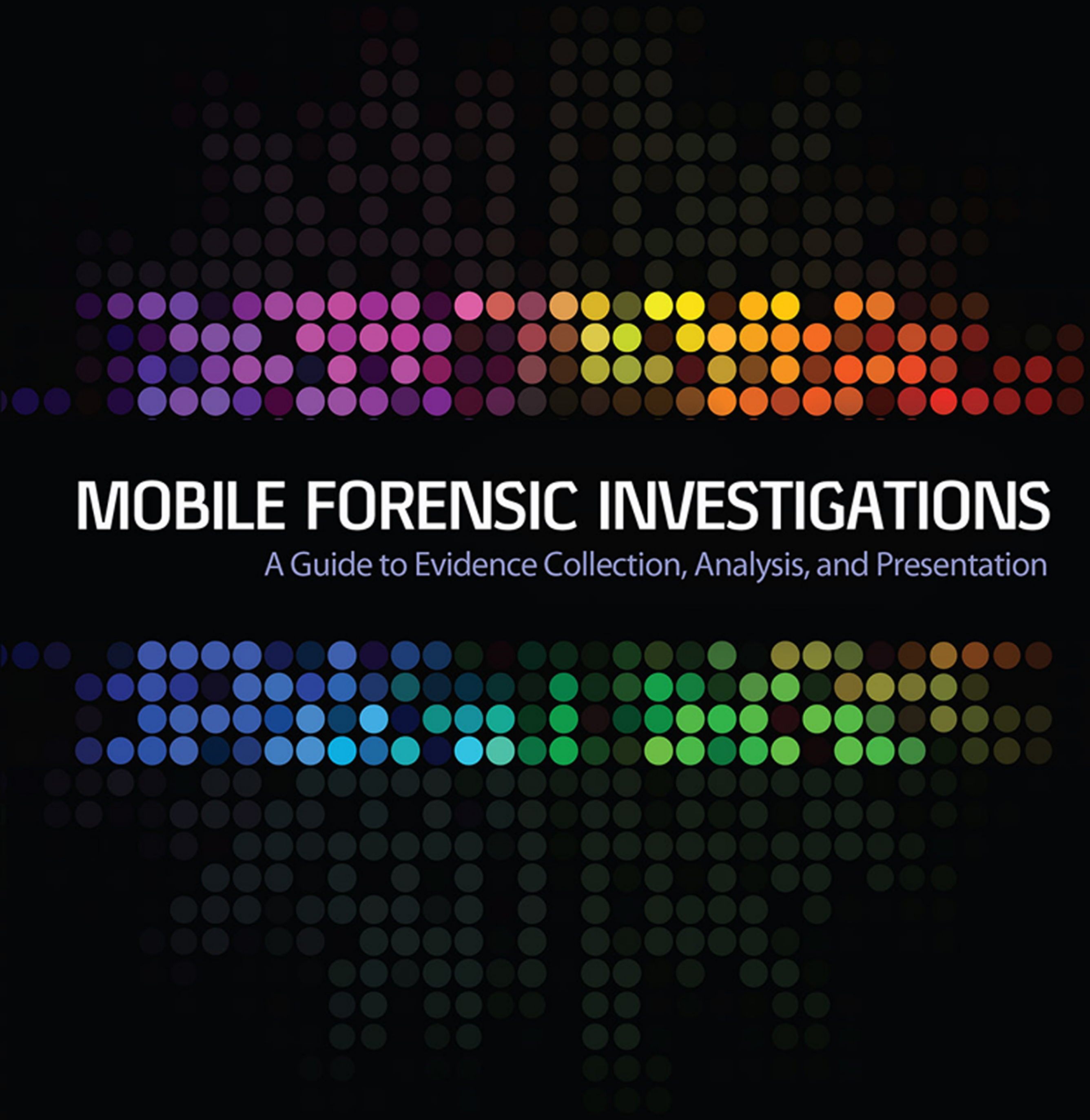

MOBILE FORENSIC INVESTIGATIONS

A Guide to Evidence Collection, Analysis, and Presentation

Mc
Graw
Hill
Education

Lee Reiber

Mobile Forensic Investigations

This page intentionally left blank

Mobile Forensic Investigations

A Guide to Evidence Collection, Analysis, and Presentation

Lee Reiber

Mc Graw Hill Education

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-0-07-184364-5

MHID: 0-07-184364-7

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-184363-8,
MHID: 0-07-184363-9.

eBook conversion by codeMantra
Version 1.0

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

This book is dedicated to my wife, Amy, my biggest critic,
who has put up with 20 years of geek speak and talk about writing a book,
along with the last several months of staring at my laptop composing the book manuscript.
You inspire me.

About the Author

Lee Reiber started his journey as a member of the Boise Police Department in Boise, Idaho, where he conducted digital forensic investigations until 2009 after almost 15 years of service. During the last few years at the police department, Lee's training company, Mobile Forensics, Inc., became one of the most prominent training companies in the United States for mobile forensics, training hundreds of students from law enforcement, Fortune 500 companies, and academia. MFI specialized in instructing its students on how to interpret and analyze mobile device data collected with multiple tools. It was Lee's research that produced discoveries in data formats, date and time configurations, and file system artifacts that are still used in training today. Due to the reputation of MFI, based upon the company's success in research, development, and training in mobile device forensics, MFI became a part of a global software company in 2009. Lee was promoted to Vice President of Mobile Forensics and he created and developed the mobile forensic curriculum and mobile forensic software solution, both of which are still a part of the company's offerings. In 2015, Lee departed the company and became the COO of one of the most recognized mobile forensic software companies in the world, specializing in deep data analysis of mobile device artifacts.

Lee has testified as an expert in mobile forensics in both criminal and civil cases during his 20-year career and consulted for both international and domestic companies requesting mobile forensic assistance, mobile device collections, data analysis, and data interpretation. Due to his aptitude for deep analysis, Lee is frequently called upon to assist in high-profile cases involving data from mobile devices when alien data is encountered. Lee has written more than 50 articles on mobile forensics, has been featured in both national and international magazines and print, and has lectured around the world on mobile forensics and cyber security. This book, *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*, is a product of the 20 years spent staring at HEX and ignoring the push button philosophy.

About the Technical Editor

Michael Robinson is a senior cyber threat analyst and digital forensic examiner for a large international company, where he specializes in mobile device forensics, computer forensics, and intrusion analysis. Prior to this role, Michael was a senior digital forensic examiner for customers in the U.S. intelligence community, where he performed computer and cell phone exploitation and analysis. Previously, Michael performed computer forensic examinations in the FBI's Investigative Analysis Unit, where he assisted special agents with counterintelligence and criminal cases. Michael is the former CIO of the U.S. Department of Defense's Business Transformation Agency, where he oversaw all information technology and information assurance operations for the agency, including overseeing all incident response and forensic investigations.

Michael is the Program Coordinator and Adjunct Professor for Stevenson University's Master of Science in Cyber Forensics. At Stevenson, he was the recipient of the Rose Dawson Award for outstanding adjunct faculty member of the year. He is also an adjunct professor in George Mason University's Master of Science in Computer Forensics. He teaches courses in mobile device forensics, intrusion analysis, and cyber warfare. He holds a Bachelor of Science in Chemical Engineering, a Master of Science in Information Assurance, a Master of Science in Forensic Studies (concentrating on computer forensics), and a graduate certificate in Applied Intelligence. Michael has presented at numerous national and international conferences, including DEF CON, the DoD Cyber Crime Conference, U.S. Cyber Crime Conference, CEIC, InfoSec World, and the BCISS Conference on Intelligence Analysis. He has authored more than a dozen journal articles and a book on disaster recovery planning for nonprofit organizations.

Contents at a Glance

This page intentionally left blank

Contents

Introduction

Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation is a comprehensive, how-to guide that leads investigators through the process of collecting mobile devices, analyzing the data, and disseminating their findings. This book was created from the many questions received during training courses, lectures, and interviews over many years and a desire to impart the answers to new, seasoned, and advanced digital forensic examiners.

Until now, no direction or guidance has been available to students and practitioners other than a few manuscripts and many vendor-specific training courses. Unfortunately, examiners have been left to figure out mobile forensic procedures and techniques for themselves, and often, at least in the digital forensic circles, mobile forensics is referred to as the “wild west” of digital forensics—just point and click. By trusting only in the automated tool, most examiners today do not fully understand the methods and processes used, so this term often fits. It is the goal of this book to change this mentality and move the examination of a mobile device into today’s required standards.

This book is intended not only to educate new students coming into the field or those looking for a career in mobile forensics, but examiners who have been conducting mobile forensics for years. It helps both student and examiner understand what constitutes processes and procedures, how to formulate an examination, how to identify the evidence, and how to collect the various devices, and it culminates with advanced tools and methods the examiner can use to uncover data that most tools forget.

This book can be read from cover to cover, but it can also be used to consult individual chapters during an examination. With the many tables and figures outlining mobile device file systems, targeted files, and digital gold, the student and examiner can use *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation* for reference during many examinations.

The first two chapters help expose the reader to the world of mobile forensics and clearly define the differences and similarities between mobile forensics and computer forensics. Chapters 3 through 6 outline the steps an examiner should take when coming into contact with mobile device evidence, including how to handle the evidence, and it ends with a discussion on the types of mobile forensic tools and the multitool approach. Next, Chapters 7 and 8 begin the exploration into the first examination by setting up the collection environment and defining what problems can be encountered, along with ways to fix them for both collections and data analysis. The last part of the book in Chapters 9 through 13 is all about the data. This includes determining what type of data should be expected within the various mobile device file systems, what type of data is expected in a standard collection versus an advanced collection, and how to decipher and decode advanced data from iOS, Android, Windows Mobile, and BlackBerry devices. Chapter 14 discusses how to present the data and how to become a mobile forensic device expert. This chapter explains that without proper documentation detailing the process from collection to analysis, the recovered evidence is often confusing and could be inadmissible.

A student or examiner in mobile forensics must be prepared for tomorrow today. *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation* provides a tremendous start.

1 Introduction to the World of Mobile Device Forensics

In 2014, Cisco's Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update indicated the number of mobile devices in use exceeded the world's population. Mobile device sales have outpaced PC sales three to one since 2003, as reported in a study conducted by the National Institute of Standards and Technology (NIST). Statistically, the examination of mobile device data should be similar proportionally, but unfortunately this is not the case. In actuality, computer evidence is still more prevalent in civil and criminal cases, but mobile device evidence is on the rise, though not at the rate of induction of the actual devices.

A common theme with mobile forensic experts in both law enforcement and enterprise is the overwhelming inundation of electronic evidence from mobile devices, which is increasing at an alarming rate—so much so that the groups I've surveyed from both law enforcement and corporate organizations indicate they had to hire or assign a specialist who would examine and collect data only from mobile devices. What is truly alarming is the fact most of these examiners also indicated that little consideration is given to the actual content of the mobile device when a computer is also part of the electronic evidence scene. When an American adult spends an average of 34 hours on the Internet using a mobile device, versus only 27 hours using a PC (as reported by Nielson, a global research company), shouldn't a forensics examination reflect that? This mentality is based primarily upon the limited amount of information available on correctly processing, analyzing, and reporting on the data from a mobile device, whereas computer forensics has been time tested and is accepted by examiners and courts across the globe.

The proliferation of mobile devices will only increase with the world's population growth and as this population's dependency on technology accelerates (see Figure 1-1). Now should be the time to accept and understand that the information contained on a mobile device details, documents, and exposes the thoughts, actions, and deeds of a user substantially more than any data stored on a personal computer.

With this unprecedented amount of electronic evidence comes the need for highly skilled mobile device forensics investigators. This book is a comprehensive, how-to guide that leads investigators through the process of collecting mobile devices, analyzing the data found, and disseminating their findings. This holistic approach to mobile device forensics will not only feature the technical approach to data collection and analysis, but it will also explore

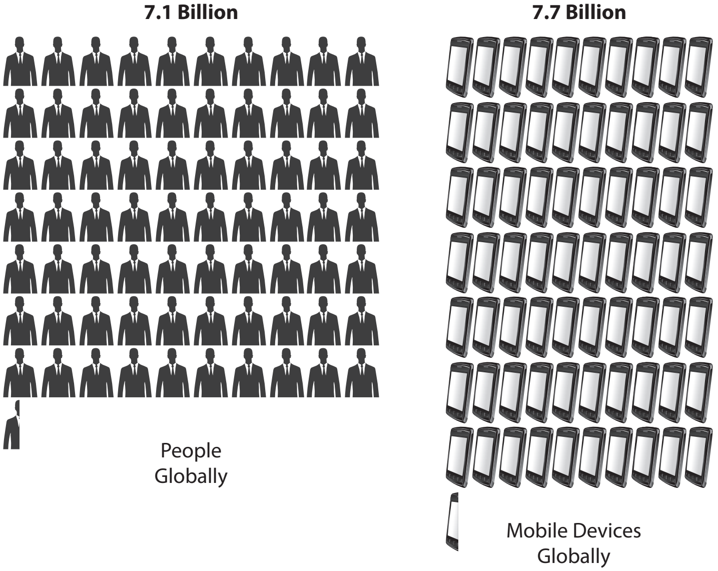

FIGURE 1-1 **There are currently more mobile devices on Earth than people.**

the legal aspects of mobile device forensics. It is widely known that today's digital forensics examinations have been "dumbed" down with a heavy reliance placed on using tools to extract and collect data. These methods have bred a systemic influx of "data collectors," rather than mobile device forensic examiners. This book attempts to counter this trend as it approaches and readies not only the newest examiners, but seasoned digital experts as well, with skills and knowledge that surpass the simple "easy button" approach.

The successful examination of digital evidence from a mobile device requires the intimate understanding of the medium that produced it. This fact is especially important when it comes to the examination of the artifacts left behind by a mobile device. Often the unique aspects of mobile devices are overlooked by examiners and students when encountering these small-scale digital devices because their first impressions are often clouded by the actual size of the device. It is a common belief that the small size of the device implies that it contains only primitive and rudimentary data, which equates to the belief that the examination of the device should be consistent with its physical size. In practice, many believe it should be as easy as inserting a flash drive and hitting the "find evidence" button. However, it is typically due to this tactic that most examiners, and quite honestly the majority of examinations, fail at the critical part of the evidence lifecycle—the dissemination of the facts.

An examiner who must testify to his or her findings will quickly realize that it is not acceptable to testify to the fact that he or she pushed the "get evidence" button and then believe that reasoning/explanation will suffice. An examiner must be ready to answer the question, "Where did the phone book come from?"—and not answer, "From the phone."

The true expert digital forensics witness will be ready to give the location of the phone book's contents as they relate to the phone's file system and to specify how the user data was not altered during the examination. Unfortunately, for most, this is a daunting task because it takes additional training, for which many admit they have neither the time nor the resources. By reading this book, understanding the principles, and, most importantly, working through the various scenarios, your experience as an examiner will have already surpassed the majority of the people conducting mobile device examinations today.

The primary goal of this book is to suggest methods and procedures for the collection and analysis of digital data from a mobile device so that your examination will stand up to the scrutiny of court. This book also aims to dispel the mobile device size myth and to prove that today's mobile devices contain more relevant and transactional data than a personal computer 100 times its size. Armed with a full understanding of the wealth of information available for discovery contained in this book, you will be prepared with not only the knowledge of how to use mobile device forensics tools to conduct investigations, but also with a holistic understanding of how and what these tools are doing.

A Brief History of the Mobile Device

Welcome to the world of mobile device forensics. The examination of data is no different from the examination of the words in any book or manuscript. To understand the words in a book, the reader must have an understanding of the letters that form the words and the words themselves to form a thought or sentence. Without this initial understanding, reading would not be possible. The same goes with understanding a mobile device. To be a truly good forensic practitioner, the examiner must understand the specimen. Before we begin a discussion of mobile forensics, let's begin with a history of the evolution of mobile devices themselves.

Mobile phones for cars and other vehicles preceded the handheld mobile phone and by all accounts were initiated by Bell Labs in 1946 in St. Louis, Missouri. This book will focus on the handheld mobile device that followed a little more than 26 years later.

Martin Cooper

In 1973, Martin Cooper from Motorola began developing a device that would enable a person to walk the streets while making calls without the need for attached wires—a portable handheld mobile phone. On April 3, 1973, Cooper demonstrated the portable phone with a call to Joel Engle of Bell Labs, Motorola's main competitor, to let Engle know he was calling on a portable handheld phone from the streets of New York City. The call was routed via a base station Motorola installed atop the Burlingame House into the AT&T landline telephone system. Cooper had been working on the development of a radio phone for many years. Ten years after he used this device to call his rival, it was brought to the mainstream market. This radio phone employed the same technology used by the military to communicate on the battlefield.

Cooper developed the DynaTAC (DYNamic Adaptive Total Area Coverage) 8000x portable phone, which allowed users to call another portable phone, landline, or radio phone. This device was approved by the U.S. Federal Communications Commission (FCC) on September 21, 1983, and was offered commercially in 1984. It weighed 2.5 pounds, with the battery contributing the majority of the size and weight. The talk time was approximately 20 minutes, and it took approximately 10 hours to charge the device between uses. This first device was, by today's standards, impractical due to its size and weight. Picture the 1980s TV show *Miami Vice* and the main character played by Don Johnson, with white cotton pants and matching jacket, with a large, angular phone and protruding black antenna—that was the DynaTAC 8000x.

The price tag of the device made it extremely impractical for widespread use against the prevalent pager or beeper of the age. When mobile radio devices came to market, prices ranged from U.S. $2000 to 4000, and they seldom worked outside of only a few major markets. The DynaTAC 8000x was priced at $3995.

Despite the introduction of the DynaTAC, car phones continued to be more popular, mainly because of the large mobile phone price tag. By 1984, the car phone was a large device with a very heavy base and typically a curly cord that ran to the handset. These devices had much better transmission and reception rates because of the constant battery power that exceeded the current ranges of the DynaTAC. Car phones were typically mounted and hardwired in vehicles and looked like a normal kitchen phone of the day. Users wanted phones that were more portable, however, so manufacturers began making the devices capable of being removed from the vehicle. The *bag phone* was born. ("Bag phone" was not the official name, but it stuck simply because the device could be carried in a zippered bag.) Impractical and extremely heavy, this device was not around for long. Who is to say what the impact of the electrical radiation might be?

Size Evolution

Shortly after the DynaTAC, cellular devices began to be manufactured in smaller form factors. In 1989, the Motorola MicroTAC was released. This device was much smaller than the DynaTAC series but still large and expensive enough that mainstream consumers were not buying. It was not until 1996 when the StarTAC series entered the market that things changed. The first cell phone to make a sizable impact with consumers was the full clamshell feature phone, which could be carried around in a pocket or small purse. The price point for the Motorola StarTAC was $1000. Because these portable devices only made and received calls, the price tag versus necessity was still out of reach for most consumers, however, so the progression away from the landline to the cell phone was not immediate.

The price for the mobile device started to drop when the technology, components, competition, and assembly became cheaper. In the mid to late 1990s, there was a shift to make the smallest device possible, but in the early 2000s, the size paradigm started to shift the other way. Today, consumers are speaking into mobile devices the size of small laptops, conveniently termed "phablet" for phone tablet. What has become important is the type and amount of data that can be transmitted, as well as what components are inside.

Data Evolution

Cell phone users quickly saw the need to send messages that they could type into a QWERTY keyboard or pound down the keys in a series of taps instead of speaking to someone. From this need, Short Message Service (SMS) was born. Limited to 140 characters, SMS enabled users to express themselves via a short sentence to other mobile device users. Today, 140 characters is still the limit. Concatenated SMS, or what some call Protocol Data Unit (PDU) mode SMS, is more widely used and provides 160 characters by changing from using 8 bits per character to 7. This was a significant advancement that moved the pager away from the businessman's belt loop and to the eventual demise of this type of communication service. The cell phone soon advanced away from the simple walkie-talkie. Mobile device users next needed storage for these text-based messages, and soon for pictures, videos, calendars, and e-mails as well—who would have foreseen the application revolution?

Note The walkie-talkie, invented by Donald L. Hings, was first used as a portable field radio for pilots flying around Canada. In 1937, when the first walkie-talkie was built, Hings referred to the device as a "two-way radio," and it has been used ever since.

Storage Evolution

Most of the original mobile phones did not contain a media type that would support the storage of data, because most were engineered to use the space as a scratch pad to run the needed process, remove the process, and move to the next process. Storage of *nonvolatile* data, or data that would continue to exist without constant power, onto a device's memory chip was not possible initially. This meant that any data that was visible on the device would not be stored, and as soon as the device was shut down, all the data disappeared. Because initially the mobile phone was used only to make and receive calls, this was not observed as a limitation.

Because of this, no phone book storage or any other settings could be maintained. The first cell phones were merely a block of circuitry that had the same combinations of buttons included on the well-known landline. The functionality was the same—attempt to recall the number of a contact from memory and key in the number (think about that—having to remember all of those phone numbers).When TDMA (Time Division Multiple Access) devices in the United States began to transition to GSM (Global Systems for Mobile Communications), which had already arrived in Europe, device information such as a phone book and SMS could be stored onto the SIM (Subscriber Identity Module). Storage areas for contacts, SMS, and last numbers dialed had already been built into the SIM standards developed by the ETSI (European Telecommunications Standards Institute), where this data could be written to and stored to the smart chip.

Since SIM cards were already storing phone data that was used in the authentication process, why not add values that stored the contacts, SMS, and last numbers dialed? The SIM card was already being used in the device as a "key" to the cellular network, assisting in the authentication of the device using stored values. TDMA devices could store a set number of contacts that users could look up and select to be dialed, plus a limited number of SMS (15–25 typically; that's it!) that could be reread, even if the device was shut off. Other carriers that did not have SIM cards started to develop devices that used nonvolatile memory so data could be stored and saved even if the device was turned off completely or the battery was removed or drained. The older feature phones used an acronym—*nvm*, for nonvolatile memory—to designate this type of data within their file systems and prefix the file and/or folder name.

This was where data was actually written to the phone and the start to the recovery of a goldmine of data.

Volatile Memory and the Visor PDA

A great example of volatile memory and mobile devices is the Visor personal digital assistant (PDA). With the technology of all PDAs at the time, most had a whopping 8MB of RAM and did not store data for long if no power was supplied.

On to the story.

A Visor seized in a search warrant was brought in for examination. The power cradle had been left at the scene, and it was a Friday, so the device was going to have to sit in the evidence locker until the following Monday. Upon arriving back at the lab on Monday, the examiner tried to start the device, but it was immediately apparent that the device had lost all power—it would not boot up. A power cradle was located for the device at a local store and the device was charged. When there was significant power to the device, the examination continued. To the dismay of the examiner, there was nothing on the device—no user content anywhere. What was puzzling was the fact that a substantial amount of data *had* existed on the device and was outlined and documented by the officers who seized it. Had someone broke into the lab over the weekend and deleted the data from the device? Had the officer somehow deleted the data or caused it to self-destruct?

The Visor documentation was consulted, as well as manufacturer's documentation, which indicated that PDAs drew constant power to keep the data on the devices populated. If the device was allowed to be completely drained of power, the data would no longer be available. Because the data resided in the device's RAM, the data was volatile, and, as such, when power was lost, the data stored in RAM was also lost. It was a hard lesson to learn but a great example of the limitations of volatile memory.

Moving forward, all devices had to have their power maintained, if possible, and most training courses on mobile forensics began to preach this lesson as well. Instruction on the use of portable charging units during transport as well as during storage began to be included in training courses and digital forensic examination kits.

Mobile Device Data: The Relevance Today

Mobile devices have come a long way since their inception. Data contained on a mobile device can now be compared to the written notes of a daily diary (often with pictures and videos), containing a company's most secure documents, our financial status, and most importantly our everyday habits, patterns, and routines. If a picture of an individual were painted with the personal data recovered from a PC, the picture would be a blurry representation with no clear edges. If, however, the data recovered from a mobile device were examined, it would most likely paint a very personal, and potentially embarrassing, picture of the individual.

Mobile Devices in the Media

Every day, the world media reports cases solved using evidence from mobile devices or a how a mobile device was involved in a crime—either a text message or chat was sent or received; a social media post was sent or interpreted; or a voicemail was heard, recorded, or hacked. In 2014, the Pew Research Center reported that 90 percent of U.S. adults owned a cellular phone, which translates to about 135 million cell phone users. It is no wonder that law enforcement digital examiners are looking to these devices as an evidence treasure trove. Mobile device data is today's equivalent to yesterday's DNA evidence.

One day, a mobile device that shows up in the lab or in the field may hold data that has never been seen by the world—the grassy knoll, the shot heard 'round the world, the missing plane's last communication, and the smoking gun. Quite simply, you can fill in the blank to determine what a mobile device might be involved in when contemplating the events of today.

Digital data from a mobile device holds the key. To the forensic examiner, this data is critical in many investigations. The following story, "Mobile Devices on the Scene," details the relevance of data on a mobile device and how its recovery is critical.

Mobile Devices on the Scene

In 2009, a fight was reported on a congested Bay Area Rapid Transit train platform. After officers responded to the scene, an officer shot one of the subjects, who later died at a nearby hospital. At the time, there were no news crews on the scene or closed-circuit television cameras in the area. What *was* on the scene were multiple people with cell phones, who captured the event both in still and video formats. These videos were uploaded and disseminated to media outlets and the Web. It is reported that the raw video of the event was downloaded more than 500,000 times in a single week! Videos from the cell phones taken from many different angles were critical to the case. The videos were irrefutable evidence of the transpiring events—a police officer was subduing an individual at the train platform, shots were fired, and the account of what happened was clear. The individual who was being subdued was shot as onlookers watched. What is different about this case is that it was not a witness's perception of the event, but the actual event caught on video in real time. Six videos were known to exist prior to the case and were subsequently used in the court cases. By all accounts, the videos from the mobile devices were critical evidence used by both prosecutors and the defense during testimony at the criminal trial, but also the civil trial.

The stories of eyewitness accounts captured with a mobile device are endless. In a traditional investigation, investigators would have to rely on an actual person recalling the event—which, as most know, can be susceptible to many different perceptions, views, and beliefs. The always on, always ready, and always filming video camera in today's mobile device has revolutionized and forever changed what an eyewitness is and will ever be.

The Overuse of the Word "Forensic"

NIST describes "forensic science" as "the application of science to the law." Forensics can include the scientific examination of fossils, a crime scene, metals, vehicles, post-mortem bodies, and of course, digital data that can be in many different forms. Digital examiners get lost in this meaning and sometimes interpret forensic science to indicate that a software application or a hardware device is forensically sound. But according to the NIST definition, the use of the tools by the examiner in a way conforming to known scientific processes and procedures is the forensic science, not the tool itself. A perfect example is the use of a write blocker when processing digital data.

Write Blockers and Mobile Devices

NIST and its Computer Forensic Tool Testing Program specifically states that the central requirement of a proper forensic procedure is that the examined original evidence must not be changed or modified in any way. One of NIST's listed requirements for a layered defense is to use a hard disk write-blocker tool to intercept any inadvertent disk writes.

Note Many different kinds of write-blocking equipment have been created by many different companies. Any mention of a specific unit here is not an endorsement of the tool; it simply indicates that the tool was used in the case or test.

A *write blocker* is a software or hardware device that stops specific communication from a computer to a mass storage device. Write blockers come in many different types. Software-based write blockers can use a simple Windows Registry change; hardware units are sophisticated boxes that are coupled to the examination computer via cables and the device to be examined attached to the other side. Some allow a connection directly to the pins located on the actual hard drive and then to the computer conducting the forensic analysis, while others have USB connections to plug a removable USB hard drive or flash drive into an available port.

Hardware tools can be used to protect disk access through the interrupt 13 BIOS interface of a PC. Because the mass storage device is attached to the hardware write blocker, all input and output (I/O) commands sent from the PC are monitored. Any commands that could modify the hard drive are not passed onto the hard drive, but intercepted by the write-blocking device. Software write-blocking tools also block the writing to attached drives plugged into the USB drive, mounted drives, and by device classes, if needed. This can be changed by editing the Registry of the Windows PC or using many of the available software tools.

Essentially, the write blocker acts as a traffic signal to data requests made by the computer. The computer makes requests to receive data from the connected device, which are accepted and processed; if a request to write data to the protected device on the other side of the write protector is made, these requests are stopped and not allowed to reach the device. The write-blocking hardware or software tool is not considered forensically sound, but the employment of the device and methods as part of the process is. To test this theory, obtain any write-protecting hardware device and attach a mobile device; then follow along with the example in "Real-World Example: Testing the Theory."

Real-World Example: Testing the Theory

This research example was conducted while I was preparing for testimony on a mobile device case in which a computer forensics expert was challenging the lack of usage of a write blocker when conducting an examination of a mobile device.

Using a Tableau USB write blocker and a Motorola Razor V3 mobile device, I began the experiment. The object of the research was to test my theory on write-protection devices and mobile devices. My theory was that since a mobile device is not observed by a PC's operating system as a mass storage device, the Tableau USB write blocker would not stop writes targeting the mobile device. (Note that this is not a limitation of the Tableau USB write-blocker product. This product, as well as all others, will operate the same as outlined in this example.)

I plugged the mobile device into the USB port of the Tableau write-blocking device. I then plugged the USB write blocker into a USB port located in the PC running Microsoft Windows.

The Tableau device immediately identified the device in the digital readout: "Motorola." Using P2K Commander, a free tool for browsing a Motorola PK device, the device's file system was read into the software. The entire device's file system was available. With the options in P2K Commander, I created a new folder within the device's file system. Since a write protector was in place, it would seem plausible that the folder would not be created. Unfortunately, however, the folder was created in the device's file system.

With the write-protector device still in place, I copied a file called *WriteProtector.txt* into the device file system and into the folder that I had created. The file showed that it was successfully transferred. I then shut down the software and collected data from the device using AccessData MPE+. The file system, as expected, contained the folder and the file that I had previously moved onto the phone with P2K Commander while the write protector was in place.

What did this mean for the write blocker used in this test? Did this mean that the write blocker did not operate as it should? Did this mean the test was not forensically sound? Of course not, but you must understand that these devices protect for writes only to mass storage devices, not devices viewed as something else by the computer's hardware. Because the Motorola was viewed as a modem, the connected computer could write any data it wanted to the attached media because writes to the modem were not halted.

As an examiner entering this field, you need to understand that the process you use to examine the mobile device and comprehend what has changed on the device is what makes the examination forensic. It is neither the software nor the hardware you use, but solely the process that you use during examination that makes it truly forensic. This concept applies not just to mobile device examinations, but also to the examination of all digital data in today's electronically driven world.