every individual contacted during the investigation, that person's role in the process, and when, where, and how he or she was contacted.
- When was the investigative agency notified, and who initially took the information? Record exact dates and times.
- A description of the incident, both in technical terms and in lay terms.
- When was the incident discovered?
- When did the incident occur? This may be a best-guess scenario.
- Who discovered the incident?
- To whom was the incident reported? This means anyone who learned of it, regardless of rank and file.
- What systems, information, or resources were impacted by the event? This includes hardware, organizational entities, and people.

- Is there any preliminary information that suggests how the offending actions were accomplished?
- What is the impact of the incident on the individual or organization affected? This includes financial impact, impact on the systems involved, and any effect it may have had on the health or mental welfare of individuals involved.
- What actions were taken between discovery of the incident and reporting it to authorities? This means everything that was done, including simple files searches.
- Who are the stakeholders as they are identified?
- As soon as possible, provide a detailed inventory of all hardware (and possibly software) that is involved in the incident. If hardware is seized, provide a separate, itemized list of seized equipment.
- Have all copies of all pertinent documentation, such as warrants, summons, written correspondence, and so forth, been added to the case file?

Any other generic information that does not fit directly into one of the other reporting categories would be included in this section. This would include expense reports, timesheets, and any other general recordkeeping.

PROCEDURAL DOCUMENTATION

During the course of the investigation, a number of tasks will be performed. The history of these tasks should be maintained as painstakingly as possible. The investigator should describe every step taken, the tools used to perform specific tasks, a description of the procedure, and a brief summary of the results. Detailed results can be included in the final report. When describing a technical process, process documentation should be provided whenever possible (as described in the next section).

Anytime the investigator chooses not to follow recommended best practice, it is essential to record the action being taken, what the recommended procedure would normally be, and what actual procedure is being used, and to explain precisely why the deviation is occurring. For the longest time, the best practice when coming upon a running suspect system was to pull the plug. The reasoning was that an orderly shutdown of the system overwrote a lot of data and drastically altered paging files. However, in a live network event that is still transpiring, it may be necessary to collect information from active memory, including current network connections, user connections, and possibly cached passwords. Shutting down the system would kill all that information. The proper course would then be to perform a live analysis and document precisely why the action was taken.

The following is a summary of events and tasks that should be meticulously reported. Some organizations performing investigations on a full-time basis have a template that the investigator follows, filling in the results as tasks are completed.

- Document the condition of the original scene, including a list of hardware found, status (on/off, logged on/logged off, etc.), along with photographs or a video tape.
- Record the names and contact information of all individuals interviewed during the investigations. A summary (or if possible, a transcript) of the interview should be provided as an attachment.
- If equipment is seized, document the make, model, and serial numbers of each device. Provide documentation authorizing the seizure as a separate attachment.
- Record the exact time materials were seized, the location it was taken from, and the name and contact information of the person performing the action.
- If equipment is transported, provide a detailed description of how the devices were packaged if antistatic or Faraday protection was provided. If not, why not?
- Describe the location where seized materials were taken, including the location and type of storage facilities used to house the materials. Record the name and contact information of the person transporting each item.
- Whenever live data acquisition is deemed necessary, record the following:
 - What type of data was acquired (memory dump, system files, paging files, etc.)?
 - What tools and procedures were used to connect to the suspect machine?
 - What tools and procedures were used to acquire the data?
 - What was the time and date the data was imaged, and what was the time and date reported by the device from which the data was acquired? The two are not always the same.
 - What are the type, make, model, and serial number of the target device to which the data was copied?
 - What is the condition of the target device (new, forensically cleaned, data-wiped, or formatted)?
 - What are the MD5 and SHA-2 hash calculations of the image?

- When devices are imaged for later analysis, record the following:
 - The type, make, model, and serial numbers of source devices
 - The type, make, model, and serial numbers of target devices
 - Precautions taken to avoid contamination or loss of data in evidence
 - For disk drives:
 - Drive parameters of disk drives, both target and source
 - Jumper settings
 - Master/slave configuration if IDE
 - Device ID if SCSI or SATA
 - For optical or flash drives:
 - Make, model, and capacity
 - Mounted or not mounted at time of seizure
 - Inventory of blank or used media
 - For seized media:
 - Form of disks (CD, DVD, Zip, etc.)
 - Capacity of disks
 - Number and type of seized disks
 - Possible evidence that there are missing disks (empty jewel boxes, etc.)
 - The date and time of each action taken.
 - The process used for mounting the seized device, including mechanisms in place to assure write-protection
 - The process and tools used to acquire the forensic image
 - MD5 and SHA-2 hash calculations of the image before and after acquisition
- Photograph computer systems before and after disassembling for transport.
- During the examination and analysis of data, record each procedure in detail, identifying any tool used. Record beginning and ending hash calculations of source data, explaining any discrepancies that may occur.
- Above all: Maintain an unbroken chain of custody that includes each piece of evidence handled throughout the course of the investigation.

As is readily apparent, case documentation is not to be taken lightly. While individuals should be treated as innocent until proven guilty, sources of evidence by default get the opposite treatment. The astute investigator always assumes that

any case he or she is working will eventually end up in court. Even the seemingly benign cases, such as uncovering evidence of employee misconduct, can end up in court as a civil (or even criminal) court case. Poor documentation can endanger what would otherwise be a sound case.

PROCESS DOCUMENTATION

Unless an investigator or an organization utilizes homegrown tools, most process documentation is likely to come from the vendors providing the hardware or software used. There are some pieces of documentation that must be generated by the agency. Process documentation includes

- User manuals
- Installation manuals
- Readme files stored on installation media
- Updates to manuals posted online by the vendor
- Logs showing updates, upgrades, or patch installations

This is the type of documentation that does not necessarily need to be provided with each investigation report. It must, however, be available if demanded by opposing counsel, a judge, or arbitrator. There are situations that occur where process documentation is used to support or refute claims that proper procedure was followed during specific steps in the investigation.

BUILDING THE TIMELINE

Key to virtually every investigation involving computer or network activity is the creation of an accurate history of events related to the incident under investigation. By creating an easily comprehensible report of the order of events that occurred, the investigator can more easily and more accurately show correlation between those events. For example, it is easier to associate a specific user to the origination of a particular file if the timeline shows that the file was created at a time when it can be shown unequivocally that the user was logged onto the computer or network.

The timeline (Figure 1.2) needs to start from a time just before the incident was known to begin or was initially discovered to the point when the evidentiary materials were acquired for analysis. This is why it is essential that the investigator do nothing that could alter the **metadata** of files stored on the computer. Metadata is information about files that can be either stored within the file itself

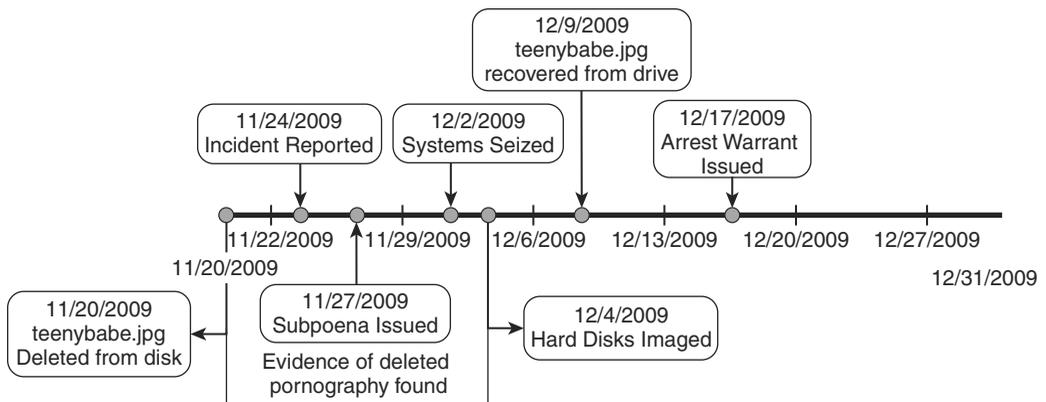


Figure 1.2 A good timeline is essential in communicating the order of events to outside parties of interest.

or extracted from other repositories, such as the Windows master file tables or registry. Three critical pieces of information are the *creation* date, *last accessed* date, and *last modified* date. Together these form the file's **MAC** (modified, accessed, and created) data. Simply viewing a file in a browser or application alters the accessed data. Copying a file from one location to another can modify both the creation and modified dates if forensically acceptable methods are not used. Metadata and ways of protecting and analyzing it will be covered in greater detail in Chapters 9 and 10.

Network and user logon activity are also critical to creating a timeline, as are Internet and e-mail usage. There are various tools that help the investigator validate times that certain events occurred. MACtime is a common forensic tool that can extract a history of user activity on a system. It creates an ASCII timeline of file activity. X-Ways Trace can be used to extract and analyze Internet history. In a network environment, event tracking in utilities such as Microsoft's Event Viewer, the registry, or log files can reveal valuable information that can be used for assembling a credible timeline.

Timelines can be assembled in graphical form that makes it easy for laypeople such as lawyers and judges to understand. Some of the forensic suites (notably Encase) produce automated timelines. Others, such as the Forensic Tool Kit, do not. It is possible, but not necessarily pleasant, to create a timeline using commercial products such as Microsoft Visio, Excel, or OpenOffice. Excel is very cumbersome for this task and is not recommended. Microsoft Visio produces more polished timelines but is limited by the fact that each event must be entered into the timeline separately. A better use of the investigator's time is to invest

in a proprietary product such as Timeline Maker for Windows or Bee Docs for Macintosh computers.

CHAIN OF CUSTODY REPORTS

For every physical unit of evidence taken into possession by an investigator or agency, there must be a continuously maintained chain of custody report. Consider it the equivalent of a timeline for evidence. The chain of custody report must be able to verify several critical pieces of information:

- Identify the item precisely, listing type of evidence, make, model, and serial number (if relevant), and make a photograph of the item (if possible).
- Specify when was the item taken into possession.
- Identify where or from whom the item was seized.
- Record who acquired the item along with the time and date acquired.
- Document who transported the item and how was it transported.
- Document how was the item stored during transport.
- Regularly record how the item was stored during possession.
- Provide a continual log, showing the time and date of each time it was checked out for examination, the purpose for checking it out, and the time and date it was checked back in for storage, identifying who had possession of the item during that time.

While an item is in possession of an individual investigator, that person should document what steps were taken to preserve the integrity of the evidence while in possession. Such documentation needs to include a precise identification of the device in possession (as defined above) and what controls were in place to protect the device from electrostatic discharge, electromagnetic interference, and other potential sources of data corruption and other protections. Document what methods were used to prevent data from being inadvertently written to the device (write-blocker devices, software write-protection, etc.). Generate before and after hash values to confirm that the data source did not change while in possession. If it did change, document what process caused the change, along with how and why the change occurred.

Any deviation from standard documentation procedures in preparing the chain of custody can, and most likely *will*, lead to challenges from opposing counsel and can possibly cause the evidence to be thrown out. No breaks can exist in the timeline, because this indicates an opportunity for the data to be replaced, corrupted, or modified.

CASE LAW: CHAIN OF CUSTODY

It is inevitably a good idea to present a flawless chain of custody in order to avoid having evidence declared inadmissible. The courts have vacillated in how they treat evidence in regards to “missing links” in the chain. In *Jeter v. Commonwealth*, Justice Roberts of the Twelfth Virginia Appellate Court wrote, “When a ‘vital link’ in the possession and treatment of the evidence is left to conjecture, the chain of custody is incomplete, and the evidence is inadmissible” (*Jeter v. Commonwealth* 2005).

Conversely, in *Hargrove v. Commonwealth*, the defendant argued that since the chain of custody did not include any signed statements or testimony from the officer who delivered the evidence to the laboratory, nor was there any evidence that an authorized agent accepted delivery of the evidence at the lab, the integrity of the evidence was in doubt. In denying this appeal, Justice Felton wrote, “It concluded that because the evidence container was received at the lab ‘sealed and intact,’ there was no evidence that it was subject to tampering between the time it left the police evidence room and the time that it was removed from the lab storage locker. We conclude that the trial court did not err in admitting the evidence container and the certificate of its analysis” (*Hargrove v. Commonwealth* 2009).

CHAPTER REVIEW

1. In what ways does Casey’s six-step model differ from the earlier four-step models of digital investigation? What is new, and what has changed?
2. Where in the Casey model would one begin to ascertain precisely what legal documentation would be required for a particular investigation?
3. Is *Zubulake v. UBS Warburg* more relevant to a criminal case or a civil matter? Explain your answer.
4. Discuss the difference between procedural documentation and process documentation. In which document would you explain what steps you took during the examination of a file system?
5. During the process of examination, you have reason to suspect that files that were deleted may still exist. What is the process for locating intact files in unallocated disk space?

CHAPTER EXERCISES

1. Look up at least one criminal case that involved data carving. Was the technique useful for the prosecution or for the defense?

2. Think of as many ways as possible in which a civil case involving electronic discovery of specific e-mails would differ from a criminal cases in which a search of a suspect's e-mail archives must be conducted. Don't try to get too specific here, as this is simply an overview chapter.
3. Throughout the investigation, a myriad of actions are performed. At what point does the chain of custody begin, and how is it relevant at each subsequent stage?

REFERENCES

- Anson, S., and S. Bunting. 2007. *Mastering Windows network forensics and investigation*. Boca Raton: Sybex.
- Casey, E. 2004. *Digital evidence and computer crime*. New York: Elsevier Academic Press.
- Hargrove v. Commonwealth*. 2009. Record No. 2410-07-2. Court of Appeals of Virginia Published Opinions. www.courts.state.va.us/wpcap.htm (accessed April 8, 2010).
- Hargrove v. Commonwealth*, 44 Va. App. 733, 607 S.E.2d 734 (2009). www.lexisone.com/lx1/caselaw/freecaselaw?action=OCLGetCaseDetail&format=FULL&sourceID=bdjcca&searchTerm=eGjb.diCa.aadj.eeWH&searchFlag=y&lloc=FCLOW (accessed April 8, 2010).
- Jeter v. Commonwealth*, 44 Va. App. 733, 737, 607 S.E.2d 734 (2005).
- Kruse, W., and J. Heiser. 2001. *Computer forensics: Incident response essentials*. Boston: Addison-Wesley.
- Lebedoff, D. 1997. *Cleaning up: The Exxon Valdez case—The story behind the biggest legal bonanza of our time*. New York: Free Press.
- Marcella, A., Jr., and D. Menendez. 2008. *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes, 2nd ed.* Florida: Auerbach Publications.
- Reyes, A. 2007. *Cyber crime investigations*. Rockland: Syngress Publishing
- Wysocki, R. 2009. *Effective project management: Traditional, agile, extreme*. 5th ed. Indianapolis: John Wiley & Sons.
- Zubulake v. UBS Warburg*, 217 F.R.D. at 320 (2003).

INDEX

- * (asterisk), in string searches, 180
- @ (at sign)
 - in e-mail addresses, 187
 - in passwords, 349
- “ ” (double quotes), Boolean operator, 205
- \$ metadata file, 136
- (minus sign), Boolean operator, 205
- + (plus sign), Boolean operator, 205
- 8.3 file names, 134
- 32-bit vs. 64-bit forensics workstations, 432, 438

- A**
- The A+ Guide to PC Hardware Maintenance and Repair*, 423
- Abbot Papyrus, 379
- Absolute direct addressing, 125
- Abstraction layers
 - lossless, 399
 - lossy, 399
 - overview, 396–398
- Access attribute, 160
- Access Data Corporation
 - certification program, 450–451
 - EDiscovery, 408
 - FTK Imager, 118, 121
 - SilentRunner, 408
- Access Data Corporation, FTK (Forensic Tool Kit)
 - case management, 383–384
 - creating timelines, 19
 - e-discovery, 370
 - EWF support, 124
 - live capture of registry entries, 331
- Access log, 243
- AccessData Certified Examiner (ACE), 451
- AccessData Mobile Examiner (AME), 451
- Accessible data
 - definition, 511
 - e-discovery, 366–367
 - forensics workstations, 425
- Accused. *See* Defendant.
- Accuser. *See* Plaintiff.
- ACE (AccessData Certified Examiner), 451
- Acquisition. *See also* Cell phones, acquisition; Data acquisition.

- Acquisition (*cont'd*)
 - and preparation for final report, 391–392
 - window for evidence collection, 255
- Active measures, detecting, 227–230
- Active online data, 366–367
- Active@KillDisk (AKD), 108
- Actual authority, 47, 511
- Addonics, 437
- Address book folder, 191
- Addressable memory *vs.* system, 114–115
- Adhesive labels, 421
- Admissible/admissibility, 511
- Adroit Photo Forensics, 146
- ADS (alternate data stream)
 - definition, 511
 - hiding data, 344–346
- Advanced Test Products, 415
- AFF (Advanced Forensic Format), 126
- Affidavits
 - definition, 511
 - of probable cause, 36
 - for search warrants, 36, 40
- After-hours warrants, 41, 511
- Agent of the government
 - definition, 511
 - in the Fourth Amendment, 25–26
- Aguilar v. Immigration and Customs Enforcement*, 157–158
- Airplane mode, cell phones, 319
- AKD (Active@KillDisk), 108
- AMD processors, 431
- AME (AccessData Mobile Examiner), 451
- Amendments to the Constitution, 24.
 - See also* Fifth Amendment; First Amendment; Fourth Amendment.
- American Society of Crime Laboratory Directors/Laboratory Crediting Board (ASCLD/LAB) certification, 481–483
- Analysis, description, 6–7. *See also* Browser history analysis.
- Analysis and Review package, 372
- Analyzing proxy server logs
 - Sawmill utility, 244
 - tools, 243–244
 - WebTrends utility, 243
- Analyzing Web server logs
 - centralized logging, 238
 - epoch time conversion, 237–238
 - logging per server, 238
 - overview, 236–238
 - rotating logs, 237
 - W3C fields, 237
- AND operator, 204
- Andrus, U.S. v.*, 83
- Anonymous remailers, 254
- Antiforensics. *See also* Artifact destruction; Hiding data.
 - definition, 512
 - overview, 327–328
- Antistatic bags, 420–421
- Antivirus logs, 267–268
- Apache Systems
 - OpenOffice suite, 439
 - Web server logs. *See* Web server logs, Apache files.
- Apparent authority
 - definition, 512
 - description, 47
- Application logs, 263, 264–268
- Appropriation of name or likeness, 30
- Artifact destruction
 - overview, 328
 - temporary files, 335–336
- Artifact destruction, extracting registry
 - history
 - deleted applications, 330
 - HKEY_USERS, Windows registry, 328–331
 - installed software, by user, 331
 - listing users, 328–331
 - MRU (most recently used) files, 328–331
 - SID (Security Identifier), 329
 - tools, 331. *See also specific tools.*

- Artifact destruction, file system metadata
DCO (Device Configuration Overlay),
331
deleted files, 334–335
event logs, 331
MFT (Master File Table), 332–335
NTFS metafiles, 333
string search, 333
- Artists Against 419, 88
- ASCII character set, 396–398
- ASCLD/LAB (American Society of Crime
Laboratory Directors/Laboratory
Crediting Board) certification,
481–483
- Assessment. *See* Identification/
assessment.
- Assumed permission, 48
- Asterisk (*), in string searches, 180
- At sign (@)
in e-mail addresses, 187
in passwords, 349
- Atech Flash Technology, 437
- Attachment statistics, e-mail analysis, 207
- Attorney/client privilege, 64–65
- \$AttrDef metadata file, 136
- Audit trails, privacy legislation, 57
- Audits, 512
- Authentication
DD (bit for bit) images, 124
definition, 512
- Authenticity of evidence
computers as containers, 79
consent search doctrine, 81–83. *See*
also Warrantless searches, with
consent.
digital evidence, 95
forensics workstations, 425
inadvertence approach, 78
multiple users on a computer, 80–81, 83
overview, 72, 77
password-encoded accounts, 80–81, 88
plain view doctrine, 77–79
proactive evidence collection, 254–255
prophylactic test, 78–79
- Authority to consent to search
actual, 47, 511
apparent, 47, 82
common, 81–82
erroneous assumption of, 83
ostensible, 49, 516
- Autoruns, 404
- AVG Antivirus logs, 268
- AWSTATS log, 236
- B**
- Bad clusters, hiding data, 181–182, 339
- \$BadClus metadata file, 135–136, 182, 339
- Baron, Jason, 205
- Barth, U.S. v.*, 39, 88
- Base addresses, 125
- Base Station Controller, 310
- Base Transceiver Station, 310
- Bates numbering, 512
- Bates numbering, 376
- Batteries, removing and handling, 103
- Bee Docs, 20
- Bellar, State v.*, 302
- Bill of Rights, 24
- BIN (Centralized Binary) Web server
logs, 234
- Binary metadata *vs.* human-readable, 156
- Bit for bit (DD) images
authentication, 124
data acquisition format, 124
file splitting, 124
- BitLocker encryption, 98, 347
- \$Bitmap metadata file, 136
- BlackBag technologies, 321
- Blackburn, Robert, 75
- BlackLight, 321
- Blanket search, 252
- Block, U.S. v.*, 81
- Blogs, First Amendment protection,
28–29

- Blue screen snapshots of memory, 112
- Body file, 163
- Books and publications
 - Computer Forensics: Incident Response Essentials*, 2
 - Crime Investigation: ...and the Police Laboratory*, 93
 - Cyber Forensics: A Field Manual...*, 91
 - Electronic Crime Scene Investigation:...*, 91
 - Guidelines for Evidence Collection and Archiving*, 112
 - A Hardware-Based Memory Acquisition...*, 119
 - PC Hardware Maintenance and Repair*, 417
 - PMBOK (Project Management Book of Knowledge)*, 14
 - “Privacy,” 30
 - Records, Computers, and the Rights of Citizens*, 56
 - The Right to Privacy*, 30
 - Searching and Seizing Computers...*, 64–65, 67
 - Steganografia*, 350
- Boolean operators
 - definition, 512
 - e-mail searches, 204–205
- \$Boot metadata file, 136
- Bradley Joseph Steiger, U.S. v.*, 86–87
- Branzburg v. Hayes*, 28
- Breadth of search, 84, 512. *See also* Scope of search.
- Briggs Software, 135, 143–144
- British Government, metadata incident, 167–168
- Broadband network access, cloud
 - computing, 278
- Browser engines, 216
- Browser history analysis
 - control of digital material, 226–227
 - counting contraband, 230
 - DAT files, displaying, 221
 - deleted files, 227–230
 - detecting active measures, 227–230
 - detecting malware, 227
 - Directory Snoop, 223, 227
 - establishing user actions, 224–230
 - evidence of deleted files, 223
 - fast meta refresh, 224
 - file wipes, 227–230
 - goal of forensic analysis, 222
 - HTTP 300 message, 224
 - identifying specific records, 221
 - job of the investigator, 222–224
 - knowledge of possession, 222–224
 - MFT (Master File Table), 223
 - MFT metadata, effects of deleting files, 229
 - for multiple users, 224
 - pop-up bombs, 224
 - present possession concept, 222
 - redirects, 224–225
 - sorting records, 221
 - timeline, creating, 227
 - tools, 221, 223, 225, 227, 230, 233
 - Trojan horse defense, 227
 - typed URLs, 225–226
 - user intent and control, 226–227
 - Web Historian, 225, 231–233
 - Website Profiler, 233
 - Windows registry, 225–226
- Browser history analysis, tools for
 - BUTIL, 243
 - The Coroner’s Toolkit, 233
 - CSAUDIT, 243
 - Directory Snoop, 223
 - e-mail analysis, 206
 - Log Parser 2.2, 236
 - MAC analysis, 163
 - Metadata Analyzer, 181
 - NWAdmin, 243
 - ODBC, 243
 - Pasco, 221

- proxy server log analysis, 243–244
- Registry Analyzer, 178
- Sawmill, 244
- summary of, 230
- Web Historian, 220, 225, 227
- WebTrends, 243
- Browsers. *See* Web browsers.
- Browsing Web sites. *See* Web browsers.
- Brute-force attacks, password cracking, 349
- Buckner, Frank Gary, 82
- Buckner, Michelle, 82
- Burden of proof, 5
- Business change control, 476–477
- Business of forensics. *See* Starting a shop.
- Business Wire, 450
- BUTIL, 243
- C**
- Cables and connectors, evidence handling, 104
- Cache log, 243
- Cached browser history, 219
- Cached files, location of, 219
- Caching browser information, 216
- Cain and Abel, 349
- Canon Imageware, 298
- Captain Nemo, 409
- Capture, 408
- Carey, U.S. v.*, 37, 78
- Carrier, Brian, 7, 119
- Carriers, steganography, 351
- carver-recovery, 149
- Carvey Harlen, 331
- CascadeShark, 255
- Case logs
 - definition, 512
 - sample forms, 508–509
 - for software tools, 412
- Case management
 - ancient example of, 379
 - file-naming conventions, 381–382
 - frameworks, 380
 - overview, 379–381
 - preparation stage, 381–382
 - presenting the results, 388–389
 - teams, 382
 - threat assessment, 381
- Case management, investigation stage
 - crime scene management, 385–386
 - evidence examination, 387–388
 - evidence handling, 386–387
 - first response, 384–385
 - lab preparation, 386
 - overview, 382–383
 - triage, 383–384
- Case summary, final report, 391
- Casey Marie Anthony, State of Florida v.*, 224
- CCE (Certified Computer Examiner), 448
- CDFE (Certified Digital Forensic Examiner), 445–446
- CDMA (Code Division Multiple Access), 310
- CDs, evidence handling, 103
- Cell phones. *See also* Mobile devices.
 - Base Station Controller, 310
 - Base Transceiver Station, 310
 - CDMA (Code Division Multiple Access), 310
 - cellular networks, 310–311
 - charging, 319
 - cocktail effect, 310
 - device information, retrieving, 315–317
 - differentiating between users, 310
 - GPS (Global Positioning System), 311–313
 - GSM (Global System for Mobile Communications), 310–311
 - HLR (Home Locator Register), 310
 - location, determining, 311–313
 - MSC (Mobile Switching Center), 310
 - passwords, extracting, 320–321
 - permanently blocked, 315

- Cell phones (*cont'd*)
 - removing moisture from, 321
 - setting to airplane mode, 319
 - TDMA (Time Division Multiple Access), 310–311
 - triangulation, 311–313
 - trilateration, 311–313
 - unlocking a PIN, 315, 320–321
 - VLR (Visitor Locator Register), 310
- Cell phones, acquisition
 - image extraction, 320–321
 - recovering deleted data, 320–321
 - reporting software, 321
 - screen capture, 320
 - SITA (search incident to arrest), 317
 - tools, 317–321. *See also specific tools.*
- Cell phones, cellular towers
 - description, 308–310
 - triangulation, 311–313
- Cell phones, data storage
 - blocking communication, 318–319
 - cloning SIM cards, 320
 - ESN (electronic serial number), 315
 - Faraday enclosures, 318–319
 - ICCID (Integrated Circuit Chip Identifier), 315
 - IMEI (International Mobile Equipment Identity), 315–316
 - MEID (mobile equipment identifier), 315–316
 - memory, 313–315
 - micro-SIM cards, 314
 - mini-SIM cards, 314
 - overview, 313
 - PIN (personal identification number), 314
 - portable charging devices, 318–319
 - printed on the case, 315–317
 - PUK (pin unlock key), 314
 - radio frequency isolation, 318–319
 - RAM (random access memory), 315
 - ROM (read-only memory), 315
 - SIM cards, 313–315, 320, 518
 - SIMless phones, 314
 - TAC (Type Allocation Code), 316
 - tools, 319. *See also specific tools.*
- Cellboost device, 319
- Cellebrite, 320–321
- Cellular networks, 310–311
- Centralized Binary (BIN) Web server logs, 234
- Centralized logging, 238
- Certification
 - areas of competency, 442
 - ASCLD/LAB, 481–483
 - licensing requirements, 451–452
 - organizational, 481–483
- Certification, vendor-neutral programs
 - CCE (Certified Computer Examiner), 448
 - CDFE (Certified Digital Forensic Examiner), 445–446
 - DFCB (Digital Forensics Certification Board), 446–447
 - Digital Forensics Certified Associate, 446–447
 - Digital Forensics Certified Practitioner, 446–447
 - fees, 447
 - GCFA (GIAC Certified Forensic Analyst), 443–444
 - GCFE (GIAC Certified Forensic Examiner), 443–445
 - GIAC (Global Information Assurance Certification), 443
 - GIAC Reverse Engineering Malware, 443
 - hard skills, 445
 - ISFCE (International Society of Forensic Computer Examiners), 448
 - MFCE (Mobile Forensics Certified Examiner), 448

- MFI (Mobile Forensics, Inc.),
448–449
overview, 442
soft skills, 445
- Certification, vendor-specific programs
AccessData, 450–451
ACE (AccessData Certified Examiner),
450–451
AME (AccessData Mobile Examiner),
451
Business Wire, 450
Encase forensic suites, 450
ENCE (Encase Certified Examiner),
450
ENCEP (Encase Certified eDiscovery
Practitioner), 450
Guidance Software, 450
overview, 450
Paraben Corporation, 451–452
PCFE (Paraben Certified Forensic
Examiner), 452
PCME (Paraben Certified Mobile
Examiner), 452
- Certified Computer Examiner
(CCE), 448
- Certified Digital Forensic Examiner
(CDFE), 445–446
- CFTT (Computer Forensics Tool Testing),
411
- Chain of command, crime scene, 96–97
- Chain of custody
case law, 21
definition, 512
documenting, 20
evidence handling, 101–102
sample forms, 509
- Change control
business change, 476–477
software change, 477–478
- Character sets, 396–398
- Charging cell phones, 318–319
- Child pornography. *See also* Pedophiles.
inadvertent discovery, 78
private searches, 86–87
- Chimel v. California*, 45
- Chinex device, 320–321
- Cisco Router Evidence Extraction Disk
(CREED), 271
- Cisco routers, 271–273
- Civil action, definition, 512
- Civil cases
defendants, 1
mobile device forensics, 323–324
plaintiff, 1
- Civil investigations
definition, 1
investigation scope, 9–10
scope of investigation, 9–10
timelines, 9
types of attacks, 9. *See also specific
attacks.*
- Class characteristics of evidence, 94
- Clearing and Sanitizing Matrix*, 142
- Client-server networking, cloud forensics,
288–289
- Clients. *See* E-mail clients.
- Cloning SIM cards, 320
- Closed container, definition, 512
- Closed container clause, 27, 38–39. *See
also* Computers as containers.
- Cloud computing. *See also*
Virtualization.
broadband network access, 278
characteristics of, 278
community cloud, 279
definition, 277
deployment models, 278–279
elasticity, 278
hybrid cloud, 279
measured service, 278
on-demand service, 278
private cloud, 278–279

- Cloud computing (*cont'd*)
 - public cloud, 279
 - resource pooling, 278
- Cloud computing, service models. *See also* specific models.
 - hosted application management, 282
 - IaaS (Infrastructure as a Service), 280–282
 - overview, 278, 279–280
 - PaaS (Platform as a Service), 284
 - SaaS (Software as a Service), 282–284
 - SSO (single sign-on) security, 283
- Cloud forensics
 - checklist of questions, 286
 - client-server networking, 288–289
 - cloud structure, overview, 287
 - communications model, 288–290
 - computational model, 287
 - data collection, 285, 290–291
 - document imaging systems, file naming conventions, 296–297
 - documents *vs.* metadata, 285
 - elasticity, 287
 - jurisdictional issues, 285
 - lack of physical disks, 285, 290–291
 - P2P (peer to peer) networking, 288
 - protecting non-targeted information, 290–291
 - real-time monitoring, 291
 - recovering deleted data, 291
 - reproducible methods, 285
 - stateful applications, 289
 - stateless applications, 289
 - storage models, 287–288
- Cloud forensics, constitutional issues
 - ESCA (Electronic Stored Communications Act), 301–302
 - exclusionary rule, 301–302
 - Fifth Amendment issues, 303
 - forced surrender of passwords, 303
 - Fourth Amendment issues, 301–302
 - overview, 300–301
 - reasonable expectation of privacy, 302
- Cloud forensics, technical aspects
 - capturing virtual machines, 299–300
 - cloud data types, 296–299
 - collecting artifacts, 296
 - database transaction logs, 298
 - LDF (log data file), 298
 - MDF (master database file), 296, 298–299
 - overview, 295–296
- CLSID (Content Class Identifier), 192, 512
- Clusters
 - definition, 513
 - Microsoft file system, 133, 138–140
- Cnty. Health Sys., Inc. U.S. ex rel. Baker v.*, 66
- Cocktail effect, 310
- Code Division Multiple Access (CDMA), 310
- Collecting evidence. *See* Data acquisition; E-discovery, data collection; Evidence handling.
- Collecting live information, 103, 104
- Commands
 - #copy startupconfig tftp, 272
 - #dir slot, 272
 - history, listing, 272
 - mem, 114–115
 - net sessions, 262
 - net share, 262
 - net use, 262
 - netstat, 262
 - nslookup, 208–209
 - P2 Commander, 331, 408
 - pipng, 124
 - router and switch forensics, 271, 272
 - #show history, 272
 - #show users, 272
- Common Log fields, 240
- Common Log (NCSA) Web server logs, 234
- Communications model, cloud forensics, 288–290

- Community cloud, 279
- CommView, 255–256
- Competence of evidence, 74–76, 513
- Competent, definition, 513
- Comprehensive Drug Testing, U.S. v.*, 44, 78–79
- Computational model, cloud forensics, 287
- Computer crimes
characteristics of, 10
defining, 10–12
most common, 10–11
types of attacks, 9
- Computer Forensics: Incident Response Essentials*, 2
- Computer Forensics Tool Testing (CFTT), 411
- Computer power, forensics workstations, 424
- Computer science vs. digital forensics, 92
- Computer Watchdog, 251
- Computers as containers. *See also* Closed container clause.
admissibility of evidence, 79
authenticity of evidence, 79
case law, 38–39
plain view doctrine, 79
- Computers for forensics work. *See* Forensics workstations.
- Concept extraction, e-discovery, 371–372
- Concept searching, e-mail searches, 207–208
- Conclusion, final report, 392–393
- Configuration log, 243
- Consent exception, proactive evidence collection, 252
- Consent search doctrine. *See also* Warrantless searches, with consent.
authenticity of evidence, 81–83
case law, 82
- Consent to warrantless search. *See* Warrantless searches, with consent.
- Constitution of the United States
amendments, 24. *See also* Fifth Amendment; First Amendment; Fourth Amendment.
Bill of Rights, 24
modifications to, 24
privacy rights, 55
right to privacy, 29–30
- Constitution of the United States, limits of
constraints on evidence, 75
digital vigilantes, 85–88
jurisdiction in cyberspace, 85–86
private searches, 86–87
self-incrimination, 27. *See also* Fifth Amendment issues.
- Constitutional issues, cloud forensics
ESCA (Electronic Stored Communications Act), 301–302
exclusionary rule, 301–302
Fifth Amendment issues, 303
forced surrender of passwords, 303
Fourth Amendment issues, 301–302
overview, 300–301
reasonable expectation of privacy, 302
- Consumer Reporting Agencies (CRA), guidelines for, 60
- Contamination teams. *See* Taint teams.
- Content Class Identifier (CLSID), 192, 512
- ContentAnalysis, 207–208
- Context triggered piecewise hashing (CTPH), 369–370
- Contraband, counting, 230
- Control of digital material, 226–227
- Cookies
definition, 217
storage location, 219
- #copy startupconfig tftp command, 272
- Copyright infringement, 29
- The Coroner’s Toolkit, 233
- Corporate departments as revenue source, 480–481

- Cost justification, starting a forensics shop, 480–481
- Costs. *See also* Revenue sources.
 - facilities improvement, 466
 - hardware acquisition, 463–464
 - software acquisition, 464–466
 - starting a forensics shop, 462–466
- Court approval of software tools, 410–413
- Cover files, steganography, 351
- Covert data, definition, 347, 513. *See also* Hiding data.
- Covert data, encryption
 - BitLocker Drive Encryption, 347
 - DESX (Data Encryption Standard eXORed)*, 347
 - EFS (Encrypting File System), 347
 - methods of, 347
 - passwords, 348–350
 - smart cards, 347
- Covert data, steganography
 - algorithms, 351
 - carriers, 351
 - cover files, 351
 - detecting, 354
 - dictionary attacks, 354
 - filtering, 351
 - lossless compression, 350
 - lossy compression, 350
 - LSB (least significant bit) insertion, 351
 - masking, 351
 - messages, 351
 - methodology, 350–351
 - null cipher, 354
 - overview, 350
 - redundant pattern encoding, 351
 - signatures, 354
 - stegoimage, 351
 - stegokey, 351
 - tools, 351–354. *See also specific tools.*
 - transformations, 351
- CRA (Consumer Reporting Agencies), guidelines for, 60
- Crack, 349
- Cracking algorithms, password cracking, 349
- Create attribute, 159–160
- Credibility of evidence, 74, 513
- Credible, definition, 513
- Credit reports, privacy legislation, 60
- CREED (Cisco Router Evidence Extraction Disk), 271
- Crime Investigation: ...and the Police Laboratory*, 93
- Crime scene management, 385–386
- Crime scenes. *See also* Digital evidence; Evidence.
 - BitLocker encryption, 98
 - chain of command, 96–97
 - concealed passwords, 100
 - devices of interest, 97–98
 - documenting, 98–99
 - Faraday bags, 98
 - hardware inventory, 99–100
 - identifying data sources, 99–100
 - laser printers, 100
 - missing devices, 99
 - safety, 97
 - scan once/print many devices, 99
 - securing the scene, 97–98
 - USB devices, 98
- Criminal action, definition, 513
- Criminal cases
 - defendants, 1
 - plaintiff, 1
- Criminal investigations
 - definition, 1
 - investigation scope, 10–12
- CSAUDIT, 243
- CSI Effect, 91
- CTPH (context triggered piecewise hashing), 369–370
- Curriculum vitae, 513
- CV (curriculum vitae), 31
- Cyber Forensics: A Field Manual...*, 91

D

- “Dance hall proprietor vs. landlord”
 - argument, 29
- Dark data. *See also* Hiding data.
 - definition, 513
 - description, 336–337
- DAT files, displaying, 221
- Data abstraction layers
 - lossless, 399
 - lossy, 399
 - overview, 396–398
- Data acquisition. *See also* Cell phones, acquisition; E-discovery, data collection.
 - blue screen snapshots of memory, 112
 - .DMP files, 112
 - Guidelines for Evidence Collection and Archiving*, 112
 - imaging process, legal argument for, 123
 - order of volatility, 112
 - from original data, 111
 - priority list for, 112
- Data acquisition from media
 - absolute direct addressing, 125
 - base addresses, 125
 - encrypted devices, 122
 - offsets, 125
 - password recovery, 122
 - tools, 124–128
 - types of media, 121
 - write-protected port replicator, 122
- Data acquisition from media, file formats
 - for disk images
 - AFF (Advanced Forensic Format), 126
 - DD (bit for bit) images, 124
 - EFW (Expert Witness Format), 124–125
 - IDIF (iLook Default Image Format), 127
 - IEIF (iLook Encrypted Image Format), 127
 - iLook, 127
 - IRBF (iLook Raw Bitstream Format), 127
 - Prodiscover, 127–128
 - proprietary formats, 126–128
 - Safeback, 126–127
 - summary of, 123
- Data acquisition from memory and running processes
 - capturing, software for, 116
 - changes over time, 113–115
 - footprints, 116
 - A Hardware-Based Memory Acquisition...*, 119
 - hardware memory capture, 119–120
 - hashing the memory image, 114
 - hooks, detecting, 117
 - kernel mode, 116
 - live response, 113–115
 - log files, creating, 118–119
 - MAC data, modifying, 121
 - MD5 hash, calculating, 118
 - mem command, 114–115
 - memory as a device, 116
 - overview, 112–115
 - paths to memory, 116
 - priority data, 114
 - procedures for, 120–121
 - rootkits, detecting, 114, 117
 - SHA1 hash, calculating, 118
 - smear images, 116
 - software memory capture, 117–119
 - system memory vs. addressable memory, 114–115
 - user mode, 116
- Data attribute, file metadata, 154
- Data carving. *See also* File recovery.
 - carver-recovery utility, 149
 - definition, 145, 513
 - description, 145–147
 - DFRSW (Digital Forensics Research Workshop), 146
 - false positives, 146
 - file headers, 145–147
 - files embedded in other files, 146
 - Foremost utility, 147–148
 - fragmented files, 146
 - overview, 145

- Data carving (*cont'd*)
 - Scalpel utility, 149
 - SmartCarving, 146
 - tools for, 146, 147–149
- Data collection, cloud forensics, 285, 290–291
- Data Encryption Standard eXORed (DESX), 347
- Data mapping, 363–364
- Data recovery
 - from slack space. *See* Data carving.
 - from unallocated space. *See* Data carving.
- Data recovery, cell phones, 320–321. *See also* File recovery.
- Data retention, policies and procedures, 471–472
- Data sources, crime scene, 99–100
- Data wiping utilities, 108–109
- Database activity logs, 266
- Database transaction logs, 298
- DATE: field, e-mail, 196–197
- Daubert Process, 400–401
- Daubert v. Merrel Dow Pharmaceuticals, 317, 401
- David, U.S. v.*, 39
- .dbx files, 192–193
- DBX files, 192–193
- DCO (Device Configuration Overlay), 331
- DD (bit for bit) images
 - authentication, 124
 - data acquisition format, 124
 - file splitting, 124
- DD (Disk Dump), 338, 405
- dd utility, 108
- DDR (dual data rate) memory, 432
- Debt collection, privacy legislation, 62
- Decryption Collection, 408
- Defendant
 - in civil cases, 1
 - in criminal cases, 1
 - definition, 513
 - as stakeholder, 12
- Deleted applications, extracting registry history, 330
- Deleted documents, proving existence of, 159–162
- Deleted files. *See also* Data recovery; File recovery; Recycle Bin.
 - browser history analysis, 223, 227–230
 - file metadata, 154–155
 - file system metadata, 334–335
- Deleting e-mail messages, 191
- Deleting files. *See also* Recycle Bin.
 - Clearing and Sanitizing Matrix*, 142
 - deletion process, 141–143
 - Department of Defense specifications, 142
 - hidden files, 142
 - INFO file, 142
 - INFO2 file, 142
 - invisible file names, 141–142
 - permanent deletion, 142–143
 - recovery process, 143–145
 - temporary files, 175
- Dentries, UNIX/Linux file systems, 137–138
- Department of Defense specifications, data destruction, 142
- Deployment models, cloud computing, 278–279
- Destroying data
 - acceptable destruction methods, 142–143
 - AKD (Active@KillDisk), 108
 - Clearing and Sanitizing Matrix*, 142
 - data wiping utilities, 108–109
 - dd utility, 108
 - Department of Defense specifications, 142
 - Disk Scrub utility, 109
 - evidence handling, 107–109
 - file wipes, 227–230

- during graceful shutdown, 143
 - permanent deletion, 142–143
 - Shred utility, 108
 - WIPE.EXE utility, 108
- DESX (Data Encryption Standard eXORed), 347
- Device Configuration Overlay (DCO), 331
- Device Seizure, 321
- DFCB (Digital Forensics Certification Board), 446–447
- DFRSW (Digital Forensics Research Workshop), 146
- Dictionary attacks, steganography, 354
- Digital Assembly, 146
- Digital audio recorder, 420
- Digital camera, as forensic tool, 419–420
- Digital evidence. *See also* Crime scene; Digital forensics.
- authenticity, 95
 - class characteristics, 94
 - individual characteristics, 94
 - latent, 94
 - longevity, 95
 - obtaining legally, 96
 - patent, 94
 - vs. physical, 94–96
 - relevance, 96
 - reliability, 95
 - stability, 95
 - types of, 94–95
- Digital forensics. *See also* Digital evidence.
- vs. computer science, 92
 - Crime Investigation: ...and the Police Laboratory*, 93
 - Cyber Forensics: A Field Manual...*, 91
 - definition, 92
 - digital evidence vs. physical, 94–96
 - Locard's exchange principle, 93
- Digital Forensics Certification Board (DFCB), 446–447
- Digital Forensics Certified Associate, 446–447
- Digital Forensics Certified Practitioner, 446–447
- Digital Forensics Research Workshop (DFRSW), 146
- Digital Intelligence, 415
- Digital Intelligence, forensics workstations, 425–427
- Digital Millennium Copyright Act (DMCA), 29
- Digital vigilantes, 85–88
- #dir slot command, 272
- Directed compound file, 335–336
- Directory Snoop
- browser history analysis, 223, 227
 - description, 409
 - examining metadata files, 135
 - restoring file under NTFS, 143–144
- Disclosure, e-discovery, 361–363
- Discoverable items, 14
- Discovery. *See also* E-discovery.
- definition, 513
 - rules for ordering, 11–12
- Disguised files. *See* File recovery.
- Disk Dump (DD), 338, 405
- Disk Explorer for FAT, 409
- Disk Explorer for NTFS, 409
- Disk images, file formats
- AFF (Advanced Forensic Format), 126
 - DD (bit for bit) images, 124
 - EWF (Expert Witness Format), 124–125
 - IDIF (iLook Default Image Format), 127
 - IEIF (iLook Encrypted Image Format), 127
 - iLook, 127
 - IRBF (iLook Raw Bitstream Format), 127
 - Prodiscover, 127–128
 - proprietary formats, 126–128

- Disk images, file formats (*cont'd*)
 - Safeback, 126–127
 - summary of, 123
 - Disk Investigator, 409
 - Disk Scrub, 109
 - DM (document management) systems, 164
 - DMCA (Digital Millennium Copyright Act), 29
 - .DMP files, 112
 - DNA testing, freeing the innocent, 95
 - DNS cache poisoning, 254
 - DNS logs, 266–267
 - DocScrubber, 168
 - Doctor. *See* Physician.
 - Document management (DM) systems, 164
 - Documentation. *See also* Report writing; Reporting.
 - legal, preparing a list of, 4–5
 - levels of, 13
 - project management, 13
 - template for, 16–17
 - Documentation, levels of
 - case timeline, 18–20
 - chain of custody, 20
 - general case, 14–15
 - procedural, 15–18
 - process, 18
 - Documenting
 - crime scenes, 98–99
 - evidence, 104–105
 - execution of search warrants, 41
 - Documents. *See also* Files.
 - authenticity, e-discovery, 375–377
 - DM (document management) systems, 164
 - imaging systems, file naming
 - conventions, 296–297
 - management systems, e-discovery, 374–375
 - metadata, hiding data in, 166–175, 178–181
 - vs.* metadata, cloud forensics, 285
 - preservation orders, 164
 - revision history, viewing, 168, 170–171
 - Doe v. U.S.*, 303
 - Domain, in e-mail addresses, 187
 - Domain name, querying e-mail by, 209–210
 - Double quotes (“ ”), Boolean operator, 205
 - DriveImageXL, 409
 - DriveLook, 409
 - Dual-channel memory, 432
 - Dual data rate (DDR) memory, 432
 - dumpchk.exe, 404
 - Duty to preserve, 362
 - DVDs, evidence handling, 103
- ## E
- E-discovery
 - analyzing potential data, 373–374
 - comparing hash values, 369–370
 - concept extraction, 371–372
 - CTPH (context triggered piecewise hashing), 369–370
 - data mapping, 363–364
 - definition, 357
 - disclosure, 361–363
 - duplicates *vs.* near duplicates, 369–370
 - duty to preserve, 362
 - EDRM (Electronic Discovery Reference Model), 359–360
 - ESI (electronically stored information), 368–369
 - filter categories, 371–372
 - focus categories, 371–372
 - identifying target data, 361–364
 - information management, 360–361
 - litigation hold, 362–363
 - metrics for potential data, 373–374
 - overview, 358

- pre-search processes, 361–363
- preservation, 368–369
- preservation order, 362–363
- privacy legislation, 61–62
- processing potential data, 370–371
- production and presentation, 374–377
- reasonable anticipation of litigation, 362
- reviewing potential data, 372–373
- rolling hash, 370
- rolling review, 372–373
- scope, 362
- search processes, 363–364
- security of potential data, 372–373
- spoliation, 361, 362–363
- trigger point, 362
- E-discovery, data collection
 - accessible data, 366–367
 - active online data, 366–367
 - determining completeness, 366
 - forms of data, 366–367
 - inaccessible data, 366–367
 - near-line data, 366–367
 - off-line storage, 366–367
 - overview, 364–365
 - search strings, 365–366
 - tools, 367–368. *See also specific tools.*
- E-discovery, production and presentation
 - analyzing potential data, 375–377
 - Bates numbering, 376
 - document authenticity, 375–377
 - document management systems, 374–375
 - native format, 374
 - near-native format, 374
 - overview, 374
 - redaction, 376
 - unique identifiers, 376
- E-mail
 - multiple inboxes, 195
 - shared inboxes, 195
 - tracing sources, 202–203, 208–210
- E-mail addresses
 - @ (at sign), 187
 - overview, 187–188
 - as passwords, 349
 - spoofing, 188
 - user domain, 187
 - user name, 187
- E-mail analysis
 - domain name, querying by, 209–210
 - IP address, querying by, 208–210
 - nslookup command, 208–209
 - WHOIS lookup, 209–210
- E-mail clients
 - address book folder, 191
 - common examples, 190
 - definition, 187
 - handling deleted messages, 191
 - mail folders, 191
 - main functions, 189, 191
 - .mbx folders, 191
 - overview, 189
 - .pst folders, 191
 - saving messages, 191
 - .wab folders, 191
- E-mail information stores, e-mail servers
 - ACK (acknowledgement) packets, 195
 - activity logs, 199–202
 - delivery agents, 194–195
 - DNS (Domain Name Services), 195
 - IMAP servers, 195
 - incoming messages, 195
 - message deletion, 195
 - NACK (nonacknowledgement) packets, 195
 - outgoing messages, 194–195
 - POP servers, 195
 - SMTP servers, 194–195
- E-mail information stores, Outlook
 - overview, 193
 - PST files, 193
 - version history, 194

- E-mail information stores, Outlook
 - Express
 - CLSID (content class identifier), 192
 - .dbx files, 192–193
 - DBX files, 192–193
 - file formats, 192
 - IDX files, 192
 - .mbx files, 192
 - MBX files, 192
 - NCH files, 192
 - overview, 192
 - version history, 192
 - overview, 191–192. *See also* specific stores.
- E-mail Mining Toolkit (EMT), 206
- E-mail protocols
 - ESMTP (Extended SMTP), 188
 - handshaking packet, 188
 - HELO packet, 188
 - IMAP (Internet Message Access Protocol), 189
 - incoming messages, 188
 - outgoing messages, 188
 - POP3 (Post Office Protocol 3), 188–189
 - port 25, 188
 - port 143, 189
 - SMTP (Simple Mail Transport Protocol), 188
- E-mail searches
 - advanced methods, 206–208
 - analyzing search results, 205–206
 - attachment statistics, 207
 - Boolean operators, 204–205
 - companies involved in, 208
 - concept searching, 207–208
 - EMT (E-mail Mining Toolkit), 206
 - false negatives, 206
 - false positives, 205–206
 - group communications, 207
 - histogram of account activity, 206
 - keyword searches, 205
 - precision, 206
 - recall, 206
 - recipient frequency, 207
 - searching messages, 203–205
 - similar users, 206
 - stationary user profiles, 206
 - tobacco industry, 205
 - tools for, 206
 - true negatives, 206
 - true positives, 206
 - warrants, 203
- E-mail servers. *See* E-mail information stores, e-mail servers.
- E-mail structure
 - DATE: field, 196–197
 - Entourage utility, 199–202
 - FROM: field, 196–197
 - header extraction, tools, 199–202
 - MIME headers, 197–202
 - MIME (Multipurpose Internet Mail Extensions), 196
 - overview, 196
 - RE: prefix, 197
 - standard headers, 196–197
 - SUBJECT: field, 196–197
 - TO: field, 196–197
- E-mail transport
 - clients, 187
 - e-mail servers, 187
 - MDA (mail delivery agent), 186, 515
 - MTA (mail transport agent), 186, 515
 - MUA (mail user agent), 186, 515
 - overview, 186–187
- Eclipse device, 320
- ECPA (Electronic Communications Privacy Act of 1986), 58–59
- ECS (Electronic Communications Services), 58
- EDiscovery, 408
- EDRM (Electronic Discovery Reference Model), 359–360
- Education, privacy legislation, 63–64
- EFS (Encrypting File System), 347

-
- EFSDump, 404
- Egyptians, ancient case document, 379
- 8.3 file names, 134
- Elasticity
- cloud computing, 278
 - cloud forensics, 287
- Electronic Crime Scene Investigation:..., 91
- Electronic discovery, privacy legislation.
- See* E-discovery.
- Electronic information in the hands of a third party, expectation of privacy, 39–40
- Electronic serial number (ESN), 315
- Electronic Stored Communications Act (ESCA), 301–302
- Electronically stored information (ESI), 368–369
- EM (entry modified) attribute, 160–162
- Embarrassing public disclosure, 30
- Embedded metadata, 164–172
- EMT (E-mail Mining Toolkit), 206
- Encase
- creating timelines, 19
 - e-discovery, 370
 - forensic suites, certification program, 450
 - saving images in EWF (Expert Witness Format), 124
- Encase Data, 118
- Encase Enterprise, 234
- Encase Forensics, 408
- ENCE (Encase Certified Examiner), 450
- ENCEP (Encase Certified eDiscovery Practitioner), 450
- Enclosures for forensics workstations, 430
- Encrypted devices, data acquisition from, 122
- Encrypting File System (EFS), 347
- Encryption
- BitLocker, 98, 347
 - DESX (Data Encryption Standard eXORed)*, 347
 - EFS (Encrypting File System), 347
 - methods of, 347
 - passwords, 348–350
 - smart cards, 347
- Endace, 255
- EndaceExtreme, 255
- Energizer device, 319
- Entourage, 199–202
- Entry modified (EM) attribute, 160–162
- Environmental Law Publishing, 72
- EO1, 118
- Epoch time conversion, 237–238
- Equifax, 60
- Erasing data. *See* Deleting files; Destroying data.
- ERRORLOG file, 266
- ESCA (Electronic Stored Communications Act), 301–302
- ESI (electronically stored information), 368–369
- ESMTP (Extended SMTP), 188
- ESN (electronic serial number), 315
- Event logs, 263–264, 331
- Event Viewer, 403–404
- Evidence. *See also* Crime scene.
- class characteristics, 94
 - collection. *See* E-discovery, data collection; Network search, post-incident evidence collection; Network search, proactive evidence collection.
 - electronic. *See* Digital evidence.
 - examination, investigation stage, 387–388
 - individual characteristics, 94
 - latent, 94
 - patent, 94
 - provided under duress, 76
 - timeline for. *See* Chain of custody.
 - types of, 94–95
 - uncovering. *See* Discovery.
-

- Evidence, admissibility. *See also*
 - Authenticity of evidence; Federal Rules of Evidence.
 - competence, 74–76
 - constitutional constraints, 75
 - credibility, 74
 - evidence provided under duress, 76
 - exclusionary rule, 72, 76
 - flowchart, 73
 - hearsay, 75–76
 - material, 72
 - opinions, 73–74
 - overview, 71–72
 - prejudice, 74
 - privileged information, 74–75
 - probitive, 72
 - relevance, 72
 - statutory restraints, 74–75
- Evidence handling. *See also* Data acquisition.
 - chain of custody, 101–102
 - collecting evidence, 100–101
 - destroying, 107–109
 - determining usability, 102
 - documenting evidence, 104–105
 - intrusion detection, 107
 - investigation stage, 386–387
 - McKeever Test, 102
 - overview, 100
 - packaging evidence, 105
 - packaging materials, 105
 - photographing evidence, 104
 - policies and procedures, 470
 - secure evidence storage facilities, 107
 - securing the storage area, 107
 - storing evidence, 106–107
 - transporting evidence, 105–106
 - video surveillance, 107
 - workflow, 100–101
- Evidence handling, computer systems
 - capturing live information, 103, 104
 - CDs, 103
 - DVDs, 103
 - floppy disks, 103
 - labeling cables and connectors, 104
 - networked computers, 104
 - overview, 102–103
 - powering off, 103–104
 - removing the battery, 103
 - standalone computers, 103–104
 - storing digital media, 103
 - VPNs (virtual private networks), 103
- EWf (Expert Witness Format), 124–125
- EWfACQUIRE, 124
- ex ante (before the fact) action, 26
- Examination, description, 6–7
- Excel
 - creating timelines, 19
 - loading registry file, 343
 - metadata, extracting, 181
- Exclusionary rule
 - cloud forensics, 301–302
 - evidence, 72, 76
 - warrantless searches, 44
- Exculpatory, definition, 513
- Exigent circumstances, mobile device forensics, 323
- Expansion slots for forensics workstations, 434
- Experion, 60
- Expert witnesses
 - becoming recognized as, 31
 - conditions for, 31
 - CV (curriculum vitae), 31
 - definition, 514
 - neutrality, 31
 - regulation of, 31
- Ext file systems, 137
- \$Extend metadata file, 136
- Extended Log fields, 242
- Extended SMTP (ESMTP), 188
- Extensible Markup Language (XML), 234

- External storage units, 416
Exxon Valdez incident, 13
Eyewitnesses, 31
- F**
- Fair Credit Reporting Act of 1970, 60
False negatives, 206
False positives, 146, 205–206
False publicity, 30
Faraday, Michael, 420
Faraday bags, 98
Faraday enclosures, 318–319
Faraday shields, 420
Fast meta refresh, 224
FAT12, 133–134
FAT16, 134, 141–142
FAT32, 134–135
FDPA (Fair Debt Collection Practices Act of 2006), 62
Federal Rules of Civil Procedure (FRCP). *See* FRCP (Federal Rules of Civil Procedure).
Federal Rules of Evidence. *See also* Evidence.
 admissibility of evidence, 11. *See also* Evidence, admissibility.
 definition, 514
 expert witnesses, 31
 eyewitnesses, 31
 issuing a warrant (41b), 40
Fees, certification, 447
Felt-tipped pens, 421
FERPA (Family Educational Rights and Privacy Act) of 2008, 63–64
Fifth Amendment issues
 cloud forensics, 303
 divulging passwords, 27
File Allocation Tables, 133–135
File extensions
 changing, 151–153
 as file identifiers, 151–153
File formats for disk images
 AFF (Advanced Forensic Format), 126
 DD (bit for bit) images, 124
 EWF (Expert Witness Format), 124–125
 IDIF (iLook Default Image Format), 127
 IEIF (iLook Encrypted Image Format), 127
 iLook, 127
 IRBF (iLook Raw Bitstream Format), 127
 Prodiscover, 127–128
 proprietary formats, 126–128
 Safeback, 126–127
 summary of, 123
File headers
 data carving, 145–147
 file metadata, 156
File metadata. *See also* Metadata.
 common examples, 178
 data attribute, 154
 for deleted files, 154–155
 file header, 156
 human-readable vs. binary, 156
 magic numbers, 157
 MFT attributes, 153–155
 NTFS attributes, 154
 overview, 153
 sample, 156
File names, Microsoft file system, 134
File objects, UNIX/Linux file systems, 137–138
File recovery. *See also* Data recovery.
 by data string, 140–141
 GREP utility, 140–141
 LBD (Long Block Data) standard, 139–140
 overview, 131–132
 from slack space. *See* Data carving.
 tools, 135, 140–141, 143–144
 from unallocated space. *See* Data carving.

- File recovery, deleted files
 - Clearing and Sanitizing Matrix*, 142
 - cloud forensics, 291
 - deletion process, 141–143
 - Department of Defense specifications, 142
 - hidden files, 142
 - INFO file, 142
 - INFO2 file, 142
 - invisible file names, 141–142
 - permanent deletion, 142–143
 - recovery process, 143–145
 - Recycle Bin, 142
- File recovery, Microsoft file systems
 - 8.3 file names, 134
 - \$BadClus metadata file, 135–136
 - clusters, 133, 138–140
 - FAT12, 133–134
 - FAT16, 134, 141–142
 - FAT32, 134–135
 - File Allocation Tables, 133–135
 - file names, 134
 - floppy disks, 133–134
 - hard disks, 133–137
 - IDEMA (International Disk Drive Equipment and Materials Association), 139
 - LBD (Long Block Data) standard, 139–140
 - metadata files, 135–137
 - MFT (Master File Table), 135, 144
 - \$Mft metadata file, 135–136
 - NTFS, 135–137
 - overview, 132–133
 - partitions, 132–133
 - sectors, 132–133, 139
 - slack space, description, 138–140
 - slack space *vs.* unallocated space, 140
 - storage devices, layout, 132–133
 - summary of, 132
 - from unallocated space, 140
- File recovery, UNIX/Linux file systems
 - directories, 137–138
 - Ext, 137
 - file objects, 137–138
 - master node, 137–138
 - metadata, 137–138
 - Reiser, 137
 - superblocks, 137–138
 - UFS (UNIX File System), 137
- File structure
 - overview, 153
 - sample, 156
- File systems. *See* Microsoft file systems; UNIX/Linux file systems.
- File Transfer Protocol (FTP), 214
- File wipes, browser history analysis, 227–230
- Filematch, 409
- Files. *See also* Documents.
 - comparing hash values, 369–370
 - creation time stamp, 159–160
 - duplicates *vs.* near duplicates, 369–370
 - embedded in other files, 146
 - internal identifiers, 153
 - last access time stamp, 160
 - last modification time stamp, 160–162
 - naming conventions for case management, 381–382
- Film cameras, as threat to privacy, 30
- Filter categories, e-discovery, 371–372
- Filtering steganography, 351
- Financial privacy. *See* Privacy legislation, financial.
- Finder, 406
- Findings, final report, 392
- Finley, U.S. v.*, 323
- Firefox, browser history, 220
- First Amendment
 - assigning accountability, 29
 - blogs, 28–29
 - copyright infringement, 29

- “dance hall proprietor vs. landlord”
argument, 29
- DMCA (Digital Millennium Copyright Act), 29
- ISPs and, 29
- LiveJournal, 29
- vs. pedophilia, 29
- pirated intellectual property, 29
- press, definition of, 28
- YouTube, 29
- First response
Electronic Crime Scene Investigation:..., 91
investigation stage, 384–385
- Flash disk files, displaying, 272
- Flash RAM, 272–273
- Floppy disks
evidence handling, 103
Microsoft file system, 133–134
- fls, 163
- Focus categories. e-discovery, 371–372
- Footprints, software, 116
- For-profit organizations, as revenue
source, 478–479
- Foremost, 147–148
- Forensic, definition, 514
- Forensic ComboDock, 122
- Forensic Computers, Inc., 415, 428–429
- Forensic Dossier, 119
- Forensic PC, 415
- Forensic Recovery of Evidence Device
Diminutive Interrogation Equipment
(FREDDIE), 425, 427
- Forensic Recovery of Evidence Device
(FRED), 425–427
- Forensic Replicator, 328, 408
- Forensic Tool Kit (FTK). *See* FTK
(Forensic Tool Kit).
- Forensic Ultra Dock, 118
- Forensics
computer analysis, 92. *See also* Digital
forensics.
definition, 92
- Forensics workstations
accessibility of data, 425
authenticity of data, 425
computer power, 424
computer security, 424
definition, 424
features, 417
- Forensics workstations, building
*The A+ Guide to PC Hardware
Maintenance and Repair*, 423
PC Hardware Maintenance and Repair,
417
requirements, 418
Upgrading and Repairing PCs, 423
- Forensics workstations, building
(hardware)
32-bit vs. 64-bit systems, 432, 438
AMD processors, 431
DDR (dual data rate) memory,
432
dual-channel memory, 432
enclosures, 430
expansion slots, 434
front side bus, 431
hot-swap bays, 435–436
I/O ports, 437
Intel processors, 431
memory, 432–433
memory card reader, 437
memory density, 433
memory errors, 432–433
motherboards, 433–434
multicore processors, 431
permanent hard disks, 434–435
processor power, 430–431
RDRAM (Rambus Dynamic Random
Access Memory), 432
system boards, 433–434
Tableau controllers, 436
Tableau write protection
devices, 436
write-protected I/O, 436–437

- Forensics workstations, building
 - (software)
 - applications, 439
 - GIMP, 439
 - image processing, 439
 - KOffice, 439
 - Linux, 438–439
 - Office, 439
 - office suites, 439
 - OpenOffice, 439
 - operating systems, 438–439
 - OpticsPro, 439
 - Photoshop, 439
 - Windows 7, 438
 - Forensics workstations, buying
 - Digital Intelligence, 425–427
 - Forensic Computers, 428–429
 - FRED (Forensic Recovery of Evidence Device), 425–427
 - FREDDIE (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment), 425, 427
 - TriTech Forensics, 429
 - WiebeTech components, 428–429
 - Forms, samples
 - case logs, 508–509
 - chain of custody, 509
 - forensic imaging data, 510
 - photographs of physical disk, 510
 - physical disk information, 510
 - search warrants, 506
 - subpoenas, 507
 - Fourth Amendment
 - agent of the government, 25–26
 - cloud forensics issues, 301–302
 - fishing expeditions, 24
 - overview, 24–25
 - probable cause, 26
 - purpose of, 24–25
 - reasonable expectation of privacy, 26
 - unreasonable search and seizure, 25–26
 - Writs of Assistance, 24
 - FQDN (Fully Qualified Domain Name), 214–215, 514
 - Fragmented files, data carving, 146
 - Frameworks for case management, 380
 - FRCP (Federal Rules of Civil Procedure)
 - civil investigations, 9
 - disclosure (Rule 26f), 361–363
 - expert witnesses, 31
 - eyewitnesses, 31
 - role of electronic documentation (Rule 34), 358
 - FRED (Forensic Recovery of Evidence Device), 425–427
 - FREDDIE (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment), 425, 427
 - Fricosu, Ramona, 75
 - Fricosu, U.S. v.*, 75, 303
 - FROM: field, e-mail, 196–197
 - Front side bus, 431
 - Fruit of a poisonous tree, 88
 - FTK (Forensic Tool Kit)
 - case management, 383–384
 - creating timelines, 19
 - e-discovery, 370
 - EWF support, 124
 - live capture of registry entries, 331
 - FTK Imager, 118–119, 121, 295
 - FTP (File Transfer Protocol), 214
 - Fully Qualified Domain Name (FQDN), 214–215, 514
- G**
- Garbage, reasonable expectation of
 - privacy, 39, 274
 - Gargoyle, 354
 - GCEA (GIAC Certified Forensic Analyst), 443–444
 - GCFE (GIAC Certified Forensic Examiner), 443–445
 - General case documentation, 14–15
 - General warrants. *See* Writs of assistance.

- Georgia v. Randolph*, 48
Ghost partitions, 338–339
GIAC Certified Forensic Analyst (GCFA), 443–444
GIAC Certified Forensic Examiner (GCFE), 443–445
GIAC (Global Information Assurance Certification), 443
GIAC Reverse Engineering Malware, 443
GIMP (Graphics Image Manipulator Program), 439
Governance, policies and procedures, 468
GPS (Global Positioning System), 311–313
Graceful shutdown, data destruction, 143
Graff, Gayle, 47–48
Graham-Leach-Bliley Act of 1999, 61–62
Grand, Joe, 119
Grants, as revenue source, 480
Graphics Image Manipulator Program (GIMP), 439
Greenwood, California v., 39, 274
GREP
 description, 140–141
 Linux, 405
 Macintosh OSX, 406
 searching hidden data, 180–181
Group communications, e-mail searches, 207
Grouping VMs (virtual machines), 292
GSM (Global System for Mobile Communications), 310–311
Guessing passwords, 348
Guest operating systems, VMs, 291–292
Guidance Software
 certification program, 450
 detecting duplicate files, 370
 Encase Forensics, 408
 evidentiary tools, 7
 EWF (Expert Witness Format), 124
 Neutrino, 408
 Tableau controllers, 436
 write-protect interfaces, 415
Guidelines for Evidence Collection and Archiving, 112
- H**
Hagopian v. Publix Supermarkets, Inc., 362
Handling evidence. *See* Evidence handling.
Handshaking packet, 188
Hard disks
 collecting data from. *See* Data acquisition from media.
 Microsoft file system, 133–137
 permanent, 434–435
 physical disk information, sample form, 510
Hard skills, certification, 445
A Hardware-Based Memory Acquisition..., 119
Hardware inventory at crime scenes, 99–100
Hardware memory capture, 119–120
Hargrove v. Commonwealth, 21
Hash, definition, 514
Hash files, reporting, 7–8
Hash utility, 409
Hash values
 comparing, 369–370
 rolling hash, 370
Hashing the memory image, 114
HDAT2, 338
HEAD, 406
Health care, privacy legislation, 62–63
Health Insurance Portability and Accountability Act (HIPAA) of 1996, 62–63
Hearsay
 admissibility as evidence, 75–76
 definition, 514
 exceptions, 75–76
Hellman tables, 349
HELO packet, 188

- Hidden files, Recycle Bin, 142. *See also* File recovery.
 - Hidden partitions, 337–338
 - Hiding data. *See also* Covert data.
 - in an ADS (alternate data stream), 344–346
 - in bad clusters, 181–182, 339
 - common file metadata, 178
 - dark data, 336–337, 513
 - document metadata, 166–175, 178–181
 - finding hidden streams, 346
 - ghost partitions, 338–339
 - hidden partitions, 337–338
 - HPA/DCO data hiding, 338
 - HPA (Host Protected Area), 337–338
 - in metadata files, 166–172
 - partition slack, 339
 - reading, 168, 178–182
 - in the registry, 176–178
 - in slack space, 338–339
 - tools for finding, 168, 178–181, 338. *See also specific tools.*
 - warrens, 337
 - Hiding data, in the registry
 - field values, 343
 - key types, 340–341
 - registry structure, 339–341
 - tools, 342. *See also specific tools.*
 - HIPAA (Health Insurance Portability and Accountability Act) of 1996, 62–63
 - Hiring, policies and procedures, 469
 - Histogram of e-mail account activity, 206
 - History of events. *See* Timeline.
 - HKEY_USERS, Windows registry, 328–331
 - HLR (Home Locator Register), 310
 - Hooks, detecting, 117
 - Horowitz, U.S. v.*, 40
 - Horton v. California*, 77–79
 - Host operating systems, VMs, 291–292
 - Host protected area, 514
 - Hosted application management, 282
 - Hot-swap bays, 435–436
 - Howard et al., U.S. v.*, 25
 - HPA/DCO data hiding, 338
 - HPA (Host Protected Area), 337–338
 - HTML (HyperText Markup Language), 216
 - HTTP 300 message, 224
 - HTTP (Hypertext Transfer Protocol)
 - Internet addresses, 214
 - status codes, 241–242
 - HTTPERR Web server logs, 235
 - HTTPS (Hypertext Transfer Protocol Secure), 214
 - Hudson v. Michigan*, 41–42
 - Human-readable metadata vs. binary metadata, 156
 - Hybrid cloud, 279
- I**
- I/O ports, 437
 - i4i Limited Partnership v. Microsoft Corporation*, 13
 - IaaS (Infrastructure as a Service), 280–282
 - ICCID (Integrated Circuit Chip Identifier), 315
 - IDEMA (International Disk Drive Equipment and Materials Association), 139
 - Identification/assessment, 4–5
 - IDIF (iLook Default Image Format), 127
 - IDX files, 192
 - IEIF (iLook Encrypted Image Format), 127
 - IIS ODBC (Open Database Connectivity)
 - Web server logs, 234
 - IIS Web server logs, 234–235
 - IISMSID Web server logs, 235
 - iLook, 127
 - Image extraction, cell phones, 320–321
 - Image processing
 - forensic imaging data, sample form, 510

- forensics workstations, 439
- legal argument for, 123
- photographs of physical disk, sample form, 510
- IMAP (Internet Message Access Protocol), 189, 514
- IMEI (International Mobile Equipment Identity), 315–316
- Inaccessible data, 366–367, 514
- Inadvertence approach
 - authenticity of evidence, 78
 - plain view doctrine, 78
- Inadvertent discovery of child pornography, 78
- Inboxes, e-mail
 - multiple per user, 195
 - sharing, 195
- Incriminating, definition, 514
- Inculpatory, definition, 514
- Indexed Log, 242–243
- Individual characteristics of evidence, 94
- INFO file, 142
- INFO2 file, 142
- Information store, definition, 514
- Infrastructure as a Service (IaaS), 280–282
- Installed software, extracting registry history by user, 331
- Instances, 282. *See also* VMs (virtual machines).
- Integrated Circuit Chip Identifier (ICCID), 315
- Intel processors, 431
- Intelligent Computer Systems, 415
- Interception devices, 251–252
- Internal investigations
 - definition, 1, 514
 - investigation scope, 8–9
- International Disk Drive Equipment and Materials Association (IDEMA), 139
- International Mobile Equipment Identity (IMEI), 315–316
- International Society of Forensic Computer Examiners (ISFCE), 448
- Internet addresses
 - FQDM (fully qualified domain name), 214–215
 - FTP (File Transfer Protocol), 214
 - HTTP (Hypertext Transfer Protocol), 214
 - HTTPS (Hypertext Transfer Protocol Secure), 214
 - overview, 213
 - scheme, 214
 - top-level domain, 215
 - URLs (Uniform Resource Locators), 213–214
- Internet Explorer, browser history, 219
- Internet history, tools for tracing, 19
- Internet Message Access Protocol (IMAP), 189, 514
- Intrusion detection, 107
- Intrusion on seclusion or solitude, 30
- Investigation model
 - analysis, 6–7
 - collection/acquisition, 5
 - examination, 6–7
 - flowchart, 3
 - identification/assessment, 4–5
 - investigator's burden of proof, 5
 - legal documentation, listing, 4–5
 - overview, 2–4
 - preservation, 5–6
 - reporting, 7–8
- Investigation scope
 - civil investigations, 9–10
 - criminal investigations, 10–12
 - internal investigations, 8–9
- Investigation stage, case management
 - crime scene management, 385–386
 - evidence examination, 387–388
 - evidence handling, 386–387
 - first response, 384–385
 - lab preparation, 386

- Investigation stage, case management
 - (*cont'd*)
 - overview, 382–383
 - triage, 383–384
- Investigations, 1. *See also specific types.*
- Invisible file names, 141–142
- Invisible files. *See* File recovery.
- IP addresses
 - querying e-mail by, 208–210
 - spoofing, 254
- IRBF (iLook Raw Bitstream Format), 127
- ISFCE (International Society of Forensic Computer Examiners), 448
- ISPs (Internet service providers), First Amendment protection, 29. *See also* Service providers, electronic communication.
- IXimager, 127
- J**
- Jackson, Dorothy, 82
- Jarrett, U.S. v.*, 87
- JavaCool Software, 168
- Jefferson, William, 67
- Jeter v. Commonwealth*, 21
- John Doe, U.S. v.*, 75
- John the Ripper, 349
- Jurisdiction in cyberspace, 85–86
- Jurisdictional issues, cloud forensics, 285
- K**
- Katz v. U.S.*, 38, 81
- Kazeon Systems, 372
- KeeLog, 251
- Kendra D'Andrea, U.S. v.*, 88
- Kernel mode, 116, 515
- KeyCapture, 251
- Keygrabber Wi-Fi, 251
- Keyloggers
 - definition, 515
 - proactive evidence collection, 251–252
- Keystrokes, recording, 251–252
- Keyword searches, e-mail, 205
- Kill switch on targeted equipment, 41–42
- Kirk, Paul L., 93
- Knock and announce rule, 41
- Knowledge of possession, 222–224
- KOffice, 439
- Kornblum, Jesse, 271
- L**
- Lab preparation, 386
- Laptop computer, as forensic tool, 419
- Laser printers, retrieving evidence from, 100
- Latent evidence, 94
- Laws. *See* Constitution of the United States; Privacy legislation; *specific laws.*
- LBD (Long Block Data) standard, 139–140
- LDE (Linux Disk Editor), 405
- LDF (log data file), 298
- Least significant bit (LSB) insertion, steganography, 351
- Legal aspects of investigations. *See* Constitution of the United States; Privacy legislation; *specific issues.*
- Legal/ethical issues of starting a forensics shop, 471–472
- Legislation. *See* Constitution of the United States; Privacy legislation; *specific legislation.*
- Licensing, 452–453. *See also* Certification.
- Linux, forensics workstations, 438–439
- Linux, tools
 - DD (Disk Dump), 405
 - GREP, 405
 - LDE (Linux Disk Editor), 405
 - overview, 404–405
 - PhotoRec, 405–406
 - suites, 407
- Litigation, definition, 515

- Litigation hold
 - definition, 515
 - e-discovery, 362–363
 - Live acquisition, Web servers, 233–234
 - Live connection information, 261–262
 - Live response, 113–115. *See also* Data acquisition from memory.
 - LiveJournal, 29
 - Locard's exchange principle, 93
 - Lockdown, 408
 - Log files. *See also* Web server logs.
 - definition, 515
 - investigation, creating, 118–119
 - Log files, post-incident evidence collection
 - antivirus logs, 267–268
 - application logs, 263, 264–268
 - AVG Antivirus logs, 268
 - database activity logs, 266
 - DNS logs, 266–267
 - ERRORLOG file, 266
 - event logs, 263–264
 - log.trc file, 266
 - McAfee Antivirus logs, 267–268
 - overview, 262
 - security logs, 264, 265
 - SQL Server Agent log, 266
 - SQL Server Error log, 266
 - SQL Server Profile log, 266
 - SQLAGENT.OUT file, 266
 - Symantec Antivirus logs, 267
 - system logs, 263–264
 - Log Parser 2.2, 236
 - \$LogFile metadata file, 136
 - Logging per server, 238
 - Logicube, 119
 - LogParser, 342
 - Logs
 - database transaction logs, 298
 - LDF (log data file), 298
 - Windows, 403–404
 - Log.trc file, 266
 - Long Block Data (LBD) standard, 139–140
 - Longevity of digital evidence, 95
 - Lossless
 - abstraction layers, 399
 - definition, 515
 - steganography compression, 350
 - Lossy
 - abstraction layers, 399
 - definition, 515
 - steganography compression, 350
 - Lost files. *See* File recovery.
 - Lovell v. City of Griffin*, 28
 - LSB (least significant bit) insertion, steganography, 351
 - Lyons, U.S. v.*, 39
- ## M
- MAC (modify, access, create) file data
 - ~fls utility, 163
 - access attribute, 160
 - analysis tool, 163
 - body file, 163
 - create attribute, 159–160
 - creating a timeline, 19
 - definition, 515
 - DM (document management) systems, 164
 - EM (entry modified) attribute, 160–162
 - file creation time stamp, 159–160
 - investigative uses for, 162–164
 - last access time stamp, 160
 - last modification time stamp, 160–162
 - metadata, 159–162
 - modifying attribute, 160
 - protecting, 121, 159
 - The Sleuth Kit, 163
 - time stamps, viewing, 161–162
 - timeline creation, 163
 - Macintosh OSX, tools
 - Finder, 406
 - GREP, 406

- Macintosh OSX, tools (*cont'd*)
 - HEAD, 406
 - overview, 406
 - Spotlight, 406–407
- MACTime, 19
- Magic numbers, 157
- Mail delivery agent (MDA), 186, 515
- Mail folders, 191
- Mail transport agent (MTA), 186, 515
- Mail user agent (MUA), 186, 515
- Malware, detecting, 227
- Mancusi v. DeForte*, 49
- Mandiant Systems, 117
- Mann, U.S. v.*, 78
- Mapp v. Ohio*, 44–45
- Maresware, 354
- Masking, steganography, 351
- Master database file (MDF), 296, 298–299
- Master File Table (MFT), 135, 144, 223, 332–335
- Master node, 137–138
- Material evidence, 72
- Matlock, U.S. v.*, 47–48, 81
- .mbx files, 192
- MBX files, 192
- .mbx folders, 191
- McAfee Antivirus logs, 267–268
- McFadden, Martin, 45
- McKeever, U.S. v.*, 102
- McKeever Test for evidence handling, 102
- MD5 hash
 - calculating, 118
 - definition, 515
- MDA (mail delivery agent), 186, 515
- MDF (master database file), 296, 298–299
- Measured service, cloud computing, 278
- MEID (mobile equipment identifier), 315–316
- mem command, 114–115
- Memory
 - acquiring data from. *See* Data acquisition from memory.
 - cell phones, 313–315
 - density, 433
 - as a device, 116
 - errors, 432–433
 - forensics workstations, 432–433
 - system *vs.* addressable, 114–115
- Memory card reader, 437
- Memory Grabber Forensic Tool, 119
- Memoryze, 117
- Messages, steganography, 351
- Metadata. *See also* Documents, metadata; File metadata; Temporary files.
 - British Government incident, 167–168
 - definition, 515
 - deleted documents, proving existence of, 159–162
 - vs.* documents, cloud forensics, 285
 - MAC data, 159–162
 - OS, value of, 159–162
 - overview, 157–158
 - timeline research, 159–162
 - UNIX/Linux file systems, 137–138
 - viewing, 165–170
- Metadata, types of
 - embedded, 164–172
 - substantive, 164–172
 - summary, 158. *See also specific types.*
 - system, 158–164
- Metadata Analyzer, 181
- Metadata Extraction Tool, 178
- Metadata files
 - hidden data, 166–172
 - overview, 135–137
 - tools, 135
- Metadiscover, 408
- Metasploit, 182, 274, 338
- Metaviewer, 409
- Metrics for software tools, 400
- MFCE (Mobile Forensics Certified Examiner), 448–449
- MFI (Mobile Forensics, Inc.), 448–449
- MFT attributes, 153–155

- MFT (Master File Table), 135, 144, 223, 332–335
- MFT metadata, effects of deleting files, 229
- \$Mft metadata file, 135–136
- \$MftMirr metadata file, 136
- MHDD, 338
- Micro-SIM cards, 314
- Microsoft file systems
- 8.3 file names, 134
 - \$BadClus metadata file, 135–136
 - clusters, 133, 138–140
 - FAT12, 133–134
 - FAT16, 134, 141–142
 - FAT32, 134–135
 - File Allocation Tables, 133–135
 - file names, 134
 - floppy disks, 133–134
 - hard disks, 133–137
 - IDEMA (International Disk Drive Equipment and Materials Association), 139
 - LBD (Long Block Data) standard, 139–140
 - metadata files, 135–137
 - MFT (Master File Table), 135, 144
 - \$Mft metadata file, 135–136
 - NTFS, 135–137
 - overview, 132–133
 - partitions, 132–133
 - sectors, 132–133, 139
 - slack space, description, 138–140
 - slack space *vs.* unallocated space, 140
 - storage devices, layout, 132–133
 - summary of, 132
 - from unallocated space, 140
- Microsoft products. *See specific products.*
- Miller, U.S. v.*, 302
- MIME headers, 197–202
- MIME (Multipurpose Internet Mail Extensions), 196, 515
- Mini-SIM cards, 314
- Minus sign (-), Boolean operator, 205
- Mnemonics as passwords, 349
- Mobile devices, forensics. *See also specific devices.*
- in civil cases, 323–324
 - exigent circumstances, 323
 - legal aspects, 322–324
 - overview, 307–308
 - presumption of ownership, 323–324
 - search and seizure laws, 322–323
- Mobile equipment identifier (MEID), 315–316
- Mobile Forensics, Inc. (MFI), 448–449
- Mobile Forensics Certified Examiner (MFCE), 448–449
- Mobile Switching Center (MSC), 310
- Modify, access, create (MAC) file data.
See MAC (modify, access, create) file data.
- Modifying attribute, 160
- MoonSols toolkit, 118
- Most, U.S. v.*, 40
- Most recently used (MRU) files,
extracting registry history, 328–331
- Most recently used (MRU) sites, Web browsers, 217
- Motherboards, 433–434
- MRU (most recently used) files,
extracting registry history, 328–331
- MRU (most recently used) sites, Web browsers, 217
- MSC (Mobile Switching Center), 310
- MTA (mail transport agent), 186, 515
- MUA (mail user agent), 186, 515
- Multicore processors, 431
- Multiple users on a computer,
authenticity of evidence, 80–81, 83
- Multipurpose Internet Mail Extensions (MIME), 196, 515

N

- National Library of New Zealand, 178
- Native format, 374

- NCH files, 192
- NCSA (Common Log) Web server logs, 234
- Near-line data, 366–367
- Near-native format, 374
- NEAR operator, 205
- net sessions command, 262
- net share command, 262
- net use command, 262
- Netcat, 118
- Netstat, definition, 516
- netstat command, 262
- netstats.txt file, 261–262
- Network connections, listing, 262
- Network forensics, Windows tools, 403–404
- Network Instruments, 255
- Network interface cards (NICs), promiscuous mode, 257
- Network Monitor, 255–256
- Network search. *See also* Virtual networking.
 - overview, 247–248
 - response plan objectives, 250
 - scope assessment, 248–250
- Network search, evidence collection
 - overview, 250–251
 - types of, 250–251
- Network search, post-incident evidence collection
 - antivirus logs, 267–268
 - application logs, 263, 264–268
 - AVG Antivirus logs, 268
 - database activity logs, 266
 - DNS logs, 266–267
 - ERRORLOG file, 266
 - event logs, 263–264
 - log.trc file, 266
 - McAfee Antivirus logs, 267–268
 - overview, 262
 - security logs, 264, 265
 - SQL Server Agent log, 266
 - SQL Server Error log, 266
 - SQL Server Profile log, 266
 - SQLAGENT.OUT file, 266
 - Symantec Antivirus logs, 267
 - system logs, 263–264
- Network search, proactive evidence collection
 - acquisition window, 255
 - altering the source IP, 254
 - anonymous remailers, 254
 - authenticity, verifying, 254–255
 - blanket search, 252
 - collecting passwords, 251
 - consent exception, 252
 - DNS cache poisoning, 254
 - interception devices, 251
 - IP spoofing, 254
 - keyloggers, 251–252
 - live connection information, 261–262
 - net sessions command, 262
 - net share command, 262
 - net use command, 262
 - netstat command, 262
 - netstats.txt file, 261–262
 - network capture, 254–262
 - network connections, listing, 262
 - onion routing, 254
 - Ordinary Course of Business* exception, 252
 - password requirements, modifying, 262
 - promiscuous mode, 257
 - recording keystrokes, 251–252
 - sessionizing, 257
 - shared resources, listing, 262
 - system auditing, 252–254
 - tapping private computers, 252
 - tools, 251, 255–256. *See also specific tools.*
 - traffic, identifying, 255–257

- Network search, router and switch
 forensics
 analyzing data, 273–275
 Cisco routers, 271–273
 command history, listing, 272
 commands, 271, 272
 #copy startupconfig tftp command, 272
 #dir slot command, 272
 flash disk files, displaying, 272
 flash RAM, 272–273
 nonvolatile information, collecting, 272–273
 nonvolatile information, definition, 269
 NVRAM (Nonvolatile Random Access Memory), 272
 overview, 268–269
 router interfaces, 269–270
 #show history command, 272
 #show users command, 272
 startup configuration, copying, 272
 tools, 271–272, 274. *See also specific tools.*
 users, listing, 272
 volatile information, collecting, 270–272
 volatile information, definition, 268–269
 WHOIS query, 273–275
- Networked computers, evidence handling, 104
- Neutrino, 408
- nfi, 334–335
- Nicodema S. Scarfo et al., U.S. v.*, 252
- NICs (network interface cards), promiscuous mode, 257
- Nirsoft, 219–220
- No-knock warrants
 definition, 516
 description, 41–42
 knock and announce rule, 41
- Nodes, 292
- Nonprofit organizations, as revenue source, 479–480
- Nonvolatile information
 collecting, 272–273
 definition, 269
- NOT operator, 205
- Notepad++, loading registry file, 343
- Novell log files. *See* Proxy server logs, Novell.
- NSLookup, 516
- nslookup command, 208–209
- NTFS, 135–137
- NTFS attributes, 154
- NTFS metafiles, 333
- Null cipher
 definition, 516
 steganography, 354
- NVRAM files, 293
- NVRAM (Nonvolatile Random Access Memory), router and switch forensics, 272
- NWAdmin, 243
- O**
- Observer, 255
- O'Connor v. Ortega, 324
- ODBC, 243
- Off-line storage, 366–367
- Office, 439
- Office suites, 439
- Offsets, 125, 516
- Oliver v. U.S.*, 39
- Omnibus Control and Safe Streets Act of 1968, 58
- OmniPeek, 255–256
- On-demand service, cloud computing, 278
- Onion routing, 254
- Open Database Connectivity (IIS ODBC) Web server logs, 234
- Open source tools, 408–410

- OpenOffice, 439
- Operating systems, forensics
 - workstations, 438–439
- Opinions as evidence, 73–74
- OpticsPro, 439
- OR operator, 204
- Oracle, 292
- Order of volatility, data acquisition, 112
- Ordinary Course of Business exception, 252
- Ortiz, U.S. v.*, 322
- OS metadata, value of, 159–162
- OS utilities, 401
- O’Scannlain, Diarmuid F., 49
- Ostensible authority
 - definition, 516
 - description, 49
- Outgoing messages, 188
- Outlook
 - overview, 193
 - PST files, 193
 - version history, 194
- Outlook Express
 - CLSID (content class identifier), 192
 - .dbx files, 192–193
 - DBX files, 192–193
 - file formats, 192
 - IDX files, 192
 - .mbx files, 192
 - MBX files, 192
 - NCH files, 192
 - overview, 192
 - version history, 192
- Outsourcing, 478–479
- P**
- P2 Commander, 331, 408
- P2 Explorer, 328
- P2P (peer to peer) networking, 288
- PaaS (Platform as a Service), 284
- Packaging evidence, 105
- Paraben Certified Forensic Examiner (PCFE), 452
- Paraben Certified Mobile Examiner (PCME), 452
- Paraben Software
 - certification program, 451–452
 - Decryption Collection, 408
 - Device Seizure, 321
 - Eclipse, 320
 - Forensic Replicator, 328, 408
 - Lockdown, 408
 - P2 Commander, 331, 408
 - P2 Explorer, 328
 - Project-A-Phone, 320
 - Registry Analyzer, 178
 - Save-A-Phone, 321
 - StrongHold pouch, 319
- Parse, definition, 516
- Particularity
 - definition, 516
 - search, 84
 - search warrant requirements, 36
- Partition slack, 339
- Partitions
 - definition, 516
 - ghost, 338–339
 - hidden, 337–338
 - Microsoft file system, 132–133
- Pasco, 221
- Password cracking
 - @ (at sign) in, 349
 - brute-force attacks, 349
 - cracking algorithms, 349
 - e-mail addresses as, 349
 - guessing, 348
 - Hellman tables, 349
 - mnemonics as, 349
 - rainbow tables, 349
 - recovering from media, 122
 - tools, 349
- Password-encoded accounts, authenticity
 - of evidence, 80–81, 88
- Passwords
 - cell phone, extracting, 320–321

- collecting during proactive evidence collection, 251
- concealed at a crime scene, 100
- encryption, 348–350
- Fifth Amendment protection, 27, 303
- forced surrender of, 303
- multiple user access to, 284
- requirements, modifying, 262
- Patent evidence, 94
- Patriot Act, sneak and peek warrants, 42
- Payton v. New York*, 38
- PC Hardware Maintenance and Repair*, 417
- PCFE (Paraben Certified Forensic Examiner), 452
- PCME (Paraben Certified Mobile Examiner), 452
- PCs for forensics work. *See* Forensics workstations.
- Pedophiles. *See also* Child pornography.
 - exposed by vigilantes, 88
 - on LiveJournal, 29
 - private citizens searching for, 88
- Peer to peer (P2P) networking, 288
- PendMoves, 404
- Personal property, warrantless searches, 47–48
- Personnel, starting a forensics shop, 472–473
- Perverved Justice, 88
- PG Pinpoint, 408
- Phone companies. *See* Service providers, electronic communication.
- Photographing evidence, 104
- PhotoRec, 405–406
- Photoshop, 439
- Physical disk information, sample form, 510
- Physical disk photographs, sample form, 510
- Physical evidence *vs.* digital, 94–96
- Physician/patient privilege, 64–65
- PII (personally identifiable information)
 - definition, 516
 - handling, 473
- PIN (personal identification number)
 - cell phones, 314
 - description, 314
 - unlocking, 315, 320–321
- Pin unlock key (PUK), 314
- Pinpoint Labs
 - Metadiscover, 408
 - PG Pinpoint, 408
 - SafeCopy, 408
- Pinpoint Tools
 - Filematch, 409
 - Hash, 409
 - Metaviewer, 409
 - Safecopy, 409
- Piping commands, 124
- Pirated intellectual property, 29
- Pivotal Guidance, 409
- Plain view doctrine
 - applied to computers, 43–44
 - authenticity of evidence, 77–79
 - computers as containers, 79
 - definition, 516
 - description, 43–44
 - exception to reasonable expectation of privacy, 39
 - inadvertence approach, 78
 - overview, 77
 - prophylactic test, 78–79
 - search and seizure, 37
 - search warrants, 43–44
- Plaintiff
 - in civil cases, 1
 - in criminal cases, 1
 - definition, 517
 - as stakeholder, 12
- Platform as a Service (PaaS), 284
- Plus sign (+), Boolean operator, 205
- PMBOK (Project Management Book of Knowledge)*, 14

- PMI (Project Management Institute), 14
- Policies and procedures, in a forensics shop
 - accepting assignments, 469
 - data retention, 471–472
 - evidence handling, 470
 - governance, 468
 - hiring, 469
 - overview, 466–468
 - procedural policies, 470
 - reporting, 470–471
 - training, 469
- Pop-up bombs, 224
- POP3 (Post Office Protocol 3), 188–189, 517
- Port 25, e-mail protocols, 188
- Port 143, e-mail protocols, 189
- Port replicator, 122
- Post-incident evidence collection. *See* Network search, post-incident evidence collection.
- Powering off devices
 - destroying data during graceful shutdown, 143
 - with encryption, 348
 - evidence handling, 103–104
 - pulling the plug, 143
- Precision, e-mail searches, 206
- Prejudiced, definition, 517
- Prejudicial of evidence, 74, 517
- Preparation stage, case management, 381–382
- Present possession concept, 222
- Presenting results, case management, 388–389
- Preservation
 - description, 5–6
 - e-discovery, 368–369
- Preservation orders
 - definition, 517
 - description, 59
 - for documents, 164
 - e-discovery, 362–363
- Press, definition of, 28
- Presslock evidence bags, 421
- Pretexting provision, 62
- Privacy, right to
 - appropriation of name or likeness, 30
 - in the Constitution of the United States, 29–30
 - embarrassing public disclosure, 30
 - false publicity, 30
 - film cameras as threat to, 30
 - individual, 30
 - intrusion on seclusion or solitude, 30
 - laws restricting, 30
 - legal precedence for, 29–30
 - “Privacy,” 30
 - The Right to Privacy*, 30
 - seclusion and solitude tort, 30
- “Privacy,” 30
- The Privacy Act of 1974, 56–58
- Privacy legislation. *See also* Reasonable expectation of privacy.
 - education, 63–64
 - FERPA (Family Educational Rights and Privacy Act) of 2008, 63–64
 - health care, 62–63
 - HIPAA (Health Insurance Portability and Accountability Act) of 1996, 62–63
 - rights covered in the Constitution, 29–30, 55
 - student information, 63–64
- Privacy legislation, financial
 - CRA (Consumer Reporting Agencies), guidelines for, 60
 - credit reports, 60
 - debt collection, 62
 - electronic discovery, 61–62
 - Fair Credit Reporting Act of 1970, 60
 - FDPA (Fair Debt Collection Practices Act of 2006), 62
 - Graham-Leach-Bliley Act of 1999, 61–62

- overview, 59
- pretexting provision, 62
- Right to Financial Privacy Act of 1978, 60–61
- The Safeguards Act, 61–62
- Privacy legislation, general privacy
 - audit trails, 57
 - ECPA (Electronic Communications Privacy Act of 1986), 58–59
 - ECS (Electronic Communications Services), 58
 - Omnibus Control and Safe Streets Act of 1968, 58
 - overview, 56
 - The Privacy Act of 1974, 56–58
 - private communications over electronic media, 58–59
 - RCS (Remote Computing Services), 58
 - SCA (Stored Communication Act), 58
 - Wiretap Act, 58
- Privacy legislation, privileged information
 - attorney/client privilege, 64–65
 - exceptions to, 66
 - identifying, 66–67
 - overview, 64
 - physician/patient privilege, 64–65
 - protective orders, 66
 - taint teams, 66–67
 - work/product doctrine, 65–66
- Private citizens performing searches
 - vs. agents of the government, 38
 - Artists Against 419, 88
 - constitutional limitations, 86–87
 - fruit of a poisonous tree, 88
 - legality of warrants, 87–88
 - limits of the Constitution, 86–87
 - for pedophiles, 88
 - Perverved Justice, 88
 - for scam artists, 88
 - “wink and the nod” approach, 87
- Private cloud, 278–279
- Private communications over electronic media, privacy legislation, 58–59
- Private investigators, as agents of the government, 25–26
- Private sector organizations
 - reasonable expectation of privacy, 49
 - warrantless searches, 48–49
- Privileged information. *See also* Privacy legislation, privileged information.
 - definition, 517
 - as evidence, 74–75
- Proactive evidence collection. *See* Network search, proactive evidence collection.
- Probable cause
 - definition, 26, 517
 - ex ante* (before the fact) action, 26
 - in the Fourth Amendment, 26
 - search warrants, 36
 - warrantless searches, 26, 46
- Probitive evidence, 72
- Procedural documentation, 15–18
- Process documentation, 18
- Processes, acquiring data from. *See* Data acquisition from memory.
- Processor power, forensics workstations, 430–431
- Prodiscover, 127–128
- Product testing, 475
- Project-A-Phone device, 320
- Project management, documentation, 13
- Project Management Book of Knowledge (PMBOK)*, 14
- Project Management Institute (PMI), 14
- Promiscuous mode, 257, 517
- Prophylactic test, 78–79
- Prosser, William, 30
- Protected mode, Web browsers, 219
- Protecting non-targeted information, 290–291
- Protective orders
 - definition, 517
 - privacy legislation, 66

Proxy, definition, 517

Proxy server logs

- access log, 243
- cache log, 243
- configuration log, 243
- file formats, 239
- file naming conventions, 239
- Squid, 243

Proxy server logs, analyzing

- Sawmill utility, 244
- tools, 243–244
- WebTrends utility, 243

Proxy server logs, Novell

- BUTIL utility, 243
- Common Log fields, 240
- CSAUDIT utility, 243
- Extended Log fields, 242
- HTTP status codes, 241–242
- Indexed Log, 242–243
- NWAdmin utility, 243
- ODBC utility, 243
- tools, 243

Proxy servers. *See also* Web servers.

- overview, 238
- purpose of, 238

PSFile, 404

PSList, 404

PSService, 404

PST files, 193

.pst folders, 191

Public cloud, 279

Public sector organizations, warrantless

- searches, 49–50

PUK (pin unlock key), 314

Putting VMs to sleep, 294–295

PyFlag, 124

Q

Quashing subpoenas, 36–37, 51

Quon, City of Ontario, California v., 324

R

Radio frequency isolation, 318–319

Rainbow tables, 349, 517

Rakas v. Illinois, 39

RAM (random access memory), 315

Ramses IX, ancient case document, 379

Rangwala, Glen, 168

RAT (Router Audit Tool), 272

RCS (Remote Computing Services), 58

RDRAM (Rambus Dynamic Random Access Memory), 432

RE: prefix, e-mail, 197

Real-time monitoring, cloud forensics, 291

Reasonable anticipation of litigation, 362

Reasonable expectation of privacy. *See also* Privacy legislation.

- case law, 38–39
- closed container clause, 38–39
- cloud forensics, 302
- definition, 517
- examples, 38–39
- factors determining, 38
- in the Fourth Amendment, 26
- garbage, 39, 274
- law enforcement exceptions, 57
- multiple users on a computer, 80–81, 83
- non-U.S. citizens, 57
- password-encoded accounts, 80–81, 88
- plain view exception, 39
- in private sector organizations, 49
- right to sue violators, 57–58
- searches, 38
- society's acceptance, 38–39
- stored electronic information in the hands of a third party, 39–40

Recall, e-mail searches, 206

Recipient frequency, e-mail

- searches, 207

Recording keystrokes, 251–252

Records, Computers, and the Rights of Citizens, 56

- Recovering files or data. *See* Data recovery; File recovery.
- Recycle Bin. *See also* Deleted files; File recovery.
deleting files, 142
for multiple users, 144–145
subdirectories, 144–145
- \$Recycle Bin file, 144
- Redaction, 376, 518
- Redirects, 224–225
- Redundant pattern encoding,
steganography, 351
- regedit (registry editor), 402–403
- Registry
accessing, 225
browser history analysis, 225–226
hidden data, 176–178
- Registry, extracting history from
deleted applications, 330
HKEY_USERS, Windows registry,
328–331
installed software, by user, 331
listing users, 328–331
MRU (most recently used) files,
328–331
SID (Security Identifier), 329
tools, 331. *See also specific tools.*
- Registry, hiding data in
field values, 343
key types, 340–341
registry structure, 339–341
tools, 342. *See also specific tools.*
- Registry Analyzer, 178
- RegRipper, 331
- Reiser file system, 137
- Relevance
definition, 518
digital evidence, 96
- Relevant, definition, 518
- Relevant evidence, 72
- Reliability of digital evidence, 95
- Remote Computing Services (RCS), 58
- Report writing, contents, 389–390
- Report writing, structure
acquisition and preparation, 391–392
case summary, 391
conclusion, 392–393
findings, 392
overview, 390–391
- Reporting. *See also* Documentation.
description, 7–8
hash files, 7–8
policies and procedures, 470–471
software for cell phones, 321
- Resource pooling, cloud
computing, 278
- Revenue sources. *See also* Costs.
corporate departments, 480–481
for-profit organizations, 478–479
grants, 480
nonprofit organizations, 479–480
outsourcing, 478–479
overview, 478
- Reviewing potential data, 372–373
- Revision history, viewing, 168, 170–171
- Reyes, U.S. v.*, 39
- Right to Financial Privacy Act of 1978,
60–61
- Right to privacy
appropriation of name or likeness, 30
in the Constitution of the United
States, 29–30
embarrassing public disclosure, 30
false publicity, 30
film cameras as threat to, 30
individual, 30
intrusion on seclusion or solitude, 30
laws restricting, 30
legal precedence for, 30
“Privacy,” 30
The Right to Privacy, 30
seclusion and solitude tort, 30

- The Right to Privacy, 30
- Riverbed, 255
- Rodriguez, U.S. v.*, 251
- Rodriquez, Illinois v.*, 82–83
- Rolling hash, 370
- Rolling review, 372–373
- ROM (read-only memory), 315
- RootkitRevealer, 404
- Rootkits
 - definition, 114
 - detecting, 114, 117
- Ross, U.S. v.*, 38
- Rotating logs, 237
- Router Audit Tool (RAT), 272
- Router forensics. *See* Network search, router and switch forensics.
- Router interfaces, 269–270
- Royal & Sunalliance ... v. Lauderdale Marine Center*, 362
- Runtime
 - Captain Nemo, 409
 - Disk Explorer for FAT, 409
 - Disk Explorer for NTFS, 409
 - DriveImageXL, 409
 - DriveLook, 409
- S**
- SaaS (Software as a Service), 282–284
- Safeback, 126–127
- SafeCard Services, Inc. v. SEC*, 366
- SafeCopy, 408–409
- The Safeguards Act, 61–62
- Salgado, U.S. v.*, 323
- Save-A-Phone product, 321
- Sawmill, 244
- SCA (Stored Communication Act), 58
- Scalpel, 149
- Scam artists, private citizens searching for, 88
- Scan once/print many devices, 99
- Schemes
 - definition, 518
 - Internet addresses, 214
- Schneckloth v. Bustamonte, 47
- Scope of search. *See also* Breadth of search.
 - defining, 84
 - definition, 518
 - e-discovery, 362
- Scope of the investigation. *See* Investigation scope.
- Screen capture, cell phones, 320
- Search, definition, 37, 518
- Search, legal bounds. *See also* Warrantless searches.
 - breadth, 84
 - defining the scope, 84
 - exceeding the scope of the warrant, 38
 - particularity, 84
 - performed by a private citizen. *See* Private citizens performing searches.
 - reasonable expectation of privacy, 38
 - specificity, 84
- Search and seizure. *See also* Unreasonable search and seizure.
 - fishing expeditions, 24
 - mobile device forensics, 322–323
 - offices of the press, 28
 - plain view doctrine, 37
 - sequence of events, 27
- Search incident to arrest (SITA), cell phones, 317
- Search processes, e-discovery, 363–364
- Search protocols, 43–44
- Search warrants
 - affidavits, 36, 40
 - after-hours, 41
 - after hours, 511
 - definition, 36, 520
 - documenting execution of, 41
 - e-mail searches, 203
 - exception to requiring. *See* Plain view doctrine.

- general. *See* Writs of assistance.
obtaining, 40–41
for offices of the press, 28
particularity requirements, 36
plain view doctrine, 43–44
private citizens performing searches,
87–88
probable cause, 36
sample form, 506
vs. subpoenas, 36–37
- Search warrants, no-knock
definition, 516
description, 41–42
knock and announce rule, 41
- Search warrants, sneak and peek
definition, 518
delayed notice, 42
description, 42
Patriot Act provisions, 42
third-party assistance, 42
- Searching. *See* E-mail searches.
- Searching and Seizing Computers...,
64–65, 67
- Seclusion and solitude tort, 30
- Sectors
definition, 518
Microsoft file system, 132–133,
139
- Secure evidence storage facilities, 107
- Secure Hash Algorithm
256-bit (SHA256), 518
512-bit (SHA512), 518
- \$Secure metadata file, 136
- Security
forensics workstations, 424
of potential data, 372–373
- Security logs, 264, 265
- Seizure, 37, 518. *See also* Search and
seizure.
- Server logs. *See* Proxy server logs; Web
server logs.
- Servers. *See* E-mail information stores,
e-mail servers; Proxy servers; Web
servers.
- Service providers, electronic
communication. *See also* ISPs
(Internet service providers).
basic subscriber information, 58
categories of customer information,
58–59
content information, 59
customer records, 58
legislation affecting, 58–59
preservation orders, 59
voluntary release of information, 59
- Serving subpoenas, 50
- Sessionizing evidence collection, 257, 518
- SHA1 hash, calculating, 118
- Shared resources, listing, 262
- #show history command, 272
- #show users command, 272
- Shred, 108
- SID (Security Identifier), 329
- Signatures, steganography, 354
- SilentRunner, 408
- SIM cards, 313–315, 320
- SIM (Subscriber Identity Module) cards,
313–315, 518
- Similar users, e-mail searches, 206
- SIMless phones, 314
- Simons, U.S. v.*, 50, 252
- Simple Mail Transport Protocol (SMTP),
188
- Single sign-on (SSO) security, 283
- SITA (search incident to arrest), cell
phones, 317
- 64-bit *vs.* 32-bit forensics workstations,
432, 438
- Slack space
definition, 518
description, 138–140
hiding data, 338–339

- Slack space (*cont'd*)
 - recovering data from. *See* Data carving.
 - vs. unallocated space, 140
- Slacker, 338
- The Sleuth Kit
 - browser history analysis, 220
 - for evidentiary use, 7
 - timelines from MAC data, 163
- Smart cards, encryption, 347
- Smart PC Solutions, 181
- SmartCarving, 146
- Smear images, 116
- SMTP (Simple Mail Transport Protocol), 188
- Snapshots, virtual machines, 294–295
- Sneak and peek warrants
 - definition, 518
 - delayed notice, 42
 - description, 42
 - Patriot Act provisions, 42
 - third-party assistance, 42
- Societal recognition of privacy, 38–39, 81
- Soft skills, certification, 445
- Software as a Service (SaaS), 282–284
- Software change control, 477–478
- Software memory capture, 117–119. *See also* Data acquisition from memory and running processes.
- Sorting records, browser history analysis, 221
- Specificity, search, 84
- Spoilation
 - definition, 518
 - e-discovery, 361, 362–363
- Spoofing
 - e-mail addresses, 188
 - IP addresses, 254
- Spotlight, 406–407
- SQL MDF viewer, 298
- SQL Server Agent log, 266
- SQL Server Error log, 266
- SQL Server Profile log, 266
- SQLAGENT.OUT file, 266
- SQUID, 519
- Squid proxy server, 243
- ssdeep fuzzy hashing algorithm, 370
- SSO (single sign-on) security, 283
- Stability of digital evidence, 95
- Stakeholders
 - accused, 12
 - accuser, 12
 - definition, 12, 519
 - identifying, 12–13
- Standalone computers, evidence
 - handling, 103–104
- Starting a shop
 - legal/ethical issues, 471–472
 - organizational certification, 481–483
 - personnel, 472–473
 - PII (personally identifiable information), handling, 473
- Starting a shop, building from scratch
 - cost justification, 480–481
 - estimating startup costs, 462–466
 - facilities improvement costs, 466
 - factors to consider, 458–459
 - hardware acquisition costs, 463–464
 - logistics of building, 460–462
 - operational planning aspects, 461–462
 - preplanning, 459
 - scope of services, 460
 - software acquisition costs, 464–466
- Starting a shop, change control
 - business change, 476–477
 - software change, 477–478
- Starting a shop, policies and procedures
 - accepting assignments, 469
 - data retention, 471–472
 - evidence handling, 470
 - governance, 468
 - hiring, 469
 - overview, 466–468
 - procedural policies, 470

- reporting, 470–471
- training, 469
- Starting a shop, revenue sources
 - corporate departments, 480–481
 - for-profit organizations, 478–479
 - grants, 480
 - nonprofit organizations, 479–480
 - outsourcing, 478–479
 - overview, 478
- Starting a shop, technology management
 - adding new technology, 475–476
 - choosing equipment, 474
 - product testing, 475
 - support infrastructure, 474–475
- Startup configuration, copying for router
 - and switch forensics, 272
- Stateful applications, 289
- Stateless applications, 289
- Statements requesting a warrant. *See* Affidavits.
- Stationary user profiles, 206
- StegAlyzer AS, 354
- StegAlyzer SS, 354
- Steganografia, 350
- Steganography
 - algorithms, 351
 - carriers, 351
 - cover files, 351
 - definition, 519
 - detecting, 354
 - dictionary attacks, 354
 - filtering, 351
 - lossless compression, 350
 - lossy compression, 350
 - LSB (least significant bit) insertion, 351
 - masking, 351
 - messages, 351
 - methodology, 350–351
 - null cipher, 354
 - overview, 350
 - redundant pattern encoding, 351
 - signatures, 354
 - stegoimage, 351
 - stegokey, 351
 - tools, 351–354
 - transformations, 351
- StegBreak, 354
- StegDetect, 354
- Stego Watch, 354
- Stegoimage, 351
- Stegokey, 351
- Storage device layout, Microsoft file system, 132–133
- Storage models, cloud forensics, 287–288
- Stored Communication Act (SCA), 58
- Storing
 - digital media, 103
 - evidence, 106–107
- streams, 346, 519
- Streams, 404
- string (Linux utility), 180
- String search, file system metadata, 333
- Strings (of text), recovering, 140–141
- strings (Windows utility)
 - description, 404
 - reading hidden data, 178–181
 - wildcard searches, 180
- StrongHold pouch, 319
- Student information, privacy legislation, 63–64
- SUBJECT: field, e-mail, 196–197
- Subjective expectation of privacy, 81
- Subpoena duces tecum
 - definition, 519
 - description, 36
- Subpoenas
 - definition, 36, 519
 - federal vs. state, 37
 - for journalists, 28
 - to produce materials. *See* Subpoena duces tecum.
 - proposing alternate conditions, 51
 - purpose of, 54

- Subpoenas (*cont'd*)
 - quashing, 36–37, 51
 - rules for issuing, serving, and executing, 50
 - sample form, 507
 - serving, 50
 - vs. warrants, 36
- Subscriber Identity Module (SIM) cards, 313–315, 518
- Substantive metadata, 164–172
- Superblocks, UNIX/Linux file systems, 137–138
- Switch forensics. *See* Network search, router and switch forensics.
- Syba I/O panels, 437
- Symantec Antivirus logs, 267
- SysInternals, 404
- SYSINTERNALS suite, 346
- System auditing, proactive evidence collection, 252–254
- System boards, 433–434
- System logs, 263–264
- System memory vs. addressable, 114–115
- System metadata, 158–164
- System Research and Application Corporation, 119
- Systools, 298
- T**
- Tableau controllers, 436
- Tableau write protection devices, 436
- TAC (Type Allocation Code), 316
- Taint teams, 66–67, 519
- Tapping private computers, 252
- Tarasoff v. Regents of the University of California, 65
- TDMA (Time Division Multiple Access), 310–311
- Teams, case management, 382. *See also* Taint teams.
- Teams of virtual machines, 292
- Technician's toolkit, 414
- Technology management
 - adding new technology, 475–476
 - choosing equipment, 474
 - product testing, 475
 - support infrastructure, 474–475
- Technology Pathways, 127
- Templates, documentation, 16–17
- Temporary files
 - artifact destruction, 335–336
 - automatic deletion, 175
 - common files, 173–175
 - creating, 172
 - Word, 335–336
- Terminal emulators, 140–141
- Terry v. Ohio*, 45
- Testimony
 - definition, 519
 - hearsay rule, 31
 - to material not witnessed by the speaker. *See* Hearsay.
- Text Retrieval Conference (TREC), 205
- Third-party assistance, sneak and peek warrants, 42
- 32-bit vs. 64-bit forensics workstations, 432, 438
- Threat assessment, case management, 381
- Time Division Multiple Access (TDMA), 310–311
- Timeline Maker, 20
- Timelines
 - browser history, creating, 220, 227
 - definition, 519
 - documenting, 18–20
 - for evidence. *See* Chain of custody.
 - researching, 159–162
- Timelines, creating
 - example, 19
 - MAC file data, 163
 - MAC (modify, access, create), file data, 19
 - overview, 18–20
 - tools for, 19–20

- Timestamps
 - browser history, 220
 - definition, 519
 - viewing, 161–162
- TO: field, e-mail, 196–197
- Tobacco industry, e-mail searches, 205
- Tools (hardware), nontechnical
 - adhesive labels, 421
 - antistatic bags, 420–421
 - digital audio recorder, 420
 - digital camera, 419–420
 - Faraday shields, 420
 - felt-tipped pens, 421
 - laptop computer, 419
 - overview, 418
 - presslock evidence bags, 421
 - video recorder, 419–420
- Tools (hardware), technical
 - Advanced Test Products, 415
 - Digital Intelligence, 415
 - external storage units, 416
 - Forensic Computers, Inc., 415
 - Forensic PC, 415
 - forensics workstations, 416–418
 - Guidance Software, 415
 - Intelligent Computer Systems, 415
 - overview, 413
 - technician's toolkit, 414
 - WiebeTech, 118, 122, 416, 428–429
 - write-protect interfaces, 414–416
- Tools (software). *See also specific tools.*
 - Adroit Photo Forensics, 146
 - applications, 407–408
 - Bee Docs, 20
 - Canon Imageware, 298
 - Captain Nemo, 409
 - Capture, 408
 - carver-recovery, 149
 - categories of, 395–396
 - cell phone acquisition, 317–321
 - cell phone storage, 319
 - CFTT (Computer Forensics Tool Testing), 411
 - cloud forensics, 295, 298
 - court approval, 11, 410–413
 - data abstraction layers, 396–398
 - data acquisition from media, 124–128
 - data carving, 146, 147–149
 - Daubert Process, 400–401
 - Decryption Collection, 408
 - demonstrating sound use of, 412–413
 - Directory Snoop, 135, 143–144, 409
 - Disk Explorer for FAT, 409
 - Disk Explorer for NTFS, 409
 - Disk Investigator, 409
 - displaying metadata files, 135
 - DocScrubber, 168
 - DriveImageXL, 409
 - DriveLook, 409
 - e-mail analysis, 206
 - e-mail header extraction, 199–202
 - e-mail searches, 206
 - EDiscovery, 408
 - EMT (E-mail Mining Toolkit), 206
 - Encase Forensics, 408
 - Entourage utility, 199–202
 - EWFACQUIRE, 124
 - Excel, 19
 - extracting registry history, 331
 - file recovery, 135, 140–141, 143–144
 - Filematch, 409
 - Forensic ComboDock, 122
 - Forensic Dossier, 119
 - Forensic Replicator, 408
 - Forensic Ultra Dock, 118
 - FTK (Forensic Tool Kit), 124
 - FTK Imager, 118–119, 121, 295
 - GREP, 140–141, 180–181
 - hardware memory capture, 119–120
 - Hash, 409
 - hidden data, reading, 168, 178–182
 - hiding data in slack space, 338
 - hiding data in the registry, 342

- Tools (software) (*cont'd*)
 - Internet history, tracing, 19
 - IXimager, 127
 - Lockdown, 408
 - Log Parser 2.2, 236
 - logging in a case log, 412
 - MAC analysis, 163
 - MACTime, 19
 - Memory Grabber Forensic Tool, 119
 - Memoryze, 117
 - Metadata Analyzer, 181
 - Metadiscover, 408
 - Metaviewer, 409
 - metrics for capabilities, 400
 - MoonSols toolkit, 118
 - Netcat, 118
 - Neutrino, 408
 - open source, 408–410
 - OS utilities, 401. *See also* specific operating systems.
 - Outlook header extraction, 199–202
 - P2 Commander, 408
 - password cracking, 349
 - PG Pinpoint, 408
 - proxy server log analysis, 243–244
 - PyFlag, 124
 - recovering temporary files, 175
 - Registry Analyzer, 178
 - Safecopy, 409
 - SafeCopy, 408
 - Scalpel, 149
 - SilentRunner, 408
 - software memory capture, 117–119
 - SQL MDF viewer, 298
 - strings, 131
 - suitability for purpose, 398–401
 - timeline creation, 19–20
 - Timeline Maker, 20
 - Trace, 408
 - Tribble, 119
 - user activity, tracing, 19
 - Visio, 19
 - Web server logs, 236
 - Web servers, 233
 - WINDD, 117–118
 - Winhex, 408, 410
 - X-Ways Trace, 19
- Tools (software), browser history
 - analysis
 - BUTIL, 243
 - The Coroner's Toolkit, 233
 - CSAUDIT, 243
 - Directory Snoop, 223
 - Log Parser 2.2, 236
 - NWAdmin, 243
 - ODBC, 243
 - Pasco, 221
 - Sawmill, 244
 - summary of, 230
 - Web Historian, 220, 225, 227
 - WebTrends, 243
- Tools (software), e-discovery
 - Analysis and Review package, 372
 - concept extraction, 372
 - data collection, 367–368
 - ZyLab Discovery, 372
- Tools (software), Encase
 - creating timelines, 19
 - e-discovery, 370
 - saving images in EWF (Expert Witness Format), 124
- Tools (software), evidence collection
 - CascadeShark, 255
 - CommView, 255–256
 - Computer Watchdog, 251
 - EndaceExtreme, 255
 - interception devices, 251–252
 - KeyCapture, 251
 - Keygrabber Wi-Fi, 251
 - keyloggers, 251
 - Network Monitor, 255–256
 - Observer, 255
 - OmniPeek, 255–256
 - WireShark, 255–256, 257–261

-
- Tools (software), FTK (Forensic Tool Kit)
 - case management, 383–384
 - creating timelines, 19
 - e-discovery, 370
 - EWF support, 124
 - live capture of registry entries, 331
 - Tools (software), Linux
 - DD (Disk Dump), 405
 - GREP, 405
 - LDE (Linux Disk Editor), 405
 - overview, 404–405
 - PhotoRec, 405–406
 - suites, 407
 - Tools (software), Macintosh OSX
 - Finder, 406
 - GREP, 406
 - HEAD, 406
 - overview, 406
 - Spotlight, 406–407
 - Tools (software), router and switch forensics
 - CREED (Cisco Router Evidence Extraction Disk), 271
 - Metasploit, 274
 - RAT (Router Audit Tool), 272
 - router and switch forensics, 271–272, 274
 - Tools (software), The Sleuth Kit
 - browser analysis, 220
 - for evidentiary use, 7
 - timelines from MAC data, 163
 - Tools (software), Windows
 - Autoruns, 404
 - downloading, 401
 - dumpchk.exe, 404
 - EFSDump, 404
 - Event Viewer, 403–404
 - network forensics, 403–404
 - PendMoves, 404
 - PSFile, 404
 - PSList, 404
 - PSService, 404
 - regedit (registry editor), 402–403
 - RootkitRevealer, 404
 - Streams, 404
 - strings, 404
 - suites, 407
 - SysInternals, 404
 - system logs, 403–404
 - Userdump, 404
 - Top-level domains
 - Internet addresses, 215
 - Web browsers, 215
 - Trace, 408
 - Tracing e-mail sources, 202–203, 208–210
 - Training, policies and procedures, 469
 - Transacted compound file, 335–336
 - Transporting evidence, 105–106
 - TransUnion, 60
 - Trash. *See* Garbage.
 - TReC (Text Retrieval Conference), 205
 - Triage, 383–384
 - Triangulation
 - between cellular towers, 311–313
 - definition, 519
 - Tribble, 119
 - Trigger point, e-discovery, 362
 - Trilateration, cell phones, 311–313
 - TriTech Forensics, forensics workstations, 429
 - Trithemius, Johannes, 350
 - Trojan horse defense, 227
 - True negatives, 206
 - True positives, 206
 - Tucker, U.S. v.*, 223
 - Turbocharge device, 319
 - Type Allocation Code (TAC), 316
- U**
- UFED (Universal Forensic Extraction Device), 320–321
 - UFS (UNIX File System), 137
-

- Unallocated space
 - definition, 519
 - recovering data from. *See* Data carving.
 - recovering files from, 140
 - vs. slack space, 140
 - Uniform Resource Locators (URLs). *See* URLs (Uniform Resource Locators).
 - Unique identifiers, 376
 - Universal Forensic Extraction Device (UFED), 320–321
 - UNIX File System (UFS), 137
 - UNIX/Linux file systems
 - dentries, 137–138
 - Ext, 137
 - file objects, 137–138
 - master node, 137–138
 - metadata, 137–138
 - Reiser, 137
 - superblocks, 137–138
 - UFS (UNIX File System), 137
 - Unknownuser (vigilante), 86–87
 - Unprovoked flight, 46
 - Unreasonable search and seizure
 - in the Fourth Amendment, 25–26
 - societal recognition of privacy, 81
 - subjective expectation of privacy, 81
 - two-component test, 81
 - \$Uppcase metadata file, 136
 - Upgrading and Repairing PCs, 423
 - Upjohn v. U.S., 65
 - URL logging, Web browsers, 217
 - URLs (Uniform Resource Locators)
 - definition, 520
 - Internet addresses, 213–214
 - typed into a browser, 225–226
 - URLSCAN Web server logs, 235
 - USB devices at crime scenes, 98
 - User mode, 116, 520
 - Userdump, 404
 - Users
 - actions, establishing, 224–230
 - activity, tracing, 19
 - extracting registry history, 328–331
 - intent and control, 226–227
 - listing, router and switch forensics, 272
 - names, in e-mail addresses, 187
- V**
- Vantec I/O panels, 437
 - Video recorder, as forensic tool, 419–420
 - Video surveillance, 107
 - Viking DNA, 95
 - Virtual adapter (VNIC), 293
 - Virtual local area networks (VLANs), 293
 - Virtual Machine Manager application, 292
 - Virtual machines (VMs). *See* VMs (virtual machines).
 - Virtual networking. *See also* Network search.
 - overview, 293–294
 - VLANs (virtual local area networks), 293
 - VNIC (virtual adapter), 293
 - VSs (virtual switches), 293–294
 - Virtual PC application, 292
 - Virtual private networks (VPNs), 103
 - Virtual server applications, 292
 - Virtual switches (VSs), 293–294
 - VirtualBox application, 291–292
 - Virtualization. *See also* Cloud computing;
Virtual networking.
 - for IaaS (Infrastructure as a Service), 281–282
 - instances, 282. *See also* VMs (virtual machines).
 - nodes, 282
 - overview, 291
 - servers. *See* Nodes.
 - virtual machines. *See* Instances.
 - Visio, 19
 - Visitor Locator Register (VLR), 310
 - VLANs (virtual local area networks), 293

- VLR (Visitor Locator Register), 310
VMDK files, 292
VMEM files, 292
VMs (virtual machines). *See also*
 Virtualization.
 capturing, 299–300
 files specific to, 292–293
 grouping, 292
 guest operating systems, 291–292
 host operating systems, 291–292
 NVRAM files, 293
 putting to sleep, 294–295
 server applications, 292
 snapshots, 294–295
 teams, 292
 VMDK files, 292
 VMEM files, 292
 VMSD files, 292
 VMSN files, 292
 VMSS files, 293
 VMTM files, 293
 VMX files, 293
 VMXF files, 293
VMSD files, 292
VMSN files, 292
VMSS files, 293
VMTM files, 293
VMWare application, 292–293
VMX files, 293
VMXF files, 293
VNIC (virtual adapter), 293
Volatile information
 collecting, 270–272
 definition, 268–269
\$Volume metadata file, 136
Voluntary release of information. *See also*
 Warrantless searches, with consent.
 consent to search, 81
 in corporate environments, 88
 medical facilities, 63
 service providers, electronic
 communication, 59
VPNs (virtual private networks), 103
VSs (virtual switches), 293–294
- W**
- W3C fields, 237
W3C Web server logs, 234
.wab folders, 191
Wardlow, Illinois v., 45
Warrantless searches
 exclusionary rule, 44
 health care information, 63
 incident to arrest, 45–46
 by medical facilities, 63
 mitigating circumstances, 45
 overview, 44–45
 probable cause, 26, 46
 unprovoked flight, 46
Warrantless searches, with consent. *See*
 also Voluntary release of information.
 actual authority, 47, 511
 apparent authority, 47, 82
 assumed permission, 48
 categories of consent, 47
 common authority, 81–82
 erroneous assumption of authority, 83
 ostensible authority, 49, 516
 overview, 46–47
 parental permission over children, 48
 personal property, 47–48
 potential issues, 46
 private sector organizations, 48–49
 public sector organizations, 49–50
 shared computers, 83
Warrants. *See* Search warrants.
Warrens, 337, 520
Washington, Earl, 95
Web browsers
 browser engine, 216
 browsing Web sites, 217
 cached files, location of, 219
 caching information, 216
 cookies, 217

- Web browsers (*cont'd*)
 - description, 216–217
 - effects on performance, 216
 - HTML (HyperText Markup Language), 216
 - MRU (most recently used) sites, 217
 - parsing HTML, 216
 - settings, 217–219
 - top-level domains, 215
 - URL logging, 217
- Web browsers, browser history
 - analysis tools, 220
 - cached history, 219
 - cookies, storage location, 219
 - Firefox, 220
 - Internet Explorer, 219
 - overview, 219
 - protected mode, 219
 - settings, 218
 - The Sleuth Kit, 220
 - timelines, creating, 220
 - timestamps, 220
 - Web Historian, 220
- Web browsers, browser history analysis
 - control of digital material, 226–227
 - counting contraband, 230
 - DAT files, displaying, 221
 - deleted files, 227–230
 - detecting active measures, 227–230
 - detecting malware, 227
 - Directory Snoop, 223, 227
 - establishing user actions, 224–230
 - evidence of deleted files, 223
 - fast meta refresh, 224
 - file wipes, 227–230
 - goal of forensic analysis, 222
 - HTTP 300 message, 224
 - identifying specific records, 221
 - job of the investigator, 222–224
 - knowledge of possession, 222–224
 - MFT (Master File Table), 223
 - MFT metadata, effects of deleting files, 229
 - for multiple users, 224
 - pop-up bombs, 224
 - present possession concept, 222
 - redirects, 224–225
 - sorting records, 221
 - timeline, creating, 227
 - tools, 221, 223, 225, 227, 230, 233
 - Trojan horse defense, 227
 - typed URLs, 225–226
 - user intent and control, 226–227
 - Web Historian, 225, 231–233
 - Website Profiler, 233
 - Windows registry, 225–226
- Web Historian, browser history
 - analysis
 - downloading, 231
 - redirected URLs, 225
 - running, 231–233
 - for undetermined browsers, 220
- Web server logs
 - AWSTATS log, 236
 - Log Parser 2.2, 236
 - parsing, 236
 - tools, 236
- Web server logs, analyzing
 - centralized logging, 238
 - epoch time conversion, 237–238
 - logging per server, 238
 - overview, 236–238
 - rotating logs, 237
 - W3C fields, 237
- Web server logs, Apache files
 - access log, 235
 - access_log, 235
 - error log, 235
 - error_log, 235
 - httpd.pid file, 236
 - NCSA (Common Log), 235
 - Rewrite log, 236
 - Script log, 236

- Web server logs, Windows
 - BIN (Centralized Binary), 234
 - HTTPERR, 235
 - IIS, 234–235
 - IIS ODBC (Open Database Connectivity), 234
 - IISMSID, 235
 - NCSA (Common Log), 234
 - URLSCAN, 235
 - W3C, 234
 - XML (Extensible Markup Language), 234
 - Web servers. *See also* Proxy servers.
 - The Coroner’s Toolkit, 233
 - description, 233–234
 - live acquisition, 233–234
 - tools, 233
 - Website Profiler, 233
 - WebTrends, 243
 - Weeks v. U.S.*, 44–45, 76
 - Wetstone Technologies, 354
 - WHOIS query, 209–210, 273–275
 - WiebeTech
 - components in forensic workstations, 428–429
 - Forensic ComboDock, 122
 - Forensic Ultra Dock, 118
 - write-protect interfaces, 416
 - William A. Gross Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co.*, 365
 - William Anderson Jarrett, U.S. v.*, 87
 - Williams, Curtis*, 79
 - Williams, Karol*, 79
 - Williams, U.S. v.*, 79
 - Wilson v. R.*, 72
 - WINDD, 117–118
 - Windows, tools
 - Autoruns, 404
 - downloading, 401
 - dumpchk.exe, 404
 - EFSDump, 404
 - Event Viewer, 403–404
 - network forensics, 403–404
 - PendMoves, 404
 - PSFile, 404
 - PSList, 404
 - PSService, 404
 - regedit (registry editor), 402–403
 - RootkitRevealer, 404
 - Streams, 404
 - strings, 404
 - suites, 407
 - SysInternals, 404
 - system logs, 403–404
 - Userdump, 404
 - Windows 7, forensics workstations, 438
 - Windows registry. *See* Registry.
 - Windows Web server logs. *See* Web server logs, Windows.
 - Winhex, 408, 410
 - “Wink and the nod” approach, 87
 - WIPE.EXE, 108
 - WireShark, 255–256, 257–261
 - Wiretap Act, 58
 - Witnesses. *See* Expert witnesses; Eyewitnesses.
 - Word
 - autosave function, 336
 - directed compound file, 335–336
 - metadata, extracting, 181
 - redo function, 336
 - temporary files, 335–336
 - transacted compound file, 335–336
 - Work/product doctrine, 65–66
 - Write-protect interfaces, 414–416
 - Write-protected I/O, 436–437
 - Write-protected port replicator, 122
 - Writing reports. *See* Report writing.
 - Writs of Assistance, 24
- X**
- X-Ways Forensics
 - Capture, 408
 - duplicate files, detecting, 370

X-Ways Forensics (*cont'd*)

Trace, 408

Winhex, 408

X-Ways Trace, 19

XML (Extensible Markup Language), 234

Y

Young, U.S. v., 323

YouTube, First Amendment protection, 29

Z

Ziegler, U.S. v., 49

Zubulake test, 11–12

Zubulake v. UBS Warburg, 11–12, 362

ZyLab Discovery, 372