Digital Forensics Explained

Greg Gogolin, Ph.D.

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed in the United States of America on acid-free paper
Version Date: 20121019

International Standard Book Number: 978-1-4398-7495-0 (Hardback)

Library of Congress Cataloging-in-Publication Data

Gogolin, Greg.
Digital forensics explained / Greg Gogolin.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4398-7495-0 (hbk. : alk. paper)
1. Computer crimes--Investigation. 2. Computer security. 3. Computer engineering. I. Title.

HV8079.C65G64 2013
363.250285--dc23 2012032424

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

1

What Is Digital Forensics, and What Should You Know About It?

Introduction

Over the years I have read many technical books that provide screenshots of particular tools and their operations. Whenever a tool is updated, such books become obsolete. This book focuses on the methodologies, techniques, resources, and mind-set that is necessary in understanding the digital forensics process. My philosophy, and that of my chapter contributors, is that an understanding of the process is primary. Adapting that understanding to tools and technologies can then be effectively realized. Attempting to develop high levels of skill with a particular tool or technology before an understanding of the big picture is attained is shortsighted and invites error. Discipline is necessary in any science and digital forensics is no different.

Digital forensics is the application of scientific principles to the process of discovering information from a digital device. A form of digital forensics has been around nearly as early as computers were invented, but forensic capabilities have witnessed many advances in the past years as digital forensic processes have matured and needs have become more prevalent. Digital forensics can involve nearly any digital device, not just computers, although technology often evolves faster than forensic capabilities do. Some of the common areas in which digital forensics is used include computers, printers, cell phones, mobile devices, global positioning systems (GPSs), and storage media. Less common areas include automobile systems, appliances, office equipment, and other programmable devices.

Forensic Science

The precise date of when forensic science began is unclear as there are many different fields in which forensic science can be applied. Certainly, people have been trying to determine how people died for thousands of years. In the Chinese book *Hsi Duan Yu* (*The Washing Away of Wrongs*), which appeared about 1248, the author details methods to distinguish the effects of different ways of dying, for example, death by drowning as opposed to death by strangulation (Kind and Overman, 1972). Nearly 700 years later, the first crime laboratory was established in the United States by the Los

Angeles Sheriff Department in 1930 (De Forest, Gaensslen, and Lee, 1983). Howard Schmidt, who served as an advisor to President George W. Bush and President Barack Obama, is credited with establishing the first U.S. government digital forensics laboratory (Defense News, 2010). Although forensic science has been evolving for many centuries, digital forensics is a relatively new development.

For something to be considered a science, it has to study, describe, and investigate phenomena in its field. A key aspect of this is that new knowledge generated by the study and investigation has to be repeatable. A peer review process is often followed, including within a lab and the publication process. A complex investigation can have many opportunities for error or misinterpretation, and the review process helps reduce the instances of error. In the digital forensics field, tools and techniques are often reviewed, but it is not uncommon for the findings that are presented in court cases to be the work of a single investigator and therefore unverified. In many situations, digital forensics does not have a scientific rigor behind it, which is present in other forensic areas such as wet labs. Part of the reason is that digital forensics is a relatively new science, and another reason is that digital technology progresses at such a rapid rate that the digital forensic processes tend to lag the pace of technological innovation. Figure 1.1 is a flowchart representation of the scientific process.

There are three aspects of the scientific process that I want to highlight. The first is to clearly define the question or purpose of the research. The second is to define a hypothesis. A hypothesis is a potential explanation for a phenomenon. A digital

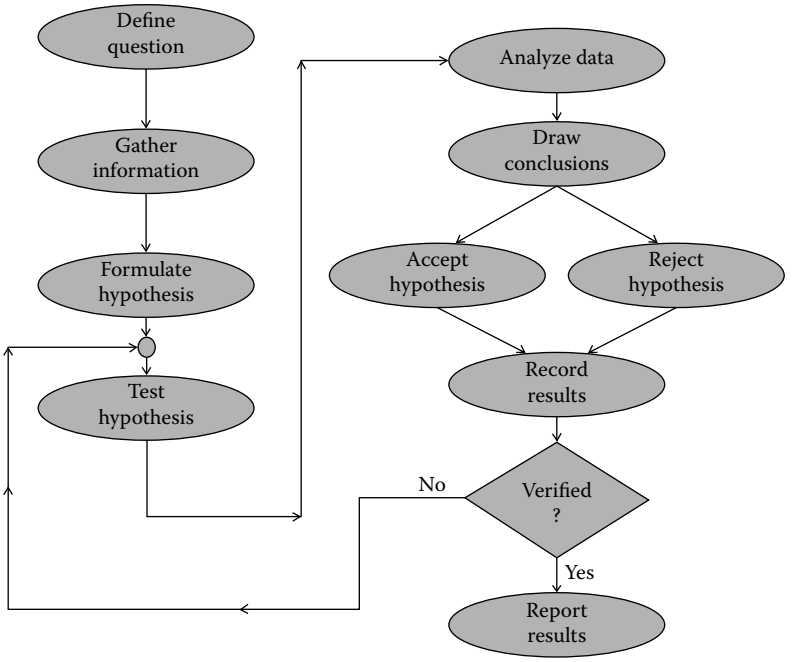

Figure 1.1 The scientific process.

forensic investigator often needs to develop a hypothesis to explain what happened on a computer and what it was used for. The third aspect that I want to emphasize is that many discussions of the scientific process overlook verification of results. Too often this is not done, and improper results are reported. Digital forensic cases can be life changing for many individuals, and every effort must be taken to ensure that the findings of the investigation are accurate. I do not want to discount the other steps in the scientific process, but I wanted to emphasize those three aspects—and in particular, verification of results.

Digital forensics is not limited to criminal investigation. It can be used to solve problems in a corporate setting such as recovering lost files and reconstructing information from damaged equipment and also to test for changes to devices that are subject to a stimulus. Malware and botnet research are other areas that use digital forensics, particularly when trying to determine impacts. An example would be to use forensic processes to establish the baseline state of a device, introduce the stimulus, and then compare the resulting state with the baseline.

What Does It Take to Be a Digital Forensic Investigator?

Digital forensic investigators need skills and interests in a variety of areas. The first question I ask someone who is considering this field is if they like puzzles. When investigating a case, you may not know any details other than that something has happened. So if someone needs to be shown or told what has occurred, they may not be a good fit for this field. Sometimes, cases come to an investigator's attention with instructions to find out what the computer or device user was doing. At times this may be an open request, whereas other times it is within a specific time frame.

Many cases follow a similar pattern, and a methodology similar to that outlined in Chapter 2 can help with a consistent investigation. However, many times the investigator needs to improvise an approach as there is not always a clear way to do things. This can be the result of new technology in which a methodology has not been developed, due to cost issues, or simply because it is the first time the investigator has encountered that situation. The point is that an investigator needs to be someone who can figure things out, not rely solely on others to do so. Another important characteristic is the ability to handle frustration because investigative tools and software do not always function without their challenges. This can be a fairly common occurrence when dealing with cell phones and small devices. I have had many students who stop their investigation in class at the first sign of difficulty rather than working through the challenges. They do not even try to find insight into their difficulty through the web or help system provided with the tool. Someone needs to be persistent and creative to be a successful investigator.

Another critical aspect of being a forensic investigator is the ability to keep your mouth closed. Case specifics usually require some level of confidentiality, and this must be maintained. Similarly, if someone is looking to enter the field as a private

investigator or law enforcement professional, lack of a criminal record may be mandatory. Within a corporate setting, investigators may not need to be licensed, but they do need to maintain a high degree of integrity within the context of the corporation. I have gone through many smartphones and computers covertly to determine the degree of an employee's misconduct. The result is that I know what personnel changes are likely to occur before anyone else.

Irrespective of whether the environment is corporate, law enforcement, or as a private investigator, a background check is likely to occur. Particularly, in law enforcement and private investigator licensing, fingerprint registration is likely a requirement. Private investigators also need bonding and/or liability insurance. Most states require that private investigators have experience before becoming licensed, so students who are fresh out of college may find that they need to work for someone else under their license before becoming individually licensed.

The work itself seems to follow a sine wave rather than a consistent flow. Cases often explode into multiple devices and locations, which can mean long and inconsistent hours. After-hours investigation may be the rule for some cases, and often this may be at a distant site. What does seem to be the rule is that cases appear when they are not expected, and it is good practice to be ready. For example, computer forensics investigations usually include taking forensic images of the computers under investigation. Typically, this means taking a forensic image of the storage devices. The location where the images are being copied to should be forensically prepared in advance. For example, if a computer has a 1-TB hard drive, the forensic image could be taken on another 1-TB hard drive. This forensic image hard drive should not just be a new hard drive that is in an unopened box from a retail store because it is unknown what may already be stored on that drive. New hard drives commonly come with utilities and other programs preinstalled. A hard drive should be completely erased and reformatted before it is used. Experienced investigators often wipe a hard drive and then overwrite the entire drive with a hex character. This process takes time, and when time is of the essence, preparing forensic storage media in advance can save considerable time.

The forensic process is discussed later in the book, including Chapter 2, but let us complete the thought on forensically prepared storage media. The purpose of forensically prepared storage media is that it allows the investigator to testify that the only information contained on the forensic image drive is the one from the suspect computer and that there is no evidence of contamination. Anything that is not part of the forensic image would be the hex character that was due to the wiping process. Hash algorithms, such as MD5 and SHA-1, are also used to verify that an exact copy has been taken.

Educational Opportunities

Education is necessary to become competent in any profession, and digital forensics is no exception. Education can take many forms including university instruction, attendance at conferences, vendor classes, workshops, and self-study. Each of these

should be evaluated to determine if it helps move someone toward their educational goal. College and university educational opportunities can be evaluated in a number of ways such as asking previous students and those affiliated with the courses and programs. Several designations and accreditation levels can help determine the maturity of the offerings. For example, the National Security Agency (NSA) has a center of academic excellence accreditation that is rigorous and appropriate. There are several levels to this designation, so inquiry into which level has been attained is good due diligence. An additional factor would be to inquire regarding the experience of the faculty. Other questions include the following: Do the faculty actively research and/or consult in digital forensics? Are they licensed and/or certified as investigators? How many cases have they investigated? What tools and technologies will the student be exposed to? How large are the classes and do they have a hands-on component? How long has the institution been offering courses?

Vendor classes focus on tools that they provide, although instructors will often provide insight into complimentary tools and techniques that are not part of the vendor's products. Some of these classes are offered online, which provides convenience in logistics and can help minimize costs. Commercial products can be expensive, and there may be other tools that also need to be purchased, so it is important to have an overall budget in place. Vendors may also sponsor their own conference and/or participate in other conferences. Conferences are a good way to develop a feel for how well products are received and what other things need to be considered.

SANS Institute provides very good education and training that is not tool specific. It offers intensive-focused instruction on specific topics that can lead to well-recognized and respected certifications. There are other similar organizations, but I have had two colleagues who have attended the SANS Institute and they gave it very high marks.

Self-study is an inexpensive way to develop skills, but it does require a large-time commitment. Personally, I think that self-study is the first step in the education process for a field like digital forensics. You can get a reasonable feel for the field and lay a foundation for a more advanced study at conferences, universities, and workshops. It is a very uncomfortable feeling to attend an educational opportunity without a foundation. The resulting insecurity may not allow you for maximizing the experience because of information overload or a simple misunderstanding that could have been avoided with preliminary self-study.

What Opportunities Are There for Digital Forensic Investigators?

Some of the more common areas for digital forensics investigators would be in law enforcement, the federal government, corporations, and as a private investigator. Typical law enforcement positions would be as a detective and/or in a crime lab, but some agencies deploy low-level forensic tools more broadly throughout the organization. Corrections personnel may also use forensic techniques to ensure

that parole conditions are being adhered to. A large portion of the focus of law enforcement digital forensic efforts include child exploitation and sexually abusive material. Cell phone analysis is also a very significant component of the law enforcement efforts.

Federal government positions may reside within agencies such as the CIA, FBI, Secret Service, ATF, and Department of Defense. An area that uses digital forensics extensively that most people do not realize is the Postmaster General. The Department of Homeland Security is an agency that contracts services more often than some of the other cabinet level agencies, and digital forensics fits into this arrangement. Various agencies and departments handle things differently. For example, one location may be a general digital forensics lab, whereas another may maintain a higher level of expertise. Some locations may specialize in certain types of forensic activity, and some agencies may have multiple levels of expertise.

A federal agency that has a significant digital forensics presence is the NSA, which is one of the top organizations in the world in digital forensics and associated technologies. People who are interested in working for the NSA should consider attending a university that has been designated a NSA center of excellence. Preference is often given for positions, internships, and scholarships for the students who graduate from these centers of excellence.

Corporate positions in digital forensics can vary considerably in terms of responsibilities and focus. An individual may focus on data recovery of damaged or deleted files, investigation of security breaches, and investigation of employees who recently left the organization to find out what they were doing in the days leading up to leaving the company. Part of the reason for this type of investigation may be to see if the individual engaged in inappropriate activities such as copying sensitive information. Other responsibilities may include fraud investigation, employee misconduct, and research and development. Particularly, for law firms, forensic investigators may be involved in electronic discovery (e-discovery). E-discovery uses forensic tools to search through computers, networks, and storage devices in the discovery phase of a law suit. Simply looking for file names is not sufficient as the sought-after-documents may be e-mail or perhaps there is a question if the information even exists. E-discovery tools crawl through computers, networks, and storage media not unlike a search engine crawls through the World Wide Web. However, the e-discovery tools crawl to search for various keywords as opposed to a search engine that indexes everything that it finds.

Private investigators may be self-employed or work for a larger organization or law firm. The tools and technologies involved in digital forensics can be quite expensive, which may lead to concentrating in various subfields. For example, cell phone forensic tools can approach a purchase price of $10,000 with an annual maintenance fee of a few thousand dollars. Usually, investigators need multiple tools, so a reasonably equipped cell phone forensic investigator may invest $25,000 into tools in addition to training and other ongoing expenses. Computer forensics

can involve a similar expense, and this does not include some of more advanced situations such as password and encryption cracking technologies.

What Are the Trends and Challenges in Digital Forensics?

One trend that is occurring is standardization and licensing of forensic investigators. In several states, it is a felony to perform digital forensic services without being licensed as a private investigator. The requirements for licensure vary, so the appropriate state agency should be consulted. It is important that individuals understand how the state within which they reside defines digital forensics so that they do not find themselves in a legal situation.

A recent study that I conducted of Michigan law enforcement (Gogolin, 2010) indicated a rapid increase in the number of cases requiring digital forensic services and a significant shortage of forensic investigators. It appears that if most criminal cases do not already have a digital aspect that they will in the near future. Surveillance devices and the prevalence of things such as cell phones are one of the main reasons for the rise in digital aspects. Social media, where planning and bragging of exploits occurs, almost guarantees that there will be digital artifacts.

Cell phone and mobile device ownership and usage surpassed 5 billion in 2010 (BBC News, 2010). This provides for the capture of information with embedded devices such as cameras, as well as for the exchange of information verbally and through technologies such as text messaging and e-mail. The integration of smartphones into the World Wide Web and social media provides for a rich and extensive number of artifacts that may be of interest to a digital forensic investigator.

Most cell phones and camera-equipped mobile devices have GPS capabilities. This allows the camera to incorporate the GPS coordinates of the location where a picture was taken into the picture file header. The analysis of pictures and videos, whether from cell phones or surveillance systems, is an explosive growth area. The images often need to be enhanced to obtain the necessary level of detail, and this expertise with graphics is a skill that requires a combination of training and technology that is not commonly available.

The movement toward a cloud environment is changing the digital forensics world. Cloud computing uses computing and storage resources from a pool. The pooled resources may be contracted from a third-party cloud provider. The third party often shares the pooled resources among many organizations. A key advantage of cloud architecture is that if a contracting organization needs extra resources for a short period they can contract the resources from the cloud provider. When they no longer need the resources, they simply revert to smaller amount of resources. This saves the organization money by eliminating the need to purchase equipment that they only need for a short period.

Cloud computing is kind of like a food catering service. If you want to throw a big party, it makes sense to rent seating and rather than buy several tables and chairs that you will not need after the party. When the party is over, the seating is cleaned and goes back

to the owner, who then is free to rent it out to someone else who needs it. When the next renter receives the seating, it is in a clean state and there is no evidence that you had the seating. This illustrates the challenge with cloud computing for a forensic investigator. When you no longer need the resources that are contracted, the resource is contracted for another purpose. This can create multiple situations of interest in terms of forensics.

Scenario 1: If the data on the cloud storage device is deleted but not wiped when it is repurposed, there is potential for reconstruction of and access to the data that was previously on the device by someone who should not have access.

Scenario 2: If the data on the cloud storage is deleted and wiped when it is repurposed, recovery of the data or artifacts is not possible—especially if the storage resource is already in use by another entity.

The cloud environment also means that artifacts may no longer be contained on a single device, which can complicate discovering where the artifact originated. The very nature of the cloud, where resources can be used for a short time and then repurposed, means that artifacts can exist one moment and then disappear the next. Someone perpetrating a crime could contract cloud resources similar to what was previously outlined in scenario 2. Once the perpetrator is finished with the resources, the evidence is wiped and the resources are used by someone else, likely completely destroying the evidence trail. This type of situation has actually been occurring for many years in the form of botnets and similar technologies. The advances in cloud computing allow taking nefarious activity to a whole new level, which makes advancements in forensics that much more critical.

Anti-forensics, which is covered in Chapter 11, is attempting to hide, destroy, or alter artifacts to prevent their reconstruction by forensic analysis. Using anti-forensic techniques can make forensic reconstruction difficult or even impossible. Many tools are created to provide security for individuals who use intense algorithms and techniques. There is little to prevent the use of these tools in activities of less-than-honorable intent, which may frustrate forensic efforts. Even when methods have been developed to address these tools, the time and computer processing power required to defeat the tools and techniques are often prohibitive.

Another aspect that is not so much a trend but rather evidence that the world is becoming a smaller place is the internationalization that is enabled through the ease of connectivity. The language and cultural implications, as well as the ability of criminal perpetrators to be in different countries at the time of their transgressions, give rise to a multitude of challenges for investigators. Very few technical degree programs require foreign language fluency, which can hamstring an investigation from the start. Foreign languages and dialects present a number of challenges in understanding communication such as e-mail, as well as the extra difficulty that slang and idiomatic expressions introduce. In part, due to the proliferation of digital devices and Internet use and network connectivity, these challenges will likely only increase.

The worldwide nature of connectivity presents other challenges. There are jurisdictional and cooperation issues to deal with. Even within the United States, a case

can be interpreted as a felony in one county but interpreted as a misdemeanor in another. State lines have not even been crossed! Crimes that cross state lines or international borders can be much more difficult to address. Perpetrators know which countries are likely to cooperate in a situation and plan accordingly. Servers are often hosted in countries that have lax laws and/or enforcement against a particular activity. Illegal online gambling servers are commonly hosted in Latin American countries (Menn, 2010).

To complicate things even further, the location of servers can quickly change with the use of virtual technology. Virtualization allows one physical computer to run multiple logical computers within it. A rough example is when someone sets up multiple accounts on their home personal computer. Little Johnny signs on to his account, with his own screen background and configuration characteristics. Stephanie signs on to the same computer using her account and uses her own configuration that is independent of Little Johnny's. Virtualization takes this farther in that the operating system can be installed multiple times in different locations on one computer, and the multiple installations can be run simultaneously and independently. Virtualization has existed in a corporate computer environment for decades, but recent advancements have reduced the cost and complexity so that it can be used by a very broad range of individuals. These virtualization capabilities help support the movement to a cloud architecture. An individual can create a virtual machine and potentially move or copy it between computers—and countries—within minutes. The implications of this in a digital forensics environment are dramatic.

Computer forensics often focuses on storage media such as a computer hard drive. Hard drives are rapidly increasing in capacity, and other storage technologies are evolving. Flash memory and solid state drives (SSD) are likely to replace hard drives in the near future because of their superior access speeds. Bell and Boddington (2010) found that SSD can confound current digital forensic techniques. Similarly, Wei et al. (2011) found that traditional hard drive sanitation techniques are ineffective on SSD. Computer technology will continue to evolve, and these examples illustrate that a forensic examiner must evolve as the paradigms within which they operate evolve.

The last trend that I want to discuss—although there are many more that could be touched on—is simply the explosion of data and storage capabilities. An individual can purchase a terabyte of hard drive storage for less than $50. This puts the ability to store multiple terabytes of data within the reach of an incredible number of people. It also means that corporations can create dramatically large databases and data warehouses that were previously inconceivable. It can take days to perform a keyword search on a 1-TB hard drive using forensic tools. Extrapolate that out to a corporate environment where the storage capacity is far greater, and it is possible to find that it is impossible to keyword searches on all of the storage media using current techniques. One challenge is that it may not be able to "freeze" all of the data in all the systems at the current state. Data is always changing and being modified by multiple systems and users. It is kind of like telling the world to stop rotating while measurements are

taken. Further, the data may reside in many locations. The point is that digital forensics is a far different environment in a corporate setting than it is when looking at an individual's private computer. But with the advancements in computer technology, some of the challenges with corporate digital forensics are appearing in the environment of an individual's private computer.

Resources Available to Digital Forensic Investigators

Before I describe some of the tools and technologies, I would like to describe some of the organizations and other resources that are available. Formal training is one of the most important considerations. In a legal situation such as a court case, competency of an investigator is going to be one of the first things evaluated. If the investigator has little or no current relevant training or certification, the outcome of the case may be in doubt. Most vendors provide training on their tools, and many conferences and information security organizations provide training opportunities.

Online resources in many instances are the most valuable. Knowledge bases and virtual communities can be invaluable in working through problems that an investigator encounters. Vendors often provide a searchable bulletin board that is frequented by users of the vendor's products. Open-source tools often have very passionate support groups. Social networks can be valuable in obtaining contacts that may help provide insight into issues. Organizations such as the International Information Systems Security Certification Consortium (ISC^2) provide training, testing, and certification in the areas that compliment digital forensics. The federal government has a variety of programs such as InfraGard and opportunities through the Department of Homeland Security that can be very beneficial. Search.org is one of many organizations that I have found that provide free online resources that I frequently take advantage of.

Many universities have research groups that specialize in digital forensics that may be willing to help. Which university or research group is appropriate to consult depends on the type of the case or situation the investigator is working on. For example, if the case involves incident response, Carnegie Mellon's CERT could prove to be a valuable resource. But if the incident is something recovery of data from damaged media, contacting a different university may be appropriate. It is also important to realize that top research universities are not the only game in town. Researchers at smaller universities may actually have broader exposure and more field experience than those at universities where research is a primary goal. A good way to wade through the maze is to find a third-party reference such as the NSA. The NSA designates universities as centers of excellence if they meet certain criteria, and most universities that have a significant presence in digital forensics have gone through this certification process. Additionally, the NSA certification is in different areas, so this can further assist finding potential resources.

Many tools and technologies are available to assist forensic examiners in addressing the challenges described earlier. Chapter 3 includes a discussion of tools and

techniques, as well as how they fit into the overall scheme of a digital forensics investigation. There are commercially available tools as well as open source. Some tools are very specialized and focus on doing one particular thing well, whereas other tools attempt to address a much broader perspective. There is often a leapfrog situation occurring where a new version of a particular tool surpasses its competitors. A short time later a competitor may introduce a new version and it becomes the leader until the next leapfrog situation. For that reason, I will not try to rank particular tools and technologies or provide detailed instructions on how to perform a specific operation with a tool. However, I am a firm believer in leaving bread crumbs for myself and anyone else to follow. So I will not hesitate to describe my experiences with tools. It is my hope that I can point out the potholes that I have encountered so that you can avoid them or at least prepare for them.

Conclusion

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to go it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favor.

References

BBC News. (2010). Over 5 Billion Mobile Phone Connections Worldwide. Retrieved on July 2, 2011 from http://www.bbc.co.uk/news/10569081.

Bell, G., and Boddington, R. (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? *The Journal of Digital Forensics, Security and Law*, Vol 5(3).

De Forest, P. R., Gaensslen, R. E., and Lee, H. C. (1983). *Forensic Science: An Introduction to Criminalistics*, McGraw-Hill, New York.

Defense News. (2010). An Online 'War'? Retrieved on June 20, 2011 from http://www.defensenews.com/story.php?i=4567292&c=FEA&s=COM.

Gogolin, G. (2010). The Digital Crime Tsunami. *Digital Investigation,* Vol. 7(1-2).

Kind, S., and Overman, M. (1972). *Science against Crime*, Aldus Books, London, UK.

Menn, J. (2010). Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, PublicAffairs, New York.

Wei, M., Grupp, L., Spada, F., and Swanson, S. (2011). Reliably Erasing Data from Flash-Based Solid State Drives. Usenix Fast 11 Conference on File and Storage Technologies, San Jose, CA.

Contents

Preface

Purpose and Approach

Most technical books tend to be tool-centric and often take on a cookbook approach to describing how to use a specific tool. These books often show a series of screen shots illustrating wizards or mouse-click sequences to perform a task. These types of books have their place, but that is not the type of book that I wanted to write. I was after something that explained the concepts of digital forensics and how the pieces fit together—kind of a "do not give someone a fish, but rather teach them how to fish" approach. I was looking to write a book that was not dependent on a version of software or a piece of technology. The challenge in digital forensics is to open your eyes, see the big picture, and think things through before you act. There is more than one way to approach most problems, and as long as you understand the big picture, you are free to use the ways that make the most sense for you.

This book is organized as follows: Chapter 1 starts with an overview of digital forensics and what you should know about it. This chapter goes over the forensic process, what it takes to be an investigator, trends in digital forensics, and some useful resources. Chapter 2 describes approaches and best practices in digital forensics. Much of this is based on what I have learned over the years while conducting investigations as well as on feedback from other investigators. Included are acquisition forms and a sequential process outline to help guide an investigation, as well as a checklist of supplies when responding to an incident. There is often more than one way to perform an investigation, but if you are not sure where to begin, then this chapter should be helpful. Chapter 3 covers the tools that are often used in an examination. This includes commercial tools, free and open-source tools, computer and mobile tools, and things as simple as extension cords.

Internet and e-mail investigations are covered in Chapter 4 and mobile forensics is covered in Chapter 5. Mobile forensics includes cell phones, iPads, music players, and other small devices that are mobile. In many ways, mobile forensics is easier to grasp than computer forensics because there are fewer parts and moving pieces. However, with the rapid advances in smart phone technology, the environment quickly becomes complex. Chapter 6 is the first chapter with a guest author, Gerald Emerick. He covers cloud computing from an architectureal perspective and its impacts on digital forensics. Chapter 7 is written by Detective Jason Otting, and he walks us through a criminal case from start to finish in a very engaging fashion. You can see the case, emotions, and impact layout in front of you in an extremely personal approach.

Cases need to be documented and presented, and they are covered in Chapter 8. A sample summary report from a simple computer investigation is presented, followed by a cover sheet for a cell phone investigation and then a look at an iPad report. The latter part of the chapter covers presentation considerations, and since reporting and presenting are often the end of a case, the chapter concludes with an overview of archiving a case.

Chapters 9 and 10 are the areas that most digital forensics books bypass. Dr. Barbara Ciaramitaro explains why these two chapters are very useful in providing information to help round out an investigation. Earlier in the book I mention that "Facebook" is a keyword search that should be done routinely in most investigations; Chapters 9 and 10 help explain why.

One thing that investigators often face is a suspect who plans ways to make his/her digital activities hard to trace. Velislav Pavlov writes about anti-forensic techniques and technologies in Chapter 11. He is one of those guys that you go to for ideas regarding breaches in security or when you want to learn about something new. Chapter 12 is the study of relationships and putting the pieces of the puzzle together. It is a topic that is not commonly found in digital forensic books or curriculum, but one that I think is central to improving its effectiveness.

Although it is the last chapter in this book, Chapter 13 is the first one that I wrote. Few articles and books speak to the psychological effects related to digital forensics investigations—and I mean primarily the effects on the investigator. If you think about a movie in which something surprising literally made you jump out of your seat, then you have a good idea of the shocking world awaiting an examiner. There are many sleepless nights ahead in digital forensics—thinking about the victims, their families, and yes, the bad guys. Additionally, I wanted to stress ethics because I have seen a lot of unethical things in the digital forensics field—including the behavior of examiners inside and outside of law enforcement. Once you cross the line into the gray area, it is extremely difficult to get back. The last piece in the chapter deals with cultural implications. I find it absolutely confounding how little culture, languages, and a broader view of the world make up the education and training of forensic examiners. Investigators need to learn foreign languages and appreciation of other cultures if they are going to meet the demands of digital forensics.

Preface is the part of the book that I looked forward to writing because although it is the first part of the book, it is that last part to write—which means that a big chunk of work is finished. Writing a book is like training to run a marathon. There is a lot to do before the event, and training does not go exactly as planned. There are injuries and setbacks, days you do not feel like running, and some things that just fall out of your control. Just like training, it always seems there is more you can do—more topics to add, a better way to do something, or some new development that is supposed to transform everything. Bottom line is you cannot do everything—inadvertent errors will be made, you forget to acknowledge someone, or some graphic could have been clearer—but it is time to get to the starting line and run the race. So with that, I hope you find value in *Digital Forensics Explained*. Feedback is always welcome, and with a name like mine, it is pretty easy to find me with Google. Thank you, and best of luck in your future endeavors!

Greg Gogolin

Digital Forensics Explained
International Standard Book Number: 978-1-4398-7495-0 (Hardback)